

LA PROTECCION DE DATOS PERSONALES Y LA PRIVACIDAD EN INTERNET EL CASO DE COLOMBIA

The protection of personal data and internet privacy
the case of Colombia

Hernando León Peláez Mosquera
hepelaez@poligran.edu.co

Alexander Riascos Trujillo
Alriascos2@poligran.edu.co

Institución Universitaria Politécnico Grancolombiano
Derecho
Colombia

Resumen

Este trabajo posee el objetivo de analizar las medidas legislativas implementadas por Colombia en torno al amparo de los datos personales en Internet. La metodología está desarrollada en un enfoque cualitativo y bajo un método descriptivo en el cual se estudia un fenómeno jurídico actual. Por otro lado, los resultados indican que existen diferentes medidas legislativas como por ejemplo las tipologías de datos y la Ley 1581 de 2012 es la que reglamenta y desarrolla este derecho constitucional a excepción de lo consagrado en los literales del artículo 2 de la misma ley y la de lo estipulado en la Ley 1266 de 2008 y 79 de 1993. Así mismo, se concluye que en cuanto a la obtención de los datos personales por Internet se debe a procesos informáticos como la captura, mercado, el consumo que generan las empresas e instituciones que se dedican al tratamiento de la información ya sea como datos públicos o de mercadeo. Igualmente, Colombia tiene diferentes desafíos como la práctica internacional, pues en este campo es un factor importante y complementario en la formulación de directrices para la supervisión de los datos de protección personal, el derecho a la Información y privacidad personal.

Palabras clave: ciberespacio, protección de datos, derecho informático, sistema de información.

Abstract

This reflection article aims to analyze the legislative measures implemented by Colombia regarding the defence of personal data on the web. The methodology is developed in a qualitative approach and under a descriptive method in which a current legal phenomenon is studied. The other pointer, the results designated that there are different legislative measures such as data typologies and Statutory Law 1581 of 2012 is the one that regulates and develops this constitutional right, except for what is preserved in the literals of investigations 2 of the same law and that of what is stipulated in Law 1266 of 2008 and 79 of 1993. Likewise, its concluded that in terms of obtaining personal data over the Internet its due to computer processes such as capture, market, consumption generated by companies and institutions that are dedicated to the treatment of information either as public or marketing data. Likewise, Colombia has different challenges such as international experience, since in this field it is an important and complementary factor in formulation of guidelines for the supervision of personal protection data, the right to Information and personal privacy.

Keywords: cyberspace, data protection, computer law, information system.

Recepción: 05.11.2020 Aceptación: 04.12.2020

Cite este artículo como:

Peláez, H. & Riascos, A. (2020). La protección de datos personales y la privacidad en Internet. El caso de Colombia. Working Paper FSCC, Volumen 1. [p.-p.]. doi: xxxxxx

Introducción

Las nuevas tecnologías y el ciberespacio han hecho que la vida cambie de lo físico a lo virtual generando una serie de impactos en lo social, cultural, económico, político y educativo.

En tal sentido, es usual que cuando se realicen registros en diferentes plataformas virtuales, sitios web o redes sociales, se introduzcan datos personales que muchas veces no tienen privacidad o las compañías dueñas de estas, no tienen un sistema de seguridad de la información conforme a las necesidades.

Por lo tanto, debido a que los datos personales de las personas son fáciles de transmitir en Internet, ha generado mucha complejidad o desafíos que la legislación general actual sobre tecnologías de la información no ha podido equilibrar. Debido a ello, la invasión del internet en la vida cotidiana permite un fenómeno imparable que supone, en efecto, la digitalización de los datos personales que al parecer es explotada por empresas y naciones.

Dentro de este contexto, la digitalización de los datos personales encamina procesos que violan la seguridad

de dicha información, provocando delitos informáticos. De ahí que, la semejanza entre el derecho a la protección de datos y la obligación de seguridad en el tratamiento de éstos envuelve reflexionar el fenómeno según niveles, como por ejemplo, las garantías fundamentales y el marco jurídico que prevalece para salvaguardarlo.

Dentro del contexto, Benussi (2020) plantea que esta escena de riesgo se ha ido confirmando año tras año, en la medida en que el método informático encuentra periódicamente violaciones a las medidas de seguridad, lo que implica la fuga de miles de datos personales, lesionando los derechos e intereses de los titulares. Los datos y los responsables de la infracción, y socavan la amistad del comprador en la compraventa electrónica.

También, afirma que En los últimos diez años, el uso de nuevas tecnologías ha ido en aumento y han surgido diversas industrias basadas en el procesamiento masivo de datos personales.

Igualmente, que la sobrepoblación del procesamiento de datos y la complejidad y fragilidad del sistema informático donde se procesan los datos aumenta significativamente el riesgo de seguridad de

los datos y derechos personales, derechos de reserva o la protección de las comunicaciones.

Por su parte, el concepto de seguridad tiene múltiples dimensiones, entre las que se encuentran la seguridad nacional, la seguridad ciudadana, la seguridad pública y un trabajo relacionado con los datos y la seguridad personales.

Así mismo, la correspondencia entre internet y seguridad suele concebirse bajo la noción de ciberseguridad. El rumbo de derechos humanos en el ciberespacio pasa por el concepto de ciberseguridad, que conduce a la forma en que se deben manejar los datos personales en el ciberespacio.

Dicha reflexión no es exclusiva, pues Coz et al (2012) establecen que tanto para las compañías y la sociedad en conjunto, proteger el ciberespacio es crucial, pues la privacidad de la información en el ciberespacio es una de las columnas sobre las que descansa la misma. Además, se aborda la materia de la compañía de la información como uno de los movimientos que surgieron a partir de la introducción de las redes sociales.

Plantean los autores que, la información y sociedad se define como un consorcio en la que la creación, difusión y operación de información es una parte significativa de las diligencias culturales y financieras.

El término sociedad de la investigación fue propuesto por primera vez por Fritz Machlup en 1962, pero no se utilizó ampliamente hasta la década de 1970, principalmente debido a los métodos de creación de riqueza que van desde el sector industrial hasta el fragmento de las tecnologías de la investigación y la declaración (TID).

Así entonces, la economía global contemporánea ha hecho del sector de las TIC una economía global. Aunque todavía en los inicios de la humanidad de la información, el ciberespacio, especialmente Internet, juegan un papel fundamental En la tendencia en desarrollo de la globalización

Lo anterior, es fundamental tener en cuenta debido a que las redes sociales como se afirma al principio, es una de las plataformas que más genera inseguridad en cuanto a los datos personales por internet.

Marco Jurídico Analítico

Disposiciones legales.

En Colombia, para proteger los datos privados, se comienza con el reconocimiento de artefactos informáticos y otros adelantos que prevén la cosecha, categorización, acopio y circulación de datos relacionados con los aspectos de la vida de las personas.

Dicha reflexión, nace del inciso secundario del artículo 15 de la Carta Magna de 1991 que expresa que la recogida, sistema y distribución de los archivos, se respetarán otras libertades garantizadas previstas en la Carta Magna. Las cartas y otras conveniencias de declaración privada son inviolables. (Const. P., 1991)

A su vez, La ley estatutaria N ° 1266 de 2008 ha logrado importantes avances en los aspectos legales, pues ha regulado los derechos básicos de hábeas data con mayor detalle.

De esta forma, los datos se aplican a fundaciones financieras, empresariales y de terceros países. Posteriormente, de acuerdo con los compendios corrientes determinados

por la Constitución, el Estatuto Ley N ° 1581 de 2012 representó un gran avance En amparo de los datos administrados por entidades públicas y privadas.

De igual forma, establece dos tipos de datos que requieren una protección especial, y habitualmente prohíbe su uso: los denominados datos sensibles, es decir, datos que conmueven la reserva de las personas o discriminan en caso de uso indebido y datos personales de niños y jóvenes. (Galvis, 2012)

Dentro de este contexto, Adarve & Acosta (2018) indican que Colombia posee un extenso lineamiento legal sólido relacionado con los datos, está encuadrado en primer lugar en la Constitución.

Además, otras disposiciones sobre seguridad en web, reserva y tecnologías de la información actualmente existen 24 leyes y 14 decretos sobre cuestiones de Internet.

Igualmente, plantean que existen algunos conocimientos básicos relacionados con los datos personales, lo que hace del Habeas Data un derecho básico, como la Ley N ° 1266 de 2008, que cuenta con calculadora de riesgo crediticio, la Ley N °

1273 tipifica delitos a través de la información, seguida la anteriormente mencionada Ley N ° 1581 de 2012 y el decreto 1377 de 2013 regulación mucho más determinada en argumentos de Habeas Data.

Además, plantean que la ley colombiana se basa en el beneplácito explícito del titular de los datos. Cuando un tercero (empresa o cualquier persona) solicita tratar datos, la credencial tiene ciertos requisitos, lo significativo es que la autorización debe informar al titular de los datos e indicar la finalidad del tratamiento.

Por otra parte, en el cuadro regulatorio de amparo de los datos particulares, es menester señalar la Ley 1273 de 2009, 1712 de 2014 entre otras disposiciones (ver tabla 1).

Tabla 1. Marco Legal y reglamentario de la Big data en Colombia.

Normas	Año	Descripción			
Ley 1273	2009	Nace un desconocido bien jurídico para la protección de la investigación.			
Ley 1266	2008	A través de esta ley se expiden las disposiciones generales de protección de datos			
			Ley 1581	2012	Aquí, se emiten términos generales para proteger los datos personales.
			Decreto 1074	2015	Este emitió un decreto reglamentario único para el comercio.
			Decreto 620	2020	Establece pautas generales para el uso y operación de los servicios ciudadanos digitales.
			Título V Circular Única SIC	2020	Establece diferentes disposiciones reglamentarias sobre la circulación de la información.
			Resolución 462	2019	Adoptó sus modificaciones y adiciones a la Resolución No. 017 de 4 de marzo de 2000.
			Decreto 1727	2009	Establece la forma en que los obradores de bases de datos deben proporcionar investigación al titular de la información.
			Decreto 2952	2010	Su propósito es desplegar el derecho constitucional de todas las personas a estar al tanto, renovar y

reprender la información recabada sobre ellas.

Decreto 1377	2013	La Ley N ° 1581 de 2012 está parcialmente regulada por este decreto.
-----------------	------	--

Nota. Fuente: elaboración propia.

Así entonces, en Colombia el legislador ha expedido diferentes leyes en pro de generar medidas para proteger activamente la circulación de la información y la big data no sólo en medios digitales en donde se utiliza Internet, sino también en cuanto al manejo que las entidades deben tener para su resguardo.

Método

Tipo de investigación y enfoque epistemológico

La presente investigación está desarrollada en un enfoque cualitativo y bajo un método descriptivo en el cuse estudia un fenómeno jurídico actual.

Al respecto, los autores Hernández et al (2014) plantean que el enfoque cualitativo esta guiado por plazas o temas de indagación importantes.

Sin embargo, no aclara preguntas y suposiciones antes de la recopilación y el análisis de datos (como la mayoría de las investigaciones cuantitativas), pero se pueden plantear preguntas y suposiciones antes, durante o después de los datos.

Esto también muestra que en la investigación se han construido diversas realidades subjetivas, diferencias de forma y contenido entre individuos, grupos y culturas. Por tanto, los investigadores cualitativos parten de la premisa de que el mundo social es "relativo" y sólo puede entenderse desde la perspectiva de los participantes de la investigación.

Por su parte, Trujillo et al (2 019) expresan que la investigación cualitativa se basa en la idea de paradigma explicativo, guiado por la ciencia social que cree que no existe una realidad social única, sino varias realidades construidas desde la perspectiva de cada individuo.

Este enfoque requiere que los investigadores renuncien a sus puntos de vista, buscando y comprendiendo las motivaciones del grupo de investigación. Este es globalmente flexible, por tanto, el observador se da cuenta de la estructura

general del fenómeno a través de diferencias individuales y estructurales.

A su vez, Tantaleán (2015) indica que el método descriptivo posee como objetivo el discernimiento de la situación presente en un entorno espaciotemporal dado. Los investigadores se centran en comprender las características del fenómeno que se evalúa.

Técnicas de recolección de la información

Para recolectar información se hizo necesario acudir a la técnica de la investigación documental. En donde se hizo uso de artículos de divulgación que fueron obtenidos en bibliotecas electrónicas como la de la Institución Universitaria Politécnico Grancolombiano, Redalyc y Scielo.

Así mismo, se acudió a fuentes secundarias como Jurisprudencia nacional, leyes y convenios internacionales.

Análisis

Nuevas tecnologías en relación con el Derecho Informático. Obtención de datos.

Para comprender la funcionalidad y marco jurídico relacionado con la protección

de la Big Data, es necesario estudiar la relación que guarda el Derecho Informático con las nuevas tecnologías de la indagación, pues por medio de este comienza el compromiso de los estados por invocar normas tendientes a garantizar el acceso a internet y la circulación de los datos que en él se introducen.

Al respecto, Jiménez & Meneses (2017) indican que exploraron la relación entre las nuevas tecnologías y el derecho como ciencia. Determinaron que el progreso de las ciencias aplicadas de la información y la noticia y el ciberespacio es un desafío a los hábitos y costumbres legales, y es estable en cuanto al concepto de dominación y la ubicación en el espacio de las diligencias.

Además, el autor cree que las tipologías de web son desafíos para Internet, es decir la creación de una nueva ley.

Lo anterior, denota que si bien las nuevas tecnologías, en concreto, Internet, tiende a ser más práctico por su rapidez y característica de circular información sin limitaciones fronterizas, para el derecho en específico, es un campo que genera desafíos; retos que, por su naturaleza de amplitud

geográfica, independencia, en torno a su cobertura y demás elementos que lo constituyen, se tornan complejos.

Aunado a ello, Chen (2010) plantea que en el entorno del comercio electrónico, los aspectos de privacidad, especialmente los relacionados con la protección de datos personales, son muy importantes.

Esto se debe a que en las transacciones comerciales que realizan los consumidores a través de páginas web, el mecanismo más utilizado es a través de contratos fijos, que se basan en un formulario prediseñado por el proveedor y requieren información personal en él.

De ahí que, el Derecho Informático es la rama encargada de que dichos consumidores tengan garantía de los procesos que realizan en la red.

Además, cabe señalar que con el desarrollo de la pandemia Covid-19 y las limitaciones ante ello. Los medios de noticia en todos los ámbitos están aumentando, lo cual es importante porque de esta forma, la tarea legal es más difícil.

Tal reflexión no es alejada de la realidad, como lo ha indicado Álvarez

(2020) que aborda los retos que tienen las autoridades con respecto a las aplicaciones que utilizan las personas, en donde se confían informaciones personales.

Plantea el autor que en muchos sentidos, 2020 es un año imperecedero. Frente a la pandemia provocada por el covid-19, y algunas personas se ven restringidas para intentar frenar su propagación, porque al menos en Chile y Latinoamérica, una gran parte de la población aún tiene que salir de sus hogares en busca de la vida diaria.

En este caso, solo legal y técnicamente, hay que sumar un ataque poderoso, y existe una conjeturada tracción entre la reserva y el amparo de datos, a veces infructuosa, a veces exitosa.

Por otro lado, en cuanto a las disposiciones técnicas del Derecho en concordancia con los procesos informáticos, es importante plantearse el tema de la obtención de datos por medio de internet desde su funcionamiento en la red, los servicios, aplicaciones y la seguridad, es decir, el proceso internacional referente a la obtención de los datos y los sistemas de la información (ver tabla 2).

Tabla 2. *Procesos y amenazas al derecho de la Big Data.*

Procesos	Descripción
Obtención de datos	Capturas, mercado, consumidores, organismos gubernamentales y afines.
Tratamiento de los datos	Cualquier operación tendiente a reproducir una información en base a datos personales proporcionados por individuos.
Acceso ilegal a sistemas	Se refiere a aquellos que, sin autorización, a un sistema de archivo.
Daños informáticos	También se denomina sabotaje informático, es un delito.
Contenidos ilícitos	Es un delito que menoscaba la confianza de las personas que acceden a la red.

Nota. Fuente: elaboración propia bajo fuente obtenida del Manual de Derecho y Nuevas Tecnologías. (Perguera et al., 2005)

Tratamiento de datos personales bajo la utilización de Bigdata.

La llegada de la economía digital es una realidad; esta gira en torno a los datos y procesa la información para obtener ganancias, de manera que las empresas puedan competir efectivamente en cualquier tipo de mercado.

En este ecosistema, el big data, que se entiende como la tecnología utilizada para recopilar, procesar, transformar y analizar grandes cantidades de datos, se ha consolidado en los últimos años y se ha transformado en el buque insignia y principal fortaleza de la transformación digital industrial.

Con la ayuda de la sistematización de procesos, la digitalización de actividades, el desarrollo de mercados en línea y redes globales de Internet, esta transformación se ha aprovechado al máximo, lo que permite a las personas generar información a partir de cantidades masivas de datos.

Esto solía ser gradual e impredecible, pero hoy, gracias a tecnologías que consienten el rastreo y captura de datos ordenados y no constituidos, es medible y su uso en las relaciones comerciales ha comenzado a llamar la atención.

Desde un punto de vista legal, la legislación colombiana intenta proteger el derecho de Habeas Data a través de documentos de autorización de los titulares de los datos.

Así, Con el advenimiento de la tecnología de big data, la autorización basada en este sistema no solo ha comenzado a perder valor, sino que también ha comenzado a convertirse en "otro documento de la burocracia organizacional" que no puede cumplir con sus funciones. Protección, que nos obliga a reconsiderar cómo proteger este derecho fundamental. (Ospina, 2019)

Industria de datos. Data Brokers.

Un agente de datos o Brokers, se refiere a una empresa dedicada a recopilar datos personales de múltiples fuentes para proporcionar productos derivados de la venta directa de estos o su análisis.

Este tipo de compañías no es desconocido; las sociedades de marketing recopilan información demográfica e indagación de utilidad para proporcionar publicidad dirigida a través de medios de impresión. Instituciones financieras como Datacrédito en Colombia recopilan encuesta sobre actividades comerciales financieras para generar apreciaciones bancarias.

Lo que ha cambiado fundamentalmente es la capacidad técnica de recopilar, almacenar, intercalar y analizar una gran cantidad de datos diversos en

diferentes formatos y en tiempo real. Estas también, agregan información de múltiples fuentes.

Las cuales pueden ser el gobierno, agencias centrales y descentralizadas, agencias de censo, empresas públicas y privadas de seguridad social, juzgados y tribunales.

En este caso, asimismo se añaden los datos sobre las prontitudes productivas de las personas. Los establecimientos venden e intercambian su encuesta sobre los hábitos del consumidor, como ventas, contratos a revistas, mercado de automóviles, estudios de mercado, fichas de compradores habituales, etc. (González, 2019)

Por otro lado, una encuesta realizada por la empresa de tecnología Loglogic especializada en productos de gestión de seguridad, encontró que el 49% de las organizaciones se preocupan por la administración de big data en cierta medida o mucho, pero el 38% de las organizaciones no entienden qué es y el 27% de las organizaciones dijeron que tienen algo de comprensión. Además, el 59% carecen de las herramientas necesarias para administrar los datos. (Camargo et al., 2014)

Así entonces, los datos personales corren riesgo en internet pues, es gran cantidad de organizaciones presentes en Internet no cuentan con herramientas para administrar los datos, de tal manera, la seguridad de dicha información es nula.

Principio de acceso y circulación masiva

Resulta evidente que la información de las personas se ha convertido en una herramienta importante para determinar la ciudadanía, utilizando las políticas públicas que orientan las estrategias económicas y financieras de muchos países.

En concordancia, la honorable Corte Constitucional define la información privada como la que pertenece al sujeto de su responsabilidad, por lo tanto, solo se puede acceder a él de acuerdo con la orden de la autoridad judicial en el desempeño de sus funciones. (Sentencia T-114/18, 2018)

A su vez, se señaló que con respecto al acceso a datos personales a través de Internet, su conocimiento puede no estar disponible porque su conocimiento se limita al propietario o un tercero autorizado por la ley.

Es decir, dado que su conocimiento se limita al propietario o un tercero

autorizado por la ley, es posible que no esté disponible o que no sea posible una consulta general. Los datos personales solo deben ser tratados de forma que la persona afectada pueda prever razonablemente para evitar un perjuicio objetivo de sus derechos. (Sentencia T-020/14, 2014)

Retos y desafíos futuros

El amparo de datos es en realidad un fenómeno que acecha globalmente. Su inclinación transfronteriza se ha transformado en un elemento importante del desarrollo del comercio electrónico.

Por lo tanto, la práctica internacional en este escenario es un factor significativo y suplementario en la formulación de pautas de protección de datos, derecho a saber y supervisión de la privacidad personal.

En ese contexto, uno de los retos de Colombia es adoptar en feliz término los patrones internacionales, no solo para avalar amparo total de sus poblaciones contra posibles abusos, sino para que tales regulaciones no sean un impedimento al progreso del comercio con otros países.

De esta forma, Colombia será catalogada como un país que garantiza un

"nivel adecuado de protección" a la información personal obtenida de la Unión Europea y Estados Unidos. (Galvis, 2012)

Por su parte, Ospina (2020) plantea que hoy en día, la transformación digital ha traído desafíos a la privacidad y la protección de datos personales en Colombia, por ello, en este entorno digital, el mejoramiento de las plataformas de medios y tecnología, como nuevo modelo de negocio, deben adaptarse a la forma en que se protegen datos personales por medio de Internet.

Además, Meza (2020) indica que en cuenta al tratamiento de datos personales en la inteligencia artificial Colombia tiene el desafío de llevar a cabo investigaciones sobre el impacto de la privacidad; incorporar la privacidad, la ética y la seguridad por diseño y de forma predeterminada; implementar el principio de prueba de responsabilidad y garantizar la calidad de los datos.

Las afirmaciones anteriores sugieren que, en Colombia si bien existe un vasto marco legal y se han implementado mecanismos o medidas para estar a la vanguardia en dicha materia, hoy se encuentra con limitaciones en la seguridad

de la información y privacidad en Internet y el entorno digital.

Conclusión

Teniendo en cuenta lo precedente, se concluye que el legislador ha expedido diferentes leyes en pro de generar medidas para proteger activamente la circulación de la información y la big data no sólo en medios digitales en donde se utiliza Internet.

Así mismo, de la presente investigación denotan que en Colombia, las medidas legislativas sobre los datos personales se han dado desde el reconocimiento de los instrumentos de la informática y progresos tecnológicos que proporcionan la cosecha, codificación, acaparamiento y tráfico de datos relativos a todos los semblantes de la vida de los individuos a partir del artículo 15 de la Carta Magna de 1991.

Desde entonces, el legislador ha propendido por regular la protección de los datos personales, a través de leyes fundamentales como la 1581 de 2012, la 1266 de 2008 y sus decretos reglamentarios. Así mismo, en el año 2020 en torno a la pandemia generada por el Covid-19, se han

expedido lineamientos para los trámites y actividades digitales. Además:

1. Colombia tiene un marco regulatorio bastante sólido relacionado con los datos personales, está enmarcado en concordancia con la Constitución Política de 1991.
2. La mayoría de las compañías o empresas nacionales presentes en la web, no cuentan con las herramientas acordes para resguardar los datos personales.
3. El big data, que se entiende como la tecnología utilizada para recopilar, procesar, transformar y analizar grandes cantidades de datos.
4. Las nuevas tecnologías y el ciberespacio han hecho que la vida cambie de lo físico a lo virtual generando una serie de impactos en lo social, cultural, económico, político y educativo.
5. Colombia debe adoptar los estándares internacionales, no solo para garantizar la protección total de sus ciudadanos contra posibles abusos, sino para que tales regulaciones no

sean un obstáculo al desarrollo del comercio electrónico con otros países.

Referencias bibliográficas

- Adarve , L. H., & Acosta, J. (16 de Abril de 2018). "Colombia tiene un marco robusto en protección de datos". Obtenido de Asuntos:legales: <https://www.asuntoslegales.com.co/actualidad/colombia-tiene-un-marco-robusto-en-proteccion-de-datos-2714309>
- Álvarez, D. (2020). La protección de datos personales en contextos de pandemia y la constitucionalización del derecho a la autodeterminación informativa. *Revista chilena de Derecho y Tecnología*, 9(1), 1-4. doi:10.5354/0719-2584.2017.45760
- Benussi, C. (2020). Obligaciones de seguridad en el tratamiento de datos personales en Chile: Escenario actual y desafíos regulatorios pendientes. *Revista Chilena de Derecho y Tecnología*, 9(1), 227-279. doi:10.5354/0719-2584.2020.56660

- Camargo, J. J., Camargo, J. F., & Joyanes, L. (2014). Conociendo Big data. *Revista Facultad de Ingeniería*, 24(38), 63-77. Obtenido de <http://www.scielo.org.co/pdf/rfing/v24n38/v24n38a06.pdf>
- Chen, S. (2010). Privacidad y protección de datos: un análisis de legislación comparada. *Diálogos, Revista Electrónica de Historia*, 11(1), 111-152. Obtenido de <https://www.scielo.sa.cr/pdf/dreh/v11n1/a04v11n1.pdf>
- Coz, J. R., Fojón, E., Heradio, R., & Cerrada, J. A. (2012). Evaluación de la privacidad de una Red Social virtual. *Revista Ibérica de Sistemas y Tecnologías de la Información*, 9(6), 59-72. Obtenido de <http://www.scielo.mec.pt/pdf/rist/n9/n9a06.pdf>
- Corte Constitucional [C.C.], abril 3, 2018, M.P: C. Bernal. Sentencia 114/18. Colombia. 25/10/2020. Obtenido de <https://www.corteconstitucional.gov.co/relatoria/2018/t-114-18.htm>
- Corte Constitucional [C.C.], enero 27, 2014, M.P: L. Guerrero. Sentencia 020/14. Colombia. 25/10/2020. Obtenido de <https://www.corteconstitucional.gov.co/relatoria/2014/T-020-14.htm>
- Galvis, L. (2012). Protección de datos en Colombia, avances y retos. *Revista LEBRET*(4), 195-214. Obtenido de <http://revistas.ustabuca.edu.co/index.php/LEBRET/article/view/336>
- González , L. D. (2019). Control de nuestros datos personales en la era del big data: el caso de rastreo web de terceros. *Revista Estudios Socio-jurídicos*, 21(1), 209-244. Obtenido de <https://revistas.urosario.edu.co/index.php/sociojuridicos/article/view/6941/6696>
- Hernández, R., Fernández , C., & Baptista, P. (2014). *Metodologías de la Investigación* (Sexta ed.). México D.F: McGrawHill Education. Obtenido de <http://observatorio.epacartagena.gov.co/wp-content/uploads/2017/08/metodologia>

- de-la-investigacion-sexta-edicion.compressed.pdf
- Hernández, S. (2018). El reto de la era digital: privacidad y confidencialidad de la información de pacientes. *Revista Gen*, 27(1). Obtenido de http://ve.scielo.org/scielo.php?script=sci_arttext&pid=S0016-35032018000100001
- Jiménez , W. G., & Meneses, O. (2017). Derecho e internet: introducción a un campo emergente para la investigación y prácticas jurídicas. *Revista Prolegómenos - Derechos y Valores*, 20(40), 43-61. doi:<http://dx.doi.org/10.18359/prole.3040>
- Meza, A. (21 de Marzo de 2020). *Tratamiento de datos personales en la inteligencia artificial*. Obtenido de Auntos:legales: <https://www.asuntoslegales.com.co/consultorio/tratamiento-de-datos-personales-en-la-inteligencia-artificial-2981422>
- Ospina, N. (7 de Octubre de 2019). *Big data y protección de datos personales*. Obtenido de Portafolio: <https://blogs.portafolio.co/abogadotico/2019/10/07/big-data-proteccion-datos-personales/>
- Ospina, N. (21 de Octubre de 2020). *Sarlaft 4.0 y protección de datos personales*. Obtenido de Compliance: <https://www.compliance.com.co/sarlaft-4-0-y-proteccion-de-datos-personales/>
- Perguera, M., Agustinoy, A., Casas , R., Cerrillo, A., Delgado, A., Herrera, J., . . . Xalabarder, R. (2005). *Manual de Derecho y Nuevas Tecnologías*. España: Editorial UOC. Obtenido de <https://dialnet.unirioja.es/servlet/libro?codigo=8859>
- Tantaleán, R. (2015). El alcance de las investigaciones jurídicas. *Revista de Derecho y Cambio Social*, 12(41). Obtenido de <https://dialnet.unirioja.es/servlet/articulo?codigo=5456857>
- Trujillo, C., Naranjo, M., Lomas, K., & Merlo, M. (2019). *Investigación Cualitativa*. Ibarra: Universidad Técnica del Norte. Obtenido de

[https://issuu.com/rolandolomas4/docs
/libro_de_investigacion_cualitativa_](https://issuu.com/rolandolomas4/docs/libro_de_investigacion_cualitativa_)