UNIVERSIDAD DE LOS HEMISFERIOS

FACULTAD DE CIENCIAS JURIDICAS Y POLITICAS

LA PROTECCION DE LOS DATOS PERSONALES EN EL INTERNET DE LAS COSAS

AUTORES:

SANTIAGO DANIEL MERA SAÁ

NICOLAS GUILLEN BAUTISTA

CONTENIDO

INTRODUCCIÓN

1. Derecho a la Protección de Datos Personales

1.1. Antecedentes

El derecho a la protección de datos personales es el resultado de la evolución del entorno en el que los seres humanos se desarrollan. “Si bien, nace de la intimidad, el ámbito de protección que este derecho proporciona debe ampliarse ante la inserción de la tecnología en la vida cotidiana de las personas” (Marecos, 2018). En consecuencia, se reconoce el derecho a la autodeterminación informativa, que se extiende y da paso al reconocimiento y garantía de la protección al titular de datos personales.

El derecho a la protección de datos personales es autónomo. “Tiene su origen de la intimidad, sin embargo, la evolución de la sociedad crea la necesidad de ampliar el concepto, con la finalidad de extender la protección para salvaguardar la integridad y la dignidad de los seres humanos” (Garriga, 2015), es así como nace la autodeterminación informativa y posteriormente el derecho a la protección de datos personales. Por lo que, el primer antecedente de este derecho es la intimidad.

El artículo 12 de la Declaración Universal de Derechos Humanos reconoce y garantiza a las personas el derecho a la intimidad. Debemos recordar que los derechos humanos son la consecuencia a una realidad que ha sido marcada por las guerras relacionadas directamente con el abuso de poder, injusticia enfocándose directamente en los grupos que se encontraban en vulnerabilidad.

“Después de la Primera y Segunda Guerra Mundial, tras atentar con la vida de judíos, por el simple hecho de serlo, mediante el uso de fuerzas armadas que ingresaban a distintos hogares y abusaban física y sexualmente de las personas que se encontraban en ellos” (Passemard, 2004, pág. 80), la Organización de las Naciones Unidas consideró pertinente incorporar este derecho como respuesta a aquellas acciones que vulneraban la dignidad e integridad de cada uno de los seres humanos.

“Conforme lo expuesto, la intimidad nace en este contexto social, en donde se trataba de evitar el menoscabo a la dignidad humana” (García, 2003, pág. 78), preservando el fuero interno de las personas y su desarrollo en el entorno doméstico o familiar; es por eso que, este derecho protege a los seres humanos de cualquier injerencia en los aspectos personalísimos o internos y en su relación con su entorno más cercano, sean estos amigos o familia.

> Muchos años después, en una sociedad traumatizada por los hechos relacionados a distintas guerras y levantamientos sociales, se realizó el censo de población, viviendas y centros de trabajo, dentro de las preguntas ahí contenidas, se incluían cuestionamientos acerca de las creencias religiosas de las personas a quienes estaba dirigido el mismo; situación que generó inmensa preocupación en los distintos sectores de la población, originando incluso una demanda de inconstitucionalidad, respecto de los artículos 11 y 12 de la Ley del Censo de 1983, ante el Tribunal Constitucional Federal Alemán (Del Peso Navarro, 2000, págs. 9-10)

El mencionado Tribunal determinó que las personas tienen derecho a la autodeterminación informativa, es decir, se les atribuye la potestad de ejercer control y la facultad de decidir acerca de sus datos e información de carácter personal, siendo necesario que conozcan claramente la finalidad que se le va a otorgar a dichos datos en su tratamiento, evitando así que está información pueda ser utilizada para menoscabar su dignidad e integridad. Esto debido a que, los ciudadanos alemanes, pensaban que esta, en manos de personas mal intencionadas podrían facilitar el trabajo de ubicación y posterior tortura y matanza a las personas judías.

La evolución continuo con la sociedad, por tal motivo se empiezan a incorporar nuevas tecnologías de información y comunicación con el objetivo de satisfacer las necesidades de los seres humanos transformando la forma en que la humanidad se desarrolla, así, el tratamiento de datos personales y la valoración automatizada de los mismos es masiva, siendo necesario progresar del derecho a la autodeterminación informativa al derecho a la protección de datos personales; debido a que era necesario implementar una serie de derechos, principios y obligaciones que brindaran mayor protección a los seres humanos.

> El derecho a la protección de datos personales es el resultado de la evolución de la sociedad, y, si bien se origina de la intimidad, es evidente que no son lo mismo, puesto que su espectro de protección es distinto. La intimidad está destinada a evitar injerencias arbitrarias o abusos en el fuero interno y las relaciones domésticas de cada una de las personas; mientras que la protección de datos personales es un derecho dirigido a evitar el tratamiento inadecuado de dicha información, sobre todo ante la evidente injerencia actual de las TIC en la vida de los seres humanos (Garriga, 2015, pág. 55).

El derecho a la protección de datos personales es autónomo e independiente de la intimidad y la privacidad, esto no quiere decir que estos derechos dejen de reconocerse o garantizarse, sino que, más bien, cada uno tiene un objeto distinto, por lo que es necesario establecer de qué manera se protege a los individuos titulares de información personal que circula a través de la red.

1.2. Modelos de regulación

Los seres humanos seguimos creando tecnología con el paso del tiempo, la información y los datos son vitales para su desarrollo, por tal motivo estos son indispensables para encaminar las necesidades básicas de cada ser humano. Esto ha generado que exista vulneración con la información o que se le dé un uso indebido, siendo ineludible que se implementen regulaciones, en el mundo se han desarrollado 3 modelos que serán explicados a detalle a continuación:

1.2.1. Modelo estadounidense

"El modelo adoptado por los Estados Unidos y países anglosajones es el modelo de la privacy, es una corriente basada en la teoría de las esferas, con una visión que promueve la autorregulación, desarrollado con el objetivo de fomentar el comercio y la innovación" (Recio, 2016, pág. 73).

La teoría de las esferas establece que los seres humanos tienen distintos ámbitos de acción y relación. Ubica al ser humano en el centro y despliega tres esferas, "la primera se refiere al entorno íntimo, es decir el fuero interno o personalísimo de un ser humano, aquel que

refiere mayor protección; en lo posterior se extiende la esfera privada, misma que describe las relaciones de una persona con su familia, amigos y en su ambiente doméstico" (Álvarez M. , 2015, págs. 28-29), finalmente; se presenta al área pública, en donde la gente se relaciona de forma que no necesita ninguna protección por parte de la legislación y los derechos relacionados a la intimidad o privacidad.

Se reconoce el derecho a estar solo, únicamente se protege aquello que hace referencia a la vida privada o intima de las personas. Se ha aplicado este derecho al tratamiento masivo de datos personales, no se regula la recopilación, procesamiento, almacenamiento y cesión de datos, solamente se brinda protección cuando en estas operaciones se ha interferido con su intimidad o privacidad.

"Además, se promueve la autorregulación, esto quiere decir que se deja a criterio de los responsables de bases de datos, la facultad de implementar medidas de seguridad o herramientas que fomenten un tratamiento adecuado" (Almuzara, 2007, pág. 612)

La corriente anglosajona es un modelo de regulación orientado a proteger a las personas en relación a su actividad en las distintas esferas en que pueden desarrollarse; esta visión no se refiere al tratamiento de datos personales, sino que ha sido aplicado a la actividad que diversos usuarios realizan en línea que pueda poner en riesgo su derecho a la privacidad y a la intimidad; prevé que aquellos que se encargan de tratar datos personales implementen medidas que salvaguarden a sus usuarios y promuevan el desarrollo comercial y económico.

1.2.2. Modelo europeo

El modelo europeo se basa en el reconocimiento y garantía de un derecho autónomo, orientado a proteger a las personas frente al tratamiento automatizado o no de sus datos personales, respondiendo a una realidad social que implementa a la tecnología como herramienta ideal para satisfacer las necesidades más básicas del ser humano.

“Está visión considera a los datos personales como un elemento esencial de la personalidad humana” (Piñar, 2016, págs. 16-18), pues estos les otorgan singularidad a los individuos, y su tratamiento inadecuado puede significar un menoscabo a su dignidad e intimidad.

Está forma de regulación supone que el garantizar la dignidad de las personas es primordial, pues son los seres humanos la base de todo lo que se construye en el mundo, es así, por ejemplo: el comercio, la economía, el progreso y el desarrollo, por lo que salvaguardar a la colectividad frente a cualquier abuso debe ser fundamental.

“Este modelo no se basa en la autorregulación, sino más bien en la tendencia de implementar requerimientos y lineamientos que precautelen un tratamiento adecuado de datos personales, con la finalidad de evitar que las personas sufran cualquier detrimento en su dignidad” (Díaz, 2016, págs. 405-407)

En consecuencia, es un enfoque de derecho que considera la participación del Estado como un ente activo responsable de implementar medidas y herramientas que permitan su efectivo goce y ejercicio.

1.2.3. Modelo latinoamericano

> “La mayoría de las Constituciones a lo largo de Latinoamérica reconocen y garantizan el derecho a la protección de datos personales siendo a primera vista un enfoque de derecho, no obstante, lo cual, las legislaciones de los países en mención agregan en su ordenamiento la garantía constitucional de hábeas data, como herramienta que permita efectivizar este derecho” (Palazzi, 2002, pág. 53).

Este modelo es un hibrido entre la perspectiva estadounidense y la europea, pues se implementan dentro de la normativa elementos que caracterizan a cada una de estas visiones. Es por eso que, se ha determinado la necesidad de definirlo como un tercer modelo y no como la secuencia de una de las dos corrientes descritas anteriormente.

“Sin embargo, la tendencia de las legislaciones de América del sur es seguir el modelo europeo, por ejemplo, Uruguay y Argentina se encuentran calificados como niveles adecuados de protección por la Unión Europea” (Álvarez J. , 2011, pág. 428), objetivo que

ha tomado en cuenta Ecuador para la elaboración del Proyecto de Ley Orgánica de Protección de Datos Personales.

> Esto debido a que las normas de los países latinoamericanos son garantistas, puesto que requieren la implementación de lineamientos y medidas que permitan la efectiva tutela de los derechos de los seres humanos, siendo necesario contar con herramientas jurídicas adecuadas que permitan un correcto tratamiento de datos personales (Acedo, 2013).

La visión europea y la anglosajona no son compatibles, la primera se caracteriza por la primacía de la garantía de derechos, la segunda promueve la autorregulación con la finalidad de no entorpecer el progreso económico y social, y la tercera que es la latinoamericana, busca un balance entre las dos visiones, siempre que se proteja la integridad y dignidad de las personas.

1.3. Concepto de dato personal

"Los datos personales en la actualidad tienen un valor sumamente importante, puesto que son esenciales para el desarrollo de nuevas tecnologías que permiten la eficiencia en la toma de decisiones. Muchas veces se confunde el término dato con información" (Dueñas, 2014) , haciendo necesario el desarrollo de contenidos que aclaren la diferencia, puesto que solo así se puede comprender el alcance real de la garantía que ofrece el derecho a la protección de datos personales.

Para entender integralmente la definición de dato personal, es necesario comprender qué es la información y el conocimiento, esto con la finalidad de evitar confusiones a la hora de aplicar el derecho a la protección de datos de esta índole.

De acuerdo con la Real Academia de la Lengua Española dato es información, lo que es cuestionable, pues como se manifestó con anterioridad, si existe una diferencia; dato es una representación de distintas variables, mientras que la información es el conjunto de datos estructurado que le da un valor a algo, el conocimiento por su parte es la capacidad de aprendizaje basado en la experiencia, se traduce en el raciocinio.

Una vez entendida está diferencia es importante acotar que para evitar usar la palabra dato de manera repetitiva a lo largo del desarrollo del presente ensayo y en atención a las diferentes definiciones que se procederá a citar, se usarán las palabras dato e información como sinónimos. Como, por ejemplo, la Real Academia Española define al dato como "Información sobre algo concreto que permite su conocimiento exacto o sirve para deducir las consecuencias derivadas de un hecho" (2014).

Ahora bien, es necesario centrarse en el estudio conceptual de los datos personales, como el elemento angular del derecho al que se refiere el presente estudio. La Agencia Española de Protección de Datos los define como "cualquier información numérica, alfabética, gráfica, fotográfica, acústica, o de cualquier otro tipo concerniente a personas físicas identificadas e identificables" (2009).

> "En la actualidad, con el impacto de las tecnologías de la información y comunicación, los datos han ganado protagonismo, pues para el desarrollo de estas, la implementación de bienes y servicios y el perfeccionamiento de estrategias para la toma de decisiones a nivel empresarial y gubernamental, son estos indispensables, sobre todo cuando a datos personales nos referimos, por lo que, para muchos esta información tiene un valor equiparable a la del dinero" (Kroenke, 2003, pág. 515)

Los datos personales requieren la creación de medidas que regulen un uso adecuado, sin embargo los datos personales sensibles requieren de una protección especial, aquellos que pueden causar lesiones irreversibles en los derechos fundamentales de las personas, vulnerando su integridad física, emocional o psicológica de manera grave, estos hacen referencia a la salud, ideología, creencia religiosa, determinación política, orientación sexual, entre otros.

El concepto de dato personal se centra en cualquier representación que permite identificar y hacer identificable a una persona, con este concepto se prevé que dato personal son los datos o metadatos que pueden identificar, o que mediante esfuerzos razonables vuelve identificable a una persona, al respecto la sentencia del caso Lindqvist, emitida el 06 de noviembre de 2003 y resuelta por el Tribunal de Justicia de la Unión Europea empleando el artículo 3 de la Directiva 95/46 señala que dato personal es "toda información sobre una persona física identificada o identificable. Este concepto incluye, sin duda, el nombre de

una persona junto a su número de teléfono o a otra información relativa a sus condiciones de trabajo o a sus aficiones".

En este contexto, puede parecer a simple vista irrelevante como un "me gusta" en una red social o el tiempo de visita en una página web, evidenciando que la definición de este es muy amplia dado el impacto y desarrollo de tecnologías emergentes.

1.4. Elementos esenciales del derecho a la protección de datos personales

"Los datos personales en la era actual han ganado protagonismo, pues mediante su tratamiento se puede impulsar el desarrollo social, económico, comercial, cultural, científico, etc. Toda esta información circula de manera masiva por la red" (Suárez, 2010, pág. 43), y a primera vista regular este procesamiento puede evitar la promoción de los beneficios y el impacto positivo que han generado las tecnologías de la información y comunicación.

Ante esta realidad, los seres humanos se encuentra vulnerables, puesto que se puede menoscabar su dignidad e integridad si se le da un tratamiento abusivo, razón por la cual la instrumentalidad es la característica más importante del derecho a la protección de datos personales, ya que permite salvaguardar los derechos fundamentales de las personas como el honor, acceso a la educación, la salud, entre otros.

> "Es por eso que, podemos decir que el derecho a la protección de datos personales es la atribución o facultad que tienen las personas de decidir sobre la información que las identifique o las haga identificables, para lo cual aquellos responsables de tratar dicha información deberán respetar y hacer efectivos los derechos de acceso, rectificación, cancelación, oposición, anulación, eliminación, olvido, información entre otros; este procesamiento debe basarse en principios generales como el de consentimiento informado, seguridad, calidad, finalidad, etc., y adicionalmente, deberán cumplir con obligaciones que aseguren un uso licito de la información, que se realice conforme a los principios y lineamientos que una legislación especializada en la materia debe desarrollar" (López S. , 2009, pág. 46).

El derecho a la protección de datos personales está reconocido en artículo 66 numeral 19 de la Constitución de la República del Ecuador, dotándolo de independencia, pues en el numeral 20 del mismo artículo se reconoce el derecho a la intimidad y privacidad familiar, es por eso por lo que es necesario un estudio especializado de este derecho, que tiene un enfoque de modelo latinoamericano, pues en el artículo 92 de la norma suprema, prevé una garantía constitucional que es la del habeas data.

"La garantía constitucional permite que los titulares de datos o información de carácter personal puedan ejercer sus derechos ARCO (acceso, rectificación, cancelación, oposición), es decir, permite su efectivización, sin embargo, esta garantía no es suficiente" (Gordillo, 2013, págs. 87-89), brindar una protección integral al titular de los datos personales cuando están siendo tratados de manera inadecuada, ya que es menester reconocer que la misma tiene una esencia reactiva, es decir actúa frente al daño, mientras que el derecho a la protección de datos personales presenta un espíritu preventivo.

El derecho a la protección de datos personales conforme lo manifiesta la magister Lorena Naranjo, Directora Nacional de Registro de Datos Públicos es un derecho compuesto, pues su contenido esencial se compone de principios, derechos y obligaciones, por lo que para entender su alcance es necesario enfocar el estudio de este en el análisis de cada uno de estos componentes.

Los principios, derechos y obligaciones que componen este derecho son necesarios para precautelar que el ser humano sea integralmente protegido ante los riesgos y vulneraciones que puede acarrear un tratamiento inadecuado de datos personales.

"El derecho a la protección de datos personales es autónomo, complejo e instrumental, se encarga de brindar mecanismos de prevención y herramientas reactivas que garanticen los derechos fundamentales de los seres humanos titulares de este tipo de información" (Ortiz, 2005). En el mundo existen tres modelos que regulan el flujo y tratamiento de datos personales, generando una discusión sobre cuál es el más adecuado para blindar la dignidad e integridad humana ante la creciente influencia de la tecnología y la necesidad de procesar información de este tipo para desarrollarla, sin que esto afecte el progreso de los Estados y los diferentes actores de la economía.

2. Internet de las cosas

2.1. Sociedad red

La sociedad en la que actualmente vive el ser humano es el resultado de la evolución que se ha venido dando siglos y milenios atrás. "No solo se ha transformado la estructura biológica y anatómica de las personas, sino que, además, los procesos de comunicación, generación de información y conocimiento" (Méndez, 2017, pág. 29), hacia el desarrollo de métodos o mecanismos que facilitan las actividades diarias de los individuos también han progresado.

La transformación evolutiva de la sociedad que se ha generado es producto de diversos procesos turbulentos, tal es la eventualidad que incluso ahora podemos hablar claramente de una Tercera Revolución Industrial, en donde la tecnología juega un papel fundamental.

"Las revoluciones industriales se pueden definir como procesos drásticos de cambio en donde, se empieza a dejar de depender de la actividad agrícola o artesanal y se cambia la matriz productiva, en donde se tiene a la industria como elemento primordial" (Miranda, 1978, pág. 54).

Estas revoluciones están marcadas por generar cambios económicos drásticos en las estructuras organizacionales, en la forma de convivencia de las personas, en el comercio, en consecuencia, impacta por lo general en todas las áreas en las que los individuos se desenvuelven o desarrollan.

"La Primera Revolución Industrial se originó en Gran Bretaña en el siglo XVIII y duró hasta el inicio del siglo XIV" (Marx, 1979, pág. 452), los descubrimientos e inventos que cambiaron la forma de producción fueron la máquina de hilar, la máquina a vapor que se aplicó en barcos y ferrocarriles, procesos de batir hierro fundido y finalmente en 1851 se desplegó el primer cable submarino que comunicaba directamente Europa y América.

La Segunda Revolución Industrial se llevó a cabo entre los años 1850 a 1970 durante los cuales se fortalecieron y perfeccionaron los inventos y descubrimientos de la revolución

anterior, adicionalmente la química, el acero y el petróleo empezaron a tomar protagonismo como elementos fundamentales para desarrollar herramientas, procesos y mecanismos que promovieran la producción, es así que, se creó el motor a explosión, el telégrafo electrónico, el cinematógrafo y el aeroplano.

Como es evidente las revoluciones antes descritas evidenciaron una transformación en la forma de vida e interacción de las personas, pues se han desarrollado herramientas, mecanismos y procesos que automatizan la comunicación, producción y las relaciones entre los seres humanos.

> "En el último tiempo se ha podido observar una época postindustrial, en donde se han generado y desarrollado distintas tecnologías de la información y conocimiento, en un primer momento los seres humanos se desenvolvían en una sociedad de la información caracterizada por una estructura basada en la información abierta capaz de instaurar mercados que se autorregulan y traspasan fronteras" (Del Peso Navarro, 2000).

Posteriormente, la humanidad atravesó la sociedad del conocimiento establecida a finales de los años 90 y diferenciada de la anterior por desarrollar aplicaciones de información que permiten la generación de conocimiento y procesamiento masivo de datos de distintas categorías.

Los datos, la información y el conocimiento empiezan a tomar protagonismo pues son la fuente de innovación y desarrollo en todos los ámbitos en que los individuos se desenvuelven, su valor se equipara al del dinero en la actualidad y se empiezan a generar nuevas formas de uso y tratamiento que permiten adaptar las tecnologías de la información y comunicación a las necesidades de las personas.

Para muchos la incidencia de estas tecnologías en la vida de las personas, es decir, su omnipresencia, la alta conectividad, el acceso en segundos a información, las comunicaciones instantáneas de individuos que se encuentran en partes opuestas del planeta, entre otros elementos, llevan a concluir que la sociedad red es la realidad actual.

En consecuencia, los seres humanos a través de la sociedad red entran en una realidad hiperconectada en la que los bienes y servicios requieren del diseño e implementación de

tecnologías de la información y comunicación adaptadas a la satisfacción de necesidades de cada una de las personas, todo esto en tiempo real, determinando que, los datos, la información y el conocimiento han revolucionado las formas en que los individuos interactúan y se comunican.

2.2. Internet de las cosas

Las tecnologías de la información y comunicación han tenido un impacto evidente en la vida de los seres humanos, cuando hablamos de TIC, no solo se hace referencia al Internet, pero es uno de los elementos más destacados en la actualidad, pues permite la alta conectividad, la comunicación en segundos e involucra un sin número de beneficios en la generación de bienes y servicios.

El Internet de las cosas (Internet of Tingas) conforme sus siglas en inglés, es una nueva tecnología o tecnología emergente, que conjuga todos los elementos previamente mencionados, dado que deja en evidencia la funcionalidad de la sociedad red, esto quiere decir que se puede palpar la alta conectividad en tiempos sumamente cortos permitiendo el análisis y comunicación de los actores o participantes en menos de tres segundos.

No se ha llegado a un consenso sobre la definición exacta del Internet de las Cosas, sin embargo, se puede citar algunas de los conceptos más importantes, para desglosar elementos comunes; hay que decir, además que a este tipo de terminologías no se las puede definir tradicionalmente sobre las perspectivas y análisis de diversos autores, sino que en menester que desglosar los conceptos de los mismos desarrolladores o empresas que se dedican a su impulso y explotación.

Es así como para CISCO (empresa de telecomunicaciones que tiene como objeto la fabricación, mantenimiento y venta de tecnologías de la información y comunicación, así como la realización de consultorías derivadas de su giro de negocio) el IoT puede definirse como:

La próxima evolución de Internet. Dado que los seres humanos avanzan y evolucionan mediante la conversión de datos en información, conocimiento y sabiduría, Internet de las

Cosas posee el potencial para cambiar el mundo tal como lo conocemos, para mejor. La rapidez con la que llegaremos a ese punto depende de nosotros (Dave Evans, 2001, pág. 12).

Para Alfaro Solís, en cambio, el Internet de las Cosas es:

IoT es simplemente la red de cosas/dispositivos interconectados que están embebidos con sensores, software, conectividad de red y electrónica necesaria que les permite recopilar e intercambiar datos haciéndolos responder. Más que un concepto Internet de Cosas es esencialmente un marco arquitectónico que permite la integración y el intercambio de datos entre el mundo físico y los sistemas informáticos sobre la infraestructura de red existente (Solís, 2017, pág. 4).

De estos dos conceptos podemos evidenciar que el Internet de las cosas no solo comprende Internet, entendido como la World Wilde Web, sino al conjunto de elementos como hardware y software que permiten que diversos dispositivos estén conectados a la red, en donde son los datos y la información un componente esencial, ya que su integración e intercambio genera que productos y servicios estén adaptados a la satisfacción de las necesidades de los usuarios.

El Internet de las Cosas ha evolucionado, es un concepto y tecnología que ha sufrido diversos cambios y que se ha ido mejorando con el objetivo de brindar mejores bienes o servicios.

“Entonces para hablar de su origen y transformación para llegar al resultado actual, es necesario, remontarnos al nacimiento de Internet en donde se concebía al mismo como una herramienta desarrollada por el ejército para operaciones de inteligencia” (Gerrero, 2006).

Lo que consecutivamente se desarrolló como un proyecto de investigación denominado ARPANET, un conjunto de componentes cerrados producidos para satisfacer necesidades de grupos dedicados a la exploración académica.

Con posterioridad su utilidad se expandió y se observó que se podía usar al Internet como un espacio idóneo para el desarrollo de la economía, al ser una potente herramienta comunicacional, se empezó a explotar al Internet como un espacio publicitario.

2.3. Problemática que se presenta ante el tratamiento inadecuado de datos personales en el Internet de las cosas.

> "Como se ha podido evidenciar una de las características principales del Internet de las Cosas es la hiperconexión que permite el flujo de todo tipo de datos, que en gran cantidad son personales; los procesos de transmisión, el software y la infraestructura prevén una mínima intervención humana, lo que puede ocasionar un problema pues en la mayoría de procesos automatizados los algoritmos utilizados para tratar este tipo de información no se apegan a lo establecido como requisitos mínimos para garantizar el derecho a la protección de datos personales de los individuos" (Parker, 1989, págs. 3-4).

> "En el proceso del IoT participan varios sujetos, así como funciones. En un primer momento nos encontramos frente a la recolección de los datos de la fuente de origen, su transporte al lugar de almacenamiento determinado por el responsable del tratamiento, para una vez almacenados pasar a su procesamiento, administración y análisis, sin dejar de lado que posteriormente pueden ser cedidos a terceros" (Téllez, 1996, pág. 23).

> "El Internet de las cosas está presente casi en todo, muchas veces sin que el ser humano pueda percibirlo, un ejemplo claro es nuestro teléfono, que cada cinco minutos se conecta a una antena que informa a diversos responsables entre muchas otras cosas, la ubicación de quien tenga el dispositivo en posesión, el medio en que se moviliza, ya sea a pie (a través del conteo de pasos), vehículo propio o transporte público (tiempo de traslado de un lugar a otro), información médica como latidos del corazón por minuto, cuantos mensajes se han recibido en ese tiempo, si se han realizado llamadas telefónicas, a quien, y así un variado sin número de datos que no podemos si quiera imaginar" (Bliznakoff del Valle, 2014).

> "Ahora bien, podemos decir que para un proveedor de servicio de transporte público es interesante lograr determinar a qué hora hay más gente en un lugar, para así enviar movilización con mayor frecuencia o disminuirla en horas en que la afluencia de personas es menor, esto le permite optimizar recursos económicos, humanos, entre otros, así mismo el usuario del servicio se sentirá mucho mejor al momento de consumir el mismo, lo cual generará beneficios para ambas partes" (Ospina Botero, 2001, pág. 27).

> "Sin embargo, si los datos si estos mismos datos son utilizados inadecuadamente o maliciosamente pueden llegar a afectar la integridad o dignidad de las personas titulares de dicha información; que pasará entonces si estos datos se ceden a un destinatario desconocido que utilice los mismos para ubicar a las personas y secuestrarlas, o sean utilizados por gobiernos dictatoriales para determinar que sujetos asistieron a una manifestación, identificar su ideología política y negarles el acceso a servicios básicos como medicinas, entre muchos otros ejemplos unos más graves que otros en donde se determina la necesidad de implementar en todos estos procesos medidas de protección para este tipo de información" (Murillo, 2017, pág. 23).

Es entonces evidente que los datos recolectados, almacenados y tratados con mínima intervención humana, requieren entonces medidas que protejan la privacidad, la seguridad y al titular en sí mismo de los datos personales; dado que los daños que pueden llegar a ocasionarse resultan muy nocivos para la vida de la gente.

El Centro de Seguridad TIC de la Comunidad Valenciana establece que el principal problema derivado del Internet de las Cosas es el acceso libre a los datos contenidos en el IoT.

> "Cada día son más los dispositivos que se encuentran conectados a Internet, consecuencia de esto es que el flujo de datos es cada vez mayor, enfrentado un sin número de riesgos que pueden llegar a afectar al titular de los datos gravemente; en donde la seguridad es uno de los aspectos más críticos, dado que el riesgo de pérdida de la información por amenazas externas como internas es realmente alto" (Yun & Yuxin, 2010).

Son evidentes los inconvenientes que pueden generarse a través del tratamiento inadecuado de datos personales procesados mediante el Internet de las Cosas, por este motivo varios de los proveedores de este tipo de servicios han decido implementar una serie de medidas que permitan garantizarle a las personas el derecho a la protección de sus datos, sin embargo, estas medidas no son suficientes para evitar que existan vulneraciones leves o graves a los usuarios.

> "En el año 2014 se realizó un estudio que evidencio en sus conclusiones que el 90% de dispositivos conectados a internet recababan información personal como nombre,

dirección, número de tarjeta de crédito, número telefónico, entre otros, de los cuales el 70% no cuenta con mecanismos de enmascaramiento o encriptación en su transporte o en la cesión, adicionalmente se logró determinar que el 80% no contaba con códigos de seguridad complejos, lo que generaba una falla de seguridad pues era muy sencillo para hackers acceder a estos sistemas, y que finalmente el 60% no contaban con medidas de seguridad apropiadas para resguardar la mencionada información" (Alcaraz, s.f.).

"Para muchos el Internet de las Cosas es una visión del futuro muy poco palpable en la actualidad, sin embargo, cabe destacar que es una realidad que estamos afrontando sin conocer a ciencia cierta sobre su funcionamiento o los efectos del procesamiento masivo de los datos personales que esta trae inmersa. Una de las estadísticas más notorias en este ámbito ha logrado proyectar que para el año 2020 estarán conectadas más de 50 millones cosas, lo que lleva a determinar que existe un crecimiento exponencial de esta tecnología a nivel mundial" (Bankinter, 2011, pág. 68).

"Es entonces correcto afirmar que el Internet de las Cosas es una tecnología emergente que impacta positivamente en la vida de los seres humanos, no solo como un medio que permite brindar mejores servicios para los usuarios, sino también como un medio para priorizar recursos y la prestación de experiencias personalizadas, así como más adaptadas a las necesidades de cada uno de los individuos; este nuevo tipo de tecnología prevé un alto flujo de datos personales, lo que hace necesario que se implementen elementos que protejan efectivamente a los titulares de los datos personales" (Pérez, 2011, pág. 42).

3. Protección de datos en el Internet de las Cosas

3.1 Derecho a la protección de datos personales y el Internet de las Cosas en el Ecuador

El Ecuador en la actualidad requiere que se promueva la industria para mejorar su situación económica, razón por la cual se han dictado diversas normas que creen incentivos para la inversión y producción nacional. Esto quiere decir que tiene la necesidad como país de impulsar y promover el progreso social, así como el económico.

El gobierno ecuatoriano a lo largo de los últimos años ha pactado diversos acuerdos para promover la innovación tecnológica, en donde incentivar la producción nacional de nuevas tecnologías y tecnologías emergentes como el Internet de las Cosas ha resultado esencial.

El Internet de las Cosas también es producido por empresas ecuatorianas como Aymesa o Audioelec, la primera encargada de desarrollar insumos de conectividad constante para vehículos automotores, sobre todo aquello relacionado con la geolocalización y el reporte del estado de los mismos; la segunda que se ha encargado de diseñar sistemas Smart y ensamblar televisores con Internet de las Cosas, estas dos constituyen producción nacional palpable de como el IoT, no representa un futro lejano, sino más bien que constituye una realidad actual de nuestro país.

El Ecuador ha tenido tres intentos de contar con una Ley de Protección de Datos Personales en la Asamblea Nacional, dos de los cuales se encuentran con disposición de archivo, dado que su contenido ha desnaturalizado la esencia del derecho, puesto que se ha transcrito legislación extranjera que no se adapta a nuestra realidad, o se confunde a la protección de datos personales con intimidad o privacidad.

Como lo demuestra el proyecto presentado por Gabriela Rivadeneira que lleva por título "Ley Orgánica de Protección de Derechos a la Intimidad y Privacidad sobre los Datos Personales", en donde evidentemente se transgrede lo determinado por la Constitución de la República del Ecuador, que dota de independencia y autonomía al derecho a la protección de datos personales, es más en el 2008 se superó la discusión sobre el modelo o

visión respecto del tema se va a seguir, y se determinó que debe adaptarse el ordenamiento jurídico ecuatoriano, es decir a una visión de derecho, a la que se suma la garantía de habeas data.

El derecho a la protección de datos personales se reconoce y garantiza en el artículo 66 numeral 19 de la Constitución y determina lo siguiente:

> "Artículo 66.- Se reconoce y garantizará a las personas. – 19. El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley" (Constitución del Ecuador, 2008).

Además, ha sido recogido en normativa dispersa que no puede aplicarse, dado que se trata de un derecho complejo que no solo implica un sistema reactivo, sino de la implementación de medidas que prevengan el daño o la lesión a los derechos de los sujetos.

También, en el artículo 92 del mismo cuerpo normativo se plantea al habeas data como una garantía constitucional orientada a su ejercicio:

"Artículo 92.- Toda persona por sus propios derechos o como representante legitimado para el efecto, tendrá derecho a conocer de la existencia y a acceder a los documentos, datos genéticos, bancos o archivos de datos personales e informes sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, en soporte material o electrónico. Asimismo, tendrá derecho a conocer el uso que se haga de ellos, su finalidad, su origen y destino de información personal y el tiempo de vigencia del archivo o banco de datos.

Las personas responsables de los bancos o archivos de datos personales podrán difundir la información archivada con autorización de su titular o de la ley.

> "La persona titular de los datos podrá solicitar al responsable el acceso sin costo al archivo, así como la actualización de los datos, su rectificación, eliminación o anulación. En el caso de datos sensibles, cuyo archivo deberá estar autorizado por la ley o por la persona titular,

se exigirá la adopción de las medidas de seguridad necesarias. Si no atendiera su solicitud, ésta podrá acudir a la jueza o juez. La persona afectada podrá demandar por los perjuicios ocasionados" (Constitución del Ecuador, 2008).

Podemos concluir entonces que el derecho a la protección de datos personales está reconocido por el Constitución de la República del Ecuador, y este misma comprende la garantía del habeas data, la cual no solo está orientada a garantizar el derecho objeto del presente trabajo, sino otros derechos como la propia voz e imagen, honra, reputación , entre muchos otros, además, tiene un carácter reactivo, esto quiere decir que solo entra en vigencia una vez que se ha producido un daño y es necesario acudir a un juez para que este resuelva el cese del perjuicio y la reparación integral. Los derechos en esencia son preventivos, razón por la cual es necesario que a la hora de tratar los datos personales se implementen medidas y herramientas encaminadas a que no se produzcan daños.

3.2 Principios del derecho a la protección de datos personales

"Los principios son las bases sobre las que se asientan los derechos, valores que permiten el desarrollo de ciertas instituciones jurídicas, que tienen como objeto comprender el alcance de protección de cualquier figura que ha de aplicarse en el campo del Derecho. El derecho a la protección de datos entonces requiere de la aplicación de una serie de principios que han de ser puestos a consideración a continuación" (Villalba, 2000, pág. 41).

3.2.1. Principio de consentimiento informado

"El consentimiento se refiere a la manifestación de la voluntad del titular de los datos personales, este debe ser informado, explicito e inequívoco. El consentimiento es el elemento esencial del derecho a la protección de datos personales, dado que traduce la autodeterminación informativa, esto es que el titular del dato está facultado a conocer y aceptar todo lo que vaya a realizarse con la información relacionada con él" (Santos García, 2005, pág. 58).

"Es entonces el consentimiento informado la piedra angular del derecho a la protección de datos personales, pues es la traducción aplicable de la autodeterminación informativa, y como su nombre lo manifiesta, es necesario que se le comunique al titular de los datos,

acerca de todos los procesos a los que están sujetos los mismos" (Remolina Angarita, 2013, pág. 29).

"Este consentimiento debe ser expreso e inequívoco, esto no se refiere a que exista una única forma en que pueda ser recabado, esto quiere decir que puede solicitarse el consentimiento por cualquier medio, siempre que este pueda ser probado con posterioridad, dado que es necesario que no exista duda que medio una manifestación de voluntad de la persona que identifica o hace identificable a un sujeto o persona" (Santos García, 2005, pág. 60).

3.2.2. Principio de finalidad

"Este principio es gran base de los demás, ya que en el marco de este se establecerá el consentimiento, la calidad, la proporcionalidad y conservación. Esto debido a que como es conocido la protección de datos personales actúa frente al tratamiento de los mismos y a que este como consecuencia está en la obligatoriedad de responder a ciertos objetivos" (Santos García, 2005, pág. 56).

"Estos deben ser específicos a fin de establecer las distinciones necesarias entre los mismos y con ello atender a cada sección con debido sigilo, en el mismo sentido, deberán ser explícitos, es decir manifestados de tal manera en que no medie confusión en su reconocimiento, y finalmente lícitos que como es conocido debe basarse en el respeto a la carta de derechos evitando con ello vulneraciones" (Santos García, 2005, pág. 56).

Es así como este principio se determina como la directriz del tratamiento y en el mismo contexto como delimitante ante el mismo. Ya que gracias a su injerencia y basados en el absoluto respeto hacia el mismo entonces los principios articulados a este también tendrán plena vigencia.

3.2.3. Principio de calidad

"Es de vital importancia que la esencia de la protección de datos personales, es decir los datos como tal que van a ser objeto de tratamiento, mantengan índices de calidad adecuados a fin de que se genere con ello protección al titular de los mismos frente a lo que

> se maneja respecto a si y en beneficio también de quien trata esta información ya que al mantener los datos adecuados, exactos, verídicos, proporcionados y pertinentes entonces el tratamiento también va a estar orientado a basarse a esa eficacia" (De la Torre, 2018, pág. 3).

"En relación con lo mencionado, los datos personales, además, actualmente son considerados como activos dentro del patrimonio de las empresas, es así que al encargarse de efectivizar el principio de calidad se genera como consecuencia inevitable un acto de inversión" (Vizcaíno Calderón, 2001, pág. 96).

Con esto se evidencia que, este principio es de vital injerencia por ser el que se encarga de dar un marco de eficacia a los datos y en consecuencia al tratamiento.

3.2.4. Principio de seguridad

"Reconociendo que, bajo los principios de consentimiento informado y finalidad, se ha establecido un camino hacia el tratamiento, es menester del responsable de este establecer mecanismos y herramientas de seguridad que garanticen en su totalidad el debido resguardo frente a los datos personales que serán objeto de trato" (Santos García, 2005, pág. 75).

> "Basados en este criterio, es importante reconocer que la esencia de la protección de datos personales es su espíritu preventivo, por ende, es imprescindible generar un resguardo a esta clase de información frente a cualquier posible vulneración, de manera que, las bases de datos en la que se conserve deberán responder frente al carácter preventivo y garantizar la vigencia de los derechos del titular y demás derechos articulados a la protección de datos personales y sus instrumentalidades" (Vizcaíno Calderón, 2001, pág. 105).

Al respecto la sentencia del caso Worten, emitida el 30 de mayo de 2013 y resuelta por el Tribunal de Justicia de la Unión Europea con respecto a la obligación del Estado portugués de prever medidas técnicas y organizacionales para la protección de datos atendiendo al artículo 17 de la Directiva 95/46 señala que "los Estados miembros deben establecer la obligación del responsable del tratamiento de los datos personales de aplicar las medidas técnicas y de organización destinadas a garantizar un nivel de seguridad adecuado en

relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse."

Es así como, en atención al principio de seguridad se evitará que la esencia del dato sufra adulteraciones o daños y en efecto de lo cual se impedirá cualquier tratamiento no autorizado.

3.2.5. Principio de proporcionalidad

> "Este principio pone en evidencia la obligatoriedad de que el tratamiento se vea severamente configurado con respecto a la finalidad inicialmente expuesta al titular, esto quiere decir que el responsable dirigirá su atención a los objetivos inicialmente planteados y no actuara con arbitrariedad con respecto al tratamiento" (Riascos, 2012, pág. 33).

> "En consecuencia, se encargará de que este sea adecuado, relevante y no excesivo frente a la finalidad para la que fueron recopilados. Es importante denotar que, si bien este principio está orientado al tratamiento, también recae sobre la recogida de datos, es decir, todos aquellos que sean recabados deberán atender a la finalidad expuesta, a la mira del principio del mismo nombre y además deberán ser oportunos y mantenerse en un margen de evidente necesariedad en función a la proporcionalidad" (Garriga, 2015, pág. 170).

> "La importancia de este principio se traduce en la mínima intervención del responsable frente al tratamiento, esto asegura que los datos personales no sean manipulados de forma inoportuna y descomunal, avalando con ello la prevención ante posibles riesgos generados frente a una mayor exposición de datos inapropiada" (Gerrero, 2006, pág. 206).

3.3. Derechos rectores de la protección de datos personales

Como se ha manifestado con antelación el derecho a la protección de datos personales es complejo, razón por la cual requiere se compone de una serie de elementos que se han desarrollado a lo largo del presente trabajo de titulación, como principios u obligaciones, además de los derechos que se desarrollan en el siguiente apartado:

3.3.1. Derecho de acceso

Al hablar de acceso nos referimos al derecho que tiene el titular para acceder como tal a la información que de él consta en bases de datos. Este es un criterio que se aplica a los datos en general, en consecuencia, no se limita frente a si la base es pública o privada.

Al respecto la sentencia del caso Rijkeboer, emitida el 07 de mayo de 2009 y resuelta por el Tribunal de Justicia de la Unión Europea, acudiendo a los términos del Abogado General señala que "los titulares de los datos tratados pueden velar por su buen uso, ejerciendo el llamado "derecho de acceso" (…) pues el acceso representa la auténtica dimensión subjetiva de la Directiva, que, en suma, permite al individuo reaccionar en defensa de sus intereses."

> "De tal manera que, basta con que sea el titular quien la solicita para efectivizar el derecho, mismo que bajo ciertas circunstancias puede complementarse incluso con la gratuidad del servicio. Su sistema es anclado por la necesidad de que el titular conozca acerca de sus datos personales que son objeto de tratamiento y así dar paso a la autodeterminación informativa, razón por la cual no es prescindible que el titular extienda una serie de motivos más allá de la efectivización del derecho" (López I. , 2005, pág. 89).

3.3.2. Derecho de rectificación

> "Este derecho se materializa frente a la existencia de datos que no reflejen el principio de calidad, puesto que, al mantener el responsable una base de datos contenidos sin haber atravesado un proceso de actualización y en consecuencia o por otras circunstancias estos se encuentren registrados de manera inexacta, falsa, o incorrecta, entonces el titular estando en calidad de efectivizar sus derechos, puede solicitar la rectificación o corrección de los mismos a fin de garantizar que el tratamiento que se les dé no sucumba en el error o la falsedad" (López I. , 2005, pág. 96).

La importancia de este derecho se refleja en la necesidad de mantener un margen de transparencia entre el responsable del tratamiento de los datos personales y el titular de estos, ya que es en función a esto que se configura e implanta una relación de confianza que marca beneficios para ambas direcciones.

3.3.3. Derecho de cancelación

> "Para entender este derecho nos vamos a remitir al principio de finalidad y proporcionalidad, debido a que, este actúa en cuanto estos dos principios han dejado de materializarse, en consecuencia, el derecho a la cancelación es aquel del que dispone el titular con el objetivo de bloquear toda información que no sea necesaria conforme la finalidad inicial que se estableció para justificar el tratamiento" (López I. , 2005, pág. 95).

Así también, puede procederse con este bloqueo cuando el tratamiento de esta información ha cumplido el objetivo inicialmente planteado y conforme el principio de proporcionalidad, cuando el uso de esta clase de información no corresponda en términos adecuados a lo que se prescinde del tratamiento.

3.3.4. Derecho de oposición

El derecho a la oposición se consagra en función al tratamiento de los datos personales ya que consiste en el derecho que tiene el titular para oponerse al mismo en tanto este sienta que se han vulnerado los derechos que se le consagran o a su vez cuando los principios han sufrido vulneraciones a causa del tratamiento.

> "En este contexto se puede establecer respecto a este derecho que, el titular, en base a la autodeterminación informativa que posee, puede oponerse al tratamiento de sus datos en cuanto sus intereses se vean afectados por este. Es importante determinar, sin embargo, que este derecho presenta excepciones, basados en la superioridad del interés colectivo frente al particular" (López I. , 2005, pág. 98).

3.3.5. Derecho de información

Conforme lo establecido en el principio de consentimiento, para que el titular pueda presentarlo se deberá informar previamente respecto a las finalidades para las que va a ejercerse tratamiento sobre sus datos personales.

> "Bajo esta premisa, el titular tiene derecho a ser informado previo al tratamiento para poder otorgar su consentimiento, sin embargo, este derecho no se limita a la información previa, sino también a cualquier circunstancia que se suscite durante el tratamiento que requiera ser conocida por el titular, entendiéndose que este es el único que puede autorizar un cambio en el tratamiento o en la finalidad" (Santos García, 2005, pág. 78).

3.4. Privacidad en el diseño y por defecto como elemento esencial para garantizar el derecho a la protección de datos personales en el Internet de las Cosas.

La privacidad por diseño surge de la visión de la protección de datos personales como un modelo preventivo, es decir que tiene la facultad de actuar con efectos protectores que advierten el daño en lugar de únicamente reaccionar ante él.

> "La adopción de esta medida recaería en los proveedores de servicios que atendiendo a lo que hoy es el principio de seguridad, se verían en la obligatoriedad de implementar mecanismos que respondan a esta finalidad explayando también el criterio de confidencialidad a fin este ser una herramienta que colabore con el propósito de protección de los datos personales. En consecuencia, la reserva no sería una opción, sino más bien, un mecanismo ineludible que colabore con la protección de los datos de los individuos, en este contexto la potestad de este tipo de información solo le pertenece al titular" (Gregorio & Ornelas, 2018, pág. 4).

> "En este sentido, quedan liberadas todas las barreras correctivas al impulsar un margen de protección predeterminado. Esto, al insistir en el espíritu preventivo de la protección de datos personales, que, distinto a actuar únicamente con respecto a la generación del daño, se encarga de evitarlo en respeto a los principios que lo consagran" (Freixas, 2001, pág. 100).

La publicidad por defecto por su parte destaca al dato personal como un activo, debido a que para las compañías esta categoría tiene su funcionalidad enfocada en sostener sus necesidades con respecto a al acceso y tratamiento de datos de esta especie con el objetivo de ser compartidos o transferidos en distintas instancias atendiendo a su giro de negocio.

CONCLUSIONES

Diariamente existe un crecimiento de forma exponencial con relación al número de dispositivos conectados a Internet; es así que la hiperconexión es la nueva realidad que enfrenta el ser humano, esto ha revolucionado la forma en que los seres humanos interactúan y se desarrollan, pues se desenvuelven en un entorno llamado Internet.

El Internet de las Cosas implica que incluso objetos del cotidiano vivir se encuentren conectados a la red, pero no solo abarca está conexión, sino también el flujo desmedido de datos que permiten mejorar los servicios o productos ofertados a los usuarios, de los cuales la gran mayoría son datos personales.

Los datos personales juegan un papel protagónico en el desarrollo e implementación de estas tecnologías emergentes. El derecho a la protección de datos personales por su parte se ha tornado especialmente relevante ante estas nuevas realidades.

Es innegable que el tratamiento inadecuado de datos personales puede acarrear diversas lesiones a los derechos humanos, por lo que para evitar que la dignidad e integridad se vea vulnerada, es necesario un mecanismo que garantice y efectivice este derecho.

El Ecuador reconoce y garantiza en la Constitución el derecho a la protección de datos personales, dotándolo de autonomía, diferenciándolo de la intimidad y privacidad, además determina que una vía para efectivizarlo una vez que se ha producido el daño es la garantía constitucional del habeas data.

El habeas data si bien constituye una forma para ejercitar el derecho a la protección de datos personales, no es la vía idónea para efectivizarlo, dado que la naturaleza de un derecho prevé una reactiva, pero también la necesidad de prevención para evitar que se vulnere la dignidad e integridad de la persona, y solo cuando habiendo agotado las medidas preventivas, se active el sistema reactivo.

Adicionalmente, en el Ecuador el derecho a la protección de datos personales se menciona en diversas normas como la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes

de Datos, el Código Ingenios, Ley de Telecomunicaciones, entre otras, a pesar de esto no puede ser aplicada por la inexistencia de un sistema unificado al tratarse de un derecho complejo, razón por la cual la Dirección Nacional de Registro de Datos Públicos en la actualidad se encuentra desarrollando un proyecto normativo que adopte la materia y sus mecanismos de implementación eficaz.

BIBLIOGRAFÍA

Acedo, A. (2013). *Introducción al derecho privado.* Madrid: Dykinson.

Alcaraz, M. (s.f.). *Internet de las Cosas.* Asunción, Paraguay: Universidad Católica Nuestra Señora de la Asunción. Obtenido de http://jeuazarru.com/wp-content/uploads/2014/10/Internet-of-Things.pdf

Almuzara, C. (2007). *Estudio práctico sobre la protección de datos de carácter personales.* Valladolid, España: Lex Nova. Obtenido de https://dialnet.unirioja.es/servlet/libro?codigo=6114

Álvarez, J. (2011). *Guía práctica sobre la protección de datos.* Valladolid, España: Lex Nova.

Álvarez, M. (2015). *Derecho al olvido en internet: El nuevo paradigma de la privacidad en la era digital.* Madrid, España: Reus. Obtenido de https://www.editorialreus.es/libros/derecho-al-olvido-en-internet-el-nuevo-paradigma-de-la-privacidad-en-la-era-digital/9788429018363/

Bankinter. (2011). El internet de las Cosas: En un mundo conectado de objetos inteligentes. *Fundación de la Innovación Bankinter*, 78. Obtenido de http://www.belt.es/expertos/imagenes/XV_FTF_El_internet_de_las_cosas.pdf

Bliznakoff del Valle, D. (2014). *Tecnologías, usos, tendencias y desarrollo futuro*. Obtenido de http://openaccess.uoc.edu/webapps/o2/bitstream/10609/40044/6/dbliznakoffTFM0115memoria.pdf

Constitución del Ecuador. (2008). *Constitución de la República.* Montecristi, Ecuador: República del Ecuador. Obtenido de https://www.oas.org/juridico/mla/sp/ecu/sp_ecu-int-text-const.pdf

De la Torre, P. (02 de 10 de 2018). *El Derecho*. Obtenido de Calidad de los datos e información de carácter personal: https://elderecho.com/calidad-de-los-datos-e-informacion-de-caracter-personal

Del Peso Navarro, E. (2000). *Ley de protección de datos: La nueva LORTAD.* Madrid, España: Díaz de Santos. Obtenido de

https://books.google.com.ec/books/about/Ley_de_protecci%C3%B3n_de_datos.html?id=2mhfiHdwYA8C

Díaz, A. (2016). *Reglamento general de protección de datos.* Madrid, España: Reus.

Dueñas, J. (2014). *Sistemas de información y bases de datos en consumo.* Madrid, España: IC Editorial. Obtenido de https://www.iceditorial.com/atencion-al-cliente-consumidor-o-usuario-comt0110/6473-sistemas-de-informacion-y-bases-de-datos-en-consumo-uf1755-9788416109845.html

Freixas, G. (2001). *La protección d elos datos de carácter personal en el derecho español.* Barcelona, España: Bosch. Obtenido de https://dialnet.unirioja.es/servlet/libro?codigo=127354

García, C. (2003). *El derecho a la intimidad y dignidad en la doctrina del Tribunal Constitucional.* Murcia, España: Universidad de Murcia Departamento de Derecho Civil.

Garriga, A. (2015). *Nuevos retos para la protección de datos.* Madrid, España: Dykinson. Obtenido de https://www.dykinson.com/libros/nuevos-retos-para-la-proteccion-de-datos-personales/9788490856536/

Gerrero, M. d. (2006). *El impacto de internet en el Derecho fundamental a la protección de datos de carácter personal.* Pamplona, España: Civitas. Obtenido de https://www.marcialpons.es/libros/el-impacto-de-internet-en-el-derecho-fundamental-a-la-proteccion-de-datos-de-caracter-personal/9788447026883/

Gordillo, A. (2013). *Tratado de derecho administrativo.* Buenos Aires, Argentina: F.D.A. Obtenido de https://www.gordillo.com/

Gregorio & Ornelas. (2018). *Protección de datos personales.* México D.F, México: Insituto Federal de acceso a la información y proteción de datos. Obtenido de https://idl-bnc-idrc.dspacedirect.org/handle/10625/46963

Kroenke, D. (2003). *Procesamiento de bases de datos: fundamentos, diseños eimplementación.* México, México: Pearson. Obtenido de https://books.google.com.ec/books/about/Procesamiento_de_bases_de_datos.html?id=7ORUWItwcNEC

López, I. (2005). *Protección de datos personales:manual práctico para empresas.* Madrid, España: Fundación Confemetal. Obtenido de https://books.google.com.ec/books/about/Protecci%C3%B3n_de_datos_personales.html?id=MMVwqkyky-cC

López, S. (2009). *El acceso a la información como un derecho fundamental.* México, México: Insituto Federal de acceso a la información pública. Obtenido de https://archivos.juridicas.unam.mx/www/bjv/libros/1/7/5.pdf

Marecos, A. (04 de 10 de 2018). *Access Press Lite*. Obtenido de Configuración jurídica del derecho a la autodeterminación informativa: http://oiprodat.com/2013/03/15/configuracion-juridica-del-derecho-a-la-autodeterminacion-informativa/

Marx, K. (1979). *El Capital.* Madrid, España: Luarna. Obtenido de http://www.ataun.net/bibliotecagratuita/Cl%C3%A1sicos%20en%20Espa%C3%B1ol/Karl%20Marx/El%20capital%20I.pdf

Méndez, M. (2017). *Cultural and Smart City.* Madrid, España: Dykinson. Obtenido de https://www.dykinson.com/libros/cultural-and-smart-city-torre-pacheco/9788491484585/

Miranda, M. (1978). *La educación como proceso conectivo de la sociedad, laciencia, la tecnología y la política.* México, Trillas: Trillas. Obtenido de http://repositorio.pucp.edu.pe/index/bitstream/handle/123456789/49238/educacion_proceso_mario_miranda.pdf?sequence=1

Murillo, L. (2017). *El derecho a la autodeterminación informativa y la protección de datos personales.* Azpicueta: BIBLID. Obtenido de https://dialnet.unirioja.es/servlet/articulo?codigo=3049840

Ortiz, C. (2005). *La protección de datos personales: Un derecho autónomo con base en los conceptos de intimidad y privacidad.* Madrid, España: Dykinson. Obtenido de https://www.casadellibro.com/libro-la-proteccion-de-datos-personales-un-derecho-autonomo-con-base-e-n-los-conceptos-de-intimidad-y-privacidad/9788497725972/1016231

Ospina Botero, D. (2001). *Introducción al muestreo.* Bogotá, Colombia: UNIBIBLOS. Obtenido de http://www.uneditorial.com/introduccion-al-muestreo-estadistica.html

Palazzi, P. (2002). *La transmisión internacional de datos personales y la protección de la privacidad: América Latina, Estados Unidos y la Unión Europea.* Texas, Estados Unidos: Ad-Hoc. Obtenido de https://www.amazon.com/Transmision-Internacional-Datos-Personales-Proteccion/dp/9508943181

Parker, D. (1989). *Computer Crimen.* Washintong D.C, Estados Unidos: National Institute of Justice.

Passemard, E. (2004). *¿Seguridad, privacidad, confidencialidad? el desafío de la protección de datos personales.* Montevideo, Uruguay: Trilce. Obtenido de https://books.google.com.ec/books/about/Seguridad_privacidad_confidencialidad.html?id=SzcVQq3tkq0C&redir_esc=y

Pérez, S. (04 de 10 de 2011). *Readwrite*. Obtenido de Mobile phones will serve as central hub to internet of things: https://readwrite.com/2011/02/16/mobile-phones-will-serve-as-hubs-to-internet-of-things/

Piñar, J. (2016). *Reglamento general de protección de datos.* Madrid, España: Reus. Obtenido de https://www.editorialreus.es/libros/reglamento-general-de-proteccion-de-datos/9788429019360/

Recio, M. (2016). *Protección de datos personales e innovación: ¿Imcompatibles?* Madrid, España: Reus. Obtenido de https://books.google.com.ec/books/about/Protecci%C3%B3n_de_datos_personales_e_innova.html?id=VL1UDwAAQBAJ&redir_esc=y

Remolina Angarita, N. (2013). *Tratamiento de datos personales.* Quito, Ecuador: Legis. Obtenido de https://www.legis.com.co/editorial-libros-trm/p

Riascos, L. (2012). *Los delitos contra los datos personales y el.* Bogotá, Colombia: Derecho y Realidad. Obtenido de file:///C:/Users/AMERICAN/Downloads/4868-Texto%20del%20art%C3%ADculo-10933-1-10-20160707.pdf

Santos García, D. (2005). *Nociones generales de la Ley Orgánica de Protección de datos.* Madrid, España: TECNOS. Obtenido de https://www.casadellibro.com/libro-nociones-generales-de-la-ley-organica-de-proteccion-de-datos/9788430942299/1022258

Suárez, R. (2010). *Tecnologías de la información y comunicación.* Madrid, España: Ideas Propias. Obtenido de https://www.ideaspropiaseditorial.com/manuales-transversales/129-tecnologias-de-la-informacion-y-la-comunicacion-modulo.html

Téllez, J. (1996). *Derecho informático.* México D.F, México: Interamericana de México S.A de C.V. Obtenido de https://clauditha2017.files.wordpress.com/2017/09/derecho-informatico-cuarta-edicion-julio-tc3a9llez-valdc3a9z.pdf

Villalba, C. (2000). *La protección intelectual de los bancos de datos.* Quito: Librería Jurídica Cevallos.

Vizcaíno Calderón, M. (2001). *Comentarios de la Ley Orgánica de protección de datos de carácter personal.* Madrid, España: Ellacuría. Obtenido de https://www.casadellibro.com/libro-comentarios-a-la-ley-organica-de-proteccion-de-datos-de-caracter-personal/9788447016075/779168

Yun & Yuxin, M. B. (2010). *Research on the architecture and key technology of internet things (IoT) applied on smart grid.* Beijin, China. Obtenido de https://ieeexplore.ieee.org/document/5557611