FACULTAD DE DERECHO Y CIENCIAS SOCIALES

LA PROBLEMÁTICA DE LA PROTECCIÓN DE DATOS PERSONALES Y LA GEOLOCALIZACIÓN.

AUTORA

Emilia Dominique Salvador Aguas

AÑO

2018

FACULTAD DE DERECHO Y CIENCIAS SOCIALES

LA PROBLEMÁTICA DE LA PROTECCIÓN DE DATOS PERSONALES Y LA GEOLOCALIZACIÓN.

Trabajo de Titulación en conformidad con los requisitos establecidos para optar el título de Abogada de los Tribunales y Juzgados de la República.

Profesor Guía

Rafael Eduardo Serrano Barona

Autora

Emilia Dominique Salvador Aguas

Año

2018

DECLARACIÓN DEL PROFESOR GUÍA

"Declaro haber dirigido el trabajo, La Problemática de la Protección de Datos Personales y la Geolocalización, a través de reuniones periódicas con la estudiante Emilia Dominique Salvador Aguas, en el semestre 2018-2, orientando sus conocimientos y competencias para un eficiente desarrollo del tema escogido y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación".

_____

Rafael Eduardo Serrano Barona

Abogado Especialista En Derecho De Alta Tecnología

C. C.: 1712980935

DECLARACIÓN PROFESOR CORRECTOR

“Declaro haber revisado este trabajo, La Problemática de la Protección de Datos Personales y la Geolocalización, de la estudiante Emilia Dominique Salvador Aguas, en el semestre 2018-2, dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación”

_____

Lorena Naranjo Godoy

Magister En Derecho De Las Nuevas Tecnologías

C. C.: 1708293780

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

“Declaro que este trabajo es original, de mi autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes”.

_____

Emilia Dominique Salvador Aguas

C.C.: 1719002899

AGRADECIMIENTOS

A Dios quien guía mi camino eternamente.

A mis padres Rodrigo y Myriam quienes me brindaron todo su amor y apoyo incondicional.

A mis hermanos Daniela, Juan José y Paola por estar siempre a mi lado.

Y a todos quienes me brindaron su respaldo y cariño.

DEDICATORIA

Con todo mi amor a mis padres y hermanos quienes son las personas más importantes en mi vida. Y a todas las personas que me han apoyado siempre.

RESUMEN

La sociedad ha avanzado en su integridad, convirtiendo a los adelantos tecnológicos en algo indispensable para el diario vivir. Sin embargo, en muchas ocasiones los titulares de los derechos y consecuentemente los generadores de la información de forma inconsciente permiten el acceso a los distintos sistemas que levantan, retienen y filtran su información.

Generando la necesidad de regular la protección de datos personales, ya que si se da un mal manejo de este pueden verse afectados la intimidad y privacidad del sujeto y al libre desarrollo de su personalidad varios derechos fundamentales entre ellos. Esta protección se encuentra reconocida dentro de nuestra Constitución como derechos a sí mismo, así como ciertas normativas específicas. Existe una facilidad de recolectar los datos por medio de dispositivos electrónicos, sin embargo, estos también producen georreferenciaciones de los sujetos que los utilizan.

La geolocalización comprende al conglomerado de tecnologías que levanta y generan datos georreferénciales. Los datos de localización, consolida la geolocalización, la cual que se desempeña como una herramienta muy útil, al servicio de la tecnología y de la ciencia, no es distante también al derecho.
Por lo que, en pleno siglo XXI, los juristas encuentran grandes retos, al analizar el poder de uso y alcance del mismo. Examinando si podría existir algún tipo de vulneración, causada por el mismo. Los mecanismos para recabar datos de localización que han permitido incrementar la recolección de datos son las aplicaciones electrónicas especialmente aquellas disponibles en dispositivos móviles.

Se generan datos como ubicación en tiempo real e interconexión a otras aplicaciones. Y su relevancia se asocia a que están vinculadas a una persona es decir son datos personales aun cuando sean producidos dentro de medios de Geolocalización.

ABSTRACT

The society has advanced in its own integrity, turning the technologic advances in something required for the daily life. Nevertheless, in many occasions the right owners and therefore the ones who generate the information in an unconscious way allow the access to different systems that rise, hold and leak their information.

Generating the need to regulate the protection of personal data, since if it is handle in a wrong way the rights of intimacy and privacy of the subject may be affected. This protection may be found in our Constitution and other specific normative. There exists an ease of recollecting through electronic devices, nevertheless, these ones also produce georeferences of the subjects who use them.

Geolocation is a conglomerate of technology that rises and generates georeferential data. Localization data, consolidates the geolocation, which performs as an useful tool, at the service of technology and science also not far from the law.

Which is why in the XXI century, the jurists have to face great challenges, by analyzing the power of usage and the reach of it. Examining if there could exist any kind of infringement, cause for the very same. The mechanism to obtain localization data that has allowed to increase the obtainment of data are the electronic apps by installing in mobile devices.

Generating data like real time location and connection between other apps. We must understand the relevance that the protection of data has even when they are produced inside media of geolocation.

ÍNDICE

INTRODUCCIÓN

La utilización de la tecnología de la información y comunicación es una herramienta indispensable para el desenvolvimiento en sociedad de las personas en los distintos ámbitos, laboral, educacional y familiar. Indistintamente de la clase social a la que los individuos pertenezcan, se encuentran rodeados de tecnología y consecuentemente se ven en la obligación de generar nichos de desenvolvimiento de esta. “La irrupción explosiva de la informativa en la sociedad y su interrelación con las telecomunicaciones ha permitido la aparición de nuevos tipos de documentos y nuevas formas de identificación del autor de toda declaración de voluntad electrónica” (Altmark & Molina Quiroga, 2012, p. 187).

En este sentido, proveedores de sistemas informáticos, redes sociales y demás procesos, están en la obligación de cuando menos a presentar una propuesta de aceptación para que los usuarios que acceden a estos sistemas, logren entrar a su información personal sin problema alguno. La información no solo incluye bases de datos de registro de cuentas, más comúnmente como: correos electrónicos o de tarjetas de crédito y de usuarios, si no ubicaciones espaciales en tiempo real, lo que se denomina georreferenciación. Es una herramienta útil, en general cuando se presenta una necesidad de ubicación en tiempo real. Pero antagónicamente su abuso constituye una violación a los derechos personales que se encuentran protegidos construccionalmente como privacidad, intimidad, autodeterminación, informativa y protección de datos personales.

La recopilación de datos no es una nueva actividad, ni tampoco ha surgido con la tecnología de la información, la clasificación de datos personales incluyendo las rudimentarias técnicas de sistematización de datos, se remontan a la antigüedad, e incluso en ese entonces eran ya susceptibles a vulneraciones y posibles desvíos de los propósitos para las que fueron creadas. En el presente trabajo se realizará un análisis jurídico de las normas que protegen esta información para los usuarios y las consecuencias jurídicas que generarían las violaciones a la protección personal de datos.

1. DATOS PERSONALES

1.1 Distinción Entre Dato e Información

Partiremos de las definiciones entre dato e información, estas se dan como conceptos similares dentro de la sociedad, generando de tal forma interpretaciones erróneas de los datos personales. La Corte Constitucional ecuatoriana, dentro de la Sentencia No. 001-2014-PJO-CC, menciona ciertas distinciones entre “dato” e “información”, señala:

> Algunos entienden “datos” a la representación de hechos, conceptos o instrucciones bajo una forma adaptada a la comunicación, a la interpretación o al tratamiento por seres humanos o máquinas, y por “informaciones” al significado que toman los datos de acuerdo con convenciones vinculadas a estos. De acuerdo con la distinción conceptual citada, el dato adquiere la calidad de información en tanto cumple una función en el proceso comunicativo (Sentencia No. 001-2014-PJO-CC, 2014).

En la misma sentencia “la información, entonces, requiere una interpretación del dato, que dota de carga valorativa y funcionalidad concreta a la descripción que este hace”. (Sentencia No. 001-2014-PJO-CC, 2014, p. 44) Sin embargo, al momento de brindar una protección no se deberá limitar únicamente a los datos que tengan una carga valorativa y funcional, ya que los datos inocuos o con poco relevancia, al unirse pueden crease perfiles de completos de individuos (Naranjo Godoy, 2017, p. 73).

Teniendo de tal forma una diferenciación sobre dato e información, daremos paso a explicar la definición de dato personal.

1.2 Definición de Datos personales

Rodolfo Daniel Uicich, expresa sobre el dato electrónico, lo siguiente: “El dato es tan solo el impulso electrónico que queda grabado en un programa o sistema y que puede ser recuperado, es decir vuelto a la pantalla, siguiendo determinado procedimiento” (1999, p. 46). Comprendiendo que por medio del manejo de la tecnología el dato queda almacenado a través de métodos sistemáticos, que se encargan de ordenar lo recopilado, ésta fue obtenida de modo estándar. Utilizada comúnmente por compañías, instituciones, empresas multinacionales y nacionales, tienen una misma función, la cual es la recopilación de información, esto con el fin de generar réditos.

El diccionario de la Real Academia Española determina al dato como: “1.-Información sobre algo concreto que permite su conocimiento exacto o sirve para deducir las consecuencias derivadas de un hecho; 2.-Informacion dispuesta de manera adecuada para su tratamiento por una computadora” (RAE, 2017).

La Corte Constitucional de Colombia afirma en su Sentencia No. T-414/92 que:

> El dato constituye un elemento de la identidad de la persona que en conjunto con otros datos sirve para identificarla a ella y solo a ella, y por lo tanto el dato es de su propiedad en el sentido de que tendría ciertos derechos sobre su uso porque sus señales particulares, relaciones de propiedad y de familia, aspectos de su personalidad y señales de identidad de diversa índole que van emergiendo en la actividades de la vida son equivalentes a una huella digital que no debe ser desvirtuada por la elaboración de perfiles de datos que crearía de una especie de persona virtual cuya imagen permitiría perjudicar en múltiples aspectos a la persona real o a la que pretende plasmar (1999, p. 80).

Los datos personales son información adquirida, que, mediante proceso de segregación a través de métodos sistemáticos, permiten y desarrollar lo adquirido. Dichos datos pueden ser almacenados, en lugares físicos o virtuales, para su posterior utilización. Se manifiestan en representaciones literales o

numéricas, alfabéticas, sonidos, imágenes conforme a las cualidades (Altmark & Molina Quiroga, 2012, p. 319) .

Al ser recopilados los datos, deben ser sometidos a un procedimiento por descarte, el cual se ordena, se adjunta y se clasifica, generando la información de cada persona. El resultado es el surgimiento de lo que denominamos un dato personal. De manera que estos son la información de cada persona, cuyo principal objetivo es identificar rasgos, particularidades o especificidades de las personas, que pueden ser desde su fecha de nacimiento hasta su número de seguro social, o simplemente lo que realizó en un día. Al momento de discernir cada dato se observa que tienen características específicas, las cuales se explicarán a continuación.

1.3 Características de los datos personales

Debemos mencionar que, dentro del concepto, datos personales existen ciertas características, al respecto dentro el grupo legislativo en la Comisión del Parlamento Europeo en su Dictamen número 4/2007, del Grupo de Trabajo en su artículo 29 de la Directiva 95/46/CE, intentó ampliar el concepto de dato personal lo más posible, determinándolo como:

> «datos personales": toda información sobre una persona física identificada o identificable (el "interesado"); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social» (Grupo de protección de las personas en lo que respecta al tratamiento, 1995, p. 4).

Realizaremos un análisis de las principales características intrínsecas al concepto, mismo que de acuerdo a lo determinado por el grupo de protección de las personas en lo que respecta al tratamiento de datos personales, creado en

virtud de la directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 indica que son:

- Toda información
- Sobre
- Identificada o Identificable
- Persona Física

A) Toda Información

Al referirnos al aspecto de “toda información”, debemos explicar que esta conforma de la información subjetiva y objetiva (Grupo de protección de las personas en lo que respecta al tratamiento, 1995, p. 5), ya que con esto se puede determinar la identidad del sujeto que brinda sus datos, en otras palabras, es aquella que permite identificar al individuo.

Por ejemplo, los datos de seguros, que nos sirve para identificar con una mayor facilidad al dueño o sujeto que proporcionó la información, a pesar de esto no se puede asegurar que la información sea real (Grupo de protección de las personas en lo que respecta al tratamiento, 1995, p. 6).

B) Sobre

Debemos señalar que es el acontecimiento de la conexión o relación, que se le da entre persona y la información, “De modo general, se puede considerar que la información versa «sobre» una persona cuando se refiere a ella” (Grupo de protección de las personas en lo que respecta al tratamiento, 1995, p. 9).

Esta característica está encaminada a la determinación o especificidad que se le dará a la información, en el mismo contexto, la comisión menciona varios ejemplos dentro de los cuales, si bien se puede levantar información sobre objetos, esta solo se convierte en un dato personal al momento de la

determinación de la relación existente con la persona, es decir cuál es el vínculo de como características de un objeto enmarcan a un sujeto.

En este sentido, el elemento “sobre” puede ser identificado en virtud del contenido de la información, es decir las circunstancias o características que rodean el objeto o el sujeto; o respecto de la finalidad de la información, es decir con el propósito que esta tiene; y el resultado, esto es, los efectos que produciría en la persona sobre la cual se levantó la información la determinación de estos datos.

Finalmente, es importante recalcar lo determinado por la comisión: que los “elementos (contenido, finalidad y resultado) deben considerarse como condiciones alternativas y no acumulativas” (Grupo de protección de las personas en lo que respecta al tratamiento, 1995, p. 10).

C) Identificable o identificado

El dato identificable tiene como objetivo encontrar las particularidades o distinciones de cada una de las personas, estas pueden ser directas o indirectas, a través de la evidencia de datos denominados identificadores, vinculando así los datos almacenados con cada sujeto (Grupo de protección de las personas en lo que respecta al tratamiento, 1995, p. 10). El dato más comúnmente identificado es el nombre y apellidos de una persona, sin embargo, para lograr una mejor distinción se deben considerar otros elementos con los cuales se puede llegar a diferenciar a la persona.

D) Personas físicas

La protección que se intenta brindar a los datos personales, exclusivamente que se da a las personas naturales, se considera dentro del artículo 6 de la Declaración de los Derechos Humanos. Ampara a todo sujeto contra la violación de sus derechos, reconociendo su personalidad jurídica, independientemente

del espacio en que se encuentre, tiene derecho a la protección de su información, y consecuentemente a que este esté protegido y garantizado (Grupo de protección de las personas en lo que respecta al tratamiento, 1995, p. 24).

Recapitulando, los datos personales son información que los individuos generan a través de fuentes, instrumentos, procesos o procedimientos sea en el transcurso diario que vive cada sujeto, o sea con la información que se genera desde su concepción que permita determinarlo o identificarlo. En ocasiones la información puede provenir de terceros, pero si versa o se encamina a un sujeto esta pertenecerá a quien esté en el medio del caso. Con el avance de la tecnología en las últimas décadas o años, se ha dado la recaudación masiva de información de todos los sujetos, que en algunos casos no saben a qué momento se otorgó a terceros sus datos, en especial cuando nos referimos a información delicada o personal.

Mencionando así, que la información puede ser utilizada por ciertos sujetos, dando uso de lo entregado, sin embargo, cuando entregamos información debería existir cierto resguardo, ya que puede haber distintas características en los datos que pueden ser reservadas. La idea en general de información que puede ser utilizada no se especifica, por lo que yacen interrogantes como: la manera en la que se va a utilizar, o si es el dueño de la información quien la va a recuperar. Estas inquietudes son necesarias de solventar al momento de otorgar o tener acceso a esos datos.

1.4 Tipos de Datos

Considerando como ha avanzado la tecnología, los datos no son solo números o palabras, el análisis y recolección de datos sobre cada individuo y los métodos de agrupación permiten hacer distintas clasificaciones, recabando las principales y coincidiendo con distintos autores encontramos:

1.4.1 Dato Anónimo

Es un dato estadístico o general que no personaliza ni permite la personalización (Uicich, 1999, p. 47). Este determina el comportamiento de ciertos grupos, fijaciones o preferencias tanto en el aspecto social, económico o geográfico.

1.4.2 Datos Sensibles

A través de este dato se permite “identificar a la persona, confeccionando su perfil ideológico, racial, sexual, económico, o de cualquier otra índole”. (Concepción Conde Ortiz, 2005, p. 66) La raza, la religión o incluso preferencias políticas o sexuales, por sus características al momento de ser tratados, son información que no podría ser compartida libremente, ya que ocasionaría una posible discriminación al dueño de esta (Jiménez García, 20018, p. 5).

1.4.3 Datos Notorios y privados

Los datos notorios son toda información que una persona de manera libre dé a conocer, sin ningún tipo de coerción. Por otra parte, el dato privado se enfoca en la información individual y no divulgada por las personas, las características, gustos e incluso fijaciones que no salen a la luz pública (Garzón, 2008, p. 6).

El valor individual de la información, está garantizada por el legítimo reconocimiento de los derechos por el Estado, y consecuentemente protegido y garantizado a través de la normativa vigente. La inadecuada utilización de los datos personales los habitantes, así como la recolección y aplicación de la información puede afectar la manera directa e indirecta tanto en el ejercicio de los derechos personales en forma individual como en la toma de decisiones, por parte de los organismos Gubernamentales, es por este motivo que se presenta la necesidad de realizar acciones afirmativas para proteger estos datos como veremos a continuación.

1.5 Protección de datos personales

La protección es inherente a los datos personales, con el desarrollo y el avance de las nuevas tecnologías, se observa una facilidad de obtención de datos personales. Sin embargo, en algunos casos se generan vulneraciones, a los derechos de los individuos sobre la publicación de la información, al ser perpetrada, se produce un abuso y apropiación de datos.

Las oportunidades creadas al momento de la recopilación de datos, pueden generar una pérdida del anonimato en las personas. Por consiguiente, se deberá establecer una protección a los distintos tipos de información personal, siendo que esta se encuentra ilimitada al momento de transferir, tratar o almacenar los datos de cada individuo (González Pascual, 2009, p. 948).

Un punto clave de la protección de datos personales son los derechos que se afectarían de producirse un supuesto de vulneración, estos principalmente se radican en las siguientes: autodeterminación informativa, intimidad, privacidad, libre desarrollo de la personalidad y la propia dignidad humana.

1.6 Derechos Reconocidos en Protección de Datos

Uno de los enfoques más utilizados sobre la protección de los datos personales es el que nos brinda la Carta de Derechos Fundamentales de la Unión Europea, expuesta en el año 2000 en Niza, catalogando al derecho de protección de datos personales como un derecho fundamental. La Carta de Derechos Fundamentales de la Unión Europea establece dentro de su artículo 7 el derecho al respeto de la vida privada, y en su artículo 8 el derecho a la protección de datos personales, encontrándose consagradas ambos como derechos ganadores y prioritarios, pero de manera independiente.

El artículo 8, de la Carta de Derechos Fundamentales de la Unión Europea, cuyo título es Protección de Datos Personales de carácter personal indica:

> 1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan. 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.3. El respeto de estas normas quedará sujeto al control de una autoridad independiente (Carta de los Derechos Fundamentales de la Unión Europea, 2000, p. 9).

Para la elaboración del artículo mencionado en la Carta de Derechos Fundamentales de la Unión Europea, la directiva 95/46/CE se realizó un exhaustivo trabajo por parte del Parlamento Europeo. Cabe señalar que sirvió como base fundamental las tradiciones constitucionales que tenían en común los Estados Miembros de la Unión Europea, dentro del artículo 17 del Pacto Internacional de derechos civiles y políticos, y el artículo 18 de la Declaración del Parlamento Europeo el cual declaró que los Derechos fundamentales y libertades públicas son también fuente primaria del reconocimiento y protección de los derechos relacionados con los datos personales (Herrera de la Fuente, 2003, p. 148).

> La protección de datos personales no es una excepción de que todo derecho, puede llegar a ser absoluto dependiendo de la situación, sino que puede y debe, en determinadas ocasiones, ceder ante otros valores y bienes constitucionales. Por lo que esta libertad, al igual que cualquier otro derecho fundamental, puede sufrir ciertas restricciones que vengan establecidas en la Constitución directamente, ya sea que deriven de esta manera indirecta o mediata (…) (Garriga Domínguez, 2015, p. 115).

Al reconocer el derecho a la protección de datos personales debemos fomentar que este sea de manera autónoma, y que no tenga fundamento en otros

derechos como a vida privada, de manera que logre brindar una mejor tutela de forma particular y efectiva a la misma dignidad humana.

En la actualidad podemos observar que, a través de las tecnologías de información y comunicación, se ha facilitado la recolección y almacenamiento de datos, generando bancos de datos, los cuales hacen circular dicha información obtenida (Arenas Ramiro, 2006, p. 273).

1.6.1 Autodeterminación informativa

Al momento de referirnos a los derechos que emanan los datos personales, debemos hacer hincapié a la “Autodeterminación informática”, siendo que trata sobre la voluntad o decisión de cada persona al momento de compartir, cambiar, suprimir o modificar su información personal, la cual se encuentra dentro de una base de datos, tanto pública como privada (García Tinajero & Ponce Baenz, 2011, p. 7).

Convirtiéndose de esta forma para todas las personas en un cierto modo de protección, que tutela a todo tipo de dato, como el dato sensible o el dato público. Aun cuando en un inicio el dato parezca innocuo, se tendrá que tomar en cuenta la finalidad de su uso.

La humanidad a lo largo de la historia ha dado distintos conceptos sobre la autodeterminación informática, sin embargo, una de sus primeras referencias, fue en el año de 1983, expuesto por el Tribunal Constitucional Federal Alemán, dentro de la sentencia dictada, reconociendo y aludiendo a la expresión: “derecho a la autodeterminación informática”, mencionando así lo siguiente:

> [...]en las condiciones de la elaboración moderna de datos, la protección del individuo contra la recogida, almacenamiento, utilización y difusión ilimitadas de sus datos personales queda englobada en el derecho general de protección de la persona del artículo 2º, párrafo 1º, de la Ley

> Fundamental. El derecho constitucional garantiza en esta medida la facultad del individuo de determinar fundamentalmente por sí mismo la divulgación y la utilización de los datos referentes a su persona". Continúa diciendo la sentencia que: "[...] las limitaciones de este derecho a la "autodeterminación informativa" sólo son admisibles en el marco de un interés general superior y necesitan un fundamento legal basado en la Constitución, que debe corresponder al imperativo de claridad normativa inherente al Estado de Derecho. (Jurisprudencia del Tribunal Constitucional Federal Alemán, 2009, p. 78).

El Tribunal Constitucional Federal Alemán, hace referencia en su sentencia que toda persona tiene la facultad determinativa de las limitaciones sobre algunos asuntos de su vida personal, convirtiéndose en algo público o no. Teniendo como objetivo principal el desarrollo de la personalidad libre dentro de una sociedad, presumiendo la protección de los datos personales (Remolina Angarita, 2013, p. 29).

Si bien la autodeterminación informativa define y delimita los datos que pueden darse a conocer en dominio público o tratarse con el responsable en relación jurídica, al no haber una medida que facilite ver el rango de intimidad de un dato, o visualizar si este es sensible o no, se deberá tomar en cuenta la utilización y eventualidad en su aplicación. Asimismo, el tratamiento a los datos personales, no deberá afectar al derecho a la intimidad (Garriga, 2009, p. 35).

1.6.2 Derechos ARCO

Los derechos ARCO, significan: Acceso, Rectificación, Cancelación y Oposición, que recaen sobre la información personal. Es decir, es el conjunto de derechos otorgado a los dueños de datos personales, con lo que se faculta el control de los mismos (Santos Pascual & López-Vidriero, 2005, p. 87).

Al ejercer estos derechos el titular de los datos podrá solicitar el acceso, la rectificación, cancelación u oposición, a los sistemas que tengan información del mismo. La solicitud se podrá realizar el titular de los datos o por medio de un representante legal (Santos Pascual & López-Vidriero, 2005, p. 88).

1.6.3 Principios de los Datos Personales

Estos principios generales deben estar involucrados en todos los datos de carácter personal que están bajo un tratamiento, ya sean manejados por entes públicos o privados. Por tal modo, existen ciertas pautas al momento de recolectar, almacenar, grabar, crear, bloquear, eliminar, modificar y comunicar en datos de carácter personal. Para garantizar la autenticidad, utilización y congruencia de la información almacenada (Santos García, 2005, p. 51).

1.6.3.1 Finalidad

Se basa en que los datos de carácter personal recolectados y almacenados, servirá solamente para cumplir con su finalidad. En otras palabras, al obtener ciertos datos personales de los usuarios, se utilizará únicamente con el propósito de su función (Santos García, 2005, p. 56).

1.6.3.2 Calidad de dato

La calidad de dato se basa al momento de someter la información recolectada bajo tratamientos *"cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explicitas y legitimas para las que se hayan obtenido"* (de la Torre, 2017, p. 3). Por ende, los datos no podrán ser utilizados para otros fines o cuando estos sean incompatibles con la realidad (Vizcaíno Calderón, 2001, p. 92).

Al momento de que los datos de carácter personal tratados sean incompletos o inexactos, se deberá corregir, cancelar o rectificar. Una vez cumplido su función

los datos serán eliminados de la base en la que se encontraba almacenado, exceptuando las obligaciones legales. Al recolectar información por medios fraudulentos o ilegales, se considerará ilícita y prohibida para su manejo (Vizcaíno Calderón, 2001, p. 98).

1.6.3.3 La información en la recogida de los datos

Este principio se basa en informar al usuario que uso se dará a sus datos antes de ser recolectados y sometidos a un tratamiento. Los dueños de estos datos que fueron solicitados, tendrán de la misma forma derecho a solicitar su información almacenada. Los responsables de las bases de datos deberán dar cumplimiento constate de informar de forma escrita y clara, el manejo que se dará con la información que se recolectara (Santos García, 2005, pp. 57-61).

1.6.3.4 Consentimiento del afectado

Este derecho es uno de los más importantes para garantizar la protección de datos de carácter personal e intimidad. El consentimiento del afectado se refleja en la expresión o declaración de la voluntad en entregar sus datos. Al reconocer al individuo que se recogerá los datos se hará uso del derecho a la información, para que pueda decir si desea comprar o no los datos con el fichero (Santos García, 2005, pp. 62-65).

1.6.3.5 Datos especialmente protegidos

Los datos especialmente protegidos, gozan de una mayor protección, ya que tratan a con información más sensible. Invadiendo de forma más lesiva y potente a la intimidad del afectado, por ende, su tratamiento y almacenamiento deben cumple con altos índices de seguridad. Para expresar el consentimiento del sujeto, la autorización de esta deberá ser de forma clara y escrita, ya que trata

de datos como la religión, salud, preferencias sexuales o políticas, etc (Santos García, 2005, pp. 70-74).

1.6.3.6 Seguridad de datos

Al existir un fichero que contenga datos personales y que los dueños conozcan su uso, finalidad y destino, se deberá implementar una seguridad adecuada que proteja a esta información. Dicha seguridad garantiza que no se produzca perdidas, acceso no autorizado o alteraciones a los datos. Utilizando de este modo tres medidas, las cuales son: organizativas, jurídicas y técnicas (Santos García, 2005, p. 75)

Las medidas organizativas, disponen a los ficheros que aseguren el cumplimiento de deberes dentro de los derechos de protección de datos. Las medidas jurídicas, otorgan y garantizan a los afectados el derecho de protección de datos personales. Y las medidas técnicas verifica el sistema de control, asegurando de este modo la integridad del dato (Santos García, 2005, p. 76).

1.6.3.7 Confidencialidad

Este deber es relacionado con la confidencialidad e integridad referente a los datos personales. Este recae sobre el responsable que maneja el fichero, ya que se obliga profesionalmente a guardar secretos acerca de la información almacenada. Otorgando recursos por parte del encargado para concienciar a todos los sujetos que manejen y conocen la información (Santos García, 2005, p. 77-78).

2. DERECHO A LA PROTECCIÓN DE DATOS PERSONALES EN EL ORDENAMIENTOS JURÍDICO

Ha existido una evolución en los últimos años dentro de la sociedad, sobre todo en los avances tecnológicos, lo que ha facilitado la obtención de información sobre las personas. Los titulares de los datos en la mayoría de casos dan su consentimiento, para que otros sujetos realicen el tratamiento de los datos de los titulares. Sin embargo, el alcance de compartir información privado o íntimo puede tener serias repercusiones (Enríquez Álvarez, 2017, pp. 43-61).

Los Estados al ver que se puede generar una vulneración, se ven en la necesidad de crear leyes que busquen regular de alguna manera el manejo de la información. Cada uno de los países observa sus necesidades particulares, pero estos deben ser con un mismo fin, el cual es la protección de datos personales (Higareda Magaña, 2013, p. 36).

En este capítulo se analizará el marco legislativo que tienen algunos países, al tratar con los datos de las personas. Se dará la comparación con normativas de México, Colombia y España, ya que estos países siguen avanzando para adaptarse a las necesidades que generan la protección de datos. Sin embargo, se iniciará con la legislación ecuatoriana verificando, así como se brinda protección a los datos personales.

2.1 Normativa existente sobre los datos personales en el Ecuador

2.1.1 Constitución de la República del Ecuador

La Constitución de 1978, en su reforma de 1995 y la Constitución de 1998, estipulaban al Hábeas Data, como el acceso y decisión del uso de datos. La Constitución del 2008, en el Título III de Garantías Constitucionales, Capítulo Tercero de Garantías Jurisdiccionales, artículo 92, habla sobre la acción de Hábeas Data, que indica:

> 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 que 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, el 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 se atendiera su solicitud, ésta podrá acudir a la jueza o juez. La persona afectada podrá demandar por los perjuicios ocasionados (Constitución de la República del Ecuador, 2008).

El Habeas Data es una garantía constitucional, que faculta a cualquier persona natural o jurídica a acceder de forma gratuita a su propia información. El titular de estos datos puede pedir su eliminación o rectificación. Garantizar que no se generen abusos por un poder informativo, es decir, el manejo y utilización de bases de datos, que se encuentran en manos de terceros (Enríquez Álvarez, 2018, p. 44).

Aun así, con esta garantía del Habeas Data, los ciudadanos buscaban que su información este resguardada. Por lo que la Constitución del 2008, es la primera Constitución en regular el derecho a la protección de datos personales, basándose en un modelo europeo, con la finalidad de cumplir altos estándares de resguardo en materia de protección de datos (Naranjo Godoy, 2017, p. 8).

Este derecho, está establecido en el artículo 66, numeral 19, el cual nos menciona que:

> Art. 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 de la República del Ecuador, 2008).

Es así que, por medio de la autodeterminación informativa, se logra delimitar el uso de los datos personales. Es decir, la recolección, almacenamiento, procesamiento y publicación, de datos, tendrá que constar con la autorización del titular de este, o que la Ley lo faculte. Así mismo, dentro de la normativa ecuatoriana existen leyes que señalan en la protección de datos personales, como se desarrollara más adelante.

2.1.2 Ley Orgánica de Telecomunicaciones

Dicha Ley abarca únicamente en el ámbito de Telecomunicaciones y Radiofrecuencias, por lo que solo afecta a dichos medios. Siendo un sector estratégico para el Estado, tendrá como objetivo administrar, regular, controlar y gestionar. Como lo menciona su artículo dos, esta ley se aplicará a: “las actividades de establecimiento, instalación y explotación de redes, uso y explotación del espectro radioeléctrico, servicios de telecomunicaciones” (Ley Orgánica de Telecomunicaciones, 2015). Ya sean personas jurídicas o naturales, las que realicen las actividades antes mencionadas, transmitiendo de este modo la información de un lado a otro.

Garantiza los deberes y derechos, que prestan los servidores a sus usuarios. Ya sea por radiofrecuencia o manejo de telecomunicaciones, se mantiene en constante contacto con los datos. Razón por la cual se establece la protección de datos en su artículo 78, menciona la implementación de medios tecnológicos. Que dichos sistemas garanticen y protejan las bases de información, las cuales solo podrán tener acceso las personas que están facultadas por ley (Ley Orgánica de Telecomunicaciones, 2015).

El artículo 78, a su vez protege a: “los datos personales almacenados o transmitidos de la destrucción accidental o ilícita, la pérdida o alteración accidentales o el almacenamiento, tratamiento, acceso o revelación no autorizados o ilícitos” (Ley Orgánica de Telecomunicaciones, 2015). Establece estas medidas de protección, ya que los datos almacenados deben permanecer bajo un resguardo constante. Dentro de este mismo artículo, nos menciona en su numeral cuarto, lo siguiente:

> La garantía de que la información suministrada por los clientes, abonados o usuarios no será utilizada para fines comerciales ni de publicidad, ni para cualquier otro fin, salvo que se cuente con el consentimiento previo y autorización expresa de cada cliente, abonado o usuario (Ley Orgánica de Telecomunicaciones, 2015).

La información recolectada de cada persona, deberá tener la autorización expresa del consentimiento para el uso de sus datos. Ya que esta información adquirida no será para fines comerciales, a no ser que los titulares de estos hayan aceptado previamente (Ley Orgánica de Telecomunicaciones, 2015). Esta ley reconoce la protección de datos, sin embargo, su ámbito de aplicación es muy limitado, ya que solo se utiliza dentro de las Telecomunicaciones y Radiofrecuencias.

2.1.3 Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos

Esta Ley tiene como objeto regular: “los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos sistemas” (Ley de comercio electrónico, firmas electrónicas y mensajes de datos, 2002). De tal forma, se genera una limitación para la protección de datos personales, dentro del Ecuador, ya que como se mencionó anteriormente regula de modo específico la información generada electrónicamente.

Las disposiciones generales, establecidas en esta ley, define a los Datos Personales, de la siguiente forma: “son aquellos datos o información de carácter personal o íntimo, que son materia de protección en virtud de esta Ley” (Ley de comercio electrónico, firmas electrónicas y mensajes de datos, 2002).

El artículo noveno, trata de la protección de datos, determina que: “para la elaboración, transferencia o utilización de bases de datos, obtenidas directa o indirectamente del uso o transmisión de mensajes de datos, se requerirá el consentimiento expreso del titular de éstos” (Ley de comercio electrónico, firmas electrónicas y mensajes de datos, 2002). Tomando como un factor importante a la voluntad del titular de la información, es decir, a la autodeterminación informativa al momento de compartir un dato.

Por lo mencionando anteriormente debemos considerar que cada persona tiene la facultad de escoger que datos compartir con terceros. Para el almacenamiento y uso de esta información, no se vulnerará los derechos a la intimidad, privacidad y confidencialidad, ya que será necesario la voluntad del titular u orden de autoridad competente. Sin embargo, el consentimiento no será necesario para los datos considerados públicos o cuando exista relación de dependencia con la persona (Ley de comercio electrónico, firmas electrónicas y mensajes de datos, 2002).

2.1.4 Código Orgánico Monetario y Financiero

El artículo primero de este código establece el objetivo principal, el cual es regular “los sistemas monetario y financiero, así como los regímenes de valores y seguros del Ecuador” (Código Orgánico Monetario Y Financiero, 2014).Ya que, por medio de normas, control, supervisiones y redición de cuentas de las actividades realizadas, se generan sistemas de inspección. Procurando que estos procedimientos vayan acorde a la Ley (Código Orgánico Monetario Y Financiero, 2014).

El artículo 152, nos habla de los derechos de las personas ya sean naturales o jurídicas. El conocer su información de forma clara, precisa y no engañosa, se reconoce como un derecho importante. Los datos que consten en entidades financieras deberán ser exactos y actualizados, conforme la ley lo disponga, ya que estos sirven para generar reportes crediticios de los sujetos que consten en su base (Código Orgánico Monetario Y Financiero, 2014).

Superintendencia de Bancos (SB), regula el Registro de Datos Crediticios. (Registro de Datos Crediticios, 2018) Se obliga a la administración de la base de datos crediticios, creando reportes de forma exacta y actualizada. Esta información es vital para la toma de decisión en créditos que se puedan otorgar a futuro (Código Orgánico Monetario Y Financiero, 2014).

Dentro de este código se menciona la protección de la información, la cual se establece en su artículo 352. El artículo mencionado anteriormente ampara los datos personales, que se encuentran dentro de sistemas financieros nacionales. Los titulares de los datos, serán los únicos habilitados para acceder a su información, a excepción de lo dispuesto en este Código (Código Orgánico Monetario Y Financiero, 2014).

2.1.5 Ley Del Sistema Nacional de Registro De Datos Públicos

Esta ley tiene como objetivo el regular los registros públicos que maneja las entidades públicas o privadas. Garantiza, organiza y normaliza la seguridad jurídica, de forma eficiente y eficaz. Manejando adecuadamente la transparencia, publicación, accesibilidad a las nuevas tecnologías, relacionadas con uso de datos (Ley del sistema nacional del registro de datos públicos, 2010).

Esta ley es aplicable a las instituciones privadas o públicas, que manejen los registros públicos, ya sean de personas naturales o jurídicas. Esta información será entregada de forma general o específica, por escrito o a través de medios electrónicos (Ley del sistema nacional del registro de datos públicos, 2010).

La Dirección Nacional de Registro de Datos Personales (DINADARP), determina que dato se registra en las distintas entidades gubernamentales, las cuales están facultadas para la recolección de datos. Sin embargo, la Ley del Sistema Nacional del Registro de Datos Públicos, faculta a los titulares de solicitar el derecho a la indemnización, al momento que sus datos se encuentren erróneos. Otorgando una buena utilización y manejo correcto por parte de las autoridades (Ley del sistema nacional del registro de datos públicos, 2010).

2.1.4 Código Orgánico Integral Penal

Dentro del Código Orgánico Integral Penal, en artículo 178, referente a la violación de la intimidad, dispone:

> La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y video, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años (Código Orgánico Integral Penal, 2014)**.**

Se evidencia que es un derecho conexo, ya que no menciona los datos personales específicamente, pero sí la violación a la intimidad. Esta infracción es sancionada con pena privativa de libertad de uno a tres años. Recayendo al sujeto que haya violentado o afectada la autodeterminación informativa, es decir, a decidir qué información compartir o no.

Como precedente, el derecho a la intimidad antes de ser reconocido como derecho unitario, solo amparaba y reconocía manifestaciones de la intimidad como: la correspondencia privada, inviolabilidad de la comunicación y el domicilio. Pero con los años y el avance tecnológico, se ha facilitado, agilitado y simplificado la recolección de datos, los que se someten a un procedimiento de descarte, convirtiéndose de esta forma en información, como se estableció en el capítulo uno. El Estado se ve en la necesidad de generar normas que regulen el uso de estos datos (García González, 2007, p. 758).

Dentro del Código Orgánico Integral Penal, existen algunos artículos que se pueden utilizar para proteger bases de datos y que estas no sean difundidas arbitrariamente. Evitando así una vulneración a los derechos conexos como la privacidad o intimidad. Este código, aun cuando sea uno de los más recientes que tiene el Ecuador, deberá adecuarse al avance tecnológico que vivimos, ya que se ha generado nuevas formas que vulnerar derechos.

En conclusión, en el Ecuador no existe una ley en específico, para la protección de datos personales, pese que en la actualidad hay la necesidad de legislarla. A pesar que, este derecho se encuentra reconocido en la Constitución y otras leyes mencionadas anteriormente, éste no se encuentra regulado de manera adecuada. Al materializar una normativa, se busca prevenir irregularidades o daños, que se causen por mal manejo de base de datos.

Al crear esta ley se generaría un control que limite el uso de bases de información, que ciertos sujetos jurídico o naturales, lo manejan. Causando una desconfianza con otros países, que tengan estándares más altos para la

protección de datos personales. Por lo antes mencionado, se analizará la normativa que se maneja en distintos países para el amparo que se da a la información.

2.2 Derecho Comparado

En algunos países se han creado estratégicamente leyes para proteger y tratar a los datos personales. Estas leyes se adecuan a las necesidades de cada uno de sus países. Para que no existan falencias jurídicas, como vacíos legales o falta de normativa, siendo que al no existir un adecuado amparo se genera perjuicios a sus ciudadanos.

En la actualidad, se vive en una sociedad informatizada, utilizando el avance tecnológico, logrando eliminar las barreras, como la distancia o el tiempo, y facilitando la obtención de datos. En consecuencia, ya no es necesario la fuerza física, para influir o controlar a las personas, ya que se hace por medio del uso de la información. Al evitar medios coactivos, para el manejo de la conducta de los ciudadanos, utilizando los datos, se ha facilitado el manejo adecuado y preciso de los sujetos (Losano, 1989, p. 21).

Por lo expuesto, se analizará normativa de algunos países, para ver el manejo, amparo y regulación que se da a la información. Y lograr visualizar la sincronía que existe, entre países. Partiendo de esta forma con el análisis de la normativa mexicana, ya que es uno de los pilares de Latinoamérica.

2.2.1 México

Partimos desde la Constitución Política de los Estados Unidos Mexicanos, que fue reformada en 2009, incorporando un segundo párrafo en su artículo 16, mencionando así la protección de datos personales. Reconoce correlativamente a los derechos de acceso, ratificación, cancelación u oposición, es decir los

derechos ARCO (Constitución Política De Los Estados Unidos Mexicanos, 1917, p. 22).

Añade que los datos personales, que se encuentran sujetos a mecanismos de recolección, almacenamiento y tratamiento, deben estar protegidos. Este amparo se efectúa bajo circunstancias de vulneración como el acceso no autorizado por terceros a información personal. Motivo por el cual se crea una necesidad de reconocer los titulares de la información y el derecho de control sobre estos (Higareda Magaña, 2013, p. 14).

Dicha reforma también modificó el Título Tercero, Capítulo II Del Poder Legislativo, Sección III De las Facultades del Congreso, artículo 73, numeral XXIX-O, que faculta al Congreso para: “legislar en materia de protección de datos personales en posesión de particulares” (Constitución Política De Los Estados Unidos Mexicanos, 1917).

Los datos personales que estén bajo la custodia de particulares se verán regulados por Ley Federal de Protección de Datos Personales en Posesión de Particulares. Cuyo objetivo es de regular y proteger los datos personales en posesión de particulares, imponiendo obligaciones técnicas, fiscas, organizacional, o jurídicas. Esta información obtenida no deberá ser por medios fraudulentos, se custodiará los sistemas de información, donde se almacenan, organizan y envían, los datos que obtuvieron de forma voluntaria, este consentimiento podrá ser de forma verbal, escrita o por medios electrónicos (Ley Federal de Protección de Datos Personales en Posesión de Particulares, 2010).

Es necesario una revisión constante de la organización, tratamiento y protección que se brindan a los datos personales. Los titulares de esta información, o por medio de su representante legal, podrán hacer uso del derecho ARCO, es decir, podrá acceder, ratificar, cancelar y oponerse, frente a la información de cada individuo. La entrega de datos será de manera gratuita, solo se cobrará el envió

y las copias, de ser necesario (Ley Federal de Protección de Datos Personales en Posesión de Particulares, 2010).

Las compañías o particulares que manejen esta información, implementaran medidas técnicas, jurídicas, organizacionales y fiscas. Estas medidas son procesos, que son el obtener, mantener y cancelar datos, que tienen como fin gestionar y tratar de forma correcta y eficaz la información. Evaluando de este modo que los particulares cumplan con lo dispuesto con la Ley Federal de Protección de Datos Personales en Posesión de Particulares (Deloitte, 2010).

Por otro lado, cuando la información no esté bajo la custodia de particulares, se verá regulado por la Ley General De Protección De Datos Personales En Posesión De Sujetos Obligados. Esta Ley entró en vigencia el 27 de enero del 2017, la autoridad reguladora y permitida para ejercer lo dispuesto es Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales. Tiene como objetivos regular, establecer, proteger y garantizar derechos a la protección de datos personales, cuando están en posesión de los Sujetos Obligados.

Como Sujetos Obligados, se entiende a: órgano u organismo de los poderes ejecutivo, legislativo y judicial, ámbito federal, estatal y municipal, es decir, bajo cualquier entidad del Estado. Por otra parte, encontramos a los titulares de la información, que son: “los sindicatos y cualquier otra persona física o moral que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito federal” (Ley General De Protección De Datos Personales En Posesión De Sujetos Obligados, 2017, p. 94).

Esta ley regula la relación entre los Sujetos Obligados y los titulares de la información, regulando de tal forma la transparencia y remisión de datos, utilizando acciones preventivas durante su proceso. Sancionando o impugnando a los procedimientos ilegales, para proceder a una verificación de estos. Establece las obligaciones y deberes de los sujetos obligados, los que a su vez

pueden expedir, tramitar o modificar normativa (García-Cuélla Aiza y Enríquez, 2017, p. 87).

2.1.4 Colombia

Dentro del territorio colombiano, encontramos establecida en su Constitución, el derecho a la intimidad personal, familiar y al buen nombre. En el cual reconoce y garantiza a las personas el derecho a conocer, actualizar y rectificar los datos que se tenga sobra cada quien. Reconociendo a su vez a la autodeterminación informativa, ya que garantiza se respete la libertad de recolectar, proceder y circular, datos de cada sujeto (Constitución Política de Colombia, 2016, p. 35).

El ente regulador encargado de la protección de la información, es el Registro Nacional de Bases de Datos, conocido como RNBD. Este es el directorio público, que se encarga de que los sujetos administradores de dichas bases de datos, tengan control y manejo adecuado, sobre estos. Creando de esta forma en el 2012, la Ley 1581, que analizaremos a continuación (Superintendencia Industrias y Comercio, 2018).

El Régimen General de Protección de Datos Personales, o más conocida como la Ley 1581, se aplica a cualquier persona ya sea natural o jurídica, que tenga relación con bases de información. Esta Ley a su vez, designó a la Superintendencia de Industria y Comercio, como Autoridad de Protección de Datos, que se encarga de garantizar el cumplimiento de esta ley, al momento del tratamiento de Datos Personales (Registro Nacional de Bases de Datos, 2018).

Esta ley sirve para inspeccionar y controlar la cantidad de titulares de datos y de información, que se brinde de manera adecuada un tratamiento. Generando conciencia sobre sus ciudadanos sobre el manejo y otorgación de datos. Y que, a los responsables de no cumplir con lo acatado, se les impondrá distintas sanciones, por falta de administrar correcta a la información, ya sea un ente público o privado (Ley Estatutaria 1581, 2012).

El paso 18 de enero de 2018, bajo decreto 090, el Gobierno Nacional Colombiano ordenó que todo sujeto que esté obligado, deberá inscribir sus bases de datos en Registro Nacional de Bases de Datos. Dichos sujetos obligados son aquellas entidades de naturaleza jurídica, y sociedades que superen los 100 mil Unidades de Valor Tributario. Con lo que se establecieron plazos de entrega, dependiendo de cada sociedad, teniendo como último plazo el 31 de enero de 2019, que recae a las personas jurídicas y que sean entidades públicas (Superintendencia de Industias y Comercio, 2018).

Los titulares de datos por medio de esta ley, tendrá derecho a acceder, conocer, ratificar, solicitar, y revocar la autorización que se tiene sobre su información (Superintendencia Industrias y Comercio, 2018). Debemos mencionar que aun cuando esta ley haya estado vigente desde el 2012, protege y garantiza los derechos de sus ciudadanos de manera correcta y eficaz. Ya que busca prevenir la vulneración de información, concientizando la responsabilidad de cada persona.

2.1.4 España

La Constitución Española en su Título I De los derechos y deberes fundamentales, Capítulo Segundo sobre Derechos y libertades, Sección 1. ª De los derechos fundamentales y de las libertades públicas, artículo 18, numerales 1 y 4 establece:

> **1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen**. 2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito. 3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial**. 4. La ley limitará el uso de la informática para garantizar el honor y la intimidad**

> **personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos** (Constitución Española, 1978).

Este artículo hace mención más como un derecho conexo o una inclusión parcial, garantizando y limitando el uso de la información para no vulnerarlos los derechos “al honor, a la intimidad personal y familiar y a la propia imagen” (Constitución Española, 1978). Al referirse una normativa específica que regule la protección de Datos Personales, dentro de España, se encuentra al Reglamento General de Protección de Datos, cual rige en toda la Unión Europea.

Este reglamento mencionado anteriormente, fue creado por el Parlamento Europeo y Consejo de la Unión Europea, su nombre oficial es UE 2016/679, aprobada el 14 de abril de 2016, y entro en vigencia el 25 de mayo de 2018. Este reglamento recae a todas personas físicas, que viva dentro de la Unión Europea. Deroga a la Directiva 95/46/EC, es decir al Reglamento general de protección de datos. Teniendo esquemas generales que todos los países miembros deben alcanzar, al mismo tiempo, faculta a cada miembro crear su propia ley de protección de datos personales (Reglamento General de Protección de Datos, 2018).

Regulará a las compañías que tengan manejo de datos personales, cuando los titulares de esta información vivan dentro de la Unión Europea, aun cuando las compañías trabajen desde el extranjero. El Capítulo I de Dispersiones Generales, artículo cuarto de definiciones, inciso 1, define a los datos personales, como:

> Toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, **datos de localización**, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética,

> psíquica, económica, cultural o social de dicha persona (Reglamento (UE) 2016/679, 2016).

Distingue los datos de localización, que sirven para recabar información con lo que se logrará identificar a las personas, razón por la que se desarrollará en el siguiente capítulo. Este reglamento aplica a todas las personas físicas, a excepción de las personas fallecidas.

Uno de los puntos más importantes en este reglamento es la manifestación del consentimiento al entregar los datos personales. Aquí toda persona física deberá expresar claramente su voluntad de entregar sus datos, también se deberá tomar en cuenta los menores de edad, ya que hasta los 16 años su consentimiento será por medio del tutor legal (Grupo Garatu, 2018).

En este análisis de derecho comparativo, sobre la protección de datos personales, debemos mencionar que, en otros países, existe normativa vigente, la cual intenta adecuarse a la sociedad informatizada que vivimos. Estas leyes establecen limitaciones para de obtención, uso y tratamiento de la información, compartida por los titulares de esta. Generando que los sujetos obligados y particulares, mantengan principios de integridad, responsabilidad y confidencialidad de datos.

Considerando el avance tecnológico en los últimos años, las leyes vigentes, en algunos países, se han venido adecuando para el amparo en cualquier circunstancia que pueda llevar a la vulneración de la información. Es así como vimos en la normativa española, que hace mención al dato de la localización, como un dato personal. La georreferenciación, se ha venido utilizando con más frecuencia, para la obtención de datos, por lo que trataremos a continuación.

3. GEOLOCALIZACIÓN

3.1 Definición de Geolocalización y Datos Personales

“El termino Geolocalización comprende la conjunción de tecnologías que tienen como finalidad la utilización de la información recabada que se encuentre relacionada a la localización geográfica” (Laboratorio Inteco, 2018).

También conocida como Georreferenciación, se define como el posicionamiento exacto de un objeto o persona, a través de su localización, visualizada por medio de un vector, punto, volumen o área, con la utilización de un sistema de coordenadas y datos determinados. Este método es utilizado con mayor frecuencia en los Sistemas de Información Geográfica (SIG) (Carrillo, 2005, p. 9).

A su vez, los Sistemas de Información Geográfica se definen como: “conjunto organizado de hardware y software, más datos geográficos, que se encuentran diseñados especialmente para capturar, almacenar, manipular y analizar en todas sus posibles formas la información geográfica referenciada” (Geolocalización, 2008), así la información obtenida pasa por un procedimiento de selección y descarte convirtiéndose en un dato de localización.

La Directiva Europea de Privacidad 200/58/CE, dentro de su artículo segundo, nos da una definición legal al momento de referirnos a un dato de localización, menciona que: “Cualquier dato tratado en una red de comunicaciones electrónicas que indique la posición geográfica del equipo terminal de un usuario de un servicio de comunicaciones electrónicas disponible para el público” (Diario Oficial de las Comunidades Europeas, 2002).

La información geográfica se ha desarrollado y evolucionado con el tiempo, en sus inicios el acceso se limitaba por los altos costos, para su manejo. La utilización de datos de localización únicamente se hacía por medio de un manejo

satelital. No obstante, con el avance de la tecnología a pasos agigantados en los últimos años se desarrolló desde navegadores de vehículos hasta el uso de telecomunicaciones (Instituto Federal de Telecomunicaciones, 2015).

En actualidad la obtención de datos de localización se encuentra en dispositivos tecnológicos, pueden ser desde un móvil hasta camisetas con chip, existen diversas formas de aplicación para dar uso de una georreferenciación. En los últimos años se han creado aplicaciones con las que se maneja la localización de ciertos objetos o personas, a través de un simple clic (Martínez, 2015, p. 2).

Estas aplicaciones pueden mostrar nuestra ubicación en tiempo real como cuando se comparte en redes sociales, exponiendo nuestra privacidad, ya que cualquier individuo podrá conocer inmediatamente nuestra posición. Al utilizar aplicaciones que facilitan rutas vehiculares, evitando el tráfico hacia el lugar que nos dirigimos. Estos datos de localización no siempre se obtienen mediante aplicaciones, ya que pueden conseguirse por distintos tipos de geolocalización, como se describe más adelante (Martínez, 2015, p. 4).

Como se ha dicho en los últimos años se ha venido implementando la geolocalización, a través de dispositivos electrónicos. Sin embargo, en algunos casos las empresas utilizan esto para localizar a sus trabajadores, violentando la finalidad con la que fue obtenida el dato, así como otros derechos a la privacidad e intimidad. Por tal motivo, existe un dictamen emitido por el Grupo de Trabajo del artículo 29, sobre la protección de datos de localización de los trabajadores, mencionando que:

> el tratamiento de los datos de localización puede estar justificado si se lleva a cabo formando parte del control del transporte de personas o bienes o de la mejora de la distribución de los recursos para servicios en puntos remotos (por ejemplo, la planificación de operaciones en tiempo real) o cuando se trate de lograr un objetivo de seguridad en relación con el propio empleado o con los bienes o vehículos a su cargo. Por el

> contrario, el Grupo considera que el tratamiento de datos es excesivo en el caso de que los empleados puedan organizar libremente sus planes de viaje o cuando se lleve a cabo con el único fin de controlar el trabajo de un empleado, siempre que pueda hacerse por otros medios. En estos dos casos, su finalidad no justifica el uso de un tratamiento que, por el tipo de datos recogidos, supone una innegable intromisión (PymeLegal, 2015).

El sentido de este dictamen es brindar una protección a los trabajadores que se encuentren sujetos a compartir sus datos de localización, con sus empleadores. Ya que por medio de estas aplicaciones no se busca tener un control constante de los trabajadores, más bien se tiene como fin limitar el desarrollo de estos dentro del horario de trabajo. Ya que estas medidas no se encuentran sujetas a que sea un control total.

A su vez la Directiva Europea de Privacidad 2002/58/CE, dentro de su artículo noveno. Establece factores importantes de los datos de localización y su tratamiento. Partiendo desde la distinción de dato de localización con dato de tráfico, es decir, información obtenida por medio de redes de comunicación, que no indiquen posicionamiento geográfico (Diario Oficial de las Comunidades Europeas, 2002).

El tratamiento de información deberá ser cuando trate de datos anónimos o a su vez cuando los propietarios confieran su consentimiento de uso. Los usuarios son informados del procedimiento, permanencia, propósito y si estos serán otorgados a terceros. Dando la posibilidad de negarse al otorgue de datos para su uso, ya que la aceptación es previa y necesaria (Diario Oficial de las Comunidades Europeas, 2002).

3.1.1 Mecanismos de Geolocalización

Como se mencionó anteriormente los datos de geolocalización en la actualidad se adquieren por medio de distintos sistemas. Dentro de estos métodos de obtención de localización podemos encontrar: GPS, GMS y WIFI.

3.1.1.1 GPS

El Sistema de Posicionamiento Global, con sus siglas en ingles GPS (Global Position System), es un sistema global de navegación por satélite. Permite determinar la posición de un objeto o persona, en todo el mundo, variando tan solo pocos metros. En la actualidad su operación lo maneja el Gobierno de Estados Unidos de América, bajo el control del Departamento de Defensa (Badillo, José; Domínguez, Pilar; González, Iván, 2018, p. 6).

Se compone alrededor de 30 satélites, que orbitan alrededor de la tierra, estos emiten información entre sí para llevar a un receptor. Estos datos son calculados rápidamente en la tierra tomando en cuenta 3 valores: longitud, latitud y altitud. Su fin es determinar la posición geográfica de objetos y personas, con lo cual se puede dar uso de esta información (GPS.GOV, 2017).

3.1.1.2 GSM

El Sistema Global para las Comunicaciones Móviles, su significado en inglés Global System for Mobile Communications (GSM), se basa en la utilización de redes telefónicas en general. Se maneja por medio de las antenas de telecomunicación, las cuales sirven para que los teléfonos tengan cobertura. Cuenta con más de 3000 millones de usuarios a nivel mundial, brindando ventajas sus usuarios (GSMA, 2017).

El GMS valora tres puntos: la aproximación de las antenas telefónicas, el tiempo que tarda de ir la información de una torre a torre (a diferencia del GPS, ya que este va a la velocidad de la luz), y el calcular la localización del dispositivo. Este

sistema es el menos preciso ya que su margen de error puede alcanzar hasta los 200 metros (Geolocalización, Qué Es Y Cómo Funciona, 2017).

3.1.1.3 Redes de Wi-Fi

Estas redes inalámbricas emiten señales, al momento de su funcionamiento, con las que se pueden identificar el lugar de donde de donde se transmite. La manera en las que se identifica estas redes es mediante su identificador, cada una tiene distinto código. Indica cuáles aparatos se encuentran conectados, pueden ser desde un teléfono móvil hasta un ordenador (Pastor, 2015).

3.2 La Geolocalización y su utilización

Existen ciertas aplicaciones, que se utiliza a diario, estas manejan datos personales de sus usuarios. Los individuos al momento de aceptar sus términos y condiciones de uso, conceden el manejo libre de su información, afectando su intimidad y privacidad, solo por el beneficio de prestación de servicios que brindan estas aplicaciones (Socorro, 2014, p. 19).

3.2.1 Google Maps

El desarrollo de la misma trata en el proporcionar mapas, imágenes y rutas. Facilitando el uso por medio de iconos interactivos, consiguiendo un mejor manejo de este (Instituto Internacional de Marketing Digital, 2016).

Google Maps ayuda a los usuarios a trazar rutas o itinerarios de viaje, lugares que se desea ir. Sin embargo, para acceder a los beneficios que brinda, se debe otorgar información de los sujetos al aceptar sus términos de uso. Estos datos varían desde anuncios que se abrió, lugares que visito, ubicación, fotos, dirección de correo electrónico con su contraseña, contenido que se buscó, etc. (Google, 2014).

Concediendo con la aceptación un manejo casi sin límites de la información que se encuentra en los dispositivos electrónicos, con los que se accede a la aplicación. Aun cuando tienen noción de los lugares visitados, solicita la evaluación de dicho sitio. Registrando los gustos y preferencias de cada individuo, para un posterior análisis de estos (IcMarkts, 2018).

Viene entonces la duda del motivo o si existe una necesidad de recolección masiva de información. Investigaciones han determinado que algunos datos se almacenan y procesan para su venta, a industrias interesadas en publicitar productos o servicios, a un grupo específico de personas (Barredo, 2016, p. 19).

No obstante, la compañía Google ha cambiado en los últimos meses, ciertos parámetros en sus políticas de seguridad y privacidad que se brinda a los usuarios. Dando la opción de verificar que información compartir o no, pese a eso, existe un desconocimiento por la gran parte de usuarios (El Comercio, 2018). A pesar de las facilidades que nos brinda, también existen aplicaciones de entretenimiento, que de igual forma para su uso de igual se debe aceptar sus términos y condiciones para su uso.

3.2.2 Pokémon Go

Como el anterior ejemplo, pertenece a la compañía “Google”, pero su desarrollo fue por “Niantic Inc.”, es un video juego basado en la realidad aumentado, por medio de la localización de los usuarios. Su lanzamiento fue el 06 de julio de 2016, en sus primeras semanas se estimó que hubo más de 100 millones de descargas a nivel mundial. Logró ingresos de más de 10 millones de dólares diarias y superando a otras aplicaciones como Facebook o Twitter, en usuarios activos al día (Histografias, 2016).

Los datos de localización son parte fundamental, para el uso de la aplicación, como se explicará a continuación (Heath, 2017).

> Nuestros Servicios incluyen juegos basados en la ubicación cuya característica principal es procurar una experiencia de juego vinculada a su localización geográfica. En consecuencia, necesitamos saber dónde se encuentra usted para hacer que estos juegos funcionen para usted y planificar la ubicación de recursos dentro del juego. Identificamos su ubicación a través de diferentes tecnologías, incluyendo GPS, los puntos WiFi a través de los que usted accede al Servicio y la triangulación de su dispositivo/teléfono móvil con repetidores de telefonía (Niantic, 2018).

Pokémon Go, recolecta y utiliza los datos de localización a medida que se va utilizando la aplicación o está instalado en el dispositivo. Este verifica los lugares a los que el usuario se desplaza, cotidianamente. Ya que la característica principal del videojuego es la ubicación de sus usuarios.

A su vez recolectan otro tipo de información, como son páginas visitadas en los navegadores de los dispositivos, los contactos, direcciones de correos electrónicos, etc. Esta información es almacenada y entregada a sus patrocinadores, para su administración. Sin embargo, por las leyes internacionales en las que se rigen, comparten únicamente datos anónimos con terceros, para mercadotecnia, ya que analizan el sector y el mercado (Niantic, 2018).

Concluyendo que esta aplicación no solo recopila información personal de sus usuarios, para el funcionamiento del juego. Si no, almacena tanto datos anónimos como personales, para el uso y venta de los mismos. Por otra parte, veremos cómo se manejan los datos cuando son aplicaciones que se catalogan como redes sociales.

3.2.3 Instagram

A diferencia de los dos últimos casos mencionados anteriormente, Instagram pertenece a la compañía de “Facebook”, ya que esta le compró en el año 2012.

Esta aplicación se le cataloga como una red social, su principal función es que los usuarios pueden compartir fotos y videos. En la actualidad existen más de 800 millones de usuarios activos (Araújo, 2017).

En dicha aplicación se debe aceptar de igual condiciones de uso, es decir, los términos y condiciones que se disponen. Sin embargo, para utilizar este servicio las personas no deberán ser menores de 13 años. Esta prohibición se debe a que se recopila cierto tipo de información, como nombre de usuario y contraseña, dirección de correo electrónico, información que se proporciona en el perfil, páginas Web que se visitan, etc (Instagram, 2013).

Se comparten los datos y contenido de los usuarios, con negocios vinculados o por vincularse legalmente con la empresa a la que pertenece Instagram. La información que se entrega no tiene ninguna limitación, al referirse a los archivos de registro, identificadores de dispositivos, información de los navegadores y datos de uso y ubicación (Instagram, 2013).

Esta información compartida, también ayudar a precisar las tendencias de uso, con lo que se puede mejorar el servicio brindado. Identificando a su vez por medio de que dispositivo a los que se ingresan a las plataformas de la aplicación. Por otro lado, al mencionar los datos de localización, Instagram accede al GPS, para tener la ubicación, con lo que analiza los sitios que se frecuenta (Instagram, 2013).

Al permitir el acceso a los datos de los usuarios, estos seden una parte de la protección y de las garantías sobre los derechos a la intimidad y privacidad. Pero no se debería visualizar como una vulneración absoluta sobre los datos, en ocasiones compartir información genera beneficios. Existen ciertos casos en los que, por medio de la utilización de datos de localización, se han logrado concretar acciones positivas.

3.3 Casos

3.3.1 Caso Puigdemont

Carles Puigdemont, fue presidente de la Generalitat (Generalidad de Cataluña) entre 2016 a 2017. Sin embargo, España le imputó los crímenes de traición a la patria y sedición. Convirtiéndose en un político catalán exiliado, razón por la cual se mudó a Bruselas, donde debía declarar en la Audiencia Nacional, el pasado 2 de noviembre de 2017 (Business Insider España, 2018).

Puigdemont no se presentó a esta declaración y aludió que la citación, tuvo como consecuencia un euroorden, es decir una orden europea de detención, por parte de la jueza que llevaba el caso (El Mundo, 2017). Activando de forma inmediata el CNI (Centro Nacional de Inteligencia de España), el cual atrapar a Puigdemont era de misión prioritaria, razón por la que el uso de la tecnología era algo elemental (Drummond, 2018).

La CNI, en conjunto con la Policía Nacional española y la Oficina Federal de Investigación Criminal Alemana, logró la aprensión de este político, el pasado 25 de marzo de 2018. En la frontera alemana, al momento de cruzar en un coche, que venía desde Dinamarca. El arresto se produjo dentro de una gasolinera, y más tarde el detenido fue trasladado a prisión de Neumünster, al norte de Alemania (Business Insider España, 2018).

La captura se concretó gracias al rastreo satelital (GPS), del vehículo en el que se estaba movilizando y la intercepción de su teléfono móvil. La policía al momento de realizar el operativo solicitó una orden judicial, aprobada por un juez (Carbajosa, 2018).

Aun cuando Puigdemont tenía orden de captura, las leyes estipulan que, para intervenir líneas telefónicas o el GPS, de cualquier individuo, se debe contar con la autorización judicial. Sin esta, se vulneran los derechos a la privacidad e

intimidad, en este caso, del ex presidente de la Generalitat. Exponiendo los datos de localización de una persona, toda vez que temporalmente la geolocalización ya no se encuentra protegida al haber obtenido la orden judicial para su acceso.

3.3.2 Agresión Sexual Frustrada

En España, en el año 2016, presentó un caso de una joven de 17 años proveniente de Madrid. decidió ir de paseo a Alicante, donde conoció a un chico de 23 años, proveniente de Italia, este individuo le invitó a su hogar (La Vanguardia, 2016).

Una vez en el inmueble, los jóvenes comenzaron a intercambiar besos, de forma voluntaria, el problema comenzó cuando la chica decidió irse. En ese momento el joven se lanzó sobre la chica, comenzando a tocarla de manera no consentida, la chica logró escapar por un instante, llegando al baño donde se encerró (La Vanguardia, 2016).

En ese momento la menor se comunicó con emergencias, desde su dispositivo móvil sin embargo la menor no sabía la dirección exacta donde se encontraba. En ese instante la policía actuó rápido, ya que se comenzaron a comunicar por medio de una aplicación, con la que podría enviar su localización actual por medio del GPS del aparato electrónico (La Vanguardia, 2016).

Logrando así identificar la vivienda donde se encontraba la menor, encerrada en el baño. Al arribo de la policía en el sector encendieron “señales acústicas”, con lo que la menor podría verificar si estaban en el sitio correcto. Una vez encontrado el edifico, la policía comenzó a tocar cada uno de los timbres, para verificar en que numero de departamento donde se encontraba (La Vanguardia, 2016).

Localizada la chica, procedieron con irrumpir en el departamento, logrando salvar a la menor y a detener al agresor, que mantenía a la menor de edad dentro

del departamento contra su voluntad. Imputando al mismo delito de detención ilegal y abuso sexual (La Vanguardia, 2016). Evitando de esta forma que el caso llegara a peores circunstancias y observando que por medio de la Geolocalización, se logró socorrer a tiempo a la víctima.

3.3.3 Caso Presunta Extorción

Este caso se presentó este mismo año en Ecuador, en el que la Unidad de Transparencia y Lucha Contra la Corrupción de la Fiscalía, luego de haber formulado cargos por extorción contra Eudi M. y Gerardo S.. Dichos individuos por medio de dispositivos móviles, extorsionaron a servidores públicos. Razón por la que el Juez Andrés Salas, dicto prisión preventiva y retención de cuentas, a los sujetos de nacionalidad extranjera (Fiscalía General Del Estado, 2018).

La Fiscalía General del Estado, trabajo conjunto de la Unidad Antisecuestro y Extorsión, determinaron que los sospechosos utilizaron redes sociales para conocer sobre los funcionarios públicos. Lograron determinar lugar de trabajo, familia y el domicilio. Procediendo a enviar mensajes intimidantes y amenazadores, ya que si no recibían cierta cantidad de dinero les provocarían daño (Fiscalía General Del Estado, 2018).

Por ende, para la respectiva investigación se intervino los dispositivos móviles, de donde se enviaban los mensajes. Identificando el IMEI de los teléfonos, es decir la identidad internacional de equipo móvil, con lo que se determinó la geolocalización de los mismos (Fiscalía General Del Estado, 2018).

3.4 Problemática

3.4.1 Derecho a la intimidad

Al momento de apreciar la intimidad propia de cada sujeto como una idea, se la atribuye a aspectos o factores, de la personalidad, incluso esta se ha venido

desarrollando con el individualismo que se ha generado en los últimos años, particularmente refriéndonos como a la alfabetización, o el hecho de la búsqueda de la soledad (Béjar, 1995, p. 168).

Sin embrago, para tener un mejor alcance sobre el derecho a la intimidad, Cruz, menciona:

> La intimidad no parece ser un fenómeno antropológico sino más un bien cultural. Su desarrollo fue favorecido por elementos dispares como son la valoración de la consciencia de si en el cristianismo en general, la reivindicación de la consciencia interior y de la vida ordinaria con el protestantismo, y la popularización del psicoanalismo de Freud en el siglo XX (…). Con el desarrollo de la intimidad también se acentúa el valor de la privacidad, como se refleja en el diseño de los espacios físicos de las viviendas. Por ejemplo, a mediados de siglo XVII surgen en Francia actividades y espacios que son claramente propios del mundo privado. La lectura, el aseo, el reposo entre otras actividades privilegiadas, tienen lugar de ahora en adelante en espacios claramente diferenciados y privados. Esta gran transformación de mentalidades que tiene lugar en el mundo moderno se refleja en el derecho y lleva así, a la idea de un espacio de libertad negativa o de independencia frente a las intervenciones del Estado: el derecho del individuo a ser dejado solo. (Cruz Revueltas, 2009, p. 28)

Siendo así, que el derecho a la intimidad es un derecho que se reconoce a cada individuo, para decidir si el conocimiento de su información se entrega a terceros, llegando así a una exclusión de algunos acontecimientos de la vida privada de cada sujeto, involucrando de esta forma en algunos aspectos sus propias emociones o actuaciones. Cada ser humano debe mantener bajo su control el acceso que permite a terceros a saber sobre su intimidad. Encontrando la voluntad de cada persona en compartir su privacidad, o su deseo de mantener esta información como confidencial. Por tal motivo, al tener un manejo inadecuado de la Geolocalización, afecta a la intimidad.

3.4.2 Derecho a la Privacidad

El derecho a la privacidad es aquel encargado en proteger de manera psicológica y física a cada persona, de intromisiones no queridas o deseadas, efectuadas por terceros. Este derecho debe tutelar ciertos factores de las personas, como la libertad para sentirse libre de realizar acciones que generan distintas experiencias. (Omeba, 2005, p. 28)

> El derecho a la privacidad se vislumbró desde el momento en el que surgió la inquietud por preservar la intimidad de las personas y la conciencia por otorgarles esa facultad. Este derecho puede definirse como aquel que los individuos poseen para separar aspectos de su vida íntima del escrutinio público, por lo que, sin distinción, todos tenemos derecho a ella. (Mendoza, 2017, p. 89)

Aquí encontramos las relaciones de amistad o relaciones en ámbitos laborales. Sin embargo, se desarrolla en un espacio cercano a la persona. En consecuencia, la Geolocalización al ser mal utilizada podría afectar a la privacidad.

3.5 Derechos a la Protección de Datos Personales

Por otro parte, debemos enfrentar la realidad que viven los datos personales en esta era digital. Ya que cotidianamente pueden ser manejados por las tecnologías emergentes y al existir un mal tratamiento de estos pueden generar una vulneración a la integridad y dignidad de sus dueños. Para asegurar que no exista dichas afectaciones, se deben cumplir ciertos parámetros, que se observación a continuación.

Por tal motiva se tomará el caso de Google Maps (Google, 2014), en el cual se observa los parámetros para cumplir un manejo adecuado de tratamiento de los datos personales.

Tabla 1.

Principios y Derechos a cumplir en datos personales

	SI	NO
Autodeterminación Informativa	X	
Consentimiento	X	
Informado	X	
Finalidad	X	
Seguridad	X	
Acceso	X	
Rectificación	X	
Cancelación	X	
Oposición	X	

4. CONCLUSIONES

Como consecuencia de vivir en un mundo tecnológico, el uso de dispositivos electrónicos es tan cotidiano como tomar las llaves de la casa al salir. Las personas al momento de utilizar estos artefactos electrónicos generan información que, se transmite a terceros, como su posicionamiento geográfico en tiempo real.

Al referimos a la información georeferencial de un sujeto hablamos de los datos de su localización, estos datos se comparten al momento de que el individuo lo consienta de forma voluntaria. Pero el uso de éstos implica un riesgo cuando los utilizamos sin discriminar los permisos a los que consentimos cuando accedemos a utilizar la tecnología, Por lo que es importante generar conciencia informática y evitar riesgos que perjudiquen los derechos de las personas.

En algunos casos se genera vulneraciones el derecho a la protección de datos de los sujetos, por la información obtenida como: genero, edad, número telefónico, localización, etc. Esta información da beneficios o ventajas a las personas naturales o jurídicas que manejan, almacenan y comercializan, estos datos. En el Ecuador no existe normativa vigente con la que se pueda brindar una protección eficaz respecto al mal uso de los datos de localización.

Sin embargo, en nuestras leyes existen ciertas normas específicas, que tutelan los datos personales. Esta normativa reconoce la autodeterminación informativa, es decir el consentimiento que debe existir para compartir la información por parte de sus propietarios. Buscando que no se transgreda derechos fundamentales, como la privacidad o intimidad de los ciudadanos.

La protección de datos personales es un derecho que se encuentra reconocido y tipificado por la Constitución de la República. La misma que señala las limitaciones de uso de la información y el consentimiento necesario del propietario. Pero no abastece a las necesidades de tutela que se generan en la

actualidad, como el uso desmedido por las aplicaciones de los dispositivos móviles.

Por otra parte, dentro del Reglamento General de Protección de Datos 2016/679, de la Unión Europea, reconoce al dato de localización como un dato personal. Verificando de este modo la importancia que se debe brindar a la información georeferencial. Señalando que los estándares de protección de datos, por parte de la Unión Europea, son avanzados en comparación con los existentes en el Ecuador.

Concluyendo que existe la necesidad de crear una norma específica sobre la protección de datos personales dentro de nuestro país. En esta misma normativa se debe reconocer a la geolocalización como un dato personal, puesto que como hemos visto en el presente ensayo, esta información puede ser aprovechada por terceros.

REFERENCIAS

Altmark, D. R., & Molina Quiroga, E. (2012). Tratado de Derecho Informático. Buenos Aires: La Ley S.A.

Araújo, S. (2017). Instagram ya tiene 800 millones de usuarios activos, 100 millones más desde abril. Recuperado el 29 de junio de 2018, de https://www.genbeta.com/redes-sociales-y-comunidades/instagram-ya-tiene-800-millones-de-usuarios-activos-100-millones-mas-desde-abril

Arenas Ramiro, M. (2006). El derecho fundamental a la protección de datos personales en Europa. Valencia: Tirant lo Blanch.

Asamblea Nacional. (2002). Ley de comercio electrónico, firmas electrónicas y mensajes de datos (Registro Oficial Suplemento 557 ed.). Quito: CEP.

Asamblea Nacional. (2008). Constitución de la República del Ecuador. Reformas en Registro Oficial Suplemento de 13 de julio de 2011. Quito, Ecuador: Registro Oficial 449 de 20 de octubre de 2008.

Asamblea Nacional. (2010). Ley del sistema nacional del registro de datos públicos (Registro Oficial Suplemento 162 ed.). Quito: CEP.

Asamblea Nacional. (2014). Código Orgánico Integral Penal (Registro Oficial Suplemento 180 ed.). Quito: CEP.

Asamblea Nacional. (2014). Código Orgánico Monetario Y Financiero (Registro Oficial Nº 332 ed.). Quito: CEP.

Asamblea Nacional. (2015). Ley Orgánica de Telecomunicaciones (Registro Oficial Suplemento 439 ed.). Quito: CEP.

Badillo, José; Domínguez, Pilar; González, Iván. (2018). GPS Derecho de la Circulación (2ª Edición ed.). Madrid: Tirant lo Blanch. Recuperado el 15 de agosto de 2018, de http://www.topoequipos.com/dem/qu-es/terminologa/que-es-un-gps

Barredo, Á. (2016). Evita que Google comparta tus datos privados con los anunciantes. La Vanguardia, p. 19.

Béjar, H. (1995). El ámbito íntimo: privacidad, individualismo y modernidad. Madrid: Alianza Editorial.

Business Insider España. (2018). Qué es el delito de sedición y cómo se castiga en Alemania, donde está detenido Puigdemont. Recuperado el 02 de julio de 2018, de https://www.businessinsider.es/que-es-delito-sedicion-como-castiga-alemania-donde-esta-detenido-puigdemont-197410

Camisón, C. (2001). La competitividad de la empresa industrial de la Comunidad Valenciana: análisis del efecto del atractivo del entorno, los distritos industriales y las estrategias empresariales. Valencia: Tirant lo Blanch.

Carbajosa, A. (2018). Puigdemont, detenido en Alemania tras entrar en coche desde Dinamarca. Recuperado el 01 de julio de 2018, de https://politica.elpais.com/politica/2018/03/25/actualidad/1521973804_797756.html

Carbonell, M. (2005). Diccionario De Derecho Procesal Constitucional y Convecional (Edición: 2 ed.). México: Porrúa.

Carrillo. (2005). Foro Cartesia. Recuperado el 29 de junio de 2018, de http://www.cartesia.org/foro/viewtopic.php?p=2821

Concepción Conde Ortiz. (2005). La protección de datos personales: un derecho autónomo con base en los conceptos de intimidad y privacidad. Madrid: Dykinson.

Congreso General. (1917). Constitución Política De Los Estados Unidos Mexicanos (Diario Oficial de la Federación 5 de febrero de 1917 ed.). Mèxico: DOF.

Congreso General. (2010). Ley Federal de Protección de Datos Personales en Posesión de Particulares. Recuperado el 08 de junio de 2018, de http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

Congreso General. (2017). Ley General De Protección De Datos Personales En Posesión De Sujetos Obligados (Vol. Nueva Ley publicada en el Diario Oficial de la Federación el 26 de enero de 2017). Mèxico: Nueva Ley DOF 26-01-2017.

Consejo de Estado. (1980). Constitución Política De La República De Chile. Santiago de Chile: DECRETO SUPREMO N° 100.

Consejo Superior de la Judicatura. (2016). Constitución Política de Colombia. Bogota: CENDOJ. Recuperado el 15 de junio de 2018, de

http://www.corteconstitucional.gov.co/inicio/Constitucion%20politica%20de%20Colombia.pdf

Cortes Generales. (1978). Constitución Española (BOE-A-1978-31229 ed.). Madrid: «BOE» núm. 311, de 29 de diciembre de 1978.

Cortes Generales. (1999). Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos (BOE-A-1999-23750 ed.). (J. d. Estado, Ed.) Madrid: BOE.

Cruz Revueltas, J. (2009). Moral y Transparencia. Fundamentos e implicaciones morales de la transparencia. México: IFAI.

Davenport, T., & Prusak, L. (2000). *Working Knowledge: How Organizations Manage What They Know.* Estados Unidos de Norteamerica: Harvard Business School Press.

De la Torre, P. (2017). Calidad de los datos e información de carácter personal. Recuperado el 13 de 08 de 2018, de http://tecnologia.elderecho.com/tecnologia/privacidad/Calidad-datos-informacion-caracter-personal_11_1101055001.html

Definición ABC. (2008). Geolocalización. Recuperado el 25 de junio de 2018, de https://www.definicionabc.com/geografia/geolocalizacion.php#ixzz2zukmZoL5

Deloitte. (2010). Ley Federal de Protección de Datos. Recuperado el 09 de junio de 2018, de https://www2.deloitte.com/content/dam/Deloitte/mx/Documents/risk/mx(es-mx)LeyFederalprotecciondatos_260810.pdf

Diario Oficial de las Comunidades Europeas. (2002). Directiva 2002/58/CE Del Parlamento Europeo Y Del Consejo. Recuperado el 26 de junio de 2018, de https://www.acave.travel/sites/default/files/comunitarioDirectiva%202002-58-CE.pdf

Directiva 95/46/CE del Parlamento Europeo y del Consejo. (1995). Grupo de protección de las personas en lo que respecta al tratamiento. Recuperado el 06 de julio de 2018, de http://www.redipd.es/actividades/encuentros/VI/common/wp136_es.pdf

Drummond, C. (2018). Esta es la tecnología que usó el CNI para atrapar a Puigdemont. Recuperado el 01 de julio de 2018, de

https://www.businessinsider.es/esta-es-tecnologia-que-uso-cni-atrapar-puigdemont-197648

El Comercio. (2018). Esta es toda la información que Google y Facebook tienen de sus usuarios. El Comercio, p. 09.

El Congreso De Colombia. (2012). Ley Estatutaria 1581. Recuperado el 10 de junio de 2018, de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981

El Mundo. (2017). ¿Qué es y cómo se aplica una 'euroorden'? Recuperado el 03 de julio de 2018, de http://www.elmundo.es/espana/2017/11/03/59fb473146163f417a8b45fa.html

El Parlamento Europeo, el Consejo y la Comisión de la Unión Europea. (2000). Carta de los Derechos Fundamentales de la Unión Europea. Recuperado el 08 de julio de 2018, de http://www.europarl.europa.eu/charter/pdf/text_es.pdf

Enríquez Álvarez, L. (2017). La Protección de Datos Personales en una era digital. Quito: Coperación Editorail Naciconal. Recuperado el 27 de 05 de 2018, de https://www.eluniverso.com/noticias/2018/04/29/nota/6736146/ecuador-no-tiene-ley-proteger-datos-personales

Enríquez Álvarez, L. (2018). Paradigmas de la protección de datos personales en Ecuador. Análisis del proyecto de Ley Orgánica de Protección a los Derechos a la Intimidad y Privacidad sobre los Datos Personales. La Protección de Datos Personales en la Era Digital, 43-61.

Extractos de las sentencias más relevantes. (2009). Jurisprudencia del Tribunal Constitucional Federal Alemán. México: Fundación Konrad Adenauer.

Fiscalía General Del Estado. (2018). Prisión preventiva para dos ciudadanos extranjeros por su presunta participación en el delito de extorsión. Recuperado el 30 de julio de 2018, de https://www.fiscalia.gob.ec/prision-preventiva-dos-ciudadanos-extranjeros-presunta-participacion-delito-extorsion/

García González, A. (2007). La Protección De Datos Personales: Derecho Fundamental Del Siglo Xxi. Un Estudio Comparado. Boletín Mexicano de Derecho Comparado, 743 - 778.

García Tinajero, L., & Ponce Baenz, G. (2011). Las fronteras del derecho a la información. México: Novum.

García-Cuélla Aiza y Enríquez. (2017). Ley General De Protección De Datos Personales En Posesión De Sujetos Obligados. Recuperado el 03 de 07 de 2018, de https://www.creel.mx/noticias/ley-general-de-proteccion-de-datos-personales/

Garriga Domínguez, A. (2015). Nuevos Retos Para La Protección de Datos Personales. España: Dykinson S.L.

Garriga, A. (2009). Tratamiento de datos personales y derechos fundamentales. Madrid: Editorial Dykinson.

Garzón, E. (2008). Lo íntimo, lo público y lo privado (Primera edición ed.). México: INAI.

Gobierno de la Ciudad de México. (2016). Derechos ARCO. Recuperado el 11 de 08 de 2018, de http://data.finanzas.cdmx.gob.mx/oip/

González Pascual, M. (2009). El Tribunal Constitucional Federal almena ante la compatibilidad con los derechos fundamentales de la normativa nacional de origen europeo de prevención de delitos. Revista de Derecho Comunitario Europeo(34), 148.

Google. (2014). Queremos que entiendas qué tipo de datos recogemos y utilizamos. Recuperado el 27 de junio de 2018, de https://privacy.google.com/intl/es/your-data.html

GPS.GOV. (2017). Sistema de Posicionamiento Global. Recuperado el 26 de junio de 2018, de https://www.gps.gov/spanish.php

Grupo Garatu. (2018). Reglamento General de Protección de Datos. Recuperado el 19 de junio de 2018, de https://grupogaratu.com/wp-content/uploads/sites/4/2018/04/whitepaper-Nuevo-reglamento-Protección-de-Datos-UE-2018.pdf

GSMA. (2017). *What is GSM?* Recuperado el 26 de junio de 2018, de https://www.gsma.com/aboutus/gsm-technology/gsm

Heath, A. (2017). The maker of Pokémon Go just raised $200 million to build other AR games. Recuperado el 28 de junio de 2018, de

https://www.businessinsider.com.au/pokemon-go-creator-niantic-raises-200-million-to-build-more-ar-games-2017-11

Herrera de la Fuente, A. (2003). La Carta de Derechos Fundamentales de la Unión Europea : una perspectiva pluridisciplinar. (F. R. Henriques, Ed.) España.

Higareda Magaña, L. (2013). El derecho a la protección de datos personales en México. A cuatro años de su reconocimiento constitucional. Recuperado el 05 de junio de 2018, de http://oiprodat.com/2013/11/29/el-derecho-a-la-proteccion-de-datos-personales-en-mexico-a-cuatro-anos-de-su-reconocimiento-constitucional/

Histografias. (2016). La historia de Pokémon Go convertida en infografía. Recuperado el 28 de junio de 2018, de https://histografias.com/infografia-historia-pokemon-go.html

IcMarkts. (2018). He mirado todos los datos que Google tiene sobre mí, y confirmo que es el Gran Hermano definitivo. Recuperado el 27 de julio de 2018, de https://www.xataka.com/privacidad/he-mirado-todos-los-datos-que-google-tiene-sobre-mi-y-confirmo-que-es-el-gran-hermano-definitivo

Instagram. (2013). Centro de privacidad y seguridad. Recuperado el 29 de julio de 2018, de https://www.facebook.com/help/instagram/377830165708421/?helpref=hc_fnav&bc[0]=Ayuda%20de%20Instagram&bc[1]=Centro%20de%20privacidad%20y%20seguridad

Instagram. (2013). Condiciones de uso. Recuperado el 15 de agosto de 2018, de https://www.facebook.com/help/instagram/478745558852511/

Instagram. (2013). Política de privacidad. Recuperado el 29 de julio de 2018, de Centro de privacidad y seguridad: https://www.facebook.com/help/instagram/155833707900388/

Instituto de Transferencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de México y Municipios. (2017). Infoem. Recuperado el 28 de junio de 2018, de http://www.infoem.org.mx/src/htm/queEsArco.html

Instituto Federal de Telecomunicaciones. (2015). Reunión con Representantes de Red en Defensa de los Derechos Digitales y Artículo 19. Recuperado

el 25 de junio de 2018, de http://www.ift.org.mx/conocenos/pleno/agenda-publica/gabriel-oswaldo-contreras-saldivar/reunion-con-representantes-de-red-en-defensa-de-los-derechos-digitales-y-articulo-19

Instituto Internacional de Marketing Digital. (2016). Que es Google Maps, definicion y noticias. Recuperado el 27 de junio de 2018, de https://iiemd.com/google-maps/que-es-google-maps-2

Jiménez García, S. (2018). Protección de Datos de Carácter Personal. (Boletín Oficial del Estado) Recuperado el 26 de junio de 2018 de file:///C:/Users/User/Downloads/BOE-055_Proteccion_de_Datos_de_Caracter_Personal.pdf

KZBlog. (2017). Geolocalización, Qué Es Y Cómo Funciona. Recuperado el 26 de julio de 2018, de http://kzgunea.blog.euskadi.eus/blog/2017/03/31/geolocalizacion-que-es/

La Vanguardia. (2016). Una menor se encierra en el baño y logra que la policía la localice por GPS para evitar que la violen. Recuperado el 04 de 08 de 2018, de http://www.lavanguardia.com/sucesos/20160706/403004211285/menor-evita-violacion-movil-alicante.html

Laboratorio Inteco. (2018). Características de la Geolocalización Online. Recuperado el 27 de junio de 2018, de http://reader.digitalbooks.pro/book/preview/43053/id_ch_4

Losano, M. (1989). Libertad informática y leyes de protección de datos. Madrid: Centro de Estudios Constitucionales, Cuadernos y Debates.

Martínez, R. (2015). Geolocalización: entre el bien común y el derecho a la privacidad. Recuperado el 14 de julio de 2018, de http://asesoresensoluciones.com/index.php/geolocalizacion-entre-el-bien-comun-y-el-derecho-a-la-privacidad#_ftn1

Mendoza, M. (2017). El derecho a la privacidad en la era digital. Recuperado el 15 de julio de 2018 de https://www.welivesecurity.com/la-es/2017/03/02/derecho-a-la-privacidad-era-digital/

Naranjo Godoy, L. (2017). El dato personal como presupuesto. Revista de Derecho, No. 27,, 8.

Niantic. (2018). Política de Privacidad de Niati. Recuperado el 28 de 06 de 2018, de https://www.nianticlabs.com/privacy/es/

Omeba, E. J. (2005). Refiere que todo lo íntimo es necesariamente privado, pero no todo lo privado es necesariamente íntimo. Argentina: Versiòn Digital.

Parlamento Europeo; Consejo de la Unión Europea. (2016). Reglamento General de Protección de Datos. Unión Europea: Diario Oficial de la Unión Europea.

Pastor, D. (2015). WPS: ¿Qué es?¿Para qué sirve? Recuperado el 27 de junio de 2018, de https://rootear.com/seguridad/wps-que-espara-que-sirve

Puccinelli, O. (1999). El Habeas Data En Indoiberoamérica. Bogotá: Temis S.A.

PymeLegal. (2015). Protección de datos y geolocalización de trabajadores. Recuperado el 26 de junio de 2018, de https://www.pymelegal.es/es/noticias/33/proteccion-de-datos-y-geolocalizacion-de-trabajadores.html

Real Academia Española. (2017). RAE. Recuperado el 26 de 05 de 2018, de http://www.rae.es/

Registro de Datos Crediticios. (2018). Comunicado. Recuperado el 29 de junio de 2018, de https://transferencia.registrocrediticio.gob.ec/catastro/

Remolina Angarita, N. (2013). Tratamiento de datos personales. Aproximación internacional y comentarios a la ley 1581 de 2012. Colombia: Leguis.

Sánchez Bravo, A. (1998). La protección del derecho a la libertad informática en la Unión Europea. Sevilla: Universidad de Sevilla.

Santos García, D. (2005). Nociones Generales de la Ley Orgánica de Protección de Datos. Madrid: TECNOS.

Santos Pascual, E., & López-Vidriero, I. (2005). Protección de datos personales: manual práctico para empresas. Madrid: Fundación Confemetal.

Sentencia De Jurisprudencia Sobre Proteccion, No. 0067-11-JD (Corte Constitucional Del Ecuador 23 De Abril De 2014).

Sentencia No. 001-2014-PJO-CC, Gaceta Constitucional No. 007 (03 de Julio de 2014).

Socorro, J. (2014). El riesgo de aceptar los términos y condiciones de uso. Recuperado el 26 de julio de 2018, de

http://postperiodistas.com/2014/05/el-riesgo-de-aceptar-los-terminos-y-condiciones-de-uso/

Superintendencia de Industias y Comercio. (2018). Registro Nacional de Bases de Datos. Recuperado el 11 de junio de 2018, de http://www.sic.gov.co/registro-nacional-de-bases-de-datos

Superintendencia Industrias y Comercio. (2018). Registro Nacional de Bases de Datos. Recuperado el 17 de junio de 2018, de http://www.sic.gov.co/preguntas-frecuentes-rnbd

Uicich, R. D. (1999). Los Bancos de Datos y El Derecho a la Intimidad. Buenos Aires: AD-HOC S.R.L.

Vizcaíno Calderón, M. (2001). Comentarios a la Ley Orgánica de Protección de Datos de Carácter Personal. Madrid: Ellacuría.

Zabía, J. (2008). Protección de datos: comentarios al reglamento. Madrid: Lex Nova.