

**UNIVERSIDAD CATÓLICA  
DE SANTIAGO DE GUAYAQUIL  
FACULTAD DE JURISPRUDENCIA, CIENCIAS SOCIALES Y  
POLÍTICAS  
CARRERA DE DERECHO**

**TEMA**

**Derecho a la eliminación de datos personales atendiendo al  
principio de finalidad**

**AUTOR**

**Sacoto Mendoza, Susy Valeria**

**Trabajo de titulación previo a la obtención del título de  
Abogada de los Tribunales y Juzgados de la República del  
Ecuador**

**TUTOR**

**Ab. Cuadros Añezco, Xavier Paul, Mgs.**

**Guayaquil, Ecuador  
10 de febrero del 2020**



UNIVERSIDAD CATÓLICA  
DE SANTIAGO DE GUAYAQUIL

**FACULTAD DE JURISPRUDENCIA, CIENCIAS SOCIALES Y POLÍTICAS**  
**CARRERA DE DERECHO**

## **CERTIFICACIÓN**

Certificamos que el presente trabajo de titulación, fue realizado en su totalidad por **Sacoto Mendoza Susy Valeria**, como requerimiento para la obtención del título de **Abogada de los Tribunales y Juzgados de la República del Ecuador**.

### **TUTOR**

f. \_\_\_\_\_

**Ab. Cuadros Añezco Xavier Paul, Mgs.**

### **DECANO DE LA CARRERA**

f. \_\_\_\_\_

**Ab. García Baquerizo José Miguel, Mgs.**

**Guayaquil, 10 de febrero del 2020**



UNIVERSIDAD CATÓLICA  
DE SANTIAGO DE GUAYAQUIL

**FACULTAD DE JURISPRUDENCIA, CIENCIAS SOCIALES Y POLÍTICAS  
CARRERA DE DERECHO**

## **DECLARACIÓN DE RESPONSABILIDAD**

Yo, **Sacoto Mendoza Susy Valeria**

### **DECLARO QUE:**

El Trabajo de Titulación: **Derecho de eliminación de datos personales atendiendo al principio de finalidad**, previo a la obtención del título de **Abogada de los Tribunales y Juzgados de la República del Ecuador**, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

**Guayaquil, 10 de febrero del 2020**

**LA AUTORA**

f. \_\_\_\_\_  
**Sacoto Mendoza Susy Valeria**



UNIVERSIDAD CATÓLICA  
DE SANTIAGO DE GUAYAQUIL

**FACULTAD DE JURISPRUDENCIA, CIENCIAS SOCIALES Y POLÍTICAS  
CARRERA DE DERECHO**

## **AUTORIZACIÓN**

Yo, **Sacoto Mendoza Susy Valeria**

Autorizo a la Universidad Católica de Santiago de Guayaquil a la **publicación** en la biblioteca de la institución del Trabajo de Titulación: **Derecho de eliminación de datos personales atendiendo al principio de finalidad**, cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y total autoría.

**Guayaquil, 10 de febrero del 2020**

**LA AUTORA**

f. \_\_\_\_\_  
**Sacoto Mendoza Susy Valeria**





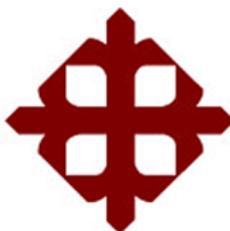
UNIVERSIDAD CATÓLICA  
DE SANTIAGO DE GUAYAQUIL

## ACTA DE INFORME PARCIAL

El abajo firmante, docente tutor del Trabajo de Titulación denominado ***“Derecho de eliminación de datos personales atendiendo al principio de finalidad”***, elaborado por la estudiante **SUSY VALERIA SACOTO MENDOZA**, certifica que durante el proceso de acompañamiento dicho estudiante ha obtenido la calificación de **DIEZ (10)** lo cual las califica como **APTAS PARA LA SUSTENTACIÓN**.

f. \_\_\_\_\_

**Ab. Cuadros Añezco Xavier Paul, Mgs.**  
**DOCENTE TUTOR**



**UNIVERSIDAD CATÓLICA  
DE SANTIAGO DE GUAYAQUIL**

**FACULTA DE JURISPRUDENCIA, CIENCIAS SOCIALES Y POLÍTICAS  
CARRERA DE DERECHO**

**TRIBUNAL DE SUSTENTACIÓN**

f. \_\_\_\_\_

**DR. JOSÉ MIGUEL GARCÍA BAQUERIZO**

DECANO

f. \_\_\_\_\_

**AB. MARITZA GINETTE REYNOSO DE WRIGHT**

COORDINADORA DEL ÁREA

f. \_\_\_\_\_

**DR. JAVIER EDUARDO AGUIRRE VALDEZ**

OPONENTE

## INDICE

CAPITULO 1 .....	2
1.1 Contexto histórico jurídico .....	2
1.2 Evolución del derecho a la privacidad e intimidad.....	3
1.3 Importancia y conceptualización de protección de datos .....	6
1.4 Naturaleza jurídica.....	9
CAPITULO 2.....	12
2.1 El derecho a la protección de datos personales en las leyes pertinentes y su esfera de aplicación internacional.....	12
2.2 Principios del derecho a la protección de datos personales .....	13
2.3 El derecho a la protección de datos personales en las leyes pertinentes y su esfera de aplicación nacional.....	16
2.4 Incidencia del proyecto Ley Orgánica de Protección de Datos Personales .....	20
2.5 Análisis del principio de finalidad y su relación con el proyecto de Ley Orgánica de Protección de Datos Personales .....	23
2.6 Jurisprudencia comparada y análisis de jurisprudencia ecuatoriana	24
CONCLUSIÓN .....	31
RECOMENDACIÓN.....	32
BIBLIOGRAFÍA.....	33

## **AGRADECIMIENTO**

El presente trabajo de tesis está dedicado a mis padres, José Sacoto Navia y Susy Mendoza Salazar, quienes con su amor, paciencia y esfuerzo me han permitido llegar a cumplir hoy un sueño más. Gracias por inculcar en mí el ejemplo de esfuerzo y valentía, de no temer a las adversidades porque Dios está siempre conmigo.

## RESUMEN

El derecho a la privacidad consiste en que el individuo tenga plena protección en persona y en propiedad es un principio tan antiguo como el derecho consuetudinario. La administración y protección de datos personales en el ámbito histórico y su efecto en el marco jurídico. En el caso del gobierno ecuatoriano que tiene como objetivo principal de preservar la privacidad para la publicación de datos es proteger la privacidad de los datos individuales mediante la propuesta del Proyecto de Ley Orgánica de Protección de Datos Personales. Actualmente, los ciudadanos se sienten vulnerables hasta el momento que no se aprueba esta Ley. Una vez aplicada esta Ley, se podría solicitar el derecho al olvido digital en caso que sea necesario sin perjuicio a terceros dentro del marco legal.

**Palabras Claves:** *Privacidad, Derecho olvido, Protección datos personales, Ecuador.*

## **ABSTRACT**

The right to privacy is that the individual has full protection in person and in property is a principle as old as customary law. The administration and protection of personal data in the historical field and its effect on the legal framework. In the case of the Ecuadorian government whose main objective is to preserve the privacy for the publication of data, it is to protect the privacy of individual data through the proposal of the Draft Law on the Protection of Personal Data. Currently, citizens feel vulnerable until this Law is not approved. Once this Law has been applied, the right to digital oblivion could be requested if necessary without prejudice to third parties within the legal framework.

**Keywords:** *Privacy, Right to forget, Protection of personal data, Ecuador.*

# CAPITULO 1

## 1.1 Contexto histórico jurídico

En las últimas décadas, el incremento del procesamiento y manejo de información de los ciudadanos ha sido exponencial. El principal administrador de datos ha sido el Estado a través de sus distintas instituciones públicas. Dicha información sirve para ejecutar sus tareas operativas. Además, la interacción con cualquier entidad concernida, es decir, los ciudadanos o las empresas. Este tipo de información, agrupada y segmentada por datos sobre recaudación de impuestos, finanzas, salud, educación, seguridad social, religión, entre otros, es compilada, procesada y almacenada por instituciones del Gobierno en todos los niveles de administración, como archivos impresos o por medios electrónicos, generando un Big Data.

“El término Big Data a menudo se define por las tres V: volumen, velocidad y variedad” (Laney, 2001, pág. 23). “El volumen se refiere a las cantidades masivas de datos recopilados, la velocidad a la velocidad de generación y análisis de datos, y la variedad a la <heterogeneidad estructural> de los datos” (Gandomi & Haider, 2015, pág. 137); Big Data no solo es nuevo “en el sentido de que ahora crea conjuntos de datos más grandes de lo que solía, sino también porque esta grandeza ha llevado a nuevos requisitos para el análisis y procesamiento de datos” (Bello-Orgaz , Jung, & Camacho, 2016, pág. 49). Un concepto relacionado es el aprendizaje automático. Para analizar los datos que se recopila, ya no se confía en la visión humana ni en el análisis estadístico de estilo antiguo. “Algunos incluso argumentan que es posible que ya no se necesite humanos en ciencia, etc. Ya que las máquinas ahora pueden reemplazarnos” (Sætra, 2018, pág. 8). Se ha creado máquinas que pueden aprender sin que se les diga explícitamente qué buscar. Simplemente se les da ciertos objetivos, y estos sistemas "mejoran su rendimiento en una tarea determinada con el tiempo a través de la experiencia" (Brundage, Avin, Clark, & Toner, 2018, pág. 9)

A medida que estos sistemas aprenden, se usa el conocimiento adquirido para realizar tareas que históricamente se pensaba que requerían inteligencia, como determinar a quién se le deberían otorgar préstamos, sugerir en qué películas podría estar interesado, etc. “Cuando se emplea de esta manera, tenemos inteligencia artificial” (Brundage, Avin, Clark, & Toner, 2018, pág. 11). En efecto, la tecnología y su aplicación a sistemas de comunicación cada vez más avanzados, pone en evidencia la necesidad de controlar y regular el movimiento creciente de bases de datos de contenido personal.

Esta evolución digital del Big data también se ha concebido en el Derecho en el ordenamiento jurídico, donde se presenta para el ciudadano un escenario abierto. Este evento puede visualizar ventajas y desventajas que afectarían a los derechos fundamentales y principio de finalidad del derecho de las personas, con relación a la información de carácter personal que se almacena, intimidad y principalmente a la vida privada. Por consiguiente, en el marco legal fundamental, han existido avances en función de cambios generacionales que van de la mano con el manejo de la información digital atendiendo al principio de finalidad. De igual importancia, la administración y protección de datos personales en el ámbito histórico y su efecto en el marco jurídico. Finalmente, en el caso del gobierno ecuatoriano que tiene como objetivo principal preservar y proteger la privacidad de los datos individuales publicados mediante el Proyecto de Ley Orgánica de Protección de Datos Personales.

## **1.2 Evolución del derecho a la privacidad e intimidad**

Es solo durante el último medio siglo que la ley ha reconocido el "derecho a ser dejado en paz", "el derecho bajo ciertas circunstancias para proteger el nombre y la fisonomía de uno para que no se conviertan en propiedad pública" (Warren & Brandeis, 1890). Ninguna mención de tal derecho se encontrará en las palabras de los grandes filósofos políticos y escritores de tratados de los siglos XVII y XVIII: Hobbes, Locke, Rousseau, Montesquieu, Spencer y otros. Al hablar sobre "Derechos naturales", "El estado de la naturaleza", "Contrato social", "solo se preocuparon por el poder del estado para reducir las libertades de las personas" (Nizer, 1940-1941). Por tanto, la sociedad aún no

se había vuelto tan compleja que la privacidad del individuo estaba en peligro de invasión.

No obstante, los cambios políticos, sociales y económicos requirieron la creación de nuevos derechos legales. La esencia del sistema judicial angloamericano era que funcione después del hecho y no antes. Decidía casos y controversias reales en lugar de intentar pronosticar mediante códigos enciclopédicos. Dado que el derecho consuetudinario no es la mera declaración formal de un código moral tradicional heredado, está recién diseñado para satisfacer necesidades imprevistas, se predestinó que la doctrina de la privacidad debería formularse. Para Nizer (1940-1941) "la regla fue el producto de su tiempo".

Por lo tanto, la necesidad social que se cristalizó en el derecho a la privacidad no se hizo insistente hasta la era de una gran expansión industrial, cuando los avances milagrosos en el transporte y las comunicaciones amenazaron con aniquilar el tiempo y el espacio, cuando la prensa atravesaba los crecientes dolores del "periodismo amarillo", Cuando el negocio se hizo grande (Pound, 1915).

El derecho a la privacidad consiste en que el individuo tenga plena protección en persona y en propiedad es un principio tan antiguo como el derecho consuetudinario; pero de vez en cuando se ha encontrado necesario definir de nuevo la naturaleza exacta y el alcance de dicha protección. "Los cambios políticos, sociales y económicos implican el reconocimiento de nuevos derechos, y el derecho consuetudinario, en su eterna juventud, crece para satisfacer las demandas de la sociedad" (Willes & Taylor, 1890, pág. 31). De acuerdo a O Meins (2017):

"Tomando en consideración que el diccionario de la lengua española no contempla el término "privacidad", se entiende como sinónimos las voces "intimidad" y "vida privada", no obstante que algunos distinguen entre ambos conceptos. Así, para determinados autores la vida privada es el género, que comprendería como núcleo central y más pequeño a la intimidad, mientras que para otros autores la vida privada es una de las facetas que integran el concepto de intimidad (pág. 222) ."

Es decir que el entorno privado o intimidad mantiene una cierta relación y equiparación con el concepto anglosajón de privacidad (privacy). Este criterio

fue conceptualizado en la Tesis Doctoral de Fernando Gómez Sáez (2014), “pues se trata de unas informaciones que el individuo desea que sean conocidas por una sola persona o grupo reducido de ellas, como la situación familiar, las creencias religiosas o las ideas políticas”(pág. 74). Esta representación resulta válida para establecer el grado de protección, que será mayor cuanto más cerca del círculo inicial se encuentre aquel en el que sea detectado.

Se podría considerar que el concepto de intimidad constantemente supondría el distanciamiento del mundo exterior en que se convive. Por tanto, se pretende una desconexión social. Fernando Gómez Sáez (2014) afirma que “la consecuencia directa de que el derecho a la intimidad deberá garantizar la protección de la autorrealización de cada individuo cuando se quiera mantener, ejerciendo su propia libertad, a distancia del cuerpo social al que se pertenece”(pág. 77). Por consiguiente, nadie de este entorno debería acceder a aspectos determinantes de la vida privada de los individuos.

El artículo 12 de la Declaración Universal de los Derechos Humanos proclamado por la Asamblea General de la ONU (1948), determina que:

“Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la Ley contra tales injerencias o ataques” (ONU, 1948).

Asimismo, la Corte Interamericana de Derechos Humanos (1979) señaló en cuanto al alcance de expresión e información lo siguiente:

“...Quienes están bajo la Convención tienen no sólo el derecho y la libertad de expresar su propio pensamiento, sino también el derecho y la libertad de buscar, recibir y difundir informaciones e ideas de toda índole (...) la libertad de expresión e información requiere, por un lado, que nadie sea arbitrariamente menoscabado o impedido de manifestar su propio pensamiento y representa, por tanto, un derecho de cada individuo; pero implica también, por otro lado, un derecho colectivo a recibir cualquier información y a conocer la expresión del pensamiento ajeno...”(OEA, 1979).

Para el año 2018, El Reglamento General de Protección de Datos (RGPD) es un reglamento sobre privacidad y derechos individuales aplicable a todos los residentes de la Unión Europea (UE). Por lo tanto, “este reglamento es aplicable en Noruega y en todos los países de la UE / Espacio Económico

Europeo (EEE), y en cualquier país que quiera hacer negocios con países de la UE / EEE a partir del 25 de mayo de 2018” (Martin, 2015, pág. 71)

Bajo estos antecedentes, la Unión Europea (UE) desarrolló un Marco Jurídico que regule las condiciones actuales en la gestión de datos, teniendo como prioridad la protección de los mismos. Toca mencionar que, en la región, los únicos países que no tienen una Ley de Protección de Datos Personales son Venezuela, Bolivia y Ecuador. Este último está proponiendo un Proyecto de Ley Orgánica de Protección de Datos Personales que le permita no sólo hacer frente a esta situación. Asimismo, armar los mecanismos jurídicos para participar comercial y activamente alineado al Reglamento Europeo de Protección de Datos (RGPD). Sin embargo, esta investigación tiene como objetivo analizar el derecho eliminación de datos personales (olvido digital) atendiendo principio de finalidad.

### **1.3 Importancia y conceptualización de protección de datos**

En Europa, el Reglamento Europeo de Protección de Datos (RGPD) está vinculado a los derechos básicos que disfruta cada individuo en la comunidad digital, incluidos los derechos relacionados con la recopilación y el almacenamiento de cualquier tipo de datos personales privados (pero generalmente datos digitales). Muchas organizaciones no tienen una comprensión clara de cómo adaptarse y aplicar estas nuevas reglas.

Entonces, la privacidad de la información es un subconjunto de la privacidad, y los conceptos de privacidad de la información se entienden principalmente en términos de construcciones a nivel individual, como actitudes e inquietudes. La recopilación de información personal surgió como un tema importante en la década de 1970 (Smith, Milberg, & Burke, 1996, pág. 189). La capacidad de recopilar y analizar la información del cliente es cada vez más importante para las empresas (Awad & Krishnan, 2006, pág. 19). Las tecnologías actuales que permiten la captura y el análisis de grandes volúmenes de datos en cualquier estructura y en tiempo casi real (también conocido como Big Data) conllevan ventajas y desventajas para el individuo (Presthuis, W; Andersen, L, 2017, pág. 1971). Las ventajas para el individuo incluyen servicios mejorados y personalizados como Netflix, redes sociales

como Facebook, identificación de terroristas en grandes multitudes y orientación sobre el tráfico (Conger, Pratt, & Loch, 2013). Ejemplos de desventajas incluyen la colocación de individuos bajo vigilancia constante y la sujeción de individuos a estigmatización (Presthus, 2012) y discriminación de precios (Martin, 2015, pág. 80). Además, la información se puede compartir con terceros, como anunciantes, o se puede alimentar a algoritmos con resultados espectaculares, como el conocido caso de embarazos de predicción de Target (Mateosian, 2013).

### **Datos Privados**

Si bien los datos personales sobre las personas (por ejemplo, datos de ubicación, comportamiento de navegación, preferencias personales, etc.) podrían ser muy útiles, también representan amenazas considerables para su privacidad (Wang, Zheng, & Jiang, 2018, pág. 24).

La fuga de datos personales, el mal uso de los mismos o los ataques de usuarios malintencionados son comunes (Tsay-Vogel, Shanahan, & Signorielli, 2018, pág. 152). La legislación sobre privacidad de datos ha evolucionado junto con las tecnologías de recopilación y procesamiento de datos personales a lo largo de los años (Raab & Szekely, 2017, pág. 428).

Ejemplos más antiguos en Europa incluyen el Artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea (UE) que garantiza a los ciudadanos el derecho a la protección de datos personales (Van Loenen, Kulk, & Ploeger, 2016, pág. 341), y la Directiva de Protección de Datos introducida en 1995 por la UE (DIR95), cuyo objetivo era salvaguardar la privacidad de los ciudadanos por un mal uso o una recolección innecesaria (Ryz & Grest, 2016, pág. 19).

En abril de 2016, el Parlamento de la UE aprobó el Reglamento general de protección de datos de la UE (GDPR). GDPR ha introducido varios cambios en comparación con DIR95, presentando nuevas definiciones y principios y aclarando los anteriores. Las computadoras se han convertido en algo común, el aumento de los teléfonos inteligentes y las redes sociales y la dependencia organizacional de los medios digitales han sido ignoradas por DIR95, en gran

parte porque no existían de la misma manera cuando se formuló el acto. Las nuevas regulaciones introdujeron multas más duras por incumplimiento e infracciones y dieron a las personas más voz sobre lo que las empresas pueden hacer con sus datos. Como ejemplo concreto, cada sujeto de datos ahora tiene derecho a ser olvidado, lo que significa esencialmente que el proveedor de servicios tiene que eliminar los datos personales del sujeto de datos a pedido. Como otro ejemplo, cada sujeto de datos ahora tiene derecho a la portabilidad de datos, lo que significa que el proveedor de servicios debe proporcionar una copia de los datos personales del sujeto de datos a pedido.

### **Datos Públicos**

Mediante la publicación de información pública, las distintas entidades pertenecientes al gobierno ponen a disposición de los ciudadanos datos que están en su poder en formatos que facilitan la redistribución, reutilización y comercialización. Además, la mayoría de ellos son considerados datos abiertos constituyen un instrumento útil para facilitar tanto el aprovechamiento de los datos públicos de la forma más efectiva como la transparencia de la administración. De acuerdo a Isaac Martín (2014):

La apertura de datos públicos comparte algunas finalidades con el acceso o la difusión de información del sector público a través de medios electrónicos aunque intenta superar algunos de sus límites, básicamente los derivados de la propia actitud de las administraciones públicas frente a la difusión de la información, y da un mayor protagonismo a los ciudadanos (pág. 376).

Por lo tanto, las personas naturales y jurídicas dispondrían de información de manera libre, con el objetivo de estar informados sobre las condiciones de entornos tales como son: económico, social, político, tecnológico, ambiental entre otros.

### **Datos personales**

Para el Parlamento Europeo y del Consejo (2016) en su convenio 108, dispone en el artículo 3 sobre los datos personales: Toda información sobre un ciudadano identificable o identificado; se considera persona física

identificable todo individuo cuya identidad puede determinarse, directa o indirectamente, en particular mediante un identificador (RUE, 2016). Por consiguiente, se detallaría a través de un número de identificación, nombres y apellidos. Igualmente, Utilizando un identificador en línea o uno a varios elementos propios de la identidad genética, económica, social, cultural, entre otras de dicho individuo. Se podría considerar que los datos personales son una gran parte de la masa de información que se maneja en el mercado. Por tanto, su importancia es fundamental para conocer las percepciones y comportamientos de consumo. Para Juan Dueñas (2014) establece que Los datos personales en la actualidad tienen un valor sumamente importante, puesto que son esenciales para el desarrollo de nuevas tecnologías que permiten la eficiencia en la toma de decisiones. Muchas veces se confunde el término dato con información (pág. 28).

Supuesto esto, es determinante enfocarse en el estudio conceptual de los datos personales, como el elemento angular del derecho al que se refiere el presente estudio. La Agencia Española de Protección de Datos los define como “cualquier información numérica, alfabética, gráfica, fotográfica, acústica, o de cualquier otro tipo concerniente a personas físicas identificadas e identificables” (AEPD, 2009)

#### **1.4 Naturaleza jurídica**

Durante el desglose y desarrollo de este primer capítulo, se ha evidenciado como la Unión Europea UE ha aplicado mecanismos jurídicos para la protección de datos, entre ellos los personales; la legislación ecuatoriana aún se encuentra en el dilema de aplicar un proyecto de Ley para su respectiva regulación. Países que conforman la Comunidad Andina como son Colombia y Perú han adoptado estas regulaciones para cumplir no solamente con la protección de datos sino con el Tratado de Libre Comercio firmado con la UE. Aunque, la Constitución de la República del Ecuador (2008) en su artículo 66, numeral 19, reconoce y garantiza la protección de datos, indicando que “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 requirieran la autorización del titular o mandato de la ley” y el numeral 20, el derecho a la intimidad personal y familiar. Por tanto, dentro de esta Ley se faculta al derecho del acceso y decisión. Igualmente, Se da garantía a las personas en lo relacionado a la protección de su información. Para ello, es necesario contar con la autorización del titular de los mismos o el mandato de la Ley para su recolección, almacenamiento, procesamiento, difusión o distribución del mismo.

Ley Orgánica de Telecomunicaciones (2015), en su Art. 22.- Derecho de los abonados, clientes y usuarios: los abonados, clientes, y usuarios de servicios de telecomunicaciones tendrán derecho: numeral 4) A la privacidad y protección de sus datos personales, por parte del prestador con el que contrate servicios, con sujeción al ordenamiento jurídico vigente. Asimismo, en el Reglamento General a la Ley de Telecomunicaciones (2016) en su Art. 3 numeral 4) Prestador del servicio del régimen general de telecomunicaciones.- Es la persona natural o jurídica que posee el título habilitante para la prestación del servicio de telecomunicaciones o de los servicios de radiodifusión de señal abierta o por suscripción. Para ello, se busca garantizar el buen manejo de los datos personales. Por consiguiente, en el Art. 24 numeral 14) Adoptar las medidas necesarias para la protección de los datos personales de sus usuarios y abonados, de conformidad con esta Ley, su Reglamento General y las normas técnicas y regulaciones respectivas (Ley Orgánica de Telecomunicaciones, 2015). En otras palabras, se pretende adoptar mecanismos básicos en la protección de datos de los usuarios y abonados. Sin embargo, esta Ley y sus Reglamentos no cuentan con una definición clara sobre los datos personales. Además, ante la inadecuada protección de datos personales este cuerpo legal no establece un régimen de responsabilidades. Pero, se designa a Arcotel como entidad pública a cargo de establecer y reglamentar mecanismos de sancionadores en lo que amerite. En la actualidad, no existe resolución expedida alguna en la que sancione en caso de violación de la protección de datos.

En el ámbito financiero, el Código Orgánico Monetario y Financiero (2014), señala en su Art. 3 numeral 2) lo siguiente: Proteger los derechos de los usuarios de los servicios financieros, de valores y seguros. Es decir, la

protección de los datos personales no entra como regulación dentro de este Código. En consecuencia, no existe un marco jurídico dentro de esta Ley que garantice el derecho de los titulares de los datos personales y las obligaciones de los responsables en el cuidado de la información.

También, Ley Orgánica de Comercio Electrónico, Firmas y Mensaje de Datos (2002) en su Art. 9 no establece los mecanismos en la administración de la información de los usuarios. Por tanto, no regula el derecho al acceso, rectificación, oposición y cancelación. Puesto que se genera una nueva disyuntiva ante una norma incompleta e imprecisa. Como resultado, no garantiza la protección de los datos personales en el escenario ecuatoriano.

Por lo expuesto, en la actualidad no existe un marco legal y jurídico de datos personales. Los usuarios en el trayecto del día a día dejan innumerables rastros de nuestras actividades diarias en las colecciones de bases de datos en rápido crecimiento. Una multitud de empresas e instituciones recopilan los diferentes fragmentos de datos, y toda la estructura que se ha configurado para recopilar datos se ha denominado el "conjunto de vigilancia" (Haggerty & Ericson, 2000). Por tanto, se requiere una normativa que precautele, proteja, controle y sancione hechos y actos que afectan de manera negativa a usuarios y quizás no tienen ni la más remota idea que sus datos han sido divulgados sin consentimiento. En el nuevo Proyecto de Ley Orgánica de Protección de Datos Personales, el cual tiene como objetivo preservar la privacidad para la publicación de datos y que los usuarios puedan ejercer el Derecho eliminación de datos personales (olvido digital) atendiendo principio de finalidad.

## **CAPITULO 2**

### **2.1 El derecho a la protección de datos personales en las leyes pertinentes y su esfera de aplicación internacional**

La Asamblea General de las Naciones Unidas (1966). Pacto Internacional de Derechos Civiles y Políticos de las Naciones Unidas que establece en su artículo 17 establece que:

Numeral 1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio su correspondencia ni de ataques ilegales a su honra y reputación. Numeral 2. Toda persona tiene derecho a la protección de la Ley contra esas injerencias o esos ataques (Asamblea General de las Naciones Unidas, 1966).

Asimismo, la Convención Americana Sobre Derechos Humanos (1969). Pacto de San José de Costa Rica, artículo 11 numeral 2 y 3 el cual expresa que:

2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación. 3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques (Convención Americana Sobre Derechos Humanos, 1969).

El Reglamento general de protección de datos de la UE (2016) expresa lo siguiente:

Art. 1: El presente Reglamento establece las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y las normas relativas a la libre circulación de tales datos. Art. 2: El presente Reglamento protege los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales.

Los convenios y directrices mencionan que los datos personales tienen que ser protegidos ante las injerencias por parte de tercera personas. En pocas palabras, protección a la intimidad. Para ello, algunos convenios internacionales como los mencionados, garantizaran su protección. Por lo

tanto, los individuos tienen derecho, al acceso, rectificación, cancelación, eliminación de datos personales, indicando que los datos se pueden obtener cuando el titular así lo desea o la ley lo permita.

## 2.2 Principios del derecho a la protección de datos personales

Para Carlos Villalba (2000) en su investigación “La Protección Intelectual de los Bancos de Datos sobre sus propios Datos” expresa que los principios son las bases sobre las que se asientan los derechos, valores que permiten el desarrollo de ciertas instituciones jurídicas, que tienen como objeto comprender el alcance de protección de cualquier figura que ha de aplicarse en el campo del Derecho (pág. 41). Por consiguiente, el derecho a la protección de datos en aquel momento necesitaría de la adopción de una serie de principios que han de ser puestos a consideración a continuación en la siguiente tabla:

<b>Principio del Derecho</b>	<b>Conceptualizaciones</b>
Consentimiento informado	“El consentimiento se refiere a la manifestación de la voluntad del titular de los datos personales, este debe ser informado, explícito e inequívoco. El consentimiento es el elemento esencial del derecho a la protección de datos personales, dado que traduce la autodeterminación informativa, esto es que el titular del dato está facultado a conocer y aceptar todo lo que vaya a realizarse con la información relacionada con él” ” (Santos García, 2005, pág. 58).
Finalidad	“Este principio es gran base de los demás, ya que en el marco de este se establecerá el consentimiento, la

	<p>calidad, la proporcionalidad y conservación. Esto debido a que como es conocido la protección de datos personales actúa frente al tratamiento de los mismos y a que este como consecuencia está en la obligatoriedad de responder a ciertos objetivos” (Santos García, 2005, pág. 56).</p>
<p>Calidad</p>	<p>“En relación con lo mencionado, los datos personales, además, actualmente son considerados como activos dentro del patrimonio de las empresas, es así que al encargarse de efectivizar el principio de calidad se genera como consecuencia inevitable un acto de inversión” (Vizcaíno Calderón, 2001, pág. 96).</p>
<p>Seguridad</p>	<p>“Basados en este criterio, es importante reconocer que la esencia de la protección de datos personales es su espíritu preventivo, por ende, es imprescindible generar un resguardo a esta clase de información frente a cualquier posible vulneración, de manera que, las bases de datos en la que se conserve deberán responder frente al carácter preventivo y garantizar la vigencia de los derechos del titular y demás derechos articulados a la</p>

	protección de datos personales y sus instrumentalidades” (Calderón, 2001, pág. 105)
Proporcionalidad	“Este principio pone en evidencia la obligatoriedad de que el tratamiento se vea severamente configurado con respecto a la finalidad inicialmente expuesta al titular, esto quiere decir que el responsable dirigirá su atención a los objetivos inicialmente planteados y no actuara con arbitrariedad con respecto al tratamiento” (Riascos, 2012, pág. 33)

Elaborado: Por la Autora

Se puede sintetizar que en relación al principio de consentimiento informado, el ciudadano es consiente que toda información proporcionada está bajo su conocimiento. En lo relacionado a la finalidad, esta soportado por cuatro ejes como son: el consentimiento, la calidad, la proporcionalidad y conservación. Por tanto, los datos personales del ciudadano responden frente al manejo de los mismos. Estos están en la obligación de responder a ciertos objetivos. Respecto a la calidad, las entidades que tienen la capacidad de administrar datos personales de los usuarios, son considerados un activo para la toma de decisiones. Por tanto, la seguridad es imprescindible. La razón que las entidades administran y salvaguardan información de los ciudadanos. Entonces, deben responder por cualquier filtración de información de los usuarios a consecuencia de existir perdida de datos. Finalmente, la proporcionalidad representa la no arbitrariedad en el manejo de la información y solo se configurará con respecto a la finalidad inicialmente expuesta al titular.

### **2.3 El derecho a la protección de datos personales en las leyes pertinentes y su esfera de aplicación nacional**

La Constitución de la República del Ecuador (2008) en su artículo 66, numeral 11 Se reconoce y garantizará a las personas:

El derecho a guardar reserva sobre sus convicciones. Nadie podrá ser obligado a declarar sobre las mismas. En ningún caso se podrá exigir o utilizar sin autorización del titular o de sus legítimos representantes, la información personal o de terceros sobre sus creencias religiosas, filiación o pensamiento político; ni sobre datos referentes a su salud y vida sexual salvo por necesidades de atención médica.

Por ende, estos derechos tienen concordancia con los principios de Protección de datos personales, detallados en el punto anterior, entre ellos, el de finalidad. Es decir que el Estado garantiza el manejo de información de manera eficiente y efectiva; de lo contrario contrario, generaría una violación al derecho de protección a la intimidad de la información. Entonces, en el mismo art. 66, numeral 22 expresa lo siguiente:

El derecho a la inviolabilidad y al secreto de la correspondencia física y virtual; esta no podrá ser retenida, abierta ni examinada, excepto en los casos previstos en la ley, previa intervención judicial y con la obligación de guardar el secreto de los asuntos ajenos al hecho que motive su examen. Este derecho protege cualquier otro tipo o forma de comunicación (Constitución de la República del Ecuador, 2008)

La ley orgánica de la gestión de la identidad y datos civiles (2016) expresa lo siguiente:

Art. 1.- Objeto. La presente Ley tiene por objeto garantizar el derecho a la identidad de las personas y normar y regular la gestión y el registro de los hechos y actos relativos al estado civil de las personas y su identificación. Art 3.- numeral 4. Proteger la confidencialidad de la información personal. Numeral5. Evitar el subregistro o carencia de datos en registro de una persona. Numeral 6. Proteger la información almacenada en archivos y bases de datos de los hechos y actos relativos al estado civil de las personas (La ley orgánica de la gestión de la identidad y datos civiles, 2016).

El artículo 11 numeral 9 de la Constitución, determina que el más alto deber del Estado consiste en respetar y hacer respetar los derechos garantizados en ella, lo cual implica la obligación estatal de adecuar formal y

materialmente, las leyes y normas de inferior jerarquía a la Constitución y los instrumentos internacionales, e implementar las normas que sean necesarias para garantizar la dignidad del ser humano (Constitución de la República del Ecuador, 2008)

Para ello, la Ley del Sistema Nacional de Registros de Datos Públicos (2010) en su art. 28 expresa lo siguiente:

Creación, finalidades y objetivos del Sistema Nacional de Registro de Datos Públicos.- Créase el Sistema Nacional de Registro de Datos Públicos con la finalidad de proteger los derechos constituidos, los que se constituyan, modifiquen, extingan y publiciten por efectos de la inscripción de los hechos, actos y/o contratos determinados por la presente Ley y las leyes y normas de registros; y con el objeto de coordinar el intercambio de información de los registros de datos públicos. En el caso de que entidades privadas posean información que por su naturaleza sea pública, serán incorporadas a este sistema. Con la finalidad de garantizar el ejercicio del derecho constitucional del acceso a la información, se crea la Ficha de Registro Único del Ciudadano, documento público electrónico y/o físico certificado, que contendrá todos los datos de registro público del ciudadano constantes en el Sistema Nacional de Registro de Datos Públicos (Ley del Sistema nacional de registros de datos públicos , 2010).

Entonces resulta que esta Ley del Sistema Nacional de Registros de Datos Públicos, tiene como finalidad proteger el derecho de los ciudadanos dentro del marco jurídico establecido y constituido.

Otro punto sería lo establecido en el Código Orgánico Integral Penal-COIP (2014), lo siguiente:

Art. 178.- Violación a la intimidad.- 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 vídeo, 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. No son aplicables estas normas para la persona que divulgue grabaciones de audio y vídeo en las que interviene personalmente, ni cuando se trata de información pública de acuerdo con lo previsto en la ley (Código Orgánico Integral Penal-COIP; , 2014) .

Igualmente, se cuenta con un mecanismo sancionador para quienes sin consentimiento del afectado acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio. La sanción sería de uno a tres años. No obstante, esto no se aplica a ciudadanos que divulgue grabaciones de audio y vídeo en las que interviene personalmente, ni cuando se trata de información pública. Por tanto, esto sigue generando una afectación tanto directa como indirecta al ciudadano afectado.

### **Habeas data**

El Habeas Data constituye, en suma, un cauce procesal para salvaguardar la libertad de la persona en la esfera informática, que cumple una función paralela, en el seno de los derechos humanos de \_la tercera generación, a la que en los de la primera generación correspondió al Habeas Corpus respecto a la libertad física o de movimientos de la persona (Luño, 1992).

Pablo Palazzi (1998) señala que: El habeas data puede ser concebido como una acción judicial para acceder a registros o bancos de datos, conocer los datos almacenados y en caso de existir falsedad o discriminación corregir dicha información o pedir su confidencialidad

Ekmekdjian & Pizzolo, (1998) expresa que habeas data se refiere al instrumento diseñado para controlar la calidad de la información personal contenida en bancos de datos, corregir o cancelar datos inexactos o indebidamente procesados, y disponer sobre su transmisión.

En el caso ecuatoriano, la Constitución de la República del Ecuador (2008) en su artículo 92 expresa lo siguiente:

Acción de hábeas data. 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).

De la misma manera en el (Código Orgánico Integral Penal-COIP (2014) que expresa lo siguiente:

Art. 229.- Revelación ilegal de base de datos.- La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años.

En concordancia con el Código Orgánico De La Función Judicial (2009) que estipula:

Art. 13.- Principio de Publicidad.- Las actuaciones o diligencias judiciales serán públicas, salvo los casos en que la ley prescriba que sean reservadas. De acuerdo a las circunstancias de cada causa, los miembros de los tribunales colegiados podrán decidir que las deliberaciones para la adopción de resoluciones se lleven a cabo privadamente. No podrán realizarse grabaciones en video de las actuaciones judiciales. Se prohíbe a las juezas y a los jueces dar trámite a informaciones sumarias o diligencias previas que atenten a la honra y dignidad de las personas o a su intimidad (Código Orgánico De La Función Judicial;, 2009).

Código de Procedimiento Penal (2000) determina lo siguiente:

Art. 255 Publicidad.-La audiencia del tribunal de garantías penales será pública; pero será reservada cuando el proceso tenga por objeto el juzgamiento de los delitos comprendidos en los Títulos I y VIII del Libro Segundo del Código Penal, y se realizará con la sola presencia del acusado, del acusador particular si lo hubiere, de los defensores, del Fiscal, y del secretario, y si fuere del caso, de los peritos y de los testigos, sin que pueda violarse la reserva, durante o después de la audiencia. No se admitirá la transmisión de la audiencia, a través de los medios de comunicación. En ningún caso, la jueza o juez o magistrado que conozca de una causa penal sometida a su resolución puede

formular declaraciones públicas o privadas a los medios de comunicación social, ni antes ni después del fallo. La violación de esta prohibición será sancionada con su destitución, sin perjuicio de las responsabilidades civiles y penales que hubieren (Código de Procedimiento Penal, 2000).

Es decir que se puede encontrar mecanismos para ejercer la respectiva defensa jurídica del derecho a la protección de los datos personales. Por tanto, se establecería una garantía administrativa en lo relacionado al acceso, manejo y actualización de la información privada de los datos personales de los titulares por parte del Estado. Mediante, el Habeas Data es considerada una vía jurídica proteccionista a favor del titular para que ejerza el derecho a conocer de la existencia y a acceder, rectificar, eliminar o anular datos genéticos, bases de datos, documentación personal sobre sí mismo, o en lo relacionado a activos, en soporte electrónico o material y la finalidad en la utilización de sus datos.

No obstante, es necesario considerar que el requerimiento de datos personales es vía judicial, es decir, por solicitud de un Juez, Fiscal o Comisión Investigadora. Sin olvidar que es bajo disposiciones legales, enfocado a la investigación establecida por las autoridades de la administración de justicia. Esto se debe a que para impartir justicia, la información requerida debe estar limitada y puntual en lo necesario sin afectar al titular en el requerimiento de datos personales que no guarden relación al caso investigado para impartir justicia, ya que es un derecho colectivo, que procura el bien común.

#### **2.4 Incidencia del proyecto Ley Orgánica de Protección de Datos Personales**

Con fecha 19 de septiembre del 2019 mediante Oficio No. T.514-SGJ-19-0740 relacionado al Proyecto Ley Orgánica de Protección de Datos Personales (2019), enviado por el Presidente de la República del Ecuador Lc. Lenin Moreno Garcés a la Asamblea Nacional del Ecuador. Este cuerpo legal comprendería de noventa artículos, siete disposiciones generales, siete disposiciones reformativas y Cinco disposiciones derogatorias.

Como primer punto, se definiría el objetivo de estudio a través del Art. 1.- Objeto: El objeto de la presente Ley es regular el ejercicio del derecho a la protección de datos personales, la autodeterminación informativa y demás derechos digitales en el tratamiento y flujo de datos personales, a través del desarrollo de principios, derechos, obligaciones y mecanismos de tutela (Ley Orgánica de Protección de Datos Personales;, 2019). Asimismo, el tratamiento de los datos debería tener un fin. Para ello, el proyecto de Ley en su Art 2.-Finalidad: La finalidad de la presente Ley es procurar el adecuado tratamiento y flujo de datos personales para garantizar los derechos fundamentales y las libertades; promover el progreso económico y social; impulsar la producción nacional y la cooperación internacional; fomentar la competitividad, la innovación y productividad; elevar la eficiencia de los servicios públicos y/o privados; y, mejorar la calidad de vida tutela (Ley Orgánica de Protección de Datos Personales;, 2019). Por tanto, este proyecto de Ley tendría bien definido su función de regulador en el manejo de datos personales.

De igual manera, el manejo de la información sería a través de un responsable. Una definición más clara, se daría mediante Art 5.- Responsable del tratamiento de datos personales: Persona natural o jurídica, pública o privada, que decide sobre la finalidad y el tratamiento de datos personales (Ley Orgánica de Protección de Datos Personales;, 2019). Además, este proyecto de Ley (2019) establece en su

Art 8.- Principios: Sin perjuicio de otros principios establecidos en la Constitución de la República, los instrumentos internacionales ratificados por el Estado u otras normas jurídicas, la presente Ley se regirá por los principios de juridicidad, lealtad y transparencia; legitimidad; finalidad, pertinencia y minimización de datos personales; proporcionalidad del tratamiento; consentimiento; confidencialidad; calidad; conservación; seguridad de datos; responsabilidad proactiva y demostrada; aplicación favorable al titular; e, independencia de control (Ley Orgánica de Protección de Datos Personales;, 2019).

En pocas palabras, este proyecto de Ley se alinea a la Constitución en concordancia a los principios de juridicidad, lealtad y transparencia. También, se limitaría al uso de la información como lo especificaría en su Art 11.- Finalidad: las finalidades del tratamiento deberán ser determinadas, explícitas

y legítimas, no podrán tratarse datos personales con fines distintos para los cuales fueron recopilados, a menos que concurra una de las causales que habiliten un nuevo tratamiento conforme el principio de legitimidad (Ley Orgánica de Protección de Datos Personales;, 2019).

En caso de que el titular de la información desee pedir eliminación de sus datos. Esto sería mediante el Art 26.- Derecho de Eliminación que expresaría lo siguiente:

El titular tiene derecho a solicitar la supresión de sus datos personales, a fin de estos dejen de ser tratados por el responsable del tratamiento de datos personales, cuando:

1. El tratamiento no cumpla con los principios de juridicidad, lealtad, transparencia y legitimidad;
2. El interesado retire el consentimiento en que se basa el tratamiento o solicite su supresión;
3. El interesado se oponga al tratamiento, y no prevalezcan otros motivos legítimos para el tratamiento;
4. Los datos personales hayan sido tratados ilícitamente;
5. Los datos personales sean de carácter obsoleto;
6. Haya revocado o no haya otorgado el consentimiento para uno o varios fines específicos, sin necesidad de que medie justificación alguna.

El responsable del tratamiento de datos personales implementará métodos y técnicas orientadas a eliminar, anular, borrar, hacer ilegible, destruir o dejar irreconocibles de forma definitiva y segura, de conformidad con la normativa técnica emitida por la Autoridad de Protección de Datos Personales.

Finalmente, bajo el escenario que el titular de información requiera que sus datos personales sean considerados al olvido digital. Esto solo sería mediante un dictamen judicial cuando ocurran las siguientes condiciones:

Art. 27.- Derecho al olvido digital: El titular tiene el derecho a solicitar el juez competente, obtener sin dilatación indebida del responsable del tratamiento la supresión de sus datos personales que estén siendo tratados en el entorno digital, cuando concurra alguna de las circunstancias siguientes:

1. Los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados;
2. El interesado retire el consentimiento en que se basa el tratamiento o solicite su supresión;
3. El interesado se oponga al tratamiento, y no prevalezcan otros motivos legítimos para el tratamiento;
4. Los datos personales no tengan valor histórico o científico;
5. Los datos personales no sean de relevancia pública; o,

6. Los datos personales sean inadecuados, inexactos, impertinentes o excesivos con relación a los fines y al tiempo transcurrido.

Lo anterior no se aplicará cuando el tratamiento sea necesario por cualquiera de las siguientes causas:

1. Para ejercer el derecho a la libertad de expresión e información;
2. Para el cumplimiento de una obligación legal que requiera el tratamiento de datos por parte del responsable del tratamiento;
3. Por razones de interés público en el ámbito de la salud pública;
4. Con fines de archivo en interés público, fines de investigación científico o histórica o fines estadísticos; o,
5. Para la formulación, el ejercicio o la defensa de reclamaciones.

Para la aplicación del presente artículo, se estará a las siguientes definiciones:

**Datos personales tratados en el entorno digital:** Datos personales que son tratados en redes de computadoras públicas o privadas (Internet o Intranet). Se entiende por redes privadas aquellas que no están abiertas al acceso de todo público pero que si son usadas por una colectividad de usuarios autorizados.

**Datos personales de carácter obsoleto:** Datos personales que ya no están en uso, son antiguos, anticuados, o han dejado de tener vigencia o relevancia para los fines del tratamiento.

**Datos personales que no tengan valor histórico o científico:** Datos personales que no son útiles, necesarios o de valor significativo para la ciencia o la historia política o social de Ecuador.

**Datos personales que no sean de relevancia pública:** Datos personales que el público en general no necesita o no tiene interés justificado en conocer.

Por consiguiente, bajo este artículo tendría una incidencia importante relacionado al derecho eliminación de datos personales (olvido digital) atendiendo principio de finalidad.

## **2.5 Análisis del principio de finalidad y su relación con el proyecto de Ley Orgánica de Protección de Datos Personales**

El objetivo principal de preservar la privacidad para la publicación de datos es proteger la privacidad de los datos individuales y retener los patrones estadísticos implicados en los conjuntos de datos originales, al tiempo que permite el acceso público a los conjuntos de datos publicados. Por ejemplo, los hospitales, clínicas y centros de salud han recolectado grandes volúmenes de registros médicos. Para facilitar la investigación, es valioso permitir que los

investigadores estudien los datos médicos, de los cuales se pueden aprender patrones o conocimientos útiles. No obstante, al publicar esos datos útiles, se debe proteger la privacidad personal, como las enfermedades contraídas por pacientes individuales.

Este término se refiere a los efectos combinados de esfuerzos públicos y privados, mercados e instituciones que, juntos, forman un conjunto de vigilancia. Gran parte de la información es recopilada por empresas privadas, pero el gobierno "es un importante beneficiario secundario" (Cohen, 2013, pág. 1916). Trabajo bajo la suposición de que puede considerar significativamente el Big Data como un fenómeno que implica una amenaza unitaria a la libertad. Esta suposición no es indiscutible, y acepto totalmente que no hay una gran empresa, organización o gobierno que recopile u organice la recopilación de datos. Sin embargo, estoy de acuerdo con la opinión de Haggerty y Ericson (2000) de que estamos viendo una 'convergencia de sistemas de vigilancia que alguna vez fueron discretos', no una convergencia en el sentido de consolidación corporativa, sino en el sentido de que Posteriormente, se combinan, comparten, intercambian y vuelven a ensamblar innumerables flujos de información sobre individuos para proporcionar una descripción completa y completa de los individuos y sus acciones (pág. 605) .

En el caso ecuatoriano, el Proyecto de Ley Orgánica de Protección de datos personales conduciría a cambios no solo para las organizaciones sino también para los consumidores individuales. Debido a esta regulación, los ciudadanos tendrán una mayor oportunidad de obtener información sobre el uso y el procesamiento de datos privados, y tendrán más poder de decisión sobre qué datos se almacenan, dónde se almacenan y quién tiene acceso a ellos.

## **2.6 Jurisprudencia comparada y análisis de jurisprudencia ecuatoriana**

Por lo expuesto en puntos anteriores como en el caso de la Unión Europea donde se implementó un Reglamento Europeo de Protección de Datos (RGPD). Por lo tanto, ha sido un avance positivo en relación a la protección de datos. Por lo cual la jurisprudencia tendría como función llenar los vacíos

normativos y ambigüedades. Bajo este escenario, se pretende demostrar que es viable tener una garantía Constitucional. Para ello, es imprescindible seguir la estela e ir al mismo nivel que la Unión Europea entre otros países de la región en la aplicación de mecanismos jurídicos en lo referente a la protección de datos personales, en específico al derecho al olvido digital. . Asimismo, se analizará la finalidad que tendría en el Proyecto de Ley Orgánica de Protección de datos personales próximamente en Ecuador. Además, acentúa la creación de la Autoridad de Protección de Datos Personales que sería dependiente de la Función Ejecutiva con personería jurídica y gozará de autonomía administrativa y financiera.

España, por ejemplo, el 13 de mayo de 2014, el Tribunal de Justicia de la Unión Europea UE reconoció en un fallo pionero que los ciudadanos tienen derecho a ser olvidados en la Red. Como origen del proceso:

Este proceso tiene su punto de partida en la denuncia presentada por Mario Costeja, que había solicitado a Google la retirada de un anuncio de subasta por un impago contra él registrado en 1998. Este caso ha acabado en un litigio entre la Agencia Española de Protección de Datos AEPD y la compañía de internet. Este español denunció que un periódico de tirada nacional, «La Vanguardia», había publicado dos anuncios relativos a una subasta de inmuebles relacionada con un embargo ocasionado por una deuda contraída con la Seguridad Social. Tras digitalizarse la página, el denunciante pidió al diario que retirara una información al alegar que una vez introducido su nombre en el buscador aparecería una referencia a estos anuncios y, al considerar que la deuda contraída ya estaba resuelta, carecía por tanto de relevancia (Serbeto & Sánchez , 2014).

Después de 5 años de litigio, “El Tribunal de Justicia de la UE dictaba la sentencia en el asunto Mario Costeja (C-131/12) que tiene por objeto una petición de decisión prejudicial planteada por la Audiencia Nacional sobre la interpretación de la Directiva 95/46/CE de protección de datos personales. El fallo da respuesta a la controvertida cuestión del derecho al olvido o cancelación de datos en Internet y, más en concreto, en los motores de búsqueda” (Álvarez, 2014, pág. 165). En este caso, la AEPD defendió este litigio y marcó un precedente. Como resultado, los motores de búsqueda como Google, Bing o Yahoo disponen de formularios en línea para pedir la retirada de las informaciones que a los ciudadanos. Entonces, esta sentencia marcó un antes y un después en la jurisprudencia comunitaria sobre internet. El país

ibérico hasta el año 2019, “el quinto país europeo con mayor número de solicitudes, ha remitido a Google 76.893 peticiones sobre 249.359 URL o direcciones” (Radio\_Huancavilca, 2019).

En Colombia, el caso Gloria V. El Tiempo Sentencia T-277/15: Una ciudadana Colombiana llamada “Gloria” interpuso acción de tutela contra la Casa Editorial El Tiempo. En su argumento, ella considera violados sus derechos a la intimidad, al buen nombre, de petición y al trabajo. De igual manera, la falta del debido proceso. Es decir que la alegada vulneración se habría producido de la publicación de una nota periodística del medio de comunicación El Tiempo. En ella informaba sobre la supuesta participación de la accionante en hechos constitutivos de delito. “La accionante afirma que en el año dos mil (2000) trabajaba para una agencia de viajes en calidad de vendedora de tiquetes aéreos. Para lo cual, resultó estar vinculada con una red dedicada al delito de trata de blancas (Sentencia T-277/15 Gloria V. El Tiempo, 2015). No obstante, nunca fue declarada culpable. Luego, resultó “exonerada” por la fiscalía al no encontrar vinculación por el delito de trata de blancas. Por ende, El tiempo nunca informó y publicó la exoneración de los cargos contra ciudadana. Igualmente, como la posterior indexación de dicho contenido por el motor de búsqueda Google.com. Esto generó graves secuelas psicológicas y traumáticas en Gloria y su familia. Afectando el desarrollo de una vida social y laboral normal en su día cotidiano, como la búsqueda de empleo y la realización de trámites ante públicas y privadas. La Corte Suprema de Justicia (2015) Resuelve:

Primero.- LEVANTAR la suspensión de términos del presente proceso de tutela, ordenada mediante auto de veintitrés (23) de julio de dos mil catorce (2014). Segundo.- CONFIRMAR PARCIALMENTE la sentencia del dos (02) de diciembre de dos mil trece (2013) proferida por el Tribunal Superior de Cali-Sala Penal, que a su vez confirmó el fallo del once (11) de octubre de dos mil trece (2013) dictado por el Juzgado Sexto Penal del Circuito de Cali, la cual concedió del amparo de los derechos fundamentales a la intimidad, debido proceso y petición de la señora Gloria. Tercero.- REVOCAR el numeral primero de la parte resolutive de la sentencia proferida por el Tribunal Superior de Cali-Sala Penal, el cual ordenó adicionar el fallo del juez de primera instancia en el sentido de ordenar a la Casa Editorial El Tiempo eliminar y borrar de su página web la información negativa acerca de la señora Gloria, en relación con la investigación penal por el delito de trata de personas y

concierto para delinquir. Para en su lugar, ORDENAR a la Casa Editorial El Tiempo que actualice la información publicada en su página web respecto a los hechos que relacionan a la accionante con el delito de trata de personas, de tal manera que se informe que la misma no fue vencida en juicio. De igual forma, se dispone ORDENAR a la Casa Editorial el Tiempo que, por medio de la herramienta técnica “robots.txt”, “metatags” u otra similar, neutralice la posibilidad de libre acceso a la noticia “Empresa de Trata de Blancas” a partir de la mera digitación del nombre de la accionante en los buscadores de internet. Cuarto.- Por la Secretaría General, LÍBRESE la comunicación a que alude el artículo 36 del Decreto 2591 de 1991. (Sentencia T-277/15 Gloria V. El Tiempo, 2015).

Por lo expuesto, la Corte Suprema de Justicia colombiana concedió el amparo de los derechos fundamentales a la intimidad, debido proceso y petición de la señora Gloria. Luego, dispuso ordenar a la Casa Editorial El Tiempo eliminar y suprimir de su página web la información negativa acerca de la señora Gloria, en relación con la investigación penal por el delito de trata de personas y concierto para delinquir. Después, ordenó actualizar la información publicada en su página web de El Tiempo sobre los hechos que relacionan a la accionante con el delito de trata de personas, de tal manera que se informe que la misma no fue vencida en juicio. De la misma forma, dispuso ordenar a El Tiempo que, por medio de la herramienta técnica “robots.txt”, “metatags” u otra similar, neutralice la posibilidad de libre acceso a la noticia “Empresa de Trata de Blancas” a partir de la mera digitación del nombre de la accionante en los exploradores de internet.

En ambos casos, se manifiesta que el derecho al olvido permitiría objetar publicaciones que afecten a personas naturales y jurídicas. En el caso de Mario Costeja marcó unos precedentes contras motores de búsqueda como Google, Yahoo entre otros, donde los usuarios pueden solicitar que información personal o que afecte a su persona sea eliminado inmediatamente. Aunque, no haya sido suficiente quien produjo los datos haya eliminado como fue el medio de información “La Vanguardia”. Por otra parte, el caso colombiano la Corte Suprema no se dirigió a las empresas motores de búsqueda, sino que dispuso que El Tiempo tome las medidas correctivas y proceda a ejecutar mecanismos. En este caso, herramientas técnicas como “robots.txt”, “metatags” u otra similar para que neutralice la posibilidad de libre

acceso a la publicación “Empresa de Trata de Blancas” a partir de la mera digitación del nombre de la accionante en los exploradores de internet.

Sin embargo, existe otro escenario como en la Sentencia del Tribunal de Primera Instancia de Namur, de 24 de noviembre de 1997. En la jurisprudencia francesa, se ha conservado este planteamiento, argumentando que personas privadas de la libertad. Es decir, un individuo condenado judicialmente tiene un verdadero derecho al olvido. “Esto se desprende del artículo 9 del Pacto Internacional de Derechos Civiles y Políticos de Nueva York y del artículo 8 de la Convención de Roma que permite a una persona no dedicada a una actividad pública exigir el secreto y la tranquilidad, sin los que el libre progreso de la personalidad quedaría obstruido” (Bertrand, 1999).

En caso ecuatoriano, se ha dado una serie de eventos donde se ha vulnerado la privacidad de las personas. De acuerdo a la publicación en el Diario El Universo de fecha 10 de diciembre del (2019) que divulgó lo siguiente:

El video de una mujer dentro de un centro de diversión nocturna se viralizó la semana anterior en el Ecuador; en 2016 pasó algo similar con una ex jueza que agredió verbal y físicamente a policías; y en un tercer caso, en Quito un hombre grabó la salida de su pareja de un motel con otra persona..... En el más reciente caso, la joven, mediante su defensor, pide que se investigue y que se rastree a las personas que difundieron inicialmente los videos, lo que "ha provocado un daño tremendo a la ciudadana Julissa", (El\_Universo, 2019)

La agredida en el video interpuso una denuncia contra el centro nocturno. Asimismo, en el Diario Extra (2019) publicó el siguiente encabezado “Las redes sociales aniquilaron a Julissa”, el cual sus abogados Luis Cajilema, Arturo Lara y Mario Lescano coincidieron. Uno de ellos expresó lo siguiente:

“Más allá del daño causado por la difusión de los videos que se suponen eran íntimos y del bullying hecho en las redes sociales, la joven es víctima de los efectos del morbo. “Si nadie hubiera difundido, todo se queda como decía en slogan del evento: lo que pasa en Las Orquídeas, se queda en Las Orquídeas, nada de esto hubiera pasado”, expresó Lescano (Diario\_Extra, 2019).

El otro abogado, Arturo Lara, “se mantiene en que la acusación presentada en Fiscalía busca marcar un precedente y evitar que se siga violando el

derecho a la intimidad de las personas, al difundir contenidos sin autorización a las redes sociales” (Diario\_Extra, 2019). Hasta la fecha no se ha podido identificar a la persona que grabó y difundió el video sin autorización de la afectada. Una vez que se identifique al o las personas involucradas. Estás serían sancionados con una pena privativa de libertad de uno a tres años como lo expresa el Código Orgánico Integral Penal COIP, en su artículo 178.

El último caso, sucedió el 18 de enero del 2020, en el Estadio Monumental de Barcelona S.C. en la ciudad de Guayaquil donde una pareja de aficionados fueron captados en un “Kiss Cam” por las cámaras de televisión. Su video e imagen ha sido difundida y viral a quienes todos observaron y asumieron que estaban siendo infieles. Pero este hecho fue desmentido por la antigua pareja del Señor grabado quien replicó en redes sociales que las fotos de ambos son antiguas. Además, personas cercanas a la pareja captada expresaron que ellos son novios (El\_Universal, 2020).

En ambos casos suscitados en Ecuador, tienen un impacto negativo que afecta los derechos fundamentales a la intimidad. Siendo sus imágenes utilizadas para memes, burlas, bullying, chistes de mal gusto entre otros que deterioran el buen nombre y reputación de ambos. Por otra parte, la actual jurisprudencia ecuatoriana dentro las varias garantías constitucionales, la acción de Hábeas Data como se lo explica en uno de los primeros puntos desarrollados y es aquella que se tiene una similitud más a fin del cumplimiento del derecho al olvido mediante sentencia de un juez constitucional. Ante este escenario el Proyecto de la Ley Orgánica de Protección de Datos indicaría cual sería la vía para la eliminación de datos, tanto desde motores de búsqueda como Google, Bing, Yahoo. Igualmente, de redes sociales como Facebook, WhatsApp e Instagram. Finalmente, de los medios de comunicación que han publicado dicha información y sobre utilizaron los datos de los afectados, Es decir que deben eliminar y suprimir de su página web la información negativa acerca de los perjudicados. Asimismo, los medios deberán, por medio de la herramienta técnica “robots.txt”, “metatags” u otra equivalente, neutralice la posibilidad de libre acceso a la noticia de ambos casos a partir de la mera digitación del nombre de la accionante en los exploradores de internet. Bajo este escenario, se

aplicaría al derecho eliminación de datos personales (olvido digital) atendiendo principio de finalidad.

## **CONCLUSIÓN**

Es necesario llevar a debate la Ley Orgánica de Protección de Datos Personales en la Asamblea Nacional para su aprobación. Asimismo, considerar el principio de finalidad como la protección de datos con aplicación favorable al titular. De la misma manera no podrán tratarse datos personales con fines distintos para los cuales fueron recopilados, a menos que concurra una de las causales que habiliten un nuevo tratamiento conforme el principio de legitimidad. Es importante indicar que en algunos Convenios Internacionales se refieren a la protección de los datos personales frente las injerencias o intromisión de terceras personas. En Ecuador, los ciudadanos se sienten vulnerables respecto al tema hasta el momento en que no se apruebe esta Ley. Una vez aplicada, se podría solicitar el derecho al olvido digital en caso de ser necesario sin perjuicio a terceros dentro del marco legal.

## **RECOMENDACIÓN**

La Constitución, convenios y varias doctrinas, tratan y dicen que los datos personales deben ser protegidos frente las injerencias de terceras personas, indicando consigo el ámbito de protección a la intimidad. Es por esa razón que el estudio a realizado indica cual es el problema para que al momento de proteger la vida íntima y privada sea de manera más específica

Como bien lo indica algunos convenios internacionales que garantizará su protección, y de la misma manera tenemos derecho, al acceso, rectificación, cancelación, eliminación de datos personales, indicando que los datos lo podemos obtener cuando el titular así lo deseo o la ley lo permita.

## BIBLIOGRAFÍA

- AEPD. (2009). *Agencia Española de Protección de Datos*. Obtenido de <https://www.aepd.es/normativa/index.html>
- Álvarez, M. (2014). Reflexiones sobre la sentencia del TJUE en el asunto "Mario Costeja" (C-131/12) sobre derecho al olvido. *Revista Española de Derecho Europeo*(51), 165-187.
- Asamblea General de las Naciones Unidas. (16 de Diciembre de 1966). *Pacto Internacional de los Derechos Civiles y Políticos de la Naciones Unidas*. Obtenido de <http://www.ordenjuridico.gob.mx/TratInt/Derechos%20Humanos/D47.pdf>
- Awad, N., & Krishnan, M. (2006). The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to be Profiled Online for Personalization. *MIS Quarterly*, 30(1), 13–28.
- Bélanger, F., & Crossler, R. (2011). Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. *MIS Quarterly*, 35(4), 1017–1041.
- Bello-Orgaz , G., Jung, J., & Camacho, D. (2016). Social big data: recent achievements and new challenges. *Inf. Fusion*, 28, 45–59.
- Bertrand, A. (1999). *Droit à la vie privée et droit à l'image*. París: Litec.
- Brundage, M., Avin, S., Clark, J., & Toner, H. (Febrero de 2018). *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation*. Recuperado el 9 de Noviembre de 2019, de Future of Humanity Institute: <https://arxiv.org/ftp/arxiv/papers/1802/1802.07228.pdf>
- Calderón, V. (2001). *Comentarios de la Ley Orgánica de protección de datos de carácter personal*. Madrid: Ellacuría.

- Código de Procedimiento Penal. (2000). *Código de Procedimiento Penal*. Obtenido de Registro Oficial 360: <https://www.registrocivil.gob.ec/wp-content/uploads/downloads/2014/01/este-es-19-Codigo-De-Procedimiento-Penal-Reglamentos-Generales.pdf>
- Código Orgánico De La Función Judicial;. (9 de Marzo de 2009). *Código Orgánico De La Función Judicial*. Obtenido de Registro Oficial Suplemento 544: [https://www.oas.org/juridico/mla/sp/ecu/sp\\_ecu-int-text-cofj.pdf](https://www.oas.org/juridico/mla/sp/ecu/sp_ecu-int-text-cofj.pdf)
- Código Orgánico Integral Penal-COIP;. (10 de Febrero de 2014). *Código Orgánico Integral Penal-COIP*. Obtenido de Registro Oficial Suplemento 180: [https://www.defensa.gob.ec/wp-content/uploads/downloads/2018/03/COIP\\_feb2018.pdf](https://www.defensa.gob.ec/wp-content/uploads/downloads/2018/03/COIP_feb2018.pdf)
- Código Orgánico Monetario y Financiero;. (12 de Septiembre de 2014). *Código Orgánico Monetario y Financiero. Registro Oficial No 332*. Quito, Ecuador.
- Cohen, J. E. (2013). What privacy is for. *Harvard Law Review*, 126, 1904–1933.
- Conger, S., Pratt, J., & Loch, K. (2013). Personal information privacy and emerging technologies. *Information Systems Journal*, 23, 401–417.
- Constitución de la República del Ecuador. (20 de Octubre de 2008). *Constitución de la República del Ecuador. Registro Oficial 449*. Quito, Ecuador.
- Convención Americana Sobre Derechos Humanos. (7 al 22 de Noviembre de 1969). *Pacto de San José de Costa Rica*. Obtenido de Convención Americana Sobre Derechos Humanos.: [http://www1.hcdn.gov.ar/folio-cgi-bin/om\\_isapi.dll?hitsperheading=on&infobase=constra.nfo&record=%7B7FF67C95%7D&softpage=Document4](http://www1.hcdn.gov.ar/folio-cgi-bin/om_isapi.dll?hitsperheading=on&infobase=constra.nfo&record=%7B7FF67C95%7D&softpage=Document4).
- Deleuze, G., & Guattari, F. (1988). *A Thousand Plateaus: Capitalism and Schizophrenia*. Bloomsbury Publishing.

- Diario\_Extra. (12 de Diciembre de 2019). *Las redes sociales aniquilaron a Julissa*. Recuperado el 23 de Diciembre de 2019, de Diario Extra: <https://www.extra.ec/buena-vida/redes-sociales-aniquilaron-julissa-CI3318206>
- Dueñas, J. (2014). *Sistema de información y bases de datos en consumo*. Obtenido de Iceditorial: <https://www.iceditorial.com/atencion-al-clienteconsumidor-o-usuario-comt0110/6473-sistemas-de-informacion-y-bases-de-datosen-consumo-uf1755-9788416109845.html>
- Ekjmekdjian, M., & Pizzolo, C. (1998). *Hábeas Data. El Derecho a la Intimidad*. Buenos Aires: Depalma.
- El\_Universal. (20 de Enero de 2020). *Agradecemos tu interés en nuestros contenidos, sin embargo; este material cuenta con derechos de propiedad intelectual, queda expresamente prohibido la publicación, retransmisión, distribución, venta, edición y cualquier otro uso de los contenidos* (i. Obtenido de El Universal: <https://www.eluniversal.com.mx/universal-deportes/futbol/hubo-infidelidad-en-el-caso-de-la-pareja-en-un-estadio>
- El\_Universo. (10 de Diciembre de 2019). *¿Qué dice la ley sobre la divulgación de videos por redes sociales?* Recuperado el 22 de Diciembre de 2019, de El Universo: <https://www.eluniverso.com/noticias/2019/12/09/nota/7640648/violacion-intimidad-derecho-imagen-videos-virales-ecuador-milagro>
- Gandomi, A., & Haider, M. (2015). Beyond the hype: big data concepts, methods, and analytics. *Int. J. Inf. Manag.*, 35(2), 137–144.
- Gómez Sáez, F. (2014). *Los reportajes de investigación con cámara oculta y sus repercusiones en los derechos fundamentales*. Recuperado el 4 de Noviembre de 2019, de Uned-Tesis Doctoral: <http://e-spacio.uned.es/fez/eserv/tesisuned:Derecho-Fgomez/Documento.pdf>

Haggerty, K., & Ericson, R. (2000). The surveillant assemblage, . *British Journal Sociology*, 51(4), 605–622.

La ley orgánica de la gestión de la identidad y datos civiles. (4 de Febrero de 2016). *La ley orgánica de la gestión de la identidad y datos civiles*. Obtenido de [https://www.registrocivil.gob.ec/wp-content/uploads/downloads/2016/03/Ley\\_Organica\\_RC\\_2016.pdf](https://www.registrocivil.gob.ec/wp-content/uploads/downloads/2016/03/Ley_Organica_RC_2016.pdf)

Laney, D. (2001). *3D data management: controlling data volume, velocity and variety*. Denver: META Group Res.

Ley del Sistema nacional de registros de datos públicos . (24 de Marzo de 2010). *Ley del Sistema nacional de registros de datos públicos* . Obtenido de <https://www.telecomunicaciones.gob.ec/wp-content/uploads/downloads/2012/11/Ley-Del-Sistema-Nacional-De-Registro-De-Datos-Publicos.pdf>

Ley Orgánica de Comercio Electrónico, F. y. (17 de Abril de 2002). Ley Orgánica de Comercio Electrónico, Firmas y Mensaje de Dato. *Registro Oficial No. 557*. Quito, Ecuador.

Ley Orgánica de Protección de Datos Personales;. (19 de Septiembre de 2019). *Proyecto Ley Orgánica de Protección de Datos Personales*. Obtenido de Presidencia de la República del Ecuador: <http://www.datospublicos.gob.ec/wp-content/uploads/downloads/2019/09/Proyecto-Ley-De-Proteccion-De-Datos-Personales.pdf>

Ley Orgánica de Telecomunicaciones. (18 de Febrero de 2015). Ley Orgánica de Telecomunicaciones. *Registro Oficial No.439*. Quito, Pichincha, Ecuador: Registro Oficial Órgano del Gobierno del Ecuador.

Luño, A. (1992). Del habeas corpus al habeas data. Informática y derecho:. *Revista iberoamericana de derecho informático*, 1, 153-161.

Martín, I. (2014). La contratación pública electrónica, en Tratado de Contratos. *Thomson-civitas*, XVI, 277 a 326.

- Martin, K. (2015). Ethical Issues in the Big Data Industry. *MIS Quarterly Executive*, 14(2), 67–85.
- Mateosian, R. (2013). Ethics of Big Data. *IEEE Computer Society*, 33(2), 61–62.
- Meins, O. (2017). Consideraciones sobre la Acción de Hábeas Data. *Ius et Praxis*, 3(1), 214-235.
- Nizer, L. (1940-1941). The Right of Privacy. A Half Century's Developments. *Michigan Law Review*, 526-535.
- OEA. (1979). *Corte Interamericana de Derechos Humanos*. Recuperado el 7 de Noviembre de 2019, de Organización de Estados Americanos OEA: <http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=623&IID=2>
- ONU. (10 de Diciembre de 1948). *La Declaración Universal de Derechos Humanos*. Recuperado el 6 de Noviembre de 2019, de Organización de las Naciones Unidas ONU: <https://www.un.org/es/universal-declaration-human-rights/>
- Palazzi, P. (1998). El Habeas Data en el Derecho Argentino. *Revista Electrónica de Derecho Informático*(4).
- Pound. (1915). Interest of Personality. *Harvard Law Review*, 343--362.
- Presthus, W. (2012). Catch Melf You Can! How Technology is Running Away from Ethics in Business Intelligence. *NOKOBIT – Norsk konferanse for organisasjoners bruk av informasjonsteknologi*, 91–104.
- Presthus, W; Andersen, L. (2017). Information Privacy from a Retail Management Perspective. *In Proceedings of the 25th European Conference on Information Systems (ECIS)*, 1968–1983.
- Raab, C., & Szekely, I. (2017). Data protection authorities and information technology. *Computer Law & Security Review*, 33(4), 421–433.

- Radio\_Huancavilca. (14 de Mayo de 2019). *Cinco años del «derecho al olvido»: ¿ha servido para algo?* Obtenido de Radio Huancavilca: <https://radiohuancavilca.com.ec/tecnologia/2019/05/14/cinco-anos-del-derecho-al-olvido-ha-servido-para-algo/>
- Reglamento General a la Ley Orgánica de Telecomunicaciones;. (25 de Enero de 2016). Reglamento General a la Ley Orgánica de Telecomunicaciones. *Registro Oficial No. 676*. Quito, Pichincha, Ecuador: Lexis.
- RGPD. (2016). *El Reglamento General de Protección de Datos de la Unión Europea*. Obtenido de Diario Oficial de la Unión Europea: <https://www.boe.es/doue/2016/119/L00001-00088.pdf>
- Riascos, L. (2012). *Los delitos contra los datos personales y el*. Bogotá, Bogotá, Colombia: Derecho y Realidad.
- RUE. (2016). *Reglamento de la Unión Europea*. Obtenido de <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1528874672298&uri=CELEX%3A32016R0679>
- Ryz, L., & Grest, L. (2016). A new era in data protection. *Computer Fraud & Security*, 3, 18–20.
- Sætra, H. S. (2018). Science as a vocation in the era of big data: the philosophy of science behind big data and humanity's continued part in science. *Integr. Psychol. Behav. Sci.*, 1–15.
- Santos García, D. (2005). *Nociones generales de la Ley Orgánica de Protección de datos*. Recuperado el 11 de Noviembre de 2019, de Casa del Libro: <https://www.casadellibro.com/libronociones-generales-de-la-ley-organica-de-proteccion-dedatos/9788430942299/1022258>
- Sentencia T-277/15 Gloria V. El Tiempo, T-277/15 (Corte Suprema de Justicia 12 de Mayo de 2015).
- Serbeto, E., & Sánchez , J. (14 de Mayo de 2014). *El TJUE respalda el «derecho al olvido» defendido por España ante Google*. Obtenido de

abc Redes: <https://www.abc.es/tecnologia/redes/20140513/abc-derecho-olvido-google-costeja-201405130850.html>

Smith, H., Milberg, S., & Burke, S. (1996). Information Privacy: Measuring Individuals' Concern about Organizational Practices. *MIS Quarterly*, 20(2), 167–196.

Tsay-Vogel, M., Shanahan, J., & Signorielli, N. (2018). Social media cultivating perceptions of privacy: A 5-year analysis of privacy attitudes and self-disclosure behaviors among facebook users. *New Media & Society*, 20(1), 141–161.

Van Loenen, B., Kulk, S., & Ploeger, H. (2016). Data protection legislation: A very hungry caterpillar: The case of mapping data in the european union. *Govern- ment Information Quarterly*, 33(2), 338–345 .

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

Wang, C., Zheng, Y., & Jiang, J. (2018). Toward privacy-preserving personalized recommendation services. *Engineering Review*, 4(1), 21–28.

Warren, & Brandeis. (1890). The Right to Privacy. *Harvard Law Review*.

Willes, J., & Taylor, M. (1890). The Right to Privacy. *The Harvard Review*, 4(5), 27-39.



## DECLARACIÓN Y AUTORIZACIÓN

Yo, **Sacoto Mendoza Susy Valeria**, con C.C: # **1312866286**, autora del trabajo de titulación: **Derecho de eliminación de datos personales atendiendo al principio de finalidad**, previo a la obtención del título de **Abogada de los Tribunales y Juzgados de la República del Ecuador** en la Universidad Católica de Santiago de Guayaquil.

1.- Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2.- Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de propiedad intelectual vigentes.

Guayaquil, 10 de febrero del 2020

f. \_\_\_\_\_

**Sacoto Mendoza Susy Valeria**

**C.C: 1312866286**



<b>REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA</b>			
<b>FICHA DE REGISTRO DE TESIS/TRABAJO DE TITULACIÓN</b>			
<b>TEMA Y SUBTEMA:</b>	<b>Derecho de eliminación de datos personales atendiendo al principio de finalidad.</b>		
<b>AUTORA</b>	Susy Valeria Sacoto Mendoza		
<b>REVISOR(ES)/TUTOR(ES)</b>	Xavier Paul Cuadros Añazco		
<b>INSTITUCIÓN:</b>	Universidad Católica de Santiago de Guayaquil		
<b>FACULTAD:</b>	Jurisprudencia, Ciencias Sociales y Políticas		
<b>CARRERA:</b>	Derecho		
<b>TITULO OBTENIDO:</b>	Abogada de los Tribunales y Juzgados de la República del Ecuador		
<b>FECHA DE PUBLICACIÓN:</b>	10 de febrero del 2020	<b>No. DE PÁGINAS:</b>	39
<b>ÁREAS TEMÁTICAS:</b>	Derecho Informático, Derecho Constitucional, Derecho Comparado		
<b>PALABRAS CLAVES/KEYWORDS:</b>	Privacidad, Derecho Olvido Digital, Garantías, Protección de Datos, Ecuador, Jurisprudencia, Derecho Informático		
<b>RESUMEN/ABSTRACT:</b>	<p>El derecho a la privacidad consiste en que el individuo tenga plena protección en persona y en propiedad es un principio tan antiguo como el derecho consuetudinario. La administración y protección de datos personales en el ámbito histórico y su efecto en el marco jurídico. En el caso del gobierno ecuatoriano que tiene como objetivo principal de preservar la privacidad para la publicación de datos es proteger la privacidad de los datos individuales mediante la propuesta del Proyecto de Ley Orgánica de Protección de Datos Personales. Actualmente, los ciudadanos se sienten vulnerables hasta el momento que no se aprueba esta Ley. Una vez aplicada esta Ley, se podría solicitar el derecho al olvido digital en caso que sea necesario sin perjuicio a terceros dentro del marco legal.</p>		
<b>ADJUNTO PDF:</b>	<input checked="" type="checkbox"/> SI	<input type="checkbox"/> NO	
<b>CONTACTO CON AUTOR:</b>	<b>Teléfono:</b> +593991719507	<b>E-mail:</b> susysacoto29@gmail.com	
<b>CONTACTO CON LA INSTITUCIÓN COORDINADOR DEL PROCESO UTE)::</b>	<b>Nombre:</b> Reynoso de Wright, Maritza Ginette		
	<b>Teléfono:</b> +593994602774		
	<b>E-mail:</b> maritzareynosodewright@gmail.com		
<b>SECCIÓN PARA USO DE BIBLIOTECA</b>			
<b>Nº. DE REGISTRO (en base a datos):</b>			
<b>Nº. DE CLASIFICACIÓN:</b>			
<b>DIRECCIÓN URL (tesis en la web):</b>			