



**UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL**

**FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES
Y POLÍTICAS**

CARRERA DE DERECHO

TEMA:

**Alcance de la protección de datos personales en el marco legal
ecuatoriano**

AUTOR:

Vivar Butiña José Javier

**Trabajo de Titulación previo a la obtención del grado de
ABOGADO DE LOS TRIBUNALES Y JUZGADOS DE LA
REPUBLICA DEL ECUADOR**

Tutora:

Dra. Palencia Núñez, Mónica Rosa Irene

Guayaquil – Ecuador

20 de febrero de 2022



UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES
Y POLÍTICAS

CARRERA DE DERECHO

CERTIFICACIÓN

Certificamos que el presente trabajo de titulación fue realizado en su totalidad por **Vivar Butiña José Javier**, como requerimiento para la obtención del Título de **Abogado de los Tribunales y Juzgados de la República del Ecuador**

TUTORA



Dra. Palencia Núñez, Mónica Rosa Irene

DIRECTORA DE LA CARRERA

Dra. María Isabel Lynch de Nath, Mgs.

Guayaquil, a los 20 días del mes de febrero del año 2022



UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL
FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES
Y POLÍTICAS

CARRERA DE DERECHO

DECLARACIÓN DE RESPONSABILIDAD

Yo, **Vivar Butiñá, José Javier**

DECLARO QUE:

El Trabajo de Titulación, **Alcance de la protección de datos personales en el marco legal ecuatoriano** previo a la obtención del Título de **Abogado de los Tribunales y Juzgados 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, a los 20 del mes de febrero del año 2021

EL AUTOR

Vivar Butiñá José Javier



UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES
Y POLÍTICAS

CARRERA DE DERECHO

AUTORIZACIÓN

Yo, **Vivar Butiña José Javier**

Autorizo a la Universidad Católica de Santiago de Guayaquil a la **publicación** en la biblioteca de la institución del Trabajo de Titulación, **Alcance de la protección de datos personales en el marco legal ecuatoriano**, cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y total autoría.

Guayaquil, a los 20 días del mes de febrero del año 2022

EL AUTOR

Vivar Butiña José Javier

REPORTE URKUND

URKUND

Lista de fuentes Bloques

Categoría	Enlace/nombre de archivo
	https://acansarena7L.wordpress.com/2020/09/18/derecho-a-la-proteccion-de-datos-personales/
Fuentes alternativas	
Fuentes no usadas	

Documento: [Tesis José Vivar Butiña.docx](#) (D127603424)

Presentado: 2022-02-10 10:25 (-05:00)

Presentado por: jose.vivar@cu.ucsg.edu.ec

Recibido: maritza.reynoso.ucs@analysis.orkund.com

Mensaje: Tesis José Vivar Butiña para obtener el certificado Urkund. [Mostrar el mensaje completo](#)

2% de estas 14 páginas, se componen de texto presente en 1 fuentes.

TUTORA:



AUTOR:

f. 
José Javier Vivar Butiña

AGRADECIMIENTOS

A Dios por haberme otorgado el regalo de la vida y por todas las bendiciones que he recibido.

A mis padres, quienes son mis pilares fundamentales y los responsables de haberme formado, con tanto amor y cariño, en la persona que soy hoy en día. Siempre estaré agradecido por los valores que me transmitieron y por haberme entregado todo en esta vida, los amo con todo mi corazón.

A mi hermano por haberse convertido en mi mejor amigo y ser siempre una persona en la que me puedo apoyar y confiar, cuando más lo necesito. No sabes el orgullo, que me siento por ti.

A mis familiares y seres cercanos por haberme permitido ser parte de su vida.

A mis docentes, por haber compartido sus conocimientos durante mi formación y por haberme transmitido la ilusión y el empeño para ejercer esta bella profesión.

A mi Tutora, una profesional a la que admiro, y quien ha contribuido en mi formación académica y en el desarrollo de este trabajo.

DEDICATORIA

Dedico este trabajo a mi madre, la Abogada Nuria Butiñá, quien fue mi mayor fuente de inspiración para realizar este trabajo. El amor e inspiración que siento por ti, fueron el motivo para que yo haya decidido estudiar Derecho. Siempre estaré orgulloso por la intachable e ilustre carrera que has tenido como profesional del Derecho. Te amo con todo mi corazón, tu hijo José.



UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

**FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES Y
POLÍTICAS**

CARRERA DE DERECHO

TRIBUNAL DE SUSTENTACIÓN

Dr. DANIEL RODRIGUEZ WILLIAMS

Oponente

Dr. XAVIER ZAVALA EGAS

Decano.

Abg. Maritza Reynoso de Wright, Mgs.

Coordinadora de UTE.



UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

Facultad: Jurisprudencia

Carrera: Derecho

Periodo: UTE B-2021

Fecha: 20 de febrero de 2022

ACTA DE INFORME FINAL

El abajo firmante, docente tutor del Trabajo de Titulación denominado Titulación “Alcance de la Protección de datos personales en el marco legal ecuatoriano” elaborado por el estudiante Vivar Butiñá, José Javier, certifica que durante el proceso de acompañamiento dicho estudiante ha obtenido la calificación de 10 (diez) lo cual lo califica como **APTO PARA LA SUSTENTACIÓN**



Docente Tutor

Índice

Resumen	vii
Abstract	viii
1. Introducción	2
2. Marco Legal Ecuatoriano	4
2.1. Constitución de la República del Ecuador	4
2.2. Ley del Sistema Nacional de Registro de Datos Públicos	5
2.3. Ley de Protección de Datos Personales	5
3. Conceptos y Definiciones	6
3.1. Datos Personales	6
3.2. Datos Públicos	8
4. Planteamiento del Problema	9
4.1. El Concepto de datos personales no está encuadrado con contenido y límites previstos en la legislación ecuatoriana.	9
4.2. La aplicación de la LOPDP en el Sistema Nacional de Registros Públicos	10
4.3. Legislación Comparada México	11
4.4. La sanción a la violación del derecho de la protección de datos personales	13
5. Conclusiones	18
6. Recomendaciones	18
7. Bibliografía	20

Resumen

El presente estudio plantea determinar hasta qué punto los datos personales de los ecuatorianos se encuentran protegidos, considerando el marco legal vigente en el país. En el país se encuentra vigente la Ley del Sistema Nacional de Registro de Datos Públicos que rige para las instituciones tanto públicas como privadas que poseen la custodia de información a la cual, de acuerdo al artículo 18 de la Constitución de la República, en su numeral segundo, todas las personas tienen derecho a acceder. El objetivo de dicha ley es garantizar la seguridad jurídica, organizar, regular, sistematizar e interconectar la información con transparencia, eficacia y eficiencia. Sin embargo, en la práctica, cuando una persona ya sea natural o jurídica ejerce este derecho, y no sólo accede, sino que procesa y almacena dicha data en otras plataformas, se obtienen espejos de información que luego resultan traspasables tanto dentro del territorio nacional o incluso en el exterior. Pese a que la SINARDAP, establece procedimientos, con altos estándares de calidad, para la custodia de datos, en la práctica, no logra articular con éxito los procesos posteriores a la salida de los mismos. Es por ello que surge una gran preocupación sobre en qué momento el acceso de terceros a dichos datos, pueden ocasionar un desmedro o afectación a la persona titular o dueña de dichas referencias. Se evidencia, por ejemplo, que la Ley de Protección de Datos no determina puntualmente qué referencias personales, se deberían considerar como sensibles a vulnerar derechos fundamentales como la intimidad y la privacidad.

PALABRAS CLAVES: Datos Personales, Datos Públicos, Protección de Datos Personales, Competencia, Sanción.

Abstract

This study aims to determine to what extent the personal data of Ecuadorians are protected, considering the current legal framework in the country. In the country, the Law of the National Public Data Registry System is in force, which governs both public and private institutions that have the custody of information to which, according to article 18 of the Constitution of the Republic, in its numeral second, all people have the right to access. The objective of this law is to guarantee legal certainty, organize, regulate, systematize and interconnect information with transparency, effectiveness and efficiency. However, in practice, when a person, whether natural or legal, exercises this right, and not only accesses, but processes and stores said data on other platforms, information mirrors are obtained that are then transferable both within the national territory or even outside. Although SINARDAP establishes procedures, with high quality standards, for the custody of data, in practice, it is unable to successfully articulate the processes subsequent to their release. That is why there is great concern about when the access of third parties to said data, can cause a detriment or affectation to the owner or owner of said references. It is evident, for example, that the Data Protection Law does not specifically determine which personal references will have to be considered as sensitive to violating fundamental rights such as intimacy and privacy.

KEY WORDS: Personal Information, Public Data, Protection of personal data, Competence, Penalty

1. Introducción

Es innegable aceptar que los avances tecnológicos conducen a las sociedades modernas a enfrentar retos inimaginables. Es así como la tecnología también evoluciona y transforma las instituciones que buscan mantenerse vigentes, incorporando en ellas mejoras palpables que se traducen en beneficios para la sociedad.

El impacto de esta vorágine, es contundente e impulsa tanto a las personas naturales, jurídicas y autoridades públicas a ser cada vez más competitivos. Sin embargo, cuando se habla de procesos tecnológicos, en especial si son destinados al manejo y protección de datos personales, estos deben enmarcarse dentro de la ley.

La protección de datos personales aparece como un derecho, dentro de una herramienta jurídica, que tiene por objeto defender la privacidad de las personas, tarea que se vuelve más vulnerable a medida que la tecnología avanza. Para lograr este objetivo, es necesario definir: el alcance de dicha información, el responsable de su tratamiento y las normas que van a regular todos los aspectos referentes a su administración y gestión tales como la seguridad, el acceso, la conservación, confidencialidad y el nivel de protección que deben tener.

El primer instrumento internacional jurídicamente vinculante adoptado para este caso, fue el Convenio 108 del Consejo de Europa, del 28 de enero de 1981, que en su artículo 1 establece como su principal objetivo proteger a cualquier persona física sean cuales fueren su nacionalidad o su residencia y hacer respetar sus derechos y libertades fundamentales, concretamente su derecho a la vida privada. Esto refiriéndose al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona (Consejo de Europa , 1981).

Los Estados y las grandes empresas, son ahora más vulnerables frente a la globalización y a la aparición de una gran cantidad de sistemas y plataformas que a través de procesos simples o automatizados e incluso utilizando minería de datos, otorgan perfiles de personalidad “que pueden usarse para provocar transgresiones no solo a la privacidad sino a otros derechos fundamentales” (Naranjo Godoy, 2017). Incluso este tipo de información permite tomar decisiones con beneficios económicos

o de otro tipo, para quienes utilizan esos datos, en desmedro de la protección del titular. Esta asimetría hace necesaria una norma que regule el uso indiscriminado y sin control de estos datos, ya que el derecho a la información es constitucional y debe ser para todos.

“Cada vez más, las naciones toman conciencia de la necesidad de crear un marco regulatorio, que brinde no solo protección sino un manejo adecuado de los datos personales” (Roldan Carrillo, 2021). En mayo de 2016, la Unión Europea promulgó el Reglamento General de Protección de Datos (en adelante, RGPD) que entró en vigor el 25 de mayo de 2018. Su objetivo principal era fortalecer la normativa de protección de datos y actualizar las antiguas directrices de la Unión Europea de la Directiva 95/46/CE que en su momento no abordaban directamente los nuevos desafíos técnicos. El RGPD creó un nuevo estándar, considerado como un punto de referencia para que otras legislaciones comiencen a desarrollar normas específicas de este tipo. Dichos estándares versan sobre un conjunto de conceptos y principios tales como establecer un procedimiento para resolución de controversias, determinar un responsable del tratamiento de la información, mayores medidas de seguridad para la protección de datos personales, establecer un alcance extraterritorial de aplicación e imponer un régimen sancionatorio, entre otros.

Incluso, “los países obtienen incentivos financieros por incorporar marcos de protección con los estándares del RGPD, pero adecuados a su legislación” (Roldán Carrillo, 2020). Brasil, México y Perú ya gozan de este tipo de legislación y otros como Chile y Argentina, se encuentran debatiendo proyectos de ley similares. Entre los incentivos que se pueden obtener por mejorar sistema de protección de datos personales, está “la apertura del mercado de inversión internacional y actividades comerciales de transmisión de dicha data, que puede generar un espacio más competitivo para las TICS” (Troncoso Reigada, 2012).

Se requiere una agencia reguladora o una entidad de control de protección de datos moderna e integral que promueva "la confianza y la seguridad jurídica en el uso de los datos como base de la sociedad de la información, la economía y la innovación" (Roldán Carrillo, 2020).

2. Marco Legal Ecuatoriano

2.1. Constitución de la República del Ecuador

La Constitución de la República del Ecuador reconoce el derecho a la protección de datos personales. A efectos de garantizar la seguridad jurídica de los ciudadanos, se establecen una serie de garantías a los derechos personales de los ciudadanos, tales como el libre acceso a la información generada en entidades públicas y en aquellas privadas que manejen fondos del Estado o realicen funciones públicas, garantizándole al ciudadano la inexistencia de reserva de información excepto en los casos expresamente establecidos en la ley. Incluye también, cuando habla del derecho a la migración de datos, la confidencialidad de aquellos de carácter personal que se encuentren en los archivos de las instituciones del Ecuador en el exterior. Además, garantiza el derecho a la protección de datos de carácter personal, incluyendo el acceso y la decisión sobre el uso de esta información.

El habeas data, es un recurso que garantiza la protección del derecho a la intimidad del titular, “ya que no toda la información relativa a este tiene el carácter de pública y por tanto no puede ser divulgada libremente” (Sentencia 182-15-sep-CC, 2015).

Otra sentencia de la Corte Constitucional define la acción del habeas data: “Se reconoce al habeas data como un mecanismo de garantía del derecho a la protección de datos personales y aparte desarrolla el concepto de autodeterminación informativa que es la verdadera expresión de este derecho” (Sentencia 001-14-PJO-C, 2015).

El problema de la acción de habeas data es que la ley de Garantías Jurisdiccionales y Control Constitucional (en adelante LOGJCC) no plantea un momento oportuno para presentarla, sino que solo hace alusión a la espera de un tiempo razonable para poder plantearla, lo cual no resuelve la incógnita. Por su naturaleza, es una medida ex post, lo que significa que solo podrá ser planteada una vez que el daño ya haya sido cometido.

Finalmente parece que la acción se desnaturaliza, cuando la LOGJCC en su artículo 51 les otorga a las personas jurídicas la legitimación activa para proponer la acción. Son las grandes empresas las que manejan bases de datos y por tanto son ellas las que pueden vulnerar el derecho de los titulares debido a un mal manejo o abuso en el ejercicio de sus actividades.

2.2. Ley del Sistema Nacional de Registro de Datos Públicos

La Ley del Sistema Nacional de Registro de Datos Públicos (SINARDAP en adelante), promulgada el 31 de marzo de 2010, crea y regula el Sistema de Registro de Datos Públicos y su acceso, a entidades públicas o privadas que administren dichas bases o registros. Su objetivo es garantizar la seguridad jurídica, organizar, regular, sistematizar e interconectar la información, así como: la eficacia y eficiencia de su manejo, su publicidad, transparencia, acceso e implementación de nuevas tecnologías. Esta ley rige para las instituciones del sector público o privado que administren bases de datos públicos. El sistema del SINARDAP se ejecuta a través de la Dirección Nacional de Registro de Datos Públicos (en adelante DINARDAP).

La DINARDAP regula, controla e interopera la información de carácter público, logrando de esta manera facilitar el acceso a la información, proporcionar su protección en la interoperabilidad de datos, es decir el cruce en línea y tiempo real de la diversa información entre las fuentes para obtener la certeza y veracidad de la misma y a su vez garantizar la protección a la privacidad de la información del ciudadano, como se contempla en la Ley y en su Reglamento de aplicación.

La interoperación de datos es el intercambio de información entre instituciones públicas mediante el uso de las tecnologías de la información y comunicación, con la finalidad de regular su integración y su acceso para mejorar procesos automatizados.

La DINARDAP también integra la disponibilidad del “bus de datos” con la finalidad de intercambiar la información con protección y seguridad jurídica, a través de las entidades públicas que integran el Sistema.

2.3. Ley de Protección de Datos Personales

La Ley Orgánica de Protección de Datos Personales (en adelante LOPDP) fue promulgada en el Quinto Suplemento del Registro Oficial No. 459 de fecha 26 de mayo de 2021. (Asamblea Nacional del Ecuador, 2021)

Esta ley establece disposiciones de carácter general que tanto instituciones públicas como privadas deben adoptar y que deberán ser cumplidas por domiciliados y no domiciliados en el Ecuador, que procesen y recolecten datos personales de titulares que residan en suelo ecuatoriano.

La LOPDP crea una máxima autoridad encargada de velar por el cumplimiento de la ley, como órgano de control y vigilancia, es decir que dirige y administra la Institución, atiende y resuelve reclamos que devengan del titular de los datos o iniciados de oficio y ostenta una potestad sancionadora en caso de incumplimiento a la ley.

La ley establece conceptos nuevos como la elección de un responsable que puede ser una persona natural o jurídica, pública o privada que solo o conjuntamente decide sobre la finalidad y el tratamiento de la base de datos personales. Establece también un encargado que realiza el tratamiento de dicha data, a nombre y por cuenta del responsable antes mencionado y la figura de un delegado que sirve como punto de contacto entre el responsable y la autoridad a cargo de la protección de esta información.

Otro de los aspectos importantes que establece la ley es que existirá consentimiento por parte del titular para el tratamiento de sus datos personales, siempre y cuando esta manifestación de voluntad sea libre, inequívoca, específica e informada, estableciendo que el consentimiento puede ser revocado en cualquier momento. La LOPDP establece la posibilidad de realizar transferencias o comunicaciones internacionales de datos siempre y cuando se cumplan con todos los requisitos establecidos por la ley y que el país que reciba los datos de filiación cumpla con los estándares internacionales en materia de protección de los mismos.

3. Conceptos y Definiciones

3.1. Datos Personales

La Unión Europea es líder en materia de protección de datos personales (Ortega Giménez & Gonzalo Domenech, 2018) y ha sido reconocida por promulgar leyes destinadas a establecer estándares globales en este campo. Su Reglamento General de Protección de Datos Personales promulgado en el 2016 (RGDP en adelante) en su artículo 4 conceptualiza a los datos personales como:

Toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable a 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. (Parlamento Europeo y Consejo de la Unión Europea, 2016).

Por otra parte, el Compendio de Lecturas y Legislación sobre protección de datos personales del Instituto Federal de Acceso a la Información Pública de México (2010) indica lo siguiente:

Los datos personales se refieren a toda aquella información relativa al individuo que lo identifica o lo hace identificable. Entre otras cosas, le dan identidad, lo describen, precisan su origen, edad, lugar de residencia, trayectoria académica, laboral o profesional. Además de ello, los datos personales también describen aspectos más sensibles o delicados sobre tal individuo, como es el caso de su forma de pensar, estado de salud, sus características físicas, ideología o vida sexual, entre otros. (Instituto Federal de Acceso a la Información Pública de México, 2010).

Es así como se consideran dos tipos de datos de acuerdo a la importancia que tienen en la seguridad de cada individuo:

Los datos sensibles: son datos personales que informan sobre los aspectos más íntimos de las personas, y cuyo mal uso pueda provocar discriminaciones o ponerles en grave riesgo, como, por ejemplo, el origen racial o étnico; estado de salud (pasado, presente y futuro); información genética; creencias religiosas, filosóficas y morales; afiliación sindical; opiniones políticas y preferencia sexual (©Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), 2017).

Los datos patrimoniales o financieros: tratan sobre la capacidad económica de las personas físicas y hacen referencia a los recursos que posee y a su capacidad para hacer frente a sus deudas. Estos pueden ser: dinero, bienes muebles e inmuebles; información fiscal; historial crediticio; ingresos y egresos; cuentas bancarias; seguros; afores; fianzas, número de tarjeta de crédito, número de seguridad, entre otros (©Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), 2017).

El derecho a la protección de datos personales es definido por la jurisprudencia española como:

El derecho a la protección de datos consiste, pues, al menos, ...en un poder de disposición y control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso (STC 292/2000, de 30 de noviembre) (Jurisprudencia Española).

3.2. Datos Públicos

Dato calificado como tal según los mandatos de la ley o de la Constitución Política y todos aquellos que no sean semiprivados o privados, de conformidad con la presente ley. Son públicos, entre otros, los datos contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas (IDECA, 2008).

4. Planteamiento del Problema

4.1. El Concepto de datos personales no está encuadrado con contenido y límites previstos en la legislación ecuatoriana.

Se analizan: a.- el artículo 18 numeral 2 de la Constitución que versa sobre el libre acceso a la información; b.- la Disposición Transitoria Primera de la Constitución de la República del Ecuador numeral 8 que establece la creación de una de una Ley que organice los registros de datos en particular los registro civil, mercantil, de la propiedad y que se establezca la existencia de un sistema de control cruzado de validación de información con el fin de obtener veracidad y acceso a la información pública; c.- la ley del SINARDAP y la LOPDP.

Luego de este análisis surge la primera inquietud: ¿Son todos los datos personales de carácter privado o existen también datos personales de carácter público? En caso de existir datos personales de carácter público, se presenta un segundo planteamiento: ¿Cuál es el alcance de la protección del dato personal? Anteriormente el artículo 6 de la ley del SINARDAP establecía taxativamente “dato” como no accesible o confidencial, pero al reformar este artículo quedan muchas interrogantes.

Este estudio considera el siguiente ejemplo: el estado civil, se puede considerar como un dato público porque produce un efecto jurídico que afecta a terceros; si este es el caso, habría que determinar el alcance de la protección, para lograr una articulación, concordancia y correlación entre las dos leyes SINARDAP y LOPDP, y así lograr el objetivo de protección de datos personales con carácter público.

Pero si el mismo ejemplo se considera como dato privado, no tendría sentido la integración de un sistema de control cruzado desde que nace de la Constitución y de la Ley del SINARDAP.

Por otra parte, la mayoría de los datos filiales provienen de registros públicos, siendo el registro civil la mayor de las fuentes pues es en sus repositorios donde eminentemente reposan datos de carácter personal, públicos y privados. No obstante, el problema radica en la definición tan imprecisa o general sobre este tipo de información, qué exactamente se considera un dato personal y por tanto sujeto a protección.

Esto se verifica en la Ley Orgánica de Gestión de la Identidad y Datos Civiles, que en su artículo 4 numeral 2 habla del principio de la unicidad y establece claramente que “existirá un número único de identificación al que se vincularán todos los datos personales públicos o privados que se tengan que inscribir y registrar por mandato legal o judicial, y se hará constar en forma obligatoria en los diferentes documentos tanto públicos como privados”. El artículo 85 de la misma ley define a la cedula de identidad como “el documento público que tiene por objeto identificar a las personas ecuatorianas y las extranjeras que se encuentren en el Ecuador”.

En esta ley sí se establece la diferencia entre datos personales de carácter público y privado, además de que le otorga al número de cédula y al estado civil la categoría de dato público. Cabe recalcar que el proceso de cedulación y certificación a cargo del Registro Civil, puede interoperarse a través del Sistema Nacional de Registro de Datos Públicos y que tanto entidades públicas como privadas pueden hacer uso de ese sistema, para fines de validación o identificación de las personas.

Finalmente, una de las atribuciones de la Dirección General de Registro Civil, Identificación y Cedulación es verificar, validar y autenticar los datos personales que constan en sus archivos para lograr la más eficiente interoperabilidad a través del SINARDAP con las demás entidades públicas, y su trazabilidad para fines de interés del Estado y de la ciudadanía.

4.2. La aplicación de la LOPDP en el Sistema Nacional de Registros Públicos

Otra falencia a señalar es que se percibe una posible duplicidad de competencias entre la Dirección Nacional del Registro de Datos Públicos (DINADARP) y la Ley Orgánica de Datos Personales LOPDP.

Tan complejo es el tema que por una parte, entre las facultades que le atribuye la LOPDP a la Máxima Autoridad de Protección de Datos se encuentra la siguiente: “Controlar y supervisar el ejercicio del derecho a la protección de datos personales dentro del tratamiento de datos llevados a cabo a través del Sistema Nacional de Registros Públicos” mientras que, por otra parte se encuentra la facultad que le otorga la propia disposición reformativa de la LOPDP a la DINARDAP que establece: “Controlar y supervisar que las entidades pertenecientes al Sistema Nacional de

Registros Públicos incorporen mecanismos de protección de datos personales, así como dar cumplimiento las disposiciones establecidas en la LOPDP... ”.

Tal como se señala en el primer párrafo de este numeral, existe una posible duplicidad de competencias y facultades de ambas autoridades en el ejercicio de sus funciones, Autoridad de Datos Públicos y la Autoridad de Datos Personales (de momento aún no creada), teniendo a dos normas que se contraponen entre sí, lo que atendería contra el principio de eficiencia de la administración pública.

Adicionalmente se encuentra vigente la disposición transitoria séptima de la Ley del SINARDAP que establece: “que las instituciones que posean información pública, deberán integrarse paulatinamente al Sistema Nacional de Registro de Datos Públicos, y en caso de que cualquier institución que estuviese en la obligación de interconectarse, no lo hiciera, la máxima autoridad de la referida institución podrá ser destituida por el Director Nacional de Registros Públicos”. Es decir que la DINARDAP tiene competencia inclusive de destituir al funcionario que no cumpliera con la obligación de integrarse al Sistema de Datos Públicos.

Este problema de competencias debió ser regulado y articulado con la creación de la Ley de Protección de Datos Personales, que fue posterior al pronunciamiento constitucional de la creación de un Sistema, para dar lugar a una efectiva protección de datos personales, que incluya una sanción civil y penal a quien utilice indebidamente los datos personales para un fin comercial particular en desmedro del derecho personal de cada ciudadano.

4.3. Legislación Comparada México

Se revisaron legislaciones de varios países, y se encuentra que en algunas ocasiones la coexistencia entre el derecho al acceso a la información y el derecho a la protección de datos personales entran en conflicto.

El análisis del marco normativo de México demuestra que ellos cuentan con una acertada regulación en materia de protección de datos personales en el campo del sector privado y el sector público, así como el acceso a la información por parte de las entidades públicas. Su marco constitucional se parece bastante al de Ecuador, ya que el derecho al acceso a la información y el derecho a la protección de datos personales se encuentran garantizados y respaldados como derechos humanos.

La diferencia con el ordenamiento jurídico ecuatoriano es que en México el derecho a la protección de datos personales, regido por entidades privadas y públicas y el derecho al acceso a la información, se encuentran bien instrumentados en dos leyes federales, la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP) que regula el acceso a la información y la protección de datos personales en posesión de entidades públicas y la Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDPPP) que regula la posesión y tratamiento de datos personales en posesión de entidades privadas.

De primera mano se puede ver la primera gran diferencia con la LOPDP de Ecuador y es que existen dos leyes para dos escenarios diferentes, el público y el privado. Además, estas dos leyes cuentan con amplios reglamentos que regulan aspectos específicos de su aplicación.

La FTAIP y la LFPDPPP son reguladas por una autoridad competente, a diferencia del Ecuador que tiene dos autoridades que se aseguran del cumplimiento de ambas leyes. El órgano encargado de velar por el cumplimiento de las leyes es el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI). Esta entidad cuenta con un cuerpo colegiado conformado por comisionados que se encargan del cumplimiento y respeto de ambos derechos. Normalmente el derecho de protección de datos personales, entra en conflicto, cuando se trata de información manejada por instituciones públicas, por cuestiones de datos personales de carácter público y todo lo que hemos venido analizando hasta el momento.

La diferencia es que, en México, el INAI se encarga de resolver este tipo de controversias, a través de resoluciones donde se ponderan ambos derechos y se analiza la extensión y los límites de los principios de máxima publicidad y la protección de la privacidad, mediante una estructura jurídica específica, para cada caso particular. Es así que, al tener dos leyes para el sector público y el privado, el concepto de dato personal y el alcance de esa protección quedan más definidos, a diferencia de lo que ocurre actualmente en el Ecuador.

4.4. La sanción a la violación del derecho de la protección de datos personales

La LOPDP establece las solemnidades a cumplirse para poder hacer uso de la información personal, dispone al responsable y al encargado del tratamiento de la información, así también decreta la creación de un órgano controlador que vela por el cumplimiento de la ley y tiene la facultad de sancionar administrativamente cuando la finalidad que se le da al tratamiento de dicha data es distinta para la cual se autorizó; todo esto desde el punto de vista del control administrativo.

En el presente estudio ya se ha analizado la limitación del concepto de datos personal y el alcance de la protección de ciertos datos personales que se encuentran dentro de bases de datos públicas. Pero surge otra problemática, y es que en la violación del derecho a la protección de datos personales se vulnera también el derecho a la intimidad y el derecho a la privacidad de las personas.

Partiendo desde la idea de que los datos personales son como una propiedad de carácter privado, cuya protección interesa al orden público, la violación o intromisión para acceder a esos datos personales, daría lugar a un delito.

El artículo 180 del Código Orgánico Integral Penal (COIP en adelante) establece el delito de divulgación de información restringida, y el artículo 472 del COIP establece como información de circulación restringida a los datos personales cuya difusión no haya sido expresamente autorizada por su titular. Por otro lado, el COIP establece en su artículo 178 el delito de la violación a la intimidad, el cual consiste en que, la persona que, sin contar con el consentimiento o autorización legal, acceda, intercepte, difunda o publique datos personales, será sancionado con pena privativa de libertad de uno a tres años.

El artículo 178 del COIP que tipifica el delito de violación a la intimidad, tiene elementos normativos muy delicados, donde se requiere recurrir a elementos extrapenales para poder entender y determinar si, bajo este tipo penal, se puede atribuir el delito de vulneración al derecho de protección de datos personales.

Ante este escenario, el tipo penal es bastante discutible, ya que se necesita definir si es un delito que vulnera del derecho a la intimidad o el derecho a la privacidad, por lo que resulta necesario establecer primero la diferencia entre privacidad e intimidad.

“La privacidad es la potestad de toda persona de decidir qué aspectos de su vida quiere compartir con otras” (Vera, 2021). El derecho a la privacidad se lo podría entender como la facultad de una persona de decidir en qué medida o forma comparte con los demás aspectos su vida privada, sean pensamientos, sentimientos o acontecimientos.

Por otro lado, se puede definir al derecho a la intimidad como: “una esfera de protección que rodea la vida más privada del individuo frente a injerencias ajenas o conocimiento de terceros, salvo excepciones muy concretas contenidas en la Ley. Dicha esfera protege tanto elementos físicos e instrumentales” (Salgado Segúin, 2010).

Como se puede observar, la privacidad y la intimidad son diferentes, pero a lo largo del tiempo han existido corrientes que las han utilizado como sinónimos, sin dotarles de alguna diferencia, más, si se parte de un análisis pormenorizado, se encontrará que responden a concepciones y alcances complementarios, como se corrobora a continuación.

Para el tratadista German Bidart Campos y Walter Carnota la privacidad y la intimidad se definen de la siguiente manera:

la intimidad es la esfera personal que está exenta del conocimiento generalizado de tercero... y la privacidad es la posibilidad irrestricta de realizar acciones privadas (que no dañen a otros) que se cumplan a la vista de los demás y que sean conocidas por estos (Bidart & Carnota, 1998).

Por ende, es posible evidenciar la diferencia entre la intimidad y la privacidad, aunque si se lo analiza bajo criterios semánticos, puede surgir una confusión, donde efectivamente podrían entenderse como sinónimos, que direccionen al individuo a pensar que la intimidad y la privacidad son lo mismo, y por consecuencia su vulneración signifique una clara intromisión personal.

En la Constitución ecuatoriana, se entiende la intimidad como un derecho fundamental que protege la esfera más privada de la persona, por lo que su protección como bien jurídico y derecho fundamental mantiene una gama de protección singularizada y complementaria con la privacidad.

En consecuencia, de lo expuesto hasta el momento: la privacidad presenta un alcance que se entiende compatible con la intimidad, sin llegar a la premisa de que son diferentes, hasta el punto de generar como conclusión un silogismo de premisas mayores y menores: “los asuntos íntimos son privados, pero no todos los asuntos privados pueden tener carácter de íntimos”. Es decir, cuando se vulnera la intimidad, que engloba áreas muy concretas de la vida de una persona, se ha vulnerado a la vez la privacidad o aspectos generales referentes a una persona; pero cuando se ha vulnerado la privacidad, no necesariamente significa que se ha atentado contra la intimidad sin perjuicio de que efectivamente pueda llegar a producirse (Villalba Fiallos, 2017).

Volviendo al apartado de interés para este trabajo, se conoce que existen diversos derechos fundamentales relacionados con la información personal, muchos de ellos son innatos de la personalidad y guardan relación entre sí, como pueden ser el derecho al honor, a la propia imagen, a la intimidad, a la privacidad, a la protección de datos personales, el secreto a las comunicaciones y el derecho a la inviolabilidad de domicilio. A pesar de que el bien jurídico que tutela cada derecho es distinto, muchas veces no pueden ser tratados de manera separada, peor aun cuando el bien jurídico lesionado es causado por el uso de las Tics.

El derecho a la protección de datos está íntimamente ligado al de la intimidad y a la privacidad, pero goza de autonomía propia ya que si bien el derecho a la intimidad ha sido derivado del reconocimiento a la libertad personal en la primera generación de derechos, fue hasta la tercera generación que, en “respuesta al fenómeno de la denominada ‘contaminación de las libertades’ (liberties’ pollution)”, el derecho a la intimidad alcanzó mayor auge, lo que originó que éste se viera precisado a ampliar su espectro a través del reconocimiento de nuevas vertientes del mismo, para ahora tener una ramificación de derechos incorporados a él, tales como el derecho al honor, a

la propia imagen, a la vida privada (en su acepción más amplia), a la protección de datos personales, e incluso, para un sector de la doctrina, a la libertad informática (Arellano Toledo & Ochoa Villicaña, 2012).

Es así como el derecho a la protección de datos personales se forma a través del derecho a la intimidad. Ahora el cuestionamiento es ¿se perfecciona la sanción por la violación al derecho de protección de datos personales a través del artículo 178 del COIP?

Para que se configure la lesión al bien jurídico de la intimidad del titular de la información es necesario que exista una transferencia de esa información personal hacia una finalidad o un individuo que pueda causar una lesión. También sabemos que para que se configure el delito es necesario que no exista una autorización de por medio, para hacer uso de esa data. Normalmente esa transferencia y esa autorización para el tratamiento de datos personales suelen darse para una finalidad en específico, y a causa del avance de las Tics, cada vez se producen nuevas formas de vulnerar la intimidad. A raíz de esa entrega de poder y control sobre la información personal, que básicamente se podría traducir en dotar a un tercero sobre el poder de uno mismo y de su información.

Entonces entendemos que esa vulneración al derecho a la intimidad nace por la ausencia de ese consentimiento válido para acceder a los datos personales, o para hacer uso de ellos, tomando en cuenta que lo importante es la forma en la que fueron entregados esos datos personales, si es que su obtención fue otorgada de manera legítima y si es que fue utilizada para el fin acordado. En caso de no existir este consentimiento válido o si es que el fin es distinto al acordado, se estaría ante la lesión del bien jurídico de la intimidad. Esto aplica tanto para el ámbito privado como para el ámbito público (de ciertos datos de carácter personal, cuyo acceso es confidencial, y el responsable es el ente administrativo repositario de dichos datos).

Por lo tanto, se consideran elementos constitutivos del delito la falta de autorización, la existencia de esta transferencia de información personal y la finalidad que produzca ese daño moral o violación a la intimidad. El artículo 178 del COIP no establece de manera clara la lesión al bien jurídico protegido en relación a la protección de los datos personales. Por lo que este tipo penal presenta un problema

en el supuesto de hecho factico y en el supuesto de hecho legal, es decir cuando la conducta no se adecua con la fórmula que promueve el artículo 178 para llegar al resultado.

Por otro lado, existe otro tipo penal en relación a la tutela del bien jurídico de la información personal, de carácter confidencial e íntima, ya que, la información consolidada a nivel público o privado, se puede encontrar en bases de datos, ficheros o en sistemas electrónicos, protegida de su ilegal revelación en el artículo 229 del COIP, haciendo una especial alusión a los funcionarios públicos.

Se concluye que el pragma conflictivo, definido por Zaffaroni como la conducta más el resultado, no se configura dentro de este tipo penal. Lo que sucede en el mundo real no se abarca en el tipo penal. Por eso en el marco normativo del presente estudio, se hace cualquier tipo de interpretación para adecuar el ilícito al tipo penal de prohibición de circulación de información restringida o el de la violación a la intimidad. El supuesto ilícito existe y es la divulgación y uso indebido de los datos personales sin el consentimiento del titular, para un fin particular en desmedro del derecho personal del titular, priorizando tal vez, el fin mercantil que el infractor busca.

El gran problema es que la LOPDP no se articula ni tampoco define cual es el delito penal que se comete cuando se vulnera la intimidad personal a través del abuso del tratamiento de datos personales, dejando a la tutela de protección de datos personales en indefensión.

Así mismo, pudieran generarse bases de datos espejos que utilicen la información personal, procesándola con otros segmentos que beneficien a sectores crediticios que buscan únicamente satisfacer sus necesidades mercantiles, sin que exista un sistema que garantice la integridad de los diferentes archivos, proporcionando un acceso seguro a la información y salvaguardando ésta en lo que respecta al interés personal de cada ciudadano. Tampoco existe una norma o modelo de gestión que garantice protección al bien jurídico de la intimidad personal, frente a algún sistema que pudiera ser comercializado de manera indiscriminada.

5. Conclusiones

- Aunque el derecho a la protección de datos personales se encuentra consagrado en la Constitución y que se ha creado una Ley Orgánica de Protección de Datos Personales, el concepto de datos personales que ofrece la LOPDP parecería ser muy amplio, sin ofrecer una diferencia entre: datos personales de carácter público y datos personales de carácter privado o confidencial.
- La falta de precisión entre el contenido y el límite de los datos personales de carácter público y los datos personales de carácter privado o confidencial, podría provocar una confusión en cuanto al alcance de la protección de los datos personales en el sector público, lo que hace parecer que ningún dato personal es publicable, cuando los datos no publicables son solo los datos personales confidenciales y los datos íntimos.
- Existe falta de articulación entre la Ley Orgánica de Protección de Datos Personales (LOPDP) y la Ley del Sistema Nacional de Registros de Datos Públicos (SINARDAP), esa falta de articulación entre ambas normas podría ocasionar un conflicto de competencias y facultades entre un Ente Regulador y un Ente Controlador.
- Si bien es cierto en el marco legal penal, tenemos delitos como el de la violación a la intimidad, el de divulgación a la información de circulación restringida y el delito de revelación ilegal de base de datos, valdría regular la responsabilidad de las personas jurídicas, de carácter penal en las actividades de sus funcionarios (Oficiales de Cumplimiento) cuando ingresan sin autorización a la obtención de información personal.

6. Recomendaciones

- Se recomienda establecer en la LOPDP, cuáles son los datos personales de carácter confidencial y datos personales sensibles que son objeto de protección de la ley. No basta con simplemente establecer definiciones, sin especificar cuáles son los datos personales que entran dentro del ámbito de protección.
- Se recomienda reformar la ley del SINARDAP o la LOPDP para que exista una verdadera articulación entre ambas normas y de este modo el Sistema Nacional de Registro de Datos Públicos sirva como un canal de cruce de información, para el cumplimiento del objeto de la LOPDP, o que dentro de la creación del Reglamento de aplicación de la LOPDP se contemple la existencia del Sistema SINARDAP, para lograr una correcta configuración del ámbito de aplicación de la LOPDP en el sector

público y en el sector privado. De ahí la necesidad de implementar un Sistema Único, que sea capaz de cruzar y validar información, siempre y cuando se garantice la caución de su procesamiento, para lo cual la SUPERINTENDENCIA DE DATOS debe articular sus funciones a través de un sistema hoy existente (SINARDAP) para ofrecer trazabilidad y procesos que garanticen una bien estructurada seguridad jurídica.

- Se recomienda reformar el artículo 178 del COIP para que exista armonía o relación entre la conducta y el resultado, para que el delito de intromisión o uso de la información personal en desmedro de la intimidad del titular, se considere dentro del tipo penal.
- Se recomienda desarrollar doctrina que permita una mejor comprensión de la diferencia del derecho a la intimidad y el derecho a la privacidad, desde un estudio que abarque la diferencia entre sus conceptos, alcance, límites y los bienes jurídicos que ambos protegen.

7. Bibliografía

- Arellano Toledo, W., & Ochoa Villicaña, A. (28 de Julio de 2012). *Derechos de privacidad e información en la sociedad de la información y en el entorno TIC*. Obtenido de http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-21472013000100010
- Asamblea Nacional del Ecuador. (2021). *Ley Orgánica de Protección de Datos Personales*. Obtenido de Ley s/n (Quinto Suplemento del Registro Oficial 459, 26-V-2021): <https://www.consejodecomunicacion.gob.ec/wp-content/uploads/downloads/2021/07/lotaip/Ley%20Org%C3%A1nica%20de%20Protecci%C3%B3n%20de%20Datos%20Personales.pdf>
- Bidart, G., & Carnota, W. (1998). *Derecho constitucional comparado*. Buenos Aires: Ediar.
- Bojalil, P., & Vela Ireviño, C. (1 de febrero de 2019). *Despuntan las reformas en materia de protección de datos en América Latina*. Obtenido de <https://blogs.iadb.org/conocimiento-abierto/es/proteccion-de-datos-gdpr-america-latina/>
- Camarena Alarcon, A. I. (18 de Septiembre de 2020). *Derecho a la Protección de Datos Personales*. Obtenido de Tecnologías, Seguridad de la Información y otros temas...: <https://acamarena71.wordpress.com/2020/09/18/derecho-a-la-proteccion-de-datos-personales/>
- Código Orgánico Integral Penal. Registro Oficial Suplemento 180, Quito, Ecuador, 10 de febrero de 2014. Última modificación: 17 de febrero de 2021
- Consejo de Europa . (1981). *Council of Europe*. Obtenido de Convenio Para la Protección de Datos Personales: <https://www.coe.int/es/web/data-protection/convention108-and-protocol>
- Enríquez Alvarez, L. (19 de Febrero de 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*. Obtenido de <https://revistas.uasb.edu.ec/index.php/foro/article/view/500>
- Ley Orgánica de Gestión de la Identidad y Datos Civiles- LOGIDAC. Registro Oficial Segundo Suplemento No. 648, Quito Ecuador, 4 de febrero de 2016. Última Modificación 8 de diciembre del 2020.
- Ley del Sistema Nacional de Registros de Datos Públicos. Suplemento del Registro Oficial No. 162, 31 de marzo de 2010. Última Modificación Quinto Suplemento del Registro Oficial 459, 26-V-2021.
- IDECA. (2008). *La Infraestructura de Datos Espaciales (IDE) de Bogotá*. Obtenido de Ley 1266: <https://www.ideca.gov.co/recursos/glosario/dato-publico>

- Instituto Federal de Acceso a la Información Pública de México . (2010). *Compendio de Lecturas y Legislación sobre protección de datos personales* . Obtenido de <http://www.transparencia.udg.mx/sites/default/files/Protecci%C3%B3n%20de%20datos%20personales.%20Compendio%20de%20lecturas%20y%20legislaci%C3%B3n.pdf>
- Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI). (8 de Agosto de 2017). *Guía para Titulares de Datos Personales Volumen 1*. Obtenido de https://www.cinvestav.mx/Portals/0/sitedocs/tyr/GuiaTitulares-01_PDF.pdf
- Naranjo Godoy, L. (2017). *El dato personal como presupuesto del derecho a la protección de datos personales y del hábeas data en Ecuador*. Obtenido de Revista de Derecho, No. 27 ISSN 1390-2466 • UASB-E / CEN • Quito: <https://repositorio.uasb.edu.ec/bitstream/10644/5946/1/06-TC-Naranjo.pdf>
- Ortega Giménez, A., & Gonzalo Domenech, J. (2018). Nuevo marco jurídico en materia de protección de datos de carácter personal en la Unión Europea. *Revista de la Facultad de Derecho*, (44), 31-73. Obtenido de Revista de la Facultad de Derecho: <https://dx.doi.org/10.22187/rfd2018n44a2>
- Parlamento Europeo y Consejo de la Unión Europea. (2016). *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos*. Obtenido de Diario Oficial de la Unión Europea Núm. 119.: <https://www.boe.es/doue/2016/119/L00001-00088.pdf>
- Roldán Carrillo, F. (28 de Enero de 2020). *Los ejes centrales de la protección de datos: consentimiento y finalidad. Críticas y propuestas hacia una regulación de la protección de datos personales en Ecuador*. Obtenido de USFQ Law Review: <https://revistas.usfq.edu.ec/index.php/lawreview/article/view/2184>
- Roldan Carrillo, F. (2021). *USFQ Law Review*. Obtenido de Los ejes centrales de la protección de datos: consentimiento y finalidad. Críticas y propuestas hacia una regulación de la protección de datos personales en Ecuador: <https://revistas.usfq.edu.ec/index.php/lawreview/article/view/2184>
- Salgado Seguí, V. (2010). *Intimidación, privacidad y honor en Internet nuestros derechos, en riesgo*. Obtenido de Telos: Cuadernos de comunicación e innovación: <https://dialnet.unirioja.es/servlet/articulo?codigo=3414616>
- Sentencia 001-14-PJO-C, 001-14-PJO-C (Corte Constitucional del Ecuador 23 de abril de 2015).
- Sentencia 182-15-sep-CC, 182-15-sep-CC (Corte Constitucional del Ecuador 3 de junio de 2015).
- Torres, N. (Mayo de Mayo de 2013). *Acceso a la información y datos personales: una vieja tensión, nuevos desafíos* . Obtenido de https://www.palermo.edu/cele/pdf/DatosPersonales_Final.pdf

- Troncoso Reigada, A. (Diciembre de 2012). *El desarrollo de la protección de datos personales en Iberoamérica desde una perspectiva comparada y el reequilibrio en los modelos de protección de datos a nivel internacional*. Obtenido de https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/10_Antonio-troncoso_FINAL.pdf
- Vera, C. (2 de Febrero de 2021). *Diferencias entre intimidad, privacidad y protección de datos*. Obtenido de EIP Escuela Internacional Postgrados: <https://eiposgrados.com/blog-dpo/diferencias-entre-intimidad-privacidad-y-proteccion-de-datos/>
- Villalba Fiallos, A. (2017). *Reflexiones jurídicas sobre la protección de datos y el derecho a la intimidad en la autodeterminación informativa (Tema Central)*. Obtenido de <https://repositorio.uasb.edu.ec/handle/10644/5944>
- Valverde Asencio, A.J. «*Protección de datos de carácter personal y derechos de información de los representantes de los trabajadores*», *Temas Laborales* núm. 118/2013, 2013, Págs. 13-54.
- Vera Saltos, M. A. «*¿Vida privada o muerte a la privacidad?: Protección de datos personales en la relación empresa-cliente en Ecuador*». septiembre del 2019, *USFQ LAW REVIEW*, Volumen VI (12 de marzo de 2019). <https://doi.org/10.18272/lr.v6i1.1397>.

DECLARACIÓN Y AUTORIZACIÓN

Yo, **Vivar Butiñá José Javier** con C.C: # 0926427808 autor/a del trabajo de titulación: **Alcance de la protección de datos personales en el marco legal ecuatoriano** previo a la obtención del título de **Abogado de los Tribunales y Juzgados de la República** 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, 20 de febrero de 2022



Vivar Butiñá José Javier

C.C: 0926427808

REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA
FICHA DE REGISTRO DE TESIS/TRABAJO DE TITULACIÓN

TÍTULO Y SUBTÍTULO:	Alcance de la protección de datos personales en el marco legal ecuatoriano		
AUTOR(ES)	Vivar Butiñá José Javier		
REVISOR(ES)/TUTOR(ES)	Palencia Núñez Mónica Irene Rosa		
INSTITUCIÓN:	Universidad Católica de Santiago de Guayaquil		
FACULTAD:	Jurisprudencia y Ciencias Sociales y Políticas		
CARRERA:	Derecho		
TÍTULO OBTENIDO:	Abogado de los Tribunales y Juzgados de la República		
FECHA DE PUBLICACIÓN:	20 de febrero de 2022	No. DE PÁGINAS:	21
ÁREAS TEMÁTICAS:	Derecho Informático, Derecho Administrativo, Derecho Penal, Derecho Constitucional		
PALABRAS CLAVES/ KEYWORDS:	Datos Públicos, Datos Personales, Competencia, Protección de Datos		
RESUMEN/ABSTRACT (150-250 palabras):	<p>El presente estudio plantea determinar hasta qué punto los datos personales de los ecuatorianos se encuentran protegidos, considerando el marco legal vigente en el país. En el país se encuentra vigente la Ley del Sistema Nacional de Registro de Datos Públicos que rige para las instituciones tanto públicas como privadas que poseen la custodia de información a la cual, de acuerdo al artículo 18 de la Constitución de la República, en su numeral segundo, todas las personas tienen derecho a acceder. El objetivo de dicha ley es garantizar la seguridad jurídica, organizar, regular, sistematizar e interconectar la información con transparencia, eficacia y eficiencia. Sin embargo, en la práctica, cuando una persona ya sea natural o jurídica ejerce este derecho, y no sólo accede, sino que procesa y almacena dicha data en otras plataformas, se obtienen espejos de información que luego resultan traspasables tanto dentro del territorio nacional o incluso en el exterior. Pese a que la SINARDAP, establece procedimientos, con altos estándares de calidad, para la custodia de datos, en la práctica, no logra articular con éxito los procesos posteriores a la salida de los mismos. Es por ello que surge una gran preocupación sobre en qué momento el acceso de terceros a dichos datos, pueden ocasionar un desmedro o afectación a la persona titular o dueña de dichas referencias. Se evidencia, por ejemplo, que la Ley de Protección de Datos no determina puntualmente qué referencias personales, se deberían considerar como sensibles a vulnerar derechos fundamentales como la intimidad y la privacidad.</p>		
ADJUNTO PDF:	SI	NO	
CONTACTO CON AUTOR/ES:	Teléfono: +593-4-985142844	E-mail: jbutinaasociados@gmail.com	
CONTACTO CON LA INSTITUCIÓN (COORDINADOR DEL PROCESO UTE)::	Nombre: Reynoso Gaute, Maritza Ginette		
	Teléfono: +593-4-3804600		
	E-mail: maritza.reynoso@cu.ucsg.edu.ec		
SECCIÓN PARA USO DE BIBLIOTECA			
Nº. DE REGISTRO (en base a datos):			
Nº. DE CLASIFICACIÓN:			
DIRECCIÓN URL (tesis en la web):			