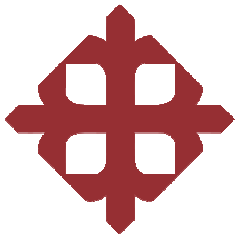


UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES Y POLITICAS

CARRERA DE DERECHO

TEMA:

ANÁLISIS DEL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES Y HABEAS DATA

AUTOR:

GRANDA MARTÍNEZ, JULISSA VICTORIA

Trabajo de titulación previo a la obtención del título de

ABOGADA DE LOS TRIBUNALES Y JUZGADOS DE LA REPUBLICA DEL ECUADOR

TUTOR:

AB. MGS. XAVIER PAÚL CUADROS AÑAZCO

Guayaquil, Ecuador

28 de agosto del 2019

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES Y POLITICAS

CARRERA DE DERECHO

CERTIFICACIÓN

Certificamos que el presente trabajo de titulación, fue realizado en su totalidad por **GRANDA MARTÍNEZ, JULISSA VICTORIA** como requerimiento para la obtención del título de **ABOGADA DE LOS TRIBUNALES Y JUZGADOS DE LA REPÚBLICA DEL ECUADOR.**

TUTOR

f. _____
AB. MGS. XAVIER PAÚL CUADROS AÑAZCO

DIRECTOR DE LA CARRERA

f. _____
AB. MARIA ISABEL LYNCH DE NATH

Guayaquil, 28 de agosto del 2019

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES Y POLITICAS

CARRERA DE DERECHO

DECLARACIÓN DE RESPONSABILIDAD

Yo, **GRANDA MARTÍNEZ JULISSA VICTORIA**

DECLARO QUE:

El Trabajo de Titulación, **ANÁLISIS DEL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES Y HABEAS DATA,** previo a la obtención del título de **ABOGADA DE LOS TRIBUNALES Y JUZGADOS DE LA REPUBLICA 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, 28 de agosto del 2019

LA AUTORA:

f. _____
GRANDA MARTINEZ JULISSA VICTORIA

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES Y POLITICAS

CARRERA DE DERECHO

AUTORIZACIÓN

Yo, **GRANDA MARTÍNEZ JULISSA VICTORIA**

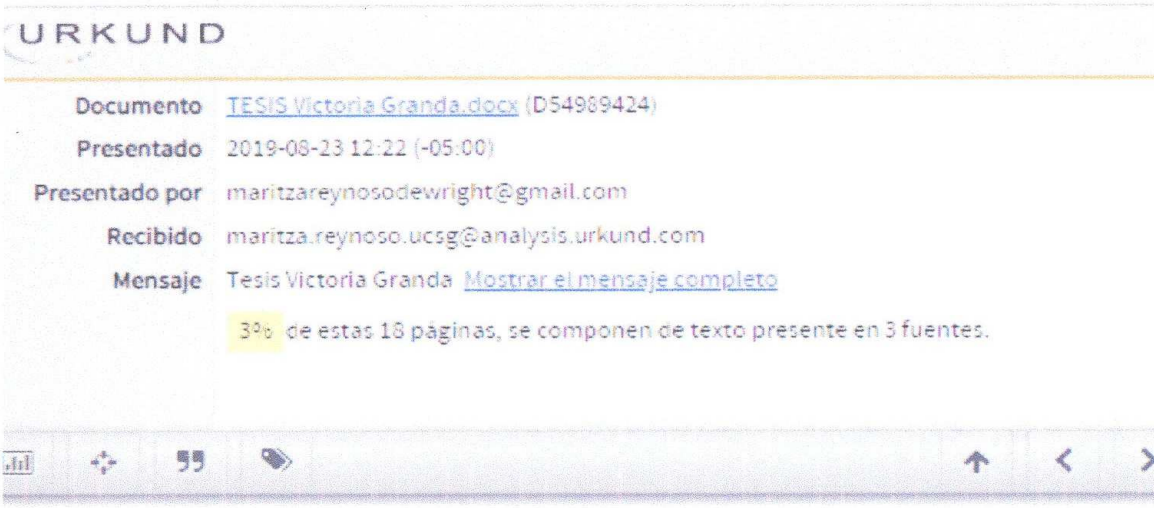
Autorizo a la Universidad Católica de Santiago de Guayaquil a la **publicación** en la biblioteca de la institución del Trabajo de Titulación, **ANÁLISIS DEL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES Y HABEAS DATA**, cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y total autoría.

Guayaquil, 28 de agosto del 2019

LA AUTORA:

f. _____
GRANDA MARTÍNEZ JULISSA VICTORIA

URKUM



AB. XAVIER PAUL CUADROS AÑAZCO

TUTOR – DOCENTE

AGRADECIMIENTO

A todas las personas, momentos y experiencias que me impulsaron a seguir mis sueños y nunca rendirme, en especial a mi familia, José Alejandro, Julissa y María Emilia. Gracias por creer siempre en mí.

A mis tíos, Judith, Jorge, Inés, Raquel, María Eugenia, Mario, Fabiola y mi abuela Bertha, que tuvieron la valentía de cuidarme y formarme en la persona que soy hoy.

A Cesar, quien tuvo la paciencia y el cariño de acompañarme en este viaje.

A Beatriz, que me ayudó a ver siempre lo bello de vivir, respirar y amar incluso cuando es difícil.

DEDICATORIA

A Lilia Beatriz Menéndez Marquínez, este trabajo es tan tuyo como mío, hermana querida.

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES Y POLITICAS

CARRERA DE DERECHO

TRIBUNAL DE SUSTENTACIÓN

f. _____

Abg. Mgs. José Miguel García Baquerizo

DECANO DE LA FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES Y POLITICAS

f. _____

Abg. Luis Eduardo Franco Mendoza

COORDINADOR DEL ÁREA

f. _____

Abg. Mgs. Santiago Efraín Velázquez Velázquez

OPONENTE

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

Facultad: Jurisprudencia

Carrera: Derecho

Periodo: UTE A-2019

Fecha: 26 de agosto de 2019

ACTA DE INFORME FINAL

El abajo firmante, docente tutor del Trabajo de Titulación denominado " ***ANÁLISIS DEL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES Y HÁBEAS DATA",*** elaborado por la estudiante ***JULISSA VICTORIA GRANDA MARTÍNEZ*** certifica que durante el proceso de acompañamiento dicho estudiante ha obtenido la calificación de ***10/10 (DIEZ),*** lo cual lo califica como ***APTO PARA LA SUSTENTACIÓN***

AB. MGS. XAVIER PAUL CUADROS AÑAZCO

INDICE

RESUMEN

El mundo globalizado, tecnológico e interconectado, genera situaciones que ponen en riesgo nuestra vida privada. Es por ello, que derechos fundamentales como la intimidad y los datos personales requieren de especial protección. La protección de datos de carácter personal no ha sido regulada en el Ecuador, a pesar de estar sujetos a protección por mandato constitucional, no obstante, no existe un mecanismo jurídico directo que los ciudadanos puedan utilizar a fin de ejercer este derecho. Se ha considerado al Habeas Data como método idóneo para su protección. Sin embargo, en este trabajo, explicaré por qué es necesario una ley orgánica de protección de datos personales y derecho a la intimidad a fin de que podamos entender la naturaleza de la protección de datos, qué protege y a quiénes protege, el ámbito de aplicación, y por qué exige una autoridad competente ante la vulneración a estos derechos.

Palabras claves: *protección de datos personales, derecho a la intimidad, derecho informático, derecho constitucional, habeas data.*

ABSTRACT

The globalized, technological and interconnected world generates situations that put our privacy at risk. This is the main reason why fundamental rights such as privacy and personal data require special protection. The protection of personal data has not been regulated in Ecuador, despite being subject to protection by constitutional mandate, however, there is no direct legal mechanism that citizens can use in order to execute it. Habeas Data has been considered as the ideal method for its protection. However, I will explain why is necessary a law on the protection of personal data and the right to privacy, in order to understand the nature of data protection, what it protects and who it protects, the range of application, and why it requires a competent authority in spite of violation of these rights.

Key Words: *Personal data Protection, Right to Privacy, Constitutional Right, habeas data, Cyberlaw.*

1.1 CAPITULO 1

1.1 CONTEXTO HISTORICO JURIDICO

Actualmente vivimos el fenómeno industrial y tecnológico conocido como Revolución Digital, esto es, de acuerdo a la *International Telecommunications Union* o ITU, el desarrollo de las TIC's – Tecnologías de la Información y Comunicación - y su aplicación en la vida cotidiana. De esta relación surge y evoluciona la Sociedad de Información, como la transformación tanto de individuos, gobiernos, empresas y organizaciones por las TICs con una incidencia directa en el desarrollo tecnológico y la aplicación de derechos fundamentales. como expresa Miguel Davara:

"..las nuevas tecnologías ya no son solamente una herramienta útil en las funciones rutinarias de gestión y control económico de la empresa en su faceta interior; las nuevas tecnologías tienen su verdadero interés en la unión - casi por naturaleza - con las telecomunicaciones y su apertura hacia el mundo exterior que, al no tener límites aparentes, plantea serias dudas en cuanto al respeto de los derechos básicos de los individuos y su estructuración en una diferente organización social, que permita no poner puertas al campo, con el paralelo respeto a los derechos de la persona y su desarrollo en libertad dentro de la convivencia." (2015, p. 25)

Esta transformación digital también se ha proyectado en el Derecho y el ordenamiento jurídico, sin embargo, esta situación crea una serie de ventajas y desventajas, que en lo principal puede afectar a los derechos fundamentales de las personas, en relación a la vida privada, intimidad, y especialmente a la información de carácter personal que se registra. En el marco de los derechos fundamentales, en concreto los personalísimos, se evidencia una evolución de los conceptos de intimidad y protección de datos de carácter personal o autodeterminación, tanto como evolución histórica, así como su impacto jurídico.

Primero nace en Grecia el concepto de libertad y la distinción entre lo público y lo privado, mas no como los conceptos actuales que aceptamos, sino como una condición personal. Que abre paso a la libertad de conciencia, libertad de expresión y respeto a la intimidad. Y es en Roma, donde estas esferas se separan y se representa claramente en el derecho romano, puesto que la intimidad se refleja en la propiedad privada. (Musti, 2000, p. 338). Como antecedente jurídico contemporáneo, tenemos el ensayo escrito por Samuel Warren y Louis Brandeis y publicado por la *Harvard Law Review* en 1890, titulado *The right to the privacy,* en este texto, mencionan el derecho a ser dejado solo o a no ser molestado, en ingles *the right to be let alone,* como parte de la esfera íntima de la persona. Así, la aplicación del derecho a la intimidad, se relacionaba con el derecho al honor y a la buena imagen, más que con la autodeterminación de la información, porque en las demandas planteadas se hacía alusión al daño de los comentarios y opiniones vertidas de la prensa acerca de ciertas figuras e individuos.

Sin embargo, es en Europa donde el desarrollo tanto social, de la información y el Derecho conforman el contexto actual, que ha tenido como consecuencia el reconocimiento del derecho a la intimidad, a la protección de datos y la progresiva creación de lo que se ha denominado cultura de protección de datos, que consiste en la creciente sensibilización hacia el valor que tienen los datos personales, sensibilización que ha ido de la mano de un mayor conocimiento de los derechos y medios de protección que el ordenamiento jurídico europeo y tratados internacionales ofrecen en este sentido.

Así, el reconocimiento y la profundización en el derecho a la intimidad personal y familiar, tuvo como primer antecedente normativo, la Declaración Universal de los Derechos del Hombre, declaración adoptada en París por la Asamblea General de las Naciones Unidas en su Resolución 217 A-III, de 10 de diciembre de 1948, el cual indica que “nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, no de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques”.

Con este precedente, inició un desarrollo extensivo, tanto a nivel legislativo como comunitario europeo en los últimos 60 años, en el cual el derecho a la intimidad y el derecho a la Protección de Datos de carácter personal se disgregan, el cual corresponde a las nuevas demandas individuales derivadas de los riesgos de la informatización y sistematización de todos los aspectos de la vida, que hace necesarios nuevos instrumentos de protección. En el Ecuador se ha efectivizado vía Constitución mediante la acción de habeas data.

1.2 CONCEPTOS Y NOCIONES DE LA PROTECCION DE DATOS

INTIMIDAD, PRIVACIDAD Y PROTECCION DE DATOS PERSONALES

La doctrina utiliza la expresión protección de datos en lo referente a la protección jurídica de la persona frente a la tecnología que automatiza sus datos. A continuación, desarrollaré los siguientes conceptos relativos a la materia, a fin de no incidir en falsos o erróneas acepciones. La intimidad, como ya vimos, es un derecho fundamental, personalísimo que protege tanto la intimidad personal como familiar, desde la esfera de la privacidad. Sin embargo, el término privacidad no debe confundirse con intimidad. En parte, la confusión se debe en parte a la traducción e introducción en el debate del término inglés *privacy*. En el derecho anglosajón es interpretado como el poder de exclusión del conocimiento de los demás de la esfera personal, como una manifestación más del derecho a la intimidad y en términos generales al derecho a no ser molestado.(Toscano, 2017, p. 540).

Por otro lado, la protección de datos de carácter personal, es un derecho derivado de la vida privada, que constituye un derecho autónomo e independiente; se trata de un derecho innato del hombre que protege de la revelación y tratamiento no consentido de datos que afecten directamente a aspectos de su personalidad y por tanto, protege a la persona frente a los tratamientos no autorizados de cualquier clase de dato personal ya que todos los tratamientos y la información obtenida a partir de ellos, puede ser relevante a estos efectos. (Zavallos, 2013, p. 86). La protección, entonces no

depende de la sensibilidad de los datos, sino del uso o fin que se les otorgue a estos; principalmente protege el consentimiento de uso de los datos de carácter personal, teniendo en cuenta que no porque una persona o la administración posea conocimiento de un dato personal incurre en una vulneración al mismo.

El objeto de protección lo constituye la persona, concretamente al respeto de sus derechos y al libre ejercicio de los mismos. Así se salvaguarda la esfera privada frente a cualquiera, incluso frente a la Administración; sin que ello suponga este sea un derecho arbitrario y sin control. (p. 86). Toda vez que el derecho a la protección de datos de carácter personal tutela el control del titular de los datos frente a injerencias ajenas de forma no autorizada; así el afectado tiene derecho a conocer de qué información disponen los terceros, con qué finalidad se realice su tratamiento y cuál será su utilización.

DATOS DE CARÁCTER PERSONAL, SENSIBLES E INFORMACION PÚBLICA

En el mundo de hoy, toda actividad humana es traducida a datos y sistematización de estos. Los datos contienen información, en consecuencia, de la información de un individuo, se pueden extraer a través de procesos de tratamiento, ciertos perfiles que podrían hacer identificable al individuo. Estos datos, a su vez, serán sensibles o no sensibles, y esto dependerá de la protección que el Estado les otorgue. Cabe indicar, como veremos más adelante, que la legislación ecuatoriana no provee definición de datos personales clara, y confunde información personal con datos sensibles.

Los datos personales consisten en toda información que nos identifica o nos pueda identificar, que son objeto de tratamiento; y no comprenden exclusiva o inclusivamente información íntima o sensible del titular. Por lo tanto, podemos señalar que se considera dato personal a toda información numérica, alfabética, también imágenes - gráfica y fotográfica -, acústica - sonidos y voces - o cualquier otro de tipo de información con las condiciones

de que puedan ser recogidas, registradas, tratadas o transmitidas y que pertenezcan a una persona física identificada o identificable. Se anota que no solo se refiere a datos habituales o comunes, sino incluso a aquellos que la persona desconozca sobre sí misma, (Davara Fernández de Marcos, 2011, p. 141).

De manera que los datos sensibles contienen información personal, y serán especialmente protegidos; según el Reglamento Europeo de Protección de Datos (2018), los relativos a: opiniones políticas, afiliación sindical, convicciones religiosas, convicciones filosóficas, origen racial o étnico, datos relativos a la salud, vida sexual, dato genético, dato biométrico y orientación sexual. Los datos personales no sensibles, serían aquellos de dominio público y que cualquier, en teoría, podría tener acceso y conocimiento, como: nombre, domicilio, teléfono, email, cedula, fecha y lugar de nacimiento, edad, nacionalidad, etc.; y serán datos públicos los datos patrimoniales, migratorios y académicos, pues los mismos reposan en ficheros o registros públicos.(Álvarez, 2017, p. 6). Adicional, debo indicar que la Dirección Nacional de Registro de Datos Públicos, ha realizado un proyecto de datos abiertos, los cuales son aquellos datos accesibles, liberados, publicados o expuestos sin naturaleza reservada o confidencial y que pueden ser utilizados, reutilizados y redistribuidos por cualquier persona.

1.3 ELEMENTOS DE LA PROTECCION DE DATOS

El derecho a la protección de datos personales existe porque nuestros datos reciben un tratamiento. Se considerará tratamiento cualquier operación que llevemos a cabo sobre datos personales, con independencia de que éste sea o no automatizado. Este tratamiento, jurídicamente interesa porque a fin de precautelar la esfera privada, debe existir un responsable y encargado del tratamiento, niveles de seguridad y confidencialidad, y una autoridad competente a la que acudir en caso de trasgresión al derecho, así como la imposición de sanciones o medidas correctivas y acciones para daños y prejuicios. Usaré como referencia jurídica el Reglamento Europeo

para la Protección de Datos, vigente desde el año 2018, el cual tiene fuerza obligatoria en el marco legal de integración comunitario.

TRATAMIENTO DATOS – ENCARGADO Y RESPONSABILIDAD

El principio para el tratamiento de los datos personales se puede manifestar en: el consentimiento a ser informado y conocer el uso que tendrán. De manera que el titular decide, quien, cuando, como y para que se trata sus datos; así como poder ejercitar, en su caso, los derechos y garantías que la ley le reconozca, así como la actualización de los datos, rectificación, anulación, cancelación; art. 92 de la Constitución de la Republica. Pero en sí, el tratamiento de datos son las operaciones que permiten procesar, conservar, transferir, registrar, o alterar los datos. Se considera como tratamiento automatizado de datos cuando los datos ingresan a los sistemas de información, esto es, que hayan sido escaneados, enviados por email, chat, u otro medio electrónico, así como su configuración en una plataforma digital o compartida en red. Los datos que se encuentren en registro de papel o físicos, o de manera análoga, son considerados manuales.

En un tratamiento de datos personales podemos distinguir las siguientes fases: Toma de datos, tratamiento de datos, utilización y en su caso comunicación. (Davara Rodríguez, 2015, p. 66). La definición de estas fases debe servir como esquema previo para el análisis de tratamientos complejos, y nos permitirá sistematizar el estudio de la materia, así como identificar los riesgos y obligaciones asociados a cada uno de ellos. Los datos personales que estén en tratamiento obedecerán a una serie de características para su protección, esto es, que sean recogidos con fines determinados explícitos y legítimos, Los datos personales deben ser adecuados, pertinentes y limitados a lo necesario en relación con el tratamiento; deben ser exactos y estar siempre actualizados. El tratamiento de datos se puede dar con el consentimiento o no del titular, dependiendo de su uso y sus excepciones, siendo por regla general que siempre se necesite el consentimiento.

Indicaba que el tratamiento tiene fases, para lo cual desde un inicio deberá existir un responsable y a su vez, un encargado. Esta figura responsable, para la Unión Europea en el REPD (2018) es “la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que solo o junto con otros, determine los fines y medios del tratamiento...”; de manera que el responsable es quien decide sobre el tratamiento de los datos. El encargado, por otro lado, será quien actúa por cuenta del responsable.

CONFIDENCIALIDAD Y SEGURIDAD

La confidencialidad incide al responsable, y del encargado, del tratamiento de datos a fin de que no se haga pública la información protegida sin el consentimiento del titular de dicha información. La confidencialidad es fundamental al momento de determinar responsabilidades civiles y penales, tomando en cuenta el incremento de ataques informáticos, la vigilancia masiva de ciertos gobiernos a sus ciudadanos, y la falta de cuidado en el manejo de datos personales por parte de instituciones públicas y privadas. (Álvarez, 2017, p. 10). La confidencialidad comporta que el responsable del tratamiento, así como todas aquellas personas que participen en cualquiera de sus fases, no puedan revelar ni dar a conocer su contenido teniendo el deber de guardarlos. Este deber es una exigencia básica y comporta que los datos tratados no pueden ser conocidos por ninguna persona o Entidad ajena fuera de los casos autorizados. Así las personas mantienen el poder de control o disposición sobre sus datos, pues se les garantiza que existe la confidencialidad y el deber de secreto.

La seguridad en la protección de datos personales es la aplicación de medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado a los riegos y prevención. El responsable y el encargado del tratamiento en cualquier fase, serán quienes apliquen estas medidas, dependiendo del nivel de seguridad que tengan los datos personales, e íntimos. De acuerdo a la REPD (2018) se deben aplicar una serie de medidas de seguridad en el tratamiento de estos datos, para ello la seguridad se valora según en el enfoque de riesgo. No obstante, se puede

implementar tres niveles de seguridad: básico, medio y alto en función al análisis de riesgo y establecer las medidas técnicas y organizativas, por lo que se debe contemplar para su implementación: a) El coste de la técnica; b) Los costes de aplicación; c) La naturaleza, el alcance, el contexto y los fines del tratamiento; y d) Los riesgos para los derechos y libertades.

En un nivel básico con gestione soportes y documentos, autorizaciones, copias de respaldo, recuperación y custodia. A un nivel intermedio, con el nombramiento del responsable de seguridad, auditorias y registro de incidencias. Y finalmente con un nivel alto, que se caracteriza por el cifrado, registro de acceso, y transmisión de datos en redes, los cuales contendrán la seudonimización o anonimización, el cifrado, la necesidad de un informe de impacto sobre la privacidad; así como un registro de accesos, con fecha y personal que accedió; y personas autorizadas.

AUTORIDAD RESPONSABLE DE LA PROTECCION DE DATOS

Es potestad de los Estados el delegar una autoridad la competencia para hacer efectiva la tutela de los derechos establecidos en las leyes de protección de datos personales. En el caso de la Unión Europea, el Reglamento delega dicha responsabilidad a cada miembro de la Unión, pero recomienda la independencia de dicha autoridad. Por ejemplo, en España la autoridad es la Agencia de Protección de Datos, un ente de derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones públicas en el ejercicio de sus funciones.

En general la autoridad de protección de datos personales está concebida como un ente de derecho público. En países de la región como Colombia depende de la Superintendencia de Industria y Comercio, a través de una delegación para la protección de datos personales; mientras que en Perú depende del Ministerio de Justicia, a través de la Dirección Nacional de Justicia. En nuestro país, la Dirección Nacional de Registro de Datos Públicos, DINARDAP, quien ha impulsado un anteproyecto en varias vías de

debates, plantea la posibilidad de ser la Autoridad Nacional de Protección de Datos Personales quien ejercería la vigilancia y control.

ACCIONES DE INDEMNIZACION Y POTESTAD SANCIONADORA DENTRO DEL REGIMEN DE PROTECCIÓN

Los tratamientos de datos personales pueden causar daños y perjuicios, tanto patrimoniales como no patrimoniales, por supuestos que recaen en un incumplimiento a la seguridad y evaluación de riesgos por parte de los responsables, encargados y delegados del tratamiento, así como también en alguna violación de un bien jurídico especialmente protegido. (Rubí Puig, 2018, p. 2) La producción de un daño derivado de un tratamiento de datos personales permitirá al afectado ejercer, en función de las características de cada caso, varías acciones para su resarcimiento. Así el titular podrá obtener una indemnización por los daños y perjuicios sufridos frente al responsable o el encargado del tratamiento de los datos personales que hubieran infringido la normativa sobre protección de datos. Todo esto, además de las vías de reparación que se prevé por la vía civil por responsabilidad extracontractual por culpa, o la reparación integral que se puede solicitar en una acción constitucional, una vez que se haya declarado mediante sentencia la vulneración al derecho o bien jurídico protegido.

Por otro lado, la Autoridad de Protección de Datos, como ya indicamos deberá ser un ente administrativo, toda vez que se le debe otorgar una potestad sancionadora. Para el efecto, podrá imponer grados de infracción, desde leve, grave y muy grave; y en función de las sanciones, la cuantía. Los criterios de graduación de las sanciones responden a un criterio del volumen de negocio o actividad del infractor. En caso de incumplimiento por las Administraciones públicas, estás tendrán como sanción la adopción de medidas correctoras, o como mucho, medidas correctoras contra el empleado público infractor. Las multas podrán imponerse como complemento o en sustitución de otras medidas como la advertencia, apercibimiento, orden de que se atienda una solicitud de ejercicio de derechos, orden de que el tratamiento se ajuste a las condiciones legales,

limitaciones temporales o definitivas del tratamiento, retirada de certificaciones y suspensión del flujo transfronterizo de datos. Además, el ánimo sancionatorio estaría a cargo de la propia Autoridad, toda vez que podrá realizar la remisión de las reclamaciones que no se hayan formulado previamente ante él, disponiendo de un plazo previo para poder resolverlas y de este modo evitar la sanción. (Medina, 2018, para. 3)

1.4 NATURALEZA JURIDICA

Como he indicado a lo largo de este capítulo, la legislación ecuatoriana no ha desarrollado una forma efectiva de precautelar ni de ejercer el derecho a la protección de datos de carácter personal, a diferencia de la Unión Europa, no existe una concientización de la protección; o un poco más cercano a nuestra región como Colombia, Uruguay y Argentina. No obstante, la Constitución de la República del Ecuador 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 (2008). Ahora bien, no existe un mecanismo jurídico directo que los ciudadanos puedan utilizar porque no existe una norma sobre la Protección de Datos; entonces estamos ante una garantía de rango constitucional que no procura una autoridad, una sanción ni una vía óptima.

La Ley de Comercio electrónico, firmas electrónicas y mensajes de datos, en el Art. 9, nos da la única definición sobre datos personales existente en la legislación ecuatoriana, e indica que “son aquellos datos o información de carácter personal o íntimo, que son materia de protección en virtud de esta Ley” (2014), la cual resulta muy amplia y vaga. Para lo cual, si existiera una ley de protección de datos de carácter personal, podría remitirse a la misma. Por otro lado, la Ley Orgánica de Telecomunicaciones (2015), hace referencia a el derecho de intimidad, al deber de la información, los

procedimientos de revelación que se debe seguir a la entrega de la información, el control técnico que se debe de tener para que se usen las medidas necesarias para proteger los datos personales, y recalca que los prestadores de servicios ya sean públicos o privados no podrán hacer use de los datos personales para fines comerciales, esto es, el tráfico de datos.

Y finalmente, encontramos en el Código Orgánico Integral Penal, el delito de violación a la intimidad, en el cual incurrirá en delito “La persona que, sin contar con el consentimiento o la autorización legal, *acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y video, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio*, será sancionada con pena privativa de libertad de uno a tres años”. Y nos encontramos ante el mismo vacío, pues no existe en nuestra legislación una definición precisa de datos personales, y el objeto en realidad no son los datos personales, sino los datos sensibles e íntimos que puedan repercutir en la intimidad de la persona afectada.

El derecho a la protección de datos personales o la autodeterminación de la información estaría inicialmente contenido en el derecho a la protección a la vida privada y familiar, como mencionamos anteriormente. Sin embargo, existen nociones que consideran que el derecho a la protección de datos personales es independiente del derecho a la vida privada y esta diferencia dependerá de la legislación de cada país. (Orellana Robalino, 2017, p. 2) En la Unión Europea y en Latinoamérica de forma general se aplica el criterio de considerar el derecho a la protección de datos personales como parte del derecho a la privacidad, mientras que en Estados Unidos el derecho a la protección de datos es independiente, porque existen datos personales que pueden ser compartidos a terceros sin mayor riesgo a que atente contra su vida privada.

En consecuencia, no existe una ley específica de datos personales, ya que hay un modelo de protección más flexible que permite la autorregulación y el control de los datos personales de conformidad con el sector e industria que los maneja, tales como bancos, compañías de e-comerce,

universidades, proveedores de servicios de internet, entre otros. (Soto L., Simpson A., 2015, p. 208). Sin embargo, existen datos sensibles como aquellos contenidos en la historia clínica de pacientes, o datos proporcionados por menores de edad en internet, entre los más importantes, que son regulados por leyes específicas.

Por lo expuesto, existe la necesidad de precautelar, proteger, controlar y sancionar los actos y hechos que afecten negativamente a los sujetos sin que estos hayan tenido conocimiento de lo que ha sucedido con los datos y mensajes proporcionados electrónicamente. Esta tarea exige la creación de una ley de protección de datos, así como un ente administrativo y autónomo que regule, sancione y proteja los datos personales de la ciudadanía, y que los individuos puedan ejercer efectivamente su protección a través de los derechos ARCO.

CAPITULO 2

2.1 EL DERECHO A LA PROTECCION DE DATOS DE CARÁCTER PERSONAL Y SU AMBITO DE APLICACION

Si bien los derechos fundamentales tienen cuatro características: máximo rango, máxima fuerza jurídica, máxima importancia del objeto, y máximo grado de indeterminación.(Carbonell, 2003, p. 33) Es evidente que la protección de datos personales es un derecho fundamental, por lo que si bien existe validez en su fundamento y en sentido positivo, el Ecuador requiere la existencia de un ámbito de aplicación objetiva y sustancial del derecho. Actualmente el rápido procesamiento, transmisión y sistematización de la información personal constituye una vulneración a la protección de datos toda vez que sirven para la elaboración de perfiles de comportamiento, hábitos de consumo, y hasta de discriminación de cualquier individuo.

De manera que la identidad personal se supondría violentada, por ejemplo, del hecho que una persona fuera injustamente discriminada, o expuesta, debido a la divulgación o tratamiento sin consentimiento del mismo. Por consiguiente, este nuevo derecho fundamental constituye “un instituto de garantía de otros derechos fundamentales, en especial del derecho a la intimidad, pero no solo de este derecho... Atribuye a su titular un haz de facultades que consiste en el poder jurídico de imponer a terceros la realización o la omisión de determinados comportamientos”. (Troncoso, 2010, p. 69).

Ahora bien, a través de esta regulación europea por la concientización de la protección de datos personales en Latinoamérica, se puede establecer principios para su aplicación: 1) ser informado en la recogida de datos; 2) Conocer la existencia de ficheros y tratamientos de datos personales; 3) Acceder a ellos para comprobar qué información personal del afectado contienen; 4) Obtener la rectificación de los que no sean exactos; 5) Obtener la cancelación de los que no deban ser tratados o hayan perdido la calidad que en su día justificó el tratamiento; 6) Oponerse a un tratamiento cuando no se requiera, conforme a la ley, el consentimiento del afectado y concurran

motivos fundados y legítimos relativos a su concreta situación personal; 7) No sufrir perjuicios como consecuencia de decisiones tomadas exclusivamente en virtud de perfiles personales obtenidos informáticamente; 8) Ser resarcido de los sufridos a causa de tratamientos que no se ajusten a las condiciones legalmente establecidas; 9) Cabe añadir a todo lo anterior ser protegido por las instituciones especializadas creadas ex profeso para defender este derecho fundamental. (Piñar Mañas, Álvarez Caro, Recio Gayo, & Adsuara Varela, 2016, p. 229)

Una vez establecido los principios que delimitarían su aplicación, se puede determinar el ámbito de aplicación formal y sustancial, que sería útil si la legislación ecuatoriana finalmente estable codificar una ley orgánica acorde; esto es, para la aplicación formal: los tratamientos automatizados y manuales que se encuentren en el sector público como privado. Para el efecto, me remito al Reglamento Europeo de Protección de Datos (2018), así como a la legislación española en concreto. Los sistemas de información y la custodia de los datos en cualquiera de sus formatos implican la necesidad de analizar a profundidad el ciclo de vida del dato, esto es, el control sobre cómo viaja la información, cuándo se reproduce o duplica, dónde y cómo se almacena, a quién y cómo se envía, cuándo y cómo se destruye. Esto implica la necesidad de llevar a cabo una revisión completa del tratamiento que se realiza de los datos personales, prestando especial interés al puesto de vista técnico para la adecuada implantación y gestión de procedimientos legales.

En la aplicación sustancial, serán los datos de personas naturales, físicas lo que se proteja; entendiéndose que serán los titulares de la protección también incluye a los menores a través de la representación de sus representantes, quien además podrán dar su consentimiento a partir de la edad de 14 años, para la legislación española, por ejemplo. En principio se excluiría de la protección a las personas jurídicas y a las personas fallecidas. Sin embargo, los datos de contacto de empresarios individuales y de profesionales liberales, establece una presunción iuris tantum de prevalencia del interés legítimo del responsable cuando se lleven a cabo determinados tratamientos. En este sentido, se hace referencia a las

relaciones comerciales, siempre y cuando el tratamiento se refiera únicamente a los datos necesarios para la localización profesional del interesado con la única finalidad de mantener relaciones de cualquier índole con la persona jurídica en la que el afectado preste sus servicios.

Así también, los datos de las personas fallecidas en primer lugar, se excluyen del tratamiento del ámbito de aplicación. Sin embargo, se permite que las personas vinculadas al fallecido por razones familiares o, de hecho, o sus herederos, puedan solicitar el acceso, rectificación o supresión de los datos de carácter personal de las mismas, excepto cuando la persona fallecida o una ley lo prohíba expresamente, al igual que las personas o instituciones a las que el fallecido hubiese designado expresamente para ejercitar los derechos antes mencionados.

Y finalmente, una aplicación territorial, para la cual además del territorio nacional, se tomaría el modelo europeo de integración para la protección tanto en el tratamiento que se de en la circunscripción ecuatoriana, como los que se procesan o están establecidos en servidores internacionales. Además de amplias disposiciones relacionadas con la protección de datos personales y la privacidad, también regula su aplicación extraterritorial, pudiendo obligar no solo a las empresas ubicadas en la UE que traten datos personales, sino también a las empresas ubicadas en otros países que traten información personal de ciudadanos europeos, lo que incide directamente en el manejo de transmisión y cesión de datos internacionales

Carlos Gregorio en su estudio Protección de datos personales: Europa vs. Estados Unidos, todo un dilema para América Latina (Concha, López Ayllón, & Tacher Epelstein, 2004), propone evitar los inconvenientes de muchas Leyes nacionales de Protección de Datos Personales y lograr una norma común; para el autor esto corresponde no solo al carácter fundamental del derecho, sino también a ventajas comerciales, como por ejemplo en Argentina, Uruguay y Perú con el desarrollo de la protección de datos y medidas de seguridad.

Por lo expuesto, cabe preguntase por qué a diferencia de países de la región como Colombia, Perú, Chile, Argentina y Brasil, que ya habían establecido algunas medidas y políticas de protección de datos personales; y, sin embargo, con la entrada en vigor del REPD (2018), han dispuesto reformas a leyes en materia de privacidad, elevando sus estándares de protección de datos personales para cumplir con lo establecido en el reglamento de la UE, el Ecuador aún no ha establecido una regulación al respecto.

2.2 DERECHOS ARCO Y DERECHOS DEL TITULAR

Los derechos de acceso, rectificación, cancelación y oposición, también conocidos como derechos ARCO o derechos de las personas o del interesado, se conforman como un conjunto de garantías que la legislación española en materia de protección de datos establece para que los titulares de los mismos puedan tener un control sobre el uso que las entidades públicas y privadas hacen de los mismos. (Serrano Pérez, 2003, p. 343). Estos conforman el núcleo del derecho fundamental a la protección de datos. Estos derechos sólo pueden ser ejercidos por el titular de los datos, por su representante legal o por un representante acreditado, de forma que el responsable del tratamiento puede denegar estos derechos cuando la solicitud sea formulada por persona distinta del afectado y no se acredite que actúa en su representación.

El ejercicio de estos derechos se debe llevar a cabo mediante medios sencillos y gratuitos puestos a disposición por el responsable del fichero, los mismos serán independientes, toda vez que, no puede entenderse que le ejercicio de ninguno de ellos sea requisito previo para el ejercicio de otro. Adicional, están sujetos a plazo, por lo que resulta necesario establecer procedimientos para su satisfacción. En la legislación española, se tutela a través de la Agencia Española de Protección de Datos (AEPD), quien actúa conforme lo establecido en la ley, su reglamento y el REPD (2018). Estos derechos pueden ser modulados por razones de seguridad pública con los requisitos establecidos legalmente, para lo que se limitará el ejercicio de

estos derechos cuando sea una medida necesaria para: seguridad del Estado, defensa y seguridad pública; y prevención, averiguación, detección y castigo de infracciones penales.

Siguiendo el análisis de María Serrano (2003, p. 353), el derecho de acceso es por el cual el ciudadano puede conocer y adquirir de manera gratuita información sobre los datos personales que están siendo usados, y que, sin embargo, tiene un carácter intermedio con respecto a los demás derechos, puesto que la consecuencia de acceder a los datos y tener conocimiento de su estado puede condicionar el paso siguiente. El derecho de cancelación y rectificación tiene como rasgo común la capacidad de ser una injerencia activa en el tratamiento que realiza el Responsable del tratamiento, característica que por otro lado comparten con el de oposición. Según la misma autora (2005, p. 357, 358), la diferencia radica en que mientras que el derecho de cancelación se ejercita cuando nos encontramos frente a un tratamiento ilegítimo de datos, el de rectificación procede cuando existe constancia de una inexactitud o carencia. Los resultados de ambos derechos también son diferentes, así el primero dará lugar a la cancelación o supresión del dato, mientras que el segundo finalizará con la corrección de la información. Cabe destacar especialmente que el derecho a cancelación se amplía al mundo digital con el derecho al olvido, dentro del REPG, un derecho importante ante las trasgresiones que se vive tanto en blogs, como redes sociales. Es el de derecho que tiene cualquier persona a que se suprima todo enlace que contenga información personal en internet, o las copias o réplicas de tales datos. Por supuesto, no es tan sencillo como que un buscador elimine o desindexe un artículo o contenido que te afecte, porque solo se puede hacer efectivo si no se trata de información de interés público.

El derecho de oposición, es el derecho que tiene el titular de los datos personales a que no se use su información o cese en el mismo, tres supuestos concretos: 1) Cuando no sea necesario el consentimiento del interesado para proceder al tratamiento de sus datos personales; 2) cuando el tratamiento tengan por finalidad la realización de actividades de publicidad y prospección comercial; 3) y cuando el tratamiento tenga por finalidad

adoptar una decisión referida al afectado y basada únicamente en un tratamiento automatizado de sus datos de carácter personal.

El derecho de Limitación, así como el de Portabilidad, son introducidos recientemente en el marco legal europeo; el derecho de limitación significa que los datos personales solo pueden ser tratados con su consentimiento para la formulación, en el ejercicio o para la defensa de reclamaciones y con miras a la protección de los derechos de otra persona física o jurídica o por razones de interés público. Mientras que el de portabilidad, interesado tendrá derecho a que el responsable transmita sus datos a otro responsable del tratamiento o al mismo interesado, mediante un formato estructurado de uso habitual y lectura mecánica, cuando el tratamiento se efectúe por medios automatizados; este derecho existe en los casos cuando la exactitud de los datos de que se trate esté en duda o cuando los datos ya no sean necesarios para el fin original, pero no se pueden borrar por motivos jurídicos.

2.3 EL HABEAS DATA VS. LA PROTECCION DE DATOS DE CARÁCTER PERSONAL

En Latinoamérica la protección de datos no tiene una tradición tan arraigada como en Europa o Estados Unidos, consecuencia directa, de una parte, del escaso nivel de desarrollo que las TIC ’s que alcanzaron en estos países – la llamada brecha tecnológica -, sobre todo en las décadas de los 70 y 80, años en los que en Europa se estaba formando la que hemos denominado *conciencia de protección de datos*. Por otra parte, la existencia de regímenes totalitarios poco receptivos al reconocimiento de los derechos fundamentales que sirvieron como base para desarrollar el derecho a la protección de datos personales (Zaballos, 2013, p. 120). En este sentido, fue la Constitución Brasileña de 1988, el primer texto fundamental que reguló la materia adoptando un procedimiento basado en la acción del Habeas Data.

Se trataba de una acción concebida como una protección constitucional contra los abusos del poder y las ilegalidades cometidas por los administradores y encargados de gestionar datos personales para los

poderes públicos. El Habeas Data fue posteriormente adoptado por otras constituciones como es el caso de Argentina, Perú, Paraguay y Ecuador. (Piñar Mañas, Canales Gil, & Blanco Antón, 2005). La norma constitucional ecuatoriana establece la acción de habeas data en el Art. 92 (2008), para muchos es el mecanismo legal idóneo (Orellana Robalino, 2017, p. 1) para garantizar el ejercicio del derecho a la protección de datos personales que protege el derecho que tiene la persona al acceso y conocimiento de sus datos personales en registro públicos y privados (Hernández, 2012, p. 69).

El Habeas Data es un instrumento, una garantía constitucional, que permite a las personas conocer la información propia contenida en bases de datos públicas o privadas con el objetivo de autorizarla, modificarla, rectificarla o eliminarla para de esta forma ejercer el control de la información existente. El objeto del hábeas data es el acceso a toda la información del individuo que se encuentre bajo custodia, administración o tenencia del Estado o institución privada, mientras que el objeto del derecho a la información es más amplio, porque es aquel que se encuentre bajo custodia del Estado, al respecto se señala que “se refiere a toda la información en bases de datos públicas significante, cuya definición debe ser amplia, incluyendo toda la que es controlada o archivada en cualquier formato y medio”(Bazán, 2012, p. 66).

2.4 JURISPRUDENCIA COMPARADA Y ANALISIS DE JUSRISPRUDENCIA ECUATORIANA

Como ya he indicado en páginas anteriores, Argentina, Uruguay, quienes cuentan incluso con certificación por la Unión Europea; Perú y Chile han realizados avances significativos en materia de protección de datos y habeas data, para el efecto la jurisprudencia se encarga de llenar las imprecisiones o los vacíos normativos. Con este apartado, pretendo indicar que es factible tener una garantía constitucional, y sin embargo es necesario evolucionar a la par que estos países, tanto en la aplicación de habeas data como en una ley que regule el tratamiento, sanciones, autoridad, para una aplicación y distinción similar; para ello también se analizará los criterios de

la corte constitucional ecuatoriana para la aplicación de habeas data. Chile, por ejemplo, ha promovido la reforma del Ley 19628 (2017) por la cual se prevé la actualización y modernización del marco normativo e institucional para la defensa del derecho a la protección de datos personales. En este último caso se destaca la implementación de una Agencia de Protección de Datos Personales.

La Corte Suprema de Justicia de Argentina señala que la protección legal de controlar la veracidad de la información y el uso que de ella se haga, forma parte de la vida privada y se trata, como el honor y la propia imagen, de uno de los bienes que integran la personalidad. El hábeas data se le atribuye la configuración del concepto de autodeterminación informativa o libertad informática, que es reconocido actualmente en forma predominante como el fundamento del hábeas data; este derecho –se dijo– puede ser restringido por medio de una ley por razones de utilidad social, pero respetando el principio de proporcionalidad y garantizando que no se produzca la vulneración del derecho a la personalidad.

En Uruguay mediante sentencia No. 12 de 2008 del Tribunal de Apelaciones refiere, en cuanto al hábeas data, se pronunció sobre “el procedimiento previsto por los arts. 37 a 45 de la Ley No. 18331 de 11/8/2008 es el común que el ordenamiento jurídico prevé para las pretensiones que tengan por objeto exclusivo el hábeas data, o sea, el acceso a la información en bases de datos, su rectificación, inclusión o supresión”. Este mismo Tribunal, en relación en la sentencia No. 4 de 2015 señala que se debe citar *expresamente y no de modo tangencial o implícito en su exposición*, el derecho a la seguridad en la protección de datos personales, a la intimidad, inviolabilidad de las comunicaciones y exclusión de las acciones privadas del quehacer estatal cuando no afectan el ordenamiento jurídico, garantizados por los artículos 7 y 10 de la constitución uruguaya.

Por su parte, el Tribunal Constitucional de Perú en la Sentencia No. 71797-2002 apunta que el derecho a la autodeterminación informativa está destinado a proteger la intimidad, personal o familiar, la imagen y la

identidad frente al peligro que representa el uso y la eventual manipulación de los datos a través de los ordenadores electrónicos. Aunque el objeto sea la protección de la intimidad, el derecho a la autodeterminación informativa no puede identificarse con el derecho a la intimidad, personal o familiar, reconocido, a su vez, por el inciso 7) del mismo artículo 2 de la Constitución. La misma sentencia, sobre el hábeas data, agrega que "comprende, en primer lugar, la capacidad de exigir jurisdiccionalmente la posibilidad de acceder a los registros de información, computarizados o no …mediante el hábeas data, un individuo puede rectificar la información, personal o familiar, que se haya registrado; impedir que esta se difunda para fines distintos de aquellos que justificaron su registro o, incluso, tiene la potestad de cancelar aquellos que razonablemente no debieran encontrarse almacenados".

La Corte Constitucional del Ecuador en la Sentencia 001-14-PJO-CC, caso No. 0067-11-JDd e 2014, recoge un precedente dentro de la autodeterminación informativa, en concreto la Corte señala que "la autodeterminación informativa está supeditada, entonces, a la existencia de información que atañe a determinado sujeto y a la necesidad de que este tenga una esfera mínima de actuación libre respecto de dicha información, sobre la cual no debería existir una interferencia ilegítima por parte de terceros; asimismo, implica la posibilidad de que dentro de los límites que franquean la Constitución y la Ley, se tenga capacidad para ejercer cierto control sobre el uso que se haga de tal información, aunque el poseedor de la misma sea otra persona…". La sentencia indica que los datos están protegidos por medio de la garantía constitucional del hábeas data, siempre que cumplan con una función informativa respecto de las personas y sus bienes y, por ende, su comunicación, interpretación o tratamiento afecta en mayor o menor medida los derechos de aquel a quien se refieren.

La sentencia concluye que, para los jueces constitucionales ecuatorianos, el dato en sí mismo no es objeto de la acción de hábeas data sino únicamente aquel que puede llegar a cumplir una finalidad informativa, y que en efecto se convierte en información.(Naranjo, 2017, p. 12) No obstante, hay que adecuar el contexto, pues el derecho a la protección de datos personales también tiene como objetivo prevenir posibles tratamientos

de datos que pudieran generar un daño, mientras que el habeas data funciona cuando la vulneración ya se ha producido y por eso el individuo debe acogerse a esta garantía. En el caso de la autodeterminación informativa, implica la necesidad de garantizar la protección de la esfera íntima de las personas, esto es, los datos de carácter personal, así como la posibilidad de ejercer control sobre los datos personales del sujeto, aunque no se encuentren en su poder.

Así la Corte Constitucional emitió reglas de carácter vinculante sobre la acción, esto es, el hábeas data no puede ser presentado como mecanismo para requerir la entrega física de los documentos, sino solamente para conocer su existencia y tener acceso a él. Considera que es argumento sobre el problema a la determinación de que una persona jurídica puede beneficiarse de una provisión constitucional debe establecerse caso por caso según la naturaleza del derecho. En cuanto a la autodeterminación informativa, implica la necesidad de la protección de la esfera íntima de las personas y la posibilidad de ejercer control sobre estos datos. Finalmente, por las características del hábeas data no se considera constitucionalmente adecuado la limitación de las personas jurídicas como titulares del mismo, pero su información solamente se extiende a las personas asociadas o sus representantes legales.

CONCLUSION

En otras palabras, el habeas data es garantía del derecho a la intimidad, los datos informativos o con función informativa, y si bien su aplicación recae sobre otros derechos protegidos por esta garantía jurisdiccional como el honor, el buen nombre y la intimidad personal y familiar, en relación a la protección de datos personales es restrictiva, toda vez que su fin es el de otorgarle el acceso al titular previa solicitud. En el caso del derecho a la protección de datos personales, una ley orgánica tendría la característica coercitiva que emana de la misma naturaleza de ley, esto es, se establezca una autoridad administrativa con potestad sancionadora, determinación de responsabilidad en los tratamientos, acciones por daños y perjuicios por el decremento patrimonial y extrapatrimonial sufrido por titular en las infracciones a fin de ser indemnizados por el responsable o el encargado del tratamiento.

El hábeas data debe adaptarse al contenido de este derecho fundamental y resguardar no solo la información personal, sino sensible que es objeto de tratamiento. Aunque inicialmente los datos personales, no son necesariamente sensibles e íntimos, y carecerían de relevancia, en el tratamiento puede crear perfiles del individuo y afectar su autodeterminación informativa e incluso otros derechos fundamentales. Así, sigue siendo necesario una ley clara al respecto del tratamiento en todas sus fases, del responsable y encargado del tratamiento, las medidas de seguridad y autoridad competente para sancionar a los infractores, desde una óptica preventiva, o de oficio, a las acciones del titular.

El Ecuador necesita una ley de protección de datos personales para proteger el derecho a la vida privada de sus ciudadanos, y promover el desarrollo de empresas ecuatorianas de servicios en internet, y que puedan tratar datos de ciudadanos de todo el mundo. El proyecto de ley elaborado por fue una iniciativa importante, pero con la vigencia del Reglamento Europeo de Protección de Datos, este se debe actualizar y seguir las tendencias de seguridad, protección, no solo del derecho fundamental, como nos corresponde, sino por un modelo de integración legal y comercial.

RECOMENDACIÓN

Que la aplicación de la protección de datos se realice bajo una modalidad más directa, sencilla y coercitiva, con la creación de la Ley Orgánica de Protección de Datos Personales, un reglamento, y la creación o delegación de un ente administrativo, independiente y autónomo, con potestad sancionadora para la imposición de multas, que vigile y controle de oficio las actuaciones de empresas, individuos, del sector público y privado.

Que dentro del marco europeo se encuentra vigente el Reglamente Europeo de Protección de Datos, para lo cual, el Ecuador debería acoger y adaptar su ordenamiento, pues el habeas data como único medio jurisdiccional es insuficiente.

Que se establezcan los derechos arco, su procedimiento y plazos; que el titular tenga a disposición acciones de daños y prejuicios por la infracción del responsable y encargado.

Que es necesidad actualizar los niveles de seguridad, realizando evaluación de riesgo, para lo cual se deberá implementar un avance en la seguridad informática, tecnológica y análoga desde macroempresas a pymes, a individuos o colectivos que traten con información sensible y personal.

REFERENCIAS

Almuzara Almaida, C. (2007). *Estudio práctico sobre la protección de datos de carácter personal*. Valladolid: Editorial Lex Nova.

Álvarez, L. E. (2017). *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*. 19.

Blázquez Entonado, F. (2001). *Sociedad de la información y educación*. Mérida: Junta de Extremadura.

Carbonell, M. (Ed.). (2003). *Neoconstitucionalismo(s)*. Madrid: Editorial Trotta.

Celis Quintal, M. A. (n.d.). *LA PROTECCIÓN DE LA INTIMIDAD COMO DERECHO FUNDAMENTAL DE LOS MEXICANOS*.

CODIGO ORGANICO INTEGRAL PENAL. , R.O.S 180 § (2014).

Concha, H. A., López Ayllón, S., & Tacher Epelstein, L. (Eds.). (2004). *Transparentar al Estado: La experiencia mexicana de acceso a la información* (1. ed). México, D.F: Universidad Nacional Autónoma de México.

CONSTITUCION DE LA REPUBLICA DEL ECUADOR. , R.O.S 449 § (2008).

Corral Rosales. (n.d.). ¿Qué propone la Ley Orgánica de Protección de Datos Personales en Ecuador? | Gestión. Retrieved June 9, 2019, from https://revistagestion.ec/index.php/estrategia-analisis/que-propone-la-ley-organica-de-proteccion-de-datos-personales-en-ecuador

Corredor Higuera, J. A. (2015). La armonización en materia de protección al consumidor financiero en América Latina. *Boletín Mexicano de Derecho Comparado*, *48*(144), 931–972. https://doi.org/10.22201/iij.24484873e.2015.144.4956

Davara Fernández de Marcos, I. (2011). *Hacia la estandarización de la protección de datos personales: Propuesta sobre una "tercera vía o tertium genus" internacional* (1a. ed). Las Rozas, Madrid: La Ley.

Davara Rodríguez, M. A. (2015). *Manual de derecho informático* (11. ed. (rev. y puesta al día)). Cizur Menor (Navarra): Aranzadi.

Figueroa, R. (2013). El Derecho a La Privacidad En La Jurisdicción De Protección. *Revista Chilena de Derecho*, *40*(3), 859–889.

Garrido Elustondo, S., Cabello Ballesteros, L., Galende Domínguez, I., Riesgo Fuertes, R., Rodríguez Barrientos, R., & Polentinos Castro, E. (2012). Investigación y protección de datos personales en atención primaria. *Atención Primaria*, *44*(3), 172–177. https://doi.org/10.1016/j.aprim.2011.02.009

Garriga Domínguez, A. (2016). *Nuevos retos para la protección de datos personales: En la Era del Big Data y de la computación ubicua*. Retrieved from http://www.jstor.org/stable/10.2307/j.ctt1k85c6p

LEY ORGANICA DE TELECOMUNICACIONES. , R.O.S 439 § (2015).

LEY ORGANICA DEL SISTEMA NACIONAL DE REGISTRO DE DATOS PUBLICOS. , R.O.S 162 § (2010).

Medina Jara, J. (2018, April 9). Efectos del incumplimiento del nuevo reglamento de protección de datos. Retrieved August 21, 2019, from El Derecho website: https://elderecho.com/consecuencias-del-incumplimiento-del-nuevo-reglamento-de-proteccion-de-datos

Moreno Bobadilla, Á. (2015). *Estudio jurídico del derecho a la intimidad y su especial incidencia en el caso de los menores de edad*. 364.

Musti, D. (2000). *Demokratía: Orígenes de una idea*. Madrid: Alianza.

Naranjo Godoy, L. (2017). El dato personal como presupuesto del derecho a la protección de datos personales y del habeas data en el Ecuador. *Foro, Revista de Derecho*, (27), 63–82.

Noain Sánchez, A. (2016). *La protección de la intimidad y vida privada en Internet: La integridad contextual y los flujos de información en las redes sociales (2004-2014)*. Madrid: Agencia Española de Protección de Datos : Agencia Estatal Boletín Oficial del Estado.

Orellana Robalino, C. (2017). De la seguridad cibernética a la resiliencia cibernética aplicada a la protección de datos personales. *Foro, Revista de Derecho*, (27), 5–21.

Piñar Mañas, J. L., Álvarez Caro, M., Recio Gayo, M., & Adsuara Varela, B. (Eds.). (2016). *Reglamento general de protección de datos: Hacia un nuevo modelo europeo de privacidad* (1a edición). Madrid: Editorial Reus.

Piñar Mañas, J. L., Canales Gil, A., & Blanco Antón, M. J. (Eds.). (2005). *Protección de datos de carácter personal en Iberoamérica: II Encuentro Iberoamericano de Protección de Datos, La Antigua-Guatemala, 2-6 de junio de 2003*. Valencia: Agencia de Protección de Datos : Tirant lo Blanch libros.

Rebollo Delgado, L., Serrano Pérez, M. M., & e-libro, C. (2008). *Introducción a la protección de datos*. Madrid: Dykinson.

Rovira Viñas, A. (n.d.). *Reflexiones sobre el derecho a la intimidad en relación con la informática, la medicina y los medios de comunicación*. 7.

Rubí Puig, A. (2018). *DAÑOS POR INFRACCIONES DEL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES*. 35.

Saldaña, M. N. (2011). *EL DERECHO A LA PRIVACIDAD EN LOS ESTADOS UNIDOS: APROXIMACIÓN DIACRÓNICA A LOS INTERESES CONSTITUCIONALES EN JUEGO*. 34.

Serrano Pérez, M. M. (2003). *El derecho fundamental a la protección de datos: Derecho español y comparado* (1. ed). Madrid [Spain]: Civitas.

Solange Maqueo Ramírez, M. (2016). Análisis comparativo de las resoluciones emitidas por el tribunal de justicia de la unión europea y el instituto federal de acceso y protección de datos respecto del motor de búsqueda gestionado por Google y la protección de datos personales. *Boletín Mexicano de Derecho Comparado*, *49*(145), 75–100. https://doi.org/10.22201/iij.24484873e.2016.145.4992

Suñé Llinás, E., & Almuzara Almaida, C. (2002). *Tratado de derecho informático*. Madrid: Universidad Complutense, Facultad Derecho, Servicio Publicaciones Instituto Español de Informática y Derecho.

Toscano, M. (2017). Sobre el concepto de privacidad: La relación entre privacidad e intimidad. *Isegoría*, *0*(57), 533–552. https://doi.org/10.3989/isegoria.2017.057.06

Troncoso Raigada, A. (2009). Reutilización de información pública y protección de datos personales. *Revista General de Información y Documentación*, *19*, 243–264. https://doi.org/-

Zaballos Pulido, E. (2013). *LA PROTECCIÓN DE DATOS PERSONALES EN ESPAÑA : EVOLUCIÓN NORMATIVA Y CRITERIOS DE APLICACIÓN*. 508.

Zavala Baquerizo, J. (1996). *La informática y el derecho a la intimidad*. 16.

DECLARACIÓN Y AUTORIZACIÓN

Yo, **GRANDA MARTÍNEZ JULISSA VICTORIA** con C.C: # 0924797244 autor/a del trabajo de titulación: **ANÁLISIS DEL DERECHO DE LA PROTECCIÓN DE DATOS PERSONALES Y HABEAS DATA,** 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, 28 de agosto del 2019

f. _____

Nombre: **GRANDA MARTÍNEZ JULISSA VICTORIA**

C.C:**0924797244**

REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA			
FICHA DE REGISTRO DE TESIS/TRABAJO DE TITULACIÓN			
TEMA Y SUBTEMA:	**ANÁLISIS DEL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES Y HABEAS DATA.**		
AUTOR(ES)	**JULISSA VICTORIA GRANDA MARTÍNEZ**		
REVISOR(ES)/TUTOR(ES)	XAVIER PAÚL CUADROS AÑAZCO		
INSTITUCIÓN:	Universidad Católica de Santiago de Guayaquil		
FACULTAD:	JURISPRUDENCIA		
CARRERA:	**DERECHO**		
TITULO OBTENIDO:	**ABOGADA DE LOS TRIBUNALES Y JUZGADOS DE LA REPUBLICA DEL ECUADOR**		
FECHA DE PUBLICACIÓN:	28 de agosto del 2019	**No. DE PÁGINAS:**	29
ÁREAS TEMÁTICAS:	DERECHO CONSTITUCIONAL, DERECHO INFORMATICO, PROTECCION DE DATOS PERSONALES		
PALABRAS CLAVES/ KEYWORDS:	*protección de datos personales, derecho a la intimidad, derecho informático, derecho constitucional, habeas data*		

RESUMEN/ABSTRACT:

El mundo globalizado, tecnológico e interconectado, genera situaciones que ponen en riesgo nuestra vida privada. Es por ello, que derechos fundamentales como la intimidad y los datos personales requieren de especial protección. La protección de datos de carácter personal no ha sido regulada en el Ecuador, a pesar de estar sujetos a protección por mandato constitucional, no obstante, no existe un mecanismo jurídico directo que los ciudadanos puedan utilizar a fin de ejercer este derecho. Se ha considerado al Habeas Data como método idóneo para su protección. Sin embargo, en este trabajo, explicaré por qué es necesario una ley orgánica de protección de datos personales y derecho a la intimidad a fin de que podamos entender la naturaleza de la protección de datos, qué protege y a quiénes protege, el ámbito de aplicación, y por qué exige una autoridad competente ante la vulneración a estos derechos.

ADJUNTO PDF:	☒ SI	☐ NO
CONTACTO CON AUTOR/ES:	**Teléfono:** 593986211597	E-mail: victoriagrandam@gmail.com
CONTACTO CON LA INSTITUCIÓN (C00RDINADOR DEL PROCESO UTE)::	**Nombre: Ab. Luis Eduardo Franco Mendoza**	
	Teléfono: +593-994748073	
	E-mail: Luis.franco04@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):	