UNIVERSIDAD DE ESPECIALIDADES ESPÍRITU SANTO

FACULTAD DE DERECHO, POLÍTICA Y DESARROLLO

NUEVA VISIÓN DEL DERECHO DE PROTECCIÓN DE DATOS PERSONALES EN ECUADOR

TRABAJO DE TITULACIÓN QUE SE PRESENTA COMO REQUISITO PREVIO A OPTAR EL GRADO DE ABOGADO DE LOS JUZGADOS Y TRIBUNALES DE LA REPÚBLICA

AUTOR: SHEILA ANABELLA ZAMORA ÁLVAREZ

TUTOR: DR. FRANCISCO XAVIER JÁCOME MARÍN

SAMBORONDÓN, ENERO, 2022

Nueva Visión del Derecho de Protección de Datos Personales en Ecuador

Sheila A. Zamora, Universidad de Especialidades Espíritu Santo, sheilazamora@uees.edu.ec, Facultad de Derecho, Política y Desarrollo, Edificio P, Universidad de Especialidades Espíritu Santo, Kilómetro 2.5, Vía La Puntilla, Samborondón.

Resumen

El desarrollo de la tecnología avanza cada año y con ello se crean nuevas herramientas que han permitido facilitar la recolección del flujo de datos personales. Este fenómeno ha sido objeto de estudio por varios juristas e investigadores a causa del evidente peligro en la falta de regulación en el tratamiento de los datos de las personas. En el derecho comparado se ha desarrollado este concepto que ha permitido elevar el Derecho a la Protección de Datos Personales en el catálogo de los derechos fundamentales. En el año 2008, la Constitución del Ecuador reconoció por primera vez la protección de los datos personales de los ciudadanos, sin embargo, en el país no existía una ley especializada en la materia, ni una autoridad competente que controle y vigile de forma continúa el tratamiento de datos personales. Es por esto, que se han vulnerado los derechos de los ecuatorianos, a tal punto que en el año 2019 se filtraron los datos de casi toda la población ecuatoriana. Las empresas ecuatorianas no han sido obligadas a implementar sistemas tecnológicos de protección de datos hasta la promulgación de la nueva Ley Orgánica de Protección de Datos Personales, la cual permitirá que por primera vez en Ecuador exista un mecanismo preventivo y sancionatorio que obligue tanto a entidades públicas y privadas a respetar el derecho de protección de datos personales.

Abstract

The development of technology advances every year and new tools are created to facilitate the flow of personal data. This phenomenon has been the object of study by several lawyers and researchers because of the obvious danger in the lack of regulation in the treatment of people security data. In comparative law, this concept has been developed that has made it possible to raise the Right to Protection of Personal Data in the catalog of fundamental rights. In 2008, the Constitution of Ecuador recognized for the first time the protection of citizens' personal data, however, we have not had a specialized law on the matter, nor an authority that continuously controls and monitors data processing. This is the rights of Ecuadorians have been violated to such an extent that in 2019 the data of almost the entire Ecuadorian population was leaked. Ecuadorian companies have not been forced to implement technological data protection systems until the enactment of the new Organic Law on Protection of Personal Data, which will allow for the first time in Ecuador to be a preventive and sanctioning mechanism that binds both public and private entities to respect the right to protection of personal data.

Keywords: personal data, data leak, data protection, lack of regulation, preventive mechanism, fundamental rights.

Introducción

Desde hace muchos años investigadores, profesionales, doctrinarios, tribunales de justicia y actores sociales han hecho eco sobre la importancia de regular el tratamiento de datos personales. El desarrollo de la tecnología hace posible la recolección y utilización de datos personales de forma ilimitada, por tanto, la fluctuación de datos va en aumento cada año. En ocasiones los datos han sido obtenidos por su titular para adquirir un producto o servicio, sin embargo, existen casos en que son obtenidos de forma indirecta sin el consentimiento del titular. El titular los entrega para una finalidad concreta, sin embargo, en la vida práctica se devía su fin y son cedidos a terceros. En muchas ocasiones el titular no es consciente de ello o ni si quiera ha sido informado acerca del destino de sus datos. Hoy en día los datos personales son considerados como un activo importante para las empresas, organizaciones y entidades públicas. La sociedad suele ignorar los peligros inminentes que podría presentar la divulgación de nuestros datos, muchas veces se desconoce quién realiza el tratamiento o para qué fines lo utiliza, no tenemos la remota idea de las decisiones que se pueden tomar en base a la información que se tiene sobre nosotros [1].

Las consecuencias de la falta de regulación en el tratamiento de datos, han llevado al legislador y en ocasiones a los jueces, establecer los límites en el tratamiento de los mismos. En el caso Facebook Inc & Cambridge Analytica, varios medios de comunicación en el año 2018 iniciaron una investigación periodistica en el que se reveló, que la compañía Cambridge Analytica habría utilizado los datos personales de más de 50

[1] GARRIGA DOMÍNGUEZ, Ana. Tratamiento de Datos Personales y Derechos Fundamentales, 2004, pp. 11-12

millones de usuarios de Facebook para realizar campañas psicográficas[2]. con el fin de alterar las elecciones de Estados Unidos en el año 2016 a favor del Donald Trump, y meses más tarde en el Reino Unido para apoyar al Brexit[3]. La recoleción de datos fue posible a través de una aplicación creada por Aleksandr Kogan que consistía en un cuestionario de personalidad en el que los usuarios aceptaban de forma voluntaria realizar un estudio psicológico con fines académicos, que permitiría a la aplicación recolectar datos personales como ubicación, preferencias, historiales, incluso información personal de perfiles de "amigos" añadidos en la red social. Kogan, posteriormente vendió la información recopilada a la compañía Cambridge Analytica. La Comisión Federal de Comercio de Estados Unidos, multó a Facebook por un monto de $5.000 millones por malas prácticas en la red social[4], que permitieron a los desarrolladores recolectar datos de una forma simple sin informar a los usuarios de su tratamiento, explotación y comercialización[5].

En Ecuador, en el año 2019 el Primer Mandatario se vió obligado a enviar el proyecto de Ley Orgánica de Protección de Datos Personales a la Asamblea, luego de que fue de conocimiento público que los datos personales de la mayoría de los ecuatorianos, incluido los de menores de edad, fue expuesta en el ciberespacio debido a un fallo técnico en la base de datos de la compañía Novaestrat, la cual fue descubierta por investigadores de seguridad de "vpnMentor". Se considera como la filtración de datos más grande de Ecuador, ya que incluso el número de personas filtradas es mucho mayor al de la población porque incluía datos de personas fallecidas. Los datos provenían tanto de

[2] VERCELI, V. La (des)protección de los datos personales: análisis del caso *Facebook Inc. – Cambrige Analytica*, p. 2. El autor sostiene que las campañas psicográficas son aquellas que combinan datos demográficos y psicológicos de las poblaciones.

[3] VERCELI, p. 2

[4] BBC News Mundo. *Cambridge Analytica* multa récord que deberá pagar Facebook por la forma en que manejó los datos de 87 millones de usuarios, 2019.

[5] VERCELI, p. 4

empresas públicas como privadas[6]. También incluía información completa de familias, tanto de hijos como de padres, que permitiría a cualquiera persona reconstruir un árbol genealógico familiar de la población entera de Ecuador. La filtración de datos de niños es sin duda, la preocupación de privacidad mas grande respecto a este incidente, lo que pudo provocar el robo de su identidad o incluso la facilidad de encontrarlos por la filtración de sus datos domiciliarios[7]. Las consecuencias de este incidente podrían ser graves como el robo de identidad, fraude financiero, espionaje, entre otros delitos. Antes del año 2021, en Ecuador a pesar de que se contemplaba el principio de Protección de Datos Personales en la constitución, no existía ninguna ley especializada en la materia, que exija a las empresas a adoptar mecanismos de prevención y protocolos de seguridad que garantizen la protección de los datos de las personas[8].

1. Nociones Introductorias

1.1 Derecho a la intimidad

Es importante partir del estudio del derecho a la intimidad ya que a raíz de éste se desprende el estudio del derecho a la protección de datos personales. El derecho a la intimidad se define como aquel derecho que permite a la persona controlar y decidir en qué medida desea compartir con otros información sobre la vida privada que a cada persona le concierne ya que su revelación o conocimiento público podría afectar su libre desarrollo[9].

---

[6] CIMPANU, Catalin. *Database leaks data on most of Ecuador's citizens, including 6.7 million children,* Zdnet, 2019.

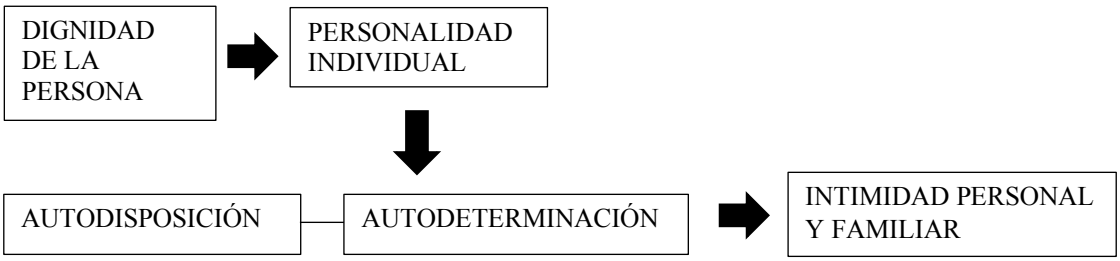
[7] Ibíd.

[8] ORAMAS, Luis. *Protección de Datos: hacia un nuevo régimen*, 2021.

[9] HERRÁN ORTIZ, Ana. *El derecho a la protección de datos personales en la sociedad de la información*, 2003, p. 9.

El Tribunal Constitucional Español, el 2 de diciembre, en sentencia STC 231/1998, determinó que el derecho a la intimidad personal esta vinculado con el libre desarrollo de la personalidad de la cual se deriva de la dignidad de la persona, principio reconocido en la constitución española. El derecho a la intimidad encuentra su justificación jurídica en la personalidad individual[10].

El libre desarrollo de la personalidad individual está compuesto por dos esferas, la autodisposición y la autodeterminación. La autodisposición implica que cada individuo es libre de su actuar sin injerencias externas, y la autodeterminación, "*nace de la libre proyección humana, que se encuentra vinculada a la idea de intimidad personal y familiar*".[11] La ex Directora Nacional del Registro de Datos Públicos, sostiene de igual manera que la protección de los datos involucra la dignidad de la persona y el libre desarrollo de su personalidad[12].



El derecho a la intimidad aspira a que exista un mecanismo de control sobre la información que involucra al titular y que no se pretenda que sea éste quien deba accionar

[10] Ibíd., 2003, p. 9.

[11] ibíd., 2003, pp. 9-10

[12] NARANJO GODOY, Lorena. *El dato personal como presupuesto al derecho de la protección de datos personales y del hábeas data en Ecuador*, 2017, p. 65.

cuando su derecho sea vulnerado. Es deber del Estado, implementar mecanismos necesarios de protección y tutela de este derecho.

El derecho a la intimidad es inaleanable, imprescriptible e irrenunciable. Sin embargo, no es un derecho absoluto, se ejerce con límites razonales y proporcionales impuestos por la ley. Ya que si bien entendemos el derecho a la intimidad como aquel derecho que protege nuestra esfera privada sin intromisiones de los demás, éste se condiciona a ciertas circunstancias establecidas en la ley, que pueden ser de exigencia pública o judiciales. Como por ejemplo, el allanamiento: mecanismo judicial que permite vulnerar el derecho a la intimidad cuando se configuran los elementos que permiten practicarla[13].

1.2 La protección de datos como derecho autónomo

El reconocimiento de los derechos fundamentales se ha llevado a lo largo de la historia en relación a los cambios y progresos de la sociedad. Los cambios estructurales e inevitables que sufre la sociedad gracias al avance de la tecnología demandan al legislador la incorporación de nuevos derechos que permitan la protección del individuo frente a este nuevo entorno tecnológico. Para el análisis del derecho a la protección de datos personales como derecho autónomo, se debe entender el concepto de dato personal en sí.

"*Por datos de carácter personal debemos entender "toda información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, susceptible de recogida, registro, tratamiento o transmisión concerniente a una persona física identificada o identificable"*[14].

[13] VILLALBA FIALLOS, Andrea. Reflexiones jurídicas sobre la protección de datos y el derecho a la intimidad en la autodeterminación informativa, 2017, p. 29.

[14] HERNÁNDEZ DELGADO, Vicente. Referentes legales para un marco protector de datos personales, 2006, p. 568.

Dato personal es aquella información que nos permite identificar a una persona ya sea de forma directa o indirecta. Algunos datos pueden ser de carácter público porque su conocimiento no implica una afectación a la intimidad, sin embargo los datos que se consideran privados deben ser protegidos para no afectar la intimidad del individuo[15].

El Tribunal Constitucional Alemán en 1983, reconoce por primera vez el término "autodeterminación informativa"[16], que es el derecho de poder controlar la información que le concierne al titular frente a un ente público o privado. El derecho a la protección de datos está dentro de los derechos de protección de la persona, pretende que sea el individuo quien tenga exclusivamente la facultad de decidir la divulgación y finalidad que se maneja sobre los datos que le concierne. Reconoce además, que dentro del mundo informático son infinitas las posibilidades que se puede dar al tratamiento de los datos personales que van desde la recolección de los datos hasta la posibilidad de intercambiar ésta información con terceros, sin que sea de conocimiento del titular. Lo fundamental en la protección de datos, no es el dato como elemento íntimo de la persona, si no el tratamiento y finalidad de la recolección de los mismos[17].

Por su parte, el 13 de enero de 1998, el Tribunal Constitucional Español reconoce la protección de datos de las personas como un derecho fundamental autónomo frente al flujo de información que concierne a cada persona, sea de su ámbito más íntimo o no, para así garantizar el pleno ejercicio de sus derechos[18].

---

[15] Ley Orgánica de Protección de Datos Personales (Registro Oficial 459 del 26 de mayo de 2021) (LOPD), establece en el artículo 4, los datos sensibles, que son aquellos que pueden dar origen a discriminación y atentar en contra de las libertades fundamentales del individuo.

[16] HASSEMER, Winfried. El derecho a la autodeterminación informativa y los retos del procesamiento automatizado de datos personales, 1997, p. 124. Sostiene el autor que el derecho a la autodeterminación informativa es un derecho a la defensa frente a los riesgos tecnológicos y un derecho activo de control frente al flujo de datos que circulan sobre cada persona.

[17] HERRÁN ORTIZ, 2003, pp. 20-21.

[18] Ibíd, p. 17

El bien jurídico tutelado dentro del derecho de protección de datos personales no se centra únicamente dentro de una esfera íntima o privada de la persona si no que su alcance es mucho más amplio ya que protege otros valores y principios como la dignidad humana y el libre desarrollo de su personalidad[19]. Además este derecho autónomo alcanza una dimensión institucional ya que su configuración conlleva la implementación de autoridades específicas de control y mecanismos de protección de este nuevo derecho. Por último, su consideración como derecho autónomo permite que existan procedimientos específicos para la tutela de este derecho frente al fenómeno informático. Es importante destacar que los derechos fundamentales tradicionales tienen su origen bajo un contexto preinformático lo que su aplicación podría resultar infecaz en la protección de los derechos de las personas frente a la tecnología[20].

La protección de los datos personales es un derecho fundamental para el individuo ya que convive en una sociedad donde la vulnerabilidad y la exposición de sus datos puede afectar a varias esferas de su vida como son: laboral, familiar y social. La protección de datos cobra mayor importancia dentro de un mundo tecnificado y globalizado que, sin un mecanismo preventivo y sancionatorio se podría perpretar la vulneración de los derechos de las personas mediante el uso de las nuevas tecnologías.

A pesar de que el derecho a la intimidad y la protección de datos puedan verse involucrados, hay dos principales razones por las cúales convergen dentro de su alcance[21]:

[19] Constitución Española. Boletín Oficial del Estado, 29 de diciembre de 1978, establece "Art. 18.4.- La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos."

[20] HERRÁN ORTIZ, 2003, p. 18.

[21] REMOLINA ANGARITA, Nelson. Aproximación Constitucional de la Protección de Datos Personales en Latinoamérica, 2012, p. 6.

1. No toda vulneración al derecho a la intimidad implica una vulneración al derecho de protección de datos. En la vulneración al derecho de protección de datos pueden verse otros derechos involucrados como el derecho al honor y buen nombre y el derecho al debido proceso.
2. El derecho de protección de datos amplía su alcance a cualquier tipo de información, pueden ser: datos personales, sensibles, públicos, datos de niñas, niños y adolescentes, datos de salud, datos de personas con discapacidad y de sus sustitutos relativos a la discapacidad[22]. Este derecho busca proteger cualquier tipo de dato personal.

1.3 El Habeas Data como Mecanismo de Protección

La Constitución de la República del Ecuador reconoce la autonomía del Derecho de Protección de Datos Personales desde el año 2008[23], sin embargo, antes de la promulgación de la Ley Orgánica de Protección de Datos Personales, no existía ningún concepto específico que abarcara la comprensión de este derecho. El único mecanismo que teníamos para la protección de los datos personales era el habeas data[24]. Ordoñez Pineda sostiene que el habeas data no sólo es un mecanismo idóneo para la protección judicial del tratamiento de datos si no que también es un mecanismo de control que exige adoptar medidas preventivas y proactivas para la seguridad en el tratamiento[25]. La Corte

[22] Ley Orgánica de Protección de Datos Personales (Registro Oficial 459 del 26 de mayo de 2021) (LOPD), véase el artículo 77.

[23] Constitución de la República Ecuador (Registro Oficial 449 del 20 de octubre del 2008) (CRE), lo consagra en el articulo 66, numeral 19.

[24] DINARDAP, Habeas Data es la acción jurídica para proteger los datos personales hasta tener una legislación.

[25] ORDOÑEZ PINEDA, Luis. El hábeas data como garantía procesal frente a las tecnologías de la información y comunicación: situación en el contexto ecuatoriano, 2019, p. 13.

Constitucional de Ecuador reconoce al habeas data como un mecanismo de garantía al derecho de protección de datos personales[26].

En la sentencia No. 2064-14-EP/21 del 27 de enero de 2021, la Corte Constitucional acepta la demanda de acción de hábeas data planteada en el caso en análisis, el cual versa sobre la divulgación de una fotografía para lo cual la Corte establece que efectivamente constituye un dato personal que permite identificar el individuo. A pesar de que una fotografía no contenga el rostro de la persona, puede tener otro elemento que permita inmediatamente reconocer la identidad del titular, lo cual constituye un dato personal. La sentencia analiza la delimitación del tratamiento de datos personales, en el que expone casos en que a diario las personas realizan tratamiento de datos personales, sin que medie el consentimiento del titular o exista un mandato o autorización legal para su uso. Por ejemplo, cuando una persona exhibe una simple fotografía de su familia a un tercero, o en el caso de que una persona le entrega a un tercero la dirección de domicilio de otra persona con la finalidad de que se envíe un regalo de cumpleaños. La Corte considera imposible que la ley determine de forma taxativa como se puede llevar a cabo el tratamiento de datos, ya que en virtud del desarrollo de las nuevas tecnologías podrían quedar fuera otros métodos definidos con antelación. Por tanto, le corresponde al juez examinar caso por caso y resolver a la luz del ordenamiento jurídico. Además, analiza la importancia de diferenciar cuando el tratamiento de datos personales se realiza en un ámbito exclusivamente personal o doméstico y los casos cuando rebasa esta esfera. Al referirnos a una actividad personal no se debe confundir con una actividad individual, ya que pueden existir varias personas dentro de un núcleo familiar realizando una actividad

[26] Dictamen de la Corte Constitucional, 3 de julio de 2014, (*001-14-PJO-C* ponente: Patricio Pazmiño Freire)

personal que consiste en la realización de un fichero para las invitaciones de una boda. En este caso la finalidad no trasciende la esfera íntima o familiar. El tratamiento es personal cuando afecta a la esfera más íntima de la persona y su finalidad no sea otra que surtir efectos en estos ámbitos. A pesar del desarrollo que realiza la Corte respecto a la delimitación del tratamiento de datos personales en el presente caso, considera idóneo el hábeas data para la protección de los datos personales de tal forma que se podría llegar a efectuar la reparación integral ante el menoscabo de los derechos del titular. Sin embargo, no es suficiente que en nuestro ordenamiento jurídico únicamente exista un mecanismo sancionatorio y reparatorio, se requiere que se desarrollen otros mecanismos de tutela que garantice el derecho de los titulares [27].

La protección de datos es protegida a nivel constitucional, sin embargo, únicamente contábamos con normas que regulaban la actuación de las entidades públicas en el manejo de datos, existiendo un vacío respecto a las actuaciones de las entidades privadas. Existen tres razones principales por las cuales el hábeas data no ha sido el mecanismo idóneo para la protección de los datos personales en Ecuador[28]:

- **No se establece un plazo en la ley para interponer la acción.**

  La Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional (LOGJCC) no estabalece un plazo para presentar la acción de habeas data, únicamente se menciona la espera de un plazo razonable, lo que resulta un término ambiguo que no responde a la problemática con respecto al tiempo.

[27] Dictamen de la Corte Constitucional, 27 de enero de 2021, (*2064-14-EP* ponente: Carmen Corral Ponce)
[28] VERA SALTOS, María y VIVERO ANDRADE, María. *¿Vida Privada o Muerte a la Privacidad?: Protección de Datos Personales en la Relación Empresa-Cliente en Ecuador*, 2019, pp. 246-248.

- **Faculta a las personas jurídicas a presentar la acción de habeas data.**

  La ley faculta tanto a las personas naturales y jurídicas a presentar la acción de habeas data, sin embargo, esto desvía el fin de la protección de los datos, ya que los principales autores de la vulneración de los datos personales son las personas jurídicas[29].

- **Es un mecanismo únicamente sancionatorio.**

  El legitimado activo únicamente podrá plantear la acción cuando el uso de su información personal ha violado un derecho fundamental[30], sin que exista una autoridad competente o mecanismo preventivo sobre el tratamiento de los datos personales.

Pese a que se amplió las facultades procesales y garantistas al derecho de Habeas Data y aunque se ha querido ampliar el contenido del derecho de protección de datos en otras leyes sectoriales, en la prática resulta necesario la existencia de una ley especializada para poder garantizar su efectivo cumplimiento[31]. Además, la existencia de normas que protegan los datos personales tienen como resultado, la necesidad de que exista un organismo independiente especializado que se dedique a la regulación, control y

[29] El Universo. *Empresas siguen usando los datos personales los ciudadanos sin su consentimiento, pese a nueva ley,* 2021.
[30] Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional. Artículo 50. (Registro Oficial 52 del 22 de octubre de 2009) (LOGJYCC)

[31] ORDOÑEZ PIÑEDA, Luis. *La protección de datos personales en los estados que conforman la Comunidad Andina: estudio comparado y precisiones para un modelo interamericano de integración*, 2017, p. 108.

prevención de los datos personales que manejan los entes públicos y privados en Ecuador[32].

2. Reconocimiento del Derecho a la Protección de Datos en el Derecho Comparado

En el año 1995, la Unión Europea (UE), se planteó la necesidad de regular el aumento del fujo de intercambio de datos personales debido a la integración económica y social entre los Estados miembros. Cada estado manejaba de forma independiente el tratamiento de datos, por lo tanto existían obstáculos para el flujo transfronterizo de datos, es así como se realizó el primer acto normativo para la protección de datos personales en la UE, a través del instrumento de la Directiva 95/46/CE que tenía como principal objetivo la libre circulación de los datos personales entre los estados miembros y a su vez proteger el tratamiento de los datos de las personas físicas[33].

La protección de datos personales a cargo de las instituciones, órganos y organismos de la Unión y de los Estados miembros, fue reconocida por primera vez como un derecho a través de la reforma que se realizó mediante el Tratado de Ámsterdam que entró en vigor en el año 1999. No tardó en manifestarse el consenso para incluir éste derecho dentro de la Carta de los Derechos Fundamentales de la Unión Europea[34].

En el año 2016, se aprobó el Reglamento General de Protección de Datos, cuyo objetivo era adaptar la normativa de protección de datos a la nueva era tecnológica y jurídica. En

---

[32] ENRÍQUEZ ÁLVAREZ, Luis. 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,, 2018, p. 46

[33] CONCELLÓN FERNANDEZ, Pilar. *El concepto de dato personal en la unión europea: una pieza clave en su protección*, p. 2.

[34] Carta de los Derechos Fundamentales de la Unión Europea, 18 de diciembre de 2000. Véase el articulo 8.

este caso el reglamento actualiza el concepto de dato personal y añade a los datos genéticos y biómetricos como datos especialmente protegidos.

El Tribunal de Justicia de la Unión Europea siguiendo lo dispuesto por el Grupo de Trabajo del artículo 29 recoge en su dictamen, que ya no es necesario llegar a identificar a una persona en sentido estricto, ya que existen sistemas automatizados que permiten identificar a una persona a través de su comportamiento. Éste tipo de sistemas otorgan un identificador único a cada usuario en línea que ha sido registrado para que no exista confusión con otro usuario. Tambíen las nuevas herramientas tecnológicas permiten identificar el comportamiento de un ordenador y de la persona que está detrás de ello, por tanto no es necesario saber el nombre y apellido para poder identificarla, basta con conocer su comportamiento a través de esos sistemas para incluir a la persona en una categoría, sobre la base de criterios socioeconómicos, psicológicos, filósoficos, entres otros. Adicional, el considerando 26 del reglamento complementa la definición de dato personal haciendo énfasis en que la protección no se aplicará a los datos anónimos que no permitan identificar a una persona, pero la protección si recae sobre los datos seudonimizados que son aquellos datos que se desasocian de datos identificativos pero que con información adicional puede volver a identificarse a la persona. Es preciso señalar que el reglamento protege tanto los datos automatizados o manuales, es decir, puede llevarse a cabo el registro mediante un ordenador o registrarse en un soporte físico. En todos los casos siempre que el registro se realice en un fichero o base de datos con criterios predeterminados, como el orden alfabético, estarán dentro del ámbito de aplicación del reglamento[35].

[35] CONCELLÓN FERNANDEZ, Pilar, p. 19.

De igual manera, el año 2014, el Tribunal de Justicia de la Unión Europea (TJUE), en sentencia analiza los datos provenientes de comunicaciones electrónicas o metadatos en el que realiza una importante distinción entre el dato simple y compuesto. Como he mencionado anteriormente, un dato personal es aquél que nos permite identificar a una persona física, por tanto si tenemos la duración de una llamada telefónica o una dirección IP, éstos datos por sí solos no nos permitirá identificar a una persona física. Por otro lado, tenemos los datos compuestos o de tráfico, en el que puede incluirse: un número de teléfono, duración de una llamada, fecha, lugar, entre otros. Cuando estamos frente a datos simples que en su conjunto nos permite identificar a una persona constituyen un dato personal[36].

3. Análisis a la nueva Ley Orgánica de Protección de Datos Personales

3.1 Principales aspectos

La ley de Protección de Datos Personales fue publicada en el Registro Oficial número 459 de 26 de mayo de 2021. Tiene su inspiración en el Reglamento General de Protección de Datos Personales de la Unión Europea. La ley es de obligatorio cumplimiento desde la fecha de su publicación, pero las sanciones, medidas correctivas y cualquier otro tipo de medidas administrativas se empezarán a aplicar desde el 26 de mayo de 2023. Según la Disposición Transitoria Primera, las medidas correctivas y regimen sancionatorio entrarán en vigencia en 2 años contados a partir de la fecha de publicación, sin embargo, los derechos consagrados ya se encuentran plenamente vigentes.

El reglamento servirá de aclaración o guía de como se aplicarán los nuevos términos contemplados en la ley. Además, con su expedición se creará la Superintendencia de

[36] POLO ROCA, Andoni. Datos, datos, datos: el dato personal, el dato no personal, el dato personal compuesto, la anonimización, la pertinencia del dato y otras cuestiones sobre datos, 2021, p. 223.

Protección de Datos Personales en Ecuador. El Superintendente será designado según la terna que remita el Presidente de acuerdo a lo establecido en la Constitución de la República[37].

El objeto y finalidad de la ley es garantizar el derecho de protección de datos personales mediante el acceso a la información y también sobre la decisión de los datos personales mediante principios, derechos, obligaciones y mecanismos de tutela[38]. El alcance de la protección de los datos será para datos que consten en un soporte informático y tambíen en soporte físico[39]. La ley contempla nuevos términos, entre los cuales destacan los siguientes para su plena comprensión:

Tratamiento: "*cualquier operación o conjunto de operaciones realizadas sobre datos personales, ya sea por procedimientos técnicos de carácter automatizado, parcialmente automatizado o no automatizado*."[40]

Responsable: decide sobre la finalidad y tratamiento de datos personales. Por ejemplo, una empresa que vende productos y utiliza la información de sus clientes para fines publicitarios. La empresa decide darle esa finalidad, por lo tanto, será la responsable del tratamiento de datos.

Encargado: es quién realiza el tratamiento de datos personales por nombre y cuenta de un responsable. Por ejemplo, un trabajador, auditor o un contratista que realiza entregas de productos, el contratista no decide cual será la finalidad de los datos, pero si realiza un tratamiento para la prestación de su servicio.

[37] Ley Orgánica de Protección de Datos Personales (Registro Oficial 459 del 26 de mayo de 2021) (LOPD), véase el artículo 77.
[38] Ibíd, véase el artículo 1.
[39] Ibíd, véase el artículo 2.
[40] Ibíd, véase el artículo 4.

Para el control y prevención de la vulneración de los derechos contemplados en la ley, se creará el Registro Único de Responsables y Encargados Incumplidos para quienes hayan incurrido en alguna infracción. Además la Autoridad de Protección de Datos, reconocerá entidades certificadoras que otorgarán certificados de cumplimiento y sellos de buenas prácticas[41].

3.2 Consentimiento del titular y finalidad del tratamiento como ejes centrales de la protección de datos

El consentimiento y finalidad configuran la piedra angular y justificación legal del derecho de protección de datos personales.[42] Para el ejercicio efectivo del derecho de protección de datos, es indispensable que el sistema normativo se adapte en ambos principios[43].

Para que el consentimiento tenga validez legal deberá tener las siguientes características[44]:

- **Libre**

  Debe estar libre de vicios del consentimiento, para ello debemos remitirnos al Código Civil como ley supletoria que establece que los vicios del consentimiento son: error fuerza y dolo[45]. Además, también puede ocurrir que el titular de los

[41] Ibíd.
[42] ROLDÁN CARRILLO, Felipe. 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, 2021, p. 177.

[43] PUYOL MONTERO, Francisco. Los Principios del Derecho a la Protección de Datos", en *Reglamento general de protección de datos*, 2017, p. 135-136.

[44] Ley Orgánica de Protección de Datos Personales (Registro Oficial 459 del 26 de mayo de 2021) (LOPD), véase el artículo 8.
[45] ROLDÁN CARILLO, 2021, p. 187.

datos se encuentre en una situación de subordinación. En este caso la aceptación o el rechazo no debe estar condicionado a una consecuencia en contra del titular[46].

- **Específico**

  Debe existir claridad en cuanto al tipo de tratamiento que consiente el titular y el dato personal sobre el cual lo autoriza, así como de quiénes serán los encargados de realizar el tratamiento. El responsable debe informar al titular la finalidad de sus datos de forma específica. La finalidad no podrá ser general, indeterminada o ilegítima[47]. El responsable únicamente deberá pedir al titular los datos estrictamente necesarios para el fin que tenga su tratamiento, de acuerdo al principio de minimización de datos[48].

- **Informado**

  Esta carácterística está estrictamente ligada con la característica anterior. La ley establece de forma específica sobre todos los aspectos en los que debe estar informado el titular para que su consentimiento sea válido.[49] La información que le sea facilitada al titular debe estar en un lenguaje claro, sencillo y de fácil comprensión. Además el titular deberá estar informado de quien será el encargado del tratamiento y cúales serían las consecuencias en caso de no consentir[50].

- **Inequívoco**

  Debe existir una acción afirmativa o declaración por parte del titular.[51] La prueba del consentimiento es importante para comprobar su veracidad y legalidad, por lo tanto no debe existir duda en cuanto a la intención del titular que otorga su

[46] Ibíd, p. 188.
[47] Reglamento General de Protección de Datos 2016/79 (RGPD), Unión Europea: Parlamento y Consejo Europeo, véase el artículo 5 numeral 1 literal b.
[48] Ley Orgánica de Protección de Datos Personales (Registro Oficial 459 del 26 de mayo de 2021) (LOPD), véase el artículo 8.
[49] Ibíd, véase el artículo 12
[50] Reglamento General de Protección de Datos 2016/79 (RGPD), Unión Europea: Parlamento y Consejo Europeo, véase el artículo 12 numeral 1.
[51] ROLDÁN CARILLO, 2021, p. 189.

consentimiento, es importante que la persona que otorga el consentimiento sea el verdadero titular de los datos[52].

- **Revocable**

  Así como consiente el titular en el tratamiento de sus datos, la ley faculta de que se pueda revocar el consentimiento para lo cual se deberá realizar un cese inmediato del tratamiento sin que sea necesario una justificación por parte del titular.

La ley establece la importancia de que la finalidad del tratamiento de datos sea límitado, es por esto que el artículo prescribe para éste principio las siguientes carácterísticas:

- **Determinada**

  No se aceptan finalidades que sean genéricas o amplias, por tanto, el encargado deberá determinar un propósito del tratamiento de datos que deberá tener una finalidad concreta y específica[53].

- **Explícita e informada al titular**

  Este requisito se cumple cuando el encargado informa al titular de datos sobre el tratamiento y su finalidad de una manera clara, concisa y en lenguaje sencillo sin tecnicismos, esto guarda relación con el requisito de consentimiento inequívoco

[52] Reglamento General de Protección de Datos 2016/79 (RGPD), Unión Europea: Parlamento y Consejo Europeo. Véase el artículo 17 numeral 1.

[53]Ibíd, véase el considerando 39.

ya que de esta manera el titular no tendría dudas respecto al propósito determinado del tratamiento de sus datos[54].

- **Legítima**

  La finalidad sería legítima cuando se adecúa a lo prescrito en el ordenamiento jurídico, si esta finalidad no cumple las condiciones requeridas en la norma, estaríamos frente a una finalidad ilegítima[55].

Además de estos requisitos la ley incluye otros requisitos para que la finalidad sea válida, entre los cuales destacan los siguientes:

- Se deberá recopilar únicamente los datos necesarios que deban perseguir un fin específico. Estos deberán ser "adecuados, pertinentes y limitados"[56].
- Los datos recopilados no podrán ser "tratados ulteriormente de manera incompatible con dichos fines" admite que a los datos pueda darse con posterioridad una finalidad adicional a la inicial siempre que esta guarde compatibilidad con la inicial, no podrá extenderse el consentimiento del titular para la finalidad ya prevista, en caso de que surga una finalidad posterior que no guarde relación con la inicial, el titular deberá otorgar nuevamente su consentimiento y ésta deberá cumplir con todos los requisitos previstos para su validez.

---

[54] TRUJILLO CABRERA, CARLOS. Las bases de legitimación del tratamiento de datos personales. En especial, el consentimiento" en: *Protección de datos, responsabilidad activa y técnicas de garantía*, 2018, p. 57.

[55] ROLDÁN CARILLO, 2021, p. 185.

[56] Ley Orgánica de Protección de Datos Personales (Registro Oficial 459 del 26 de mayo de 2021) (LOPD), véase el artículo 5.

- Los datos deben tratarse con sigilo y secreto, éstos no pueden ser divulgados ni deberán tratarse para otro fin que no sea el que consitió el titular.
- Responsabilidad proactiva y demostrada: El responsable está obligado a demostrar la adopción de todas las medidas necesarias para el cumplimiento de la ley en el cúal además de aplicar la normativa podrá a su discresión adherirse a otros mecanismos o estandarés de protección de datos. El responsable del tratamiento deberá acreditar y rendir cuentas ante el titular y la autoridad de protección de datos de que su responsabilidad proactiva es continúa y permanente. Este principio comprende la actuación del responsable de forma preventiva y no posterior a cometer alguna infracción, la ley no otorga una medida taxativa de medidas de seguridad sino que permite ampliar la posibilidad de que el resposable pueda aplicar las medidas técnicas de seguridad más convenientes según su organización y naturaleza[57].

3.3 ¿Cómo se conforma el sistema de protección de datos personales?

Titular	El propio individuo es el titular de sus datos personales que son protegidos por la Constitución. El titular tiene derecho a la reserva y confidencialidad de sus datos[58].
Responsable	La relación jurídica respecto al encargado de los datos frente al responsable debe estar regulada mediante un contrato donde se deba específicar las instrucciones y
Encargado	

[57] BELTRÁN AGUIRRE, Juan. Reglamento general de protección de datos: novedades. Adaptación de la normativa española: el proyecto de LOPD, 2018, p. 78.
[58] MENDOZA ENRÍQUEZ, Olivia. Marco jurídico de la protección de datos personales en las empresas de servicios establecidas en México: desafíos y cumplimiento, 2018, p. 274.

	finalidad en la que se realizará el tratamiento de datos.[59] Una vez que se ha cumplido y finalizado con el objeto del contrato, los datos deberán ser destruidos o devueltos al responsable bajo la supervisión de la autoridad de protección de datos personales. Si el encargado no actúa conforme a lo dispuesto en el contrato, recaerá en una infracción grave[60].
Destinatario	Persona natural o jurídica, distinta del encargado del tratamiento, a quién se le ha transferido o comunicado con datos personales[61] únicamente se podrá llevar a cabo si se cumplen todos los requisitos.
Autoridad de Protección de Datos Personales	Será el Superintendente quién tendrá la obligación de controlar y vigilar para garantizar la protección de datos personales de los ciudadanos[62].
Entidades certificadoras	Con el objetivo de ofrecer seguridad en las empresas, se creará un sistema de

[59] Ley Orgánica de Protección de Datos Personales (Registro Oficial 459 del 26 de mayo de 2021) (LOPD), véase el artículo 34 numeral 2.
[60] Ibíd, véase el artículo 70 numeral 2.
[61] Ibíd, véase el artículo 4.
[62] Ibíd, véase el artículo 76.

	certificación para aquellas empresas que reunan la cualificación. Las entidades certificadoras serán reconocidas por la Autoridad de Protección de Datos y podrán emitir certificados de cumplimiento y sellos de buenas prácticas[63].
Delegado de Protección de Datos Personales	El RGPD incluye la figura del Delegado que deberá ser nombrado cuando las actividades a cargo del Responsable o del Encargado del tratamiento sean de gran magnitud o involucren el tratamiento de datos. La autoridad de protección de datos personales ha creado un sistema de certificación de profesionales en protección de datos para tener la capacidad de desempeñar la función de Delegado[64].

3.4 Mecanismos de protección: medidas correctivas y régimen sancionatorio

Requerimiento o queja	La ley otorga la posibilidad de hacer un requerimiento o queja de forma directa al

[63] Ibíd, véase el artículo 4.
[64] MARTÍNEZ VÁSQUEZ, Francisco. El reciente marco de la protección de datos personales (RGPD y nueva LOPDP): las obligaciones del responsable y del encargado, el Delegado de Protección de Datos y el régimen sancionador, 2018, pp. 50-51.

	responsable del tratamiento en relación al ejercicio de su derechos[65].
Reclamo Administrativo	En caso de que el responsable no de contestación al requerimiento, el titular podrá iniciar un reclamo administrativo ante la autoridad de protección de datos para lo cual se atenderá a lo dispuesto en Código Orgánico Administrativo[66].
Medidas Correctivas	La autoridad de protección de datos podrá imponer medidas correctivas con el fin de prevenir y garantizar los derechos en materia de protección de datos sin perjuicio de las sanciones administrativas correspondientes. Estas medidas podrán ser aplicadas previo a un informe de la unidad técnica competente[67].
Procedimiento Administrativo Sancionatorio	Podrá ser sancionado el responsable, encargado, organismos de certificación,

[65] Ley Orgánica de Protección de Datos Personales (Registro Oficial 459 del 26 de mayo de 2021) (LOPD), véase el artículo 34 numeral 2.
[66] Ibíd, véase el artículo 64
[67] Ibíd, véase el artículo 65

	o terceros. Si se encuentran inmersos en una infracción leve, grave o muy grave, que permitirá a la Autoridad iniciar un procedimiento administrativo sancionatorio y la imposición de sanciones y medidas correctivas.

Las multas varían si se trata de un servidor o funcionario público, una entidad de derecho privado o institución pública. Estas se dividen en leves y graves y van desde 1 a 10 salarios básicos unificados del trabajador en general hasta 0,7% al 1% calculada sobre el volumen de negocio correspondiente al ejercicio económico inmediatamente anterior al de la imposición de la multa[68].

Es importante señalar que la Autoridad podrá imponer una sanción monetaria y adicional a esto, la imposición de medidas correctivas. Es posible que el infractor incurra en varias faltas, lo que permitirá a la autoridad imponer varias medidas correctivas. El perjuicio económico de incurrir en una infracción establecida en la Ley de Protección de Datos Personales es muy importante. A continuación, se pondrá de ejemplo, la imposición de multas a una empresa que genera en promedio una ganancia de $2.800 por día. Es posible que el cálculo sobre el volumen de negocio correspondiente al ejercicio económico anterior sea de $1’000.000,00.

[68] Ibíd, la ley establece en el artículo 73, que el volumen de negocios es el resultado de la venta de productos o prestación de servicios realizados durante el último ejercicio económico anterior.

VOLUMEN DE NEGOCIO	SANCIÓN LEVE	SANCIÓN GRAVE
$1’000.000,00	0,1 % - 0,7% = $1.000,00 - $ 7.000,00 POR CADA FALTA	0.7% - 1% = $7.000,00 - $10.000,00 POR CADA FALTA

Para la imposición de las multas se deberán seguir las siguientes reglas en función del principio de proporcionalidad[69].

1. Intencionalidad del infractor
2. Reiteración de la infracción. Si el infractor ya ha sido previamente sancionado
3. La naturaleza del perjuicio ocasionado
4. Reincidencia. Si la infracción impuesta anteriormente es de la misma naturaleza a la que se pretende sancionar.

El RGPD incluye otras posibilidades de graduar las multas atendiendo a diversas circunstancias atenuadoras o agravantes: el volumen de los datos procesados, los beneficios obtenidos, el grado de la intencionalidad, el esfuerzo realizado por la empresa para implementar procedimientos y medidas de seguridad, y cualquiera otra circunstancia que sea relevante para determinar el grado de culpabilidad. También incluye criterios de atenuación: en el caso de probarse la debida diligencia, reconocer de forma espontánea la culpabilidad o de probarse la inducción de la comisión de la infracción por parte del afectado, entre otras [70].

[69] Ibíd, véase el artículo 71 literal a al d
[70] VÁSQUEZ, Sonia y DE MIGUEL, Javier. Nuevo régimen sancionador de protección de datos, 2017.

4. Retos actuales y futuros para la protección de datos en Ecuador

El proceso de adaptación legal y tecnológico en Ecuador tomará tiempo. A continuación, se expondrá los posibles retos que enfrentan las empresas para evitar ser sancionados por la Autoridad de Protección de Datos Personales[71]:

- Redactar políticas acordes a la nueva normativa. Será la obligación de los abogados, redactar políticas de privacidad, condiciones de uso, manejo de cookies, etc. No se debe crear un modelo, las políticas deberán ser redactadas de forma personalizadas de acuerdo a la necesidad de cada empresa.
- Las empresas deberán adaptar los sistemas informáticos a la nueva normativa, para esto será necesario la contratación de especialistas en ciberseguridad. Además, deberán adaptar sus políticas internas a nuevos softwares.
- Es importante que las empresas generen una cultura organizacional interna en torno a estas nuevas políticas, ya que no tendría sentido redactar políticas si es que la empresa internamente no tiene una cultura de manejo de datos de acuerdo a esta nueva normativa.
- Los mecanismos de seguridad no serán iguales para todas las empresas. Hay empresas que manejan base de datos más complicadas con sistemas tecnológicos mas complejos. No es lo mismo implementar un mecanismo de seguridad en una base de datos de una agencia de viajes que la de un hospital.

[71] COLAMARCO UREÑA, Janette. Hacia una adecuada protección de los datos personales en Ecuador, 2018.

- El equipo legal y el equipo de sistemas deberán trabajar en conjunto para la protección de los datos personales en cada empresa.
- El reto más importante es la educación y el conocimiento. Los titulares deberán dar su consentimiento válido y para ello deberán estar conscientes de la importancia de estar informado acerca de la finalidad y tratamiento de sus datos personales.
- Adoptar mecanismos óptimos de protección de datos tiene efectos económicos positivos, ya que permitirá abrir nuevos espacios competitivos en el mercado. Tal como sucedió con el Reglamento de Protección de Datos de la Unión Europea que permitió facilitar el flujo transfronterizo de datos. [72]

5. Recomendaciones.

A pesar de que estamos a la espera de la expedición del Reglamento y de la existencia de la Superintendencia de Protección de Datos Personales. Es necesario que las empresas empiecen a actuar ahora. El régimen sancionatorio puede llegar a ser muy cuantioso y las medidas correctivas pueden ser especialmente complejas. Los datos, actualmente tienen un valor monetario y permite generar ingresos a las empresas.

Si se actúa con prevención antes del 26 de mayo de 2023, el costo de implementar sistemas tecnológicos de protección de datos será mucho menor al costo de la reacción. Si apenas el 26 de mayo de 2023 se empieza a implementar nuevas medidas, será mucho

[72] TRONCOSO REIGADA, Antonio. El desarrollo de la protección de datos personales en Iberoamérica desde una perspectiva comparada y el reequilibro en los modelos de protección de datos a nivel Internacional, 2012

más costoso para las empresas el manejo de base de datos, adicional a esto, deberán costear las multas y las medidas correctivas. La autoridad puede emitir algún tipo de sanción de índole práctico, por ejemplo, podría obligar a una empresa a borrar bases de datos que no se han obtenido con el consentimiento y evidentemente será costoso. Va a ser mucho más económico prevenir que reaccionar.

No hay que pensar que la Ley Orgánica de Protección de Datos y la expedición del Reglamento serán una restricción a la operación de las empresas, si no que es el respeto supremo por el dato y por el derecho de los consumidores que se encuentran en la base de datos de las empresas. Los certificados de cumplimiento y los sellos de buenas practicas van a ser un valor añadido al servicio o producto que ofrecen las empresas, porque generará más confianza en los usuarios, similar al sello de buenas prácticas ambientales. Las empresas que transiten este camino primero tendrán un valor añadido a sus productos o servicios y afrentarán de mejor manera la situación que se aproxima.

Referencias

BELTRÁN AGUIRRE, J. (2018) Reglamento general de protección de datos: novedades. Adaptación de la normativa española: el proyecto de LOPD. Vol. 28 Extraordinario XXVII Congreso 2018. Universidad Pública de Navarra.

COLAMARCO UREÑA, J. (2018) Hacia una adecuada protección de los datos personales en Ecuador, 2018. Firma Legaltech Consultores y Asesores. Ecuador.

CONCELLÓN FERNANDEZ, P. (s.f.) *El concepto de dato personal en la unión europea: una pieza clave en su protección*. Revista General de Derecho Europeo. Universidad de Oviedo.

ENRÍQUEZ ÁLVAREZ, L. (2018) Paradigmas de la protección de Datos Personales en Ecuador. Análisis del Proyecto de Ley Orgánica de Protección a los Derechos a la Intimidad y Privacidad sobre los Datos Personales. Revista de Derecho No. 27. Universidad Andina Simón Bolívar

GARRIGA DOMÍNGUEZ, A. (2004) *Tratamiento de Datos Personales y Derechos Fundamentales*. Madrid. Librería-Editorial Dykinson.

HASSEMER, W. (1997) *El derecho a la autodeterminación informativa y los retos del procesamiento automatizado de datos personales*. Buenos Aires: Editores del Puerto.

HERNÁNDEZ DELGADO, V. (2006) Referentes legales para un marco protector de datos personales.

HERRÁN ORTIZ, A. (2003) El derecho a la protección de datos personales en la sociedad de la información. Revista Ra Ximhai, Universidad Autónoma Indígena de México

MARTÍNEZ VÁSQUEZ, F. (2018) El reciente marco de la protección de datos personales (RGPD y nueva LOPDP): las obligaciones del responsable y del encargado, el Delegado de Protección de Datos y el régimen sancionador. Revista Rueda. Universidad de Cádiz.

MENDOZA ENRÍQUEZ, O. (2018) Marco jurídico de la protección de datos personales en las empresas de servicios establecidas en México: desafíos y cumplimiento. Revista del Instituto de Ciencias Jurídicas de Puebla, México.

NARANJO GODOY, L. (2017) El dato personal como presupuesto al derecho de la protección de datos personales y del hábeas data en Ecuador. Foro: Revista de Derecho No. 27. Universidad Andina Simón Bolívar.

ORAMAS, L. (2021) Protección de Datos: hacia un nuevo régimen. Coronel & Perez Abogados.

ORDOÑEZ PIÑEDA, L. (2017) La protección de datos personales en los estados que conforman la Comunidad Andina: estudio comparado y precisiones para un modelo interamericano de integración. Foro: Revista de Derecho No. 27. Universidad Andina Simón Bolívar, Ecuador.

ORDOÑEZ PINEDA, L. (2019) El hábeas data como garantía procesal frente a las tecnologías de la información y comunicación: situación en el contexto ecuatoriano, 2019. Universidad Técnica Particular de Loja, Ecuador.

POLO ROCA, A. (2021) Datos, datos, datos: el dato personal, el dato no personal, el dato personal compuesto, la anonimización, la pertinencia del dato y otras cuestiones sobre datos, 2021. Estudios de Deusto. Universidad de Deusto.

PUYOL MONTERO, F. (2017) Los Principios del Derecho a la Protección de Datos en el Reglamento general de protección de datos. Madrid. Editorial Reus.

REMOLINA ANGARITA, N.(2012) Aproximación Constitucional de la Protección de Datos Personales en Latinoamérica, 2012. Revista Internacional de Protección de Datos Personales. Universidad de los Andes. Bogotá, Colombia.

ROLDÁN CARRILLO, F. (2021) 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. USFQ Law Review.

TRONCOSO REIGADA, A. (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. Revista Internacional de Protección de Datos Personales. Revista Internacional de Protección de Datos Personales. Universidad de los Andes. Bogotá, Colombia.

TRUJILLO CABRERA (2018) Las bases de legitimación del tratamiento de datos personales. En especial, el consentimiento en: Protección de datos, responsabilidad activa y técnicas de garantía. Universidad de La Laguna, España. Editorial Reus.

VAZQUÉZ, S. & DE MIGUEL, J. (2017) Nuevo régimen sancionador de protección de datos. ECIJA Abogados. España.

VERCELI, V. (s.f.) La (des)protección de los datos personales: análisis del caso Facebook Inc. – Cambrige Analytica. SID, Simposio Argentino de Informática y Derecho.

VERA SALTOS, M. & VIVERO ANDRADE, M. (2019) *¿Vida Privada o Muerte a la Privacidad?: Protección de Datos Personales en la Relación Empresa-Cliente en Ecuador*, USFQ Law Review.

VILLALBA FIALLOS, A. (2017) Reflexiones jurídicas sobre la protección de datos y el derecho a la intimidad en la autodeterminación informativa. Foro: Revista de Derecho No. 27. Universidad Andina Simón Bolívar, Ecuador.

Legislación Interna Utilizada

Constitución de la República del Ecuador (Registro Oficial 449 del 20 de octubre del 2008)

Ley Orgánica de Protección de Datos Personales (Registro Oficial 459 del 26 de mayo de 2021)

Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional. Artículo 50. (Registro Oficial 52 del 22 de octubre de 2009)

Legislación Internacional Utilizada

Constitución Española. (Boletín Oficial del Estado, 29 de diciembre de 1978)

Reglamento General de Protección de Datos de la Unión Europea 2016/79 (RGPD)

Carta Magna de la Unión Europea.

Noticias

Cambridge Analytica multa récord que deberá pagar Facebook por la forma en que manejó los datos de 87 millones de usuarios, BBC News Mundo, 24 de julio de 2019. Obtenido de: https://www.bbc.com/mundo/noticias-49093124

CIMPANU, Catalin. Database leaks data on most of Ecuador's citizens, including 6.7 million children, Zdnet, 16 de septiembre de 2019. Obtenido de: https://www.zdnet.com/article/database-leaks-data-on-most-of-ecuadors-citizens-including-6-7-million-children/

DINARDAP, Habeas Data es la acción jurídica para proteger los datos personales hasta tener una legislación. Obtenido de: https://www.dinardap.gob.ec/habeas-data-es-la-accion-juridica-para-proteger-los-datos-personales-hasta-tener-una-legislacion/

Empresas siguen usando los datos personales de los ciudadanos sin su consentimiento, pese a nueva ley, El Universo, 4 de julio de 2021. Obtenido de: https://www.eluniverso.com/noticias/informes/empresas-siguen-usando-los-datos-personales-de-ciudadanos-sin-su-consentimiento-pese-a-nueva-ley-nota/