UNIVERSIDAD SAN FRANCISCO DE QUITO USFQ

Colegio de Jurisprudencia

Estudio Comparado del Derecho a la Protección de Datos y su Impacto Empresarial en Ecuador

Camila Artieda González

Jurisprudencia

Trabajo de fin de carrera presentado como requisito para la obtención del título de Abogada

Quito, 24 de noviembre de 2023

© DERECHOS DE AUTOR

Por medio del presente documento certifico que he leído todas las Políticas y Manuales de la Universidad San Francisco de Quito USFQ, incluyendo la Política de Propiedad Intelectual USFQ, y estoy de acuerdo con su contenido, por lo que los derechos de propiedad intelectual del presente trabajo quedan sujetos a lo dispuesto en esas Políticas.

Asimismo, autorizo a la USFQ para que realice la digitalización y publicación de este trabajo en el repositorio virtual, de conformidad a lo dispuesto en la Ley Orgánica de Educación Superior del Ecuador.

Nombres y apellidos:	Camila Artieda González
Código:	00328281
Cédula de identidad:	1723720825
Lugar y Fecha:	Quito, 24 de noviembre de 2023

ACLARACIÓN PARA PUBLICACIÓN

Nota: El presente trabajo, en su totalidad o cualquiera de sus partes, no debe ser considerado como una publicación, incluso a pesar de estar disponible sin restricciones a través de un repositorio institucional. Esta declaración se alinea con las prácticas y recomendaciones presentadas por el Committee on Publication Ethics descritas por Barbour et al. (2017) Discussion document on best practice for issues around theses publishing, disponible en http://bit.ly/COPETheses.

UNPUBLISHED DOCUMENT

Note: The followuing capstone Project is available through Universidad San Francisco de Quito USFQ institutional repository. This statement follows the recommendations presented by the Committee on Publication Ethics COPE described by Barbour et al. (2017) Discussion document on best practice for issues around theses publishing available on http://bit.ly/COPETheses.

ESTUDIO COMPARADO DEL DERECHO A LA PROTECCIÓN DE DATOS Y SU IMPACTO EMPRESARIAL EN ECUADOR[1]

COMPARATIVE STUDY OF THE RIGHT TO DATA PROTECTION AND ITS BUSINESS IMPACT IN ECUADOR

Camila Artieda González[2]
cartieda@estud.usfq.edu.ec

RESUMEN

La protección de datos personales es una cuestión de creciente importancia, caracterizado por la hiperconexión y la digitalización de espacios. Este fenómeno da lugar a la proliferación de los datos personales. Particularmente, en el contexto de la economía digital, las empresas que utilizan los datos de manera eficaz pueden obtener una ventaja competitiva significativa sobre sus competidores. En este contexto, el presente trabajo propone un análisis exhaustivo del marco jurídico en torno a la protección de datos personales, con un enfoque específico en Ecuador donde se exploran las teorías jurídicas que respaldan el surgimiento del derecho a la intimidad, así como los estándares de protección establecidos por la Unión Europea. Analizando el mercado de datos personales para identificar sus características y deficiencias. Finalmente, se adoptará una perspectiva basada en el análisis económico del derecho para ofrecer soluciones jurídicas adecuadas para abordar las fallas del mercado de protección de datos.

PALABRAS CLAVE

Protección de Datos, Derecho a la Intimidad, Empresas, Mercado de Datos Personales, Fallos del Mercado.

ABSTRACT

The protection of personal data is an issue of increasing importance, characterized by hyperconnection and the digitalization of spaces. This phenomenon gives rise to the proliferation of personal data. Particularly in the context of the digital economy, companies that use data effectively can gain a significant competitive advantage over their competitors. In this context, the present work proposes an exhaustive analysis of the legal framework around the protection of personal data, with a specific focus on Ecuador where the legal theories that support the emergence of the right to privacy are explored, as well as the standards of protection established by the European Union. Analyzing the personal data market to identify its characteristics and deficiencies. Finally, a perspective based on economic analysis of law will be adopted to offer appropriate legal solutions to address data protection market failures.

KEY WORDS

Data Protection, Right to Privacy, Companies, Personal Data Market, Market Failures.

[1] Trabajo de titulación presentado como requisito para la obtención del título de Abogada. Colegio de Jurisprudencia de la Universidad San Francisco de Quito. Dirigido por Bárbara Terán Picconi.

Fecha de lectura: 24 de noviembre de 2023

Fecha de publicación: 24 de noviembre de 2023

SUMARIO

1. Introducción

Hace 10 años, el Foro Económico Mundial preveía en su informe titulado *Rethinking Personal Data: Strengthening Trust*, la notable proliferación de información personal en el mundo digital, un fenómeno que sigue en constante expansión a través del flujo de datos que circula por las Tecnologías de la Información y Comunicación (TIC). Además, presagiaba los enormes beneficios para los gobiernos, las organizaciones, las empresas y los individuos el hecho de construir una cultura consciente del uso y tratamiento que se debe tener con la información personal.[3] En el paradigma contemporáneo, caracterizado por la hiperconexión y la digitalización de espacios sociales, la protección de la información personal se ha convertido en una cuestión de crucial importancia.

Esta preocupación trasciende la mera protección de los datos que se catalogan como privados o íntimos, extendiéndose de manera igualmente preocupante a los datos que, al hacer a un individuo identificable, despiertan cuestionamientos y retos significativos en lo que respecta a la privacidad, la seguridad, la autonomía de la persona y las libeertades fundamentales de los titulares de datos personales. Cada vez que un usuario navega por internet, realiza una transacción bancaria, adquiere alimentos o acude a una consulta médica, se encuentra en un intercambio constante de su información con diferentes individuos y entidades.

En múltiples ocasiones, esta información es esencial para que muchas empresas desarrollen su actividad mercantil con eficiencia. Numerosas empresas en sectores

[3] Foro Económico Mundial. *Rethinking Personal Data: Strengthening Trust.* (06 de mayo del 2012). Recuperado de: https://www.weforum.org/reports/rethinking-personal-data/, (último acceso: 29/09/2023)

altamente regulados como las farmacéuticas y las compañías de seguros utilizan los datos personales de manera significativa. Las compañías farmacéuticas pueden recopilar datos médicos de pacientes para llevar a cabo investigaciones clínicas o desarrollar nuevos medicamentos. Estos datos permiten crecar perfiles automatizados que identifican patrones de salud, efectividad de tratamientos y posibles efectos secundarios. El uso de los datos personales en este sector y en muchos otros es esencial para el desarrollo de su actividad mercantil por lo que es crítico garantizar la privacidad y la seguridad de estos datos personales, adaptandose a las regulaciones vigentes.

Este trabajo se propone un análisis exhaustivo de la doctrina jurídica en torno al origen de la protección de datos personales, con un enfoque específico en Ecuador y su reciente Ley Orgánica de Protección de Datos Personales de 2021 y su respectivo reglamento de aplicación, el Reglamento General de la Ley Orgánica de Protección de Datos Personales de 2023. Se explorarán las teorías jurídicas que respaldan el surgimiento del derecho a la intimidad y se evaluará constantemente la legislación ecuatoriana en relación con los estándares de protección establecidos por la Unión Europea. En este contexto, se delineará el panorama del mercado de datos personales y se destacarán sus particularidades, identificando las deficiencias inherentes y los desafíos contemporáneos que enfrentan las empresas. Asimismo, se adoptará una perspectiva basada en el análisis económico del derecho para ofrecer soluciones jurídicas adecuados para abordar las fallas del mercado de protección de datos. La metodología de investigación se fundamentará en el análisis documental y comparativo, explorando las corrientes teórico-jurídicas que han influido en la protección de datos en sectores estratégicos del mundo.

2. Marco Teórico Referencial

Para comprender la LOPDP en su origen y amplitud, es necesario contextualizar las corrientes teórico-jurídicas que impulsaron la protección de los datos personales desde diferentes directrices y analizar la forma en la que el derecho a privacidad ha evolucionado con la sociedad.

El liberalismo clásico influyó en la creación del derecho a la intimidad, desde la perspectiva de la libertad individual. Si bien en el siglo XVII, aun no se concebía la idea de intimidad, John Locke trajo consigo en su *''Ensayo sobre el gobierno civil''* de 1690, una teoría política basada en los derechos naturales al hombre, el contrato social y la limitación del poder estatal. Una visión que proviene de la corriente teórica de la libertad

negativa, una libertad que se basa en la ausencia de restricciones externas o interferencias en las acciones de un individuo.[4]

Estos ideales además de moldear el constitucionalismo británico de los siglos XVII y XVIII, también configuraron el pensamiento anglosajón del siguiente siglo sobre los derechos individuales. En el siglo XIX, con pensadores como el inglés John Stuart Mill y su obra "*On liberty"* de 1859, donde se resalta el respeto de la autonomía individual.[5] Reconociendo la prevención del daño a otros como la única justificación legítima para limitar la libertad de un individuo.[6] Varios juristas coinciden en que las nociones iniciales sobre el derecho a la vida privada surgen en Norteamérica en el siglo XIX.

En primer lugar, con el libro *"The Elements of Torts"* de autoría del juez Thomas M. Cooley en 1895.[7] Donde se delinea el derecho a la privacidad como *"the right to be let alone"*, o derecho a la inviolabilidad de la esfera personal. Criterio utilizado para resolver numerosas contiendas legales.[8] En segundo lugar, con la noción de privacidad como salvaguardia igualitaria de la personalidad individual, que nace como un principio básico del derecho universal en el common law con el trabajo de dos jóvenes abogados de Boston, S. Warren y L. Brandeis. Juntos publicaron el artículo titulado *"The Right to Privacy"*, en el Harvard Law Review de 1890.[9]

Gracias a su trabajo el derecho constitucional anglosajón identificó un conjunto de intereses cruciales que integran de forma progresiva el ámbito de la privacidad desde un enfoque pragmático. La jurisprudencia del Tribunal Supremo de Estados Unidos a lo largo del siglo XX, ha interpretado en múltiples contiendas legales que el derecho a la privacidad está tácitamente protegido por las enmiendas Primera, Cuarta, Quinta, Novena y Decimocuarta.[10] Entendiendo que es trabajo de cada generación emplear mecanismos

---

[4] David C. Snyder, "Locke on Natural Law and Property Rights", en *The Canadian Journal of Philosophy*, (1986).
[5] John Stuart Mill, *"On the liberty" 1859* (Kitchener: Batoche Books Limited, 2001).
[6] "El único propósito por el que el poder puede ser ejercido legítimamente sobre cualquier miembro de una comunidad civilizada, contra su voluntad, es prevenir el daño a otros. Sobre sí mismo, sobre su propio cuerpo y mente, el individuo es soberano".
[7] Thomas McIntyre Cooley, *The Elements of Torts* (Chicago: Callaghan and Co., 1895).
[8] Brents vs. Morgan, señalándose en él que se trata del derecho a gozar de la soledad: "(...) el derecho que tiene cada persona de no ser objeto de una publicidad ilegal; el derecho de vivir sin interferencias ilegales del público en lo concerniente a asuntos en los cuales ese público no tiene un interés legítimo".
[9] Samuel Warren y Louis Brandeis. «"The Right to Privacy"» *The Harvard Law Review.* Harvard University (1890). núm. 4, disponible en http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm;.
[10] María Nieves Saldaña, " **«**The right to privacy**»** La génesis de la protección de la privacidad en el sistema constitucional norteamericano: El centenario legado de Warren y Brandeis", *UNED: revista de Derecho Político* N.85, septiembre-diciembre (2012), 195-240.

apropiados para proteger los principios de este derecho a la luz de las desafiantes nuevas realidades sociales y tecnológicas.

Al otro lado del Atlántico, se desarrolló la *Teoría de las Esferas* por el jurista alemán Heinrich Hubmann en 1957. Este trabajo ofrece una perspicaz estructura para comprender la división de la intimidad en tres circulos: el individual, el privado y el secreto. Posteriormente se añadió la esfera de la confianza gracias a la aporte del jurista Heinkel.[11] La Teoría del Mosaico, formulada por Fulgencio Madrid Conesa en 1984, surge como una crítica a la Teoría de las Esferas y postula que la naturaleza de los datos es relativa y depende del receptor de la información, y no del contenido de la misma. Además, subraya que los datos tienen un valor ambivalente según el contexto en el que se manejen.[12]

Postura que coincide con la teoría planteada en el año 1967, denominada la Restricted Access/Limited Control Theory of Privacy o Teoría de Acceso Restringido/Control Limitado de la Privacidad, RALC, la cual explica que la información aparentemente insignificante, cuando se combina con otros datos, puede revelar la personalidad de un individuo en su totalidad, y ayuda a crear los perfiles y clasificarlos. Lo que genera un llamado al control de los individuos sobre sus datos. Esta teoría plantea que la finalidad misma de cualquier legislación debe encaminarse a cumplir el deseo de las personas de elegir libremente bajo qué circunstancias y en qué medida se exponen, su actitud y su comportamiento ante los demás.[13]

3. Estado del Arte

El presente capítulo aborda la exploración de estudios académicos concernientes a la custodia de datos personales en el contexto de la era de las Tecnologías de la Información y las Comunicaciones (TIC), enfocandose en los problemas actuales.

Los gobiernos, a lo largo de la historia, han enfrentado complejas disyuntivas entre el paradigma digital y el enfoque tradicional. La búsqueda del equilibrio entre la promoción de la libertad empresarial, el fomento a la innovación, la salvaguarda de la industria y la preservación del empleo no se presenta como una tarea de simplicidad evidente.[14] En consecuencia, es necesario buscar formulas que efectivamente se traduzcan

[11] Heinrich Hubmann, *Das Persönlichkeitsrecht,* 2.a ed, Köln Böhlau, 1967 (1.a edición, 1953), 267
[12] Fulgencio Madrid Conesa, *"Derecho a la intimidad, informática y estado de derecho"* (Valencia: 1984)
[13] Adam Westin, *"Privacy and freedom"* (New York, Atheneum, 1967), *324*
[14] Germán Darío Arias, "Las TIC y la sociedad: Doce años después de la ley'', en *Aproximación a la regulación de mercados digitales*, dir. de É. González (Colombia: Xpress Estudio Gráfico y Digital S.A.S – Xpress Kimpres, 2021), 501 - 542

en la optimización de los beneficios para los usuarios y lineamientos para las empresas, siendo estos los objetivos principales de cualquier ente regulador.

Germán Bacca, abogado especialista en Derecho de las Comunicaciones en Colombia, cataloga a las leyes de protección de datos como un régimen de protección de derechos constitucionales individuales, con el afán de proteger los datos personales de los ciudadanos para evitar su exposición, comercialización o transferencia indebida. Lo describe como un escenario en el que no se necesita de una relación contractual para que exista vulneración y responsabilidad, sino con un enfoque más amplio en el que no exista una recolección o tratamiento de los datos sin un debido consentimiento y aceptación.[15]

A medida que las grandes corporaciones de tecnología y los gobiernos amplían su capacidad para monitorear, recopilar y utilizar datos personales, surge un movimiento global de individuos y organizaciones que demandan transparencia, regulaciones justas y control sobre la información personal. Según Zuboff, el activismo digital no solo es una respuesta a las amenazas emergentes, sino una lucha proactiva para moldear un futuro digital en democracia que respete y proteja los derechos humanos fundamentales.[16]

Debido a la creciente complejidad técnica, el avance tecnológico ha impulsado la generación y el procesamiento masivo de datos, planteando desafíos nuevos a contrareloj. Conforme a los pronósticos emitidos por la firma consultora estadounidense, Gartner, se prevé que aproximadamente un 75% de la población global vera su información personal tutelada por alguna de las leyes de protección de datos para finales del año 2023.[17]

John Edwards, Comisionado de la Información del Reino Unido desde el 2022, objetiviza la discusión sobre los términos y se enfoca en los tres aspectos principales de la privacidad. Estos son la privacidad corporal, la privacidad física y la privacidad de la información. Se considera al tercer término, la privacidad de la información, como el aspecto más importante para el desarrollo del presente trabajo. Este se enfoca en la información relacionada con un individuo. Establece que la información sobre una

---

[15] Gemán Bacca, "Las TIC y la sociedad: Doce años después de la ley'', en *El derecho de la competencia frente las plataformas digitales*, dir. de É. González (Colombia: Xpress Estudio Gráfico y Digital S.A.S – Xpress Kimpres, 2021), 545 - 579

[16] Shoshana Zuboff, *"The Age of Surveillance Capitalism"*, (New York: Public Affairs, 2019)

[17] Kasey Panetta, *"Las 8 principales predicciones de ciberseguridad para 2021-2022",* (Stamford: Gartner, 2021)

persona genera un interés de privacidad que puede variar dependiendo de factores como la sensibilidad de la información y el propósito por el cual se recopila, utiliza o divulga.[18]

A pesar de que las tres dimensiones de la privacidad proporcionan un punto de partida practico para legislar, es importante evitar ser inflexible en cuanto a la categorización en el contexto dinámico actual, dadas las superposiciones emergentes entre los tres aspectos. El acádemico Daniel J. Solove señala que existe el riesgo de intentar encajar nuevos problemas en concepciones antiguas sobre privacidad. Para él, la privacidad debe ser específica del contexto y depende de examinar las intrusiones a la privacidad como perturbaciones como la interferencia con la tranquilidad de espíritu, la intrusión en la soledad o la pérdida de control sobre la propia información.[19]

4. Marco Normativo y Jurisprudencial

El presente apartado analiza la línea legal y jurisprudencial más relevante respecto al régimen de protección a los datos personales y el derecho a la intimidad en Ecuador. Posteriormente, se aborda la concepción normativa internacional y regional sobre la protección de la información personal. A continuación, la legislación y jurisprudencia aplicable.

Hasta el año 2020, Ecuador carecía de un marco legal que regulase la difusión y la recopilación de datos personales de manera concreta. Una realidad diferente a la contemporánea donde los datos personales se regulaban de forma dispersa, sin tener una forma de prever los desafíos venideros que traen consigo las nuevas tecnologías. Debido a aquella circunstancia el 10 de mayo de 2021, el pleno de la Asamblea Nacional aprobó con una amplia mayoría de 118 votos a favor, la Ley Orgánica de Protección de Datos Personales.[20] Una ley que para su formulación aplicó el derecho comparado como fuente material de derecho, en atención a la ausencia de regulación legal previa sobre protección de datos personales. Dicha ley se instauró con una clara influencia del Reglamento General de Protección de Datos de la Unión Europea, que entró en vigor el 26 de abril de 2016.[21]

---

[18] John Edwards, "Navigating the Privacy Landscape: Reflections from the Privacy Commissioner", *PDP: Revista Uruguaya de Protección de Datos Personales No. 2* (2017), 56

[19] Daniel J. Solove, "A Taxonomy of Privacy", *University of Pennsylvania Law Review Vol. 154, No. 3, p. 477*, (2006), GWU Law School Public Law Research Paper No. 129, Available at SSRN: https://ssrn.com/abstract=667622

[20] Ley Orgánica de Datos Personales, [LOPDP]. R.O. Suplemento 459 de 26 de mayo 2021.

[21] Reglamento (UE) 2016/679, *Unión Europea: Parlamento y Consejo Europeo*, 2016, deroga a la Directiva 95/46/EC, y entrará en vigencia desde el año 2018.

El derecho a la protección de los datos personales es reconocido por la Constitución del Ecuador de 2008, en su artículo 66, numeral 19 en el *"Capítulo V. De los derechos de libertad"*. Este artículo abarca el acceso y la capacidad de desición sobre la información personal, además sintetiza que para todo tipo de procesamiento de datos se requiere de la autorización del titular o el mandato de ley.[22] El reconocimiento y salvaguardia del derecho a la honra y a la intimidad personal y familiar en Ecuador, surgió medio siglo antes, por primera vez, en la Constitución de 1967.[23] Siendo este un derecho igualmente reconocido en la Constitución ecuatoriana de 2008.

El 07 de noviembre de 2023 el Presidente de la República, mediante el Decreto Ejecutivo Nro. 904, expidió el Reglamento General de la Ley Orgánica de Protección de Datos Personales, RGLOPDP. Dicho reglamente aborda varios aspectos significativos sobre la aplicación de la LOPDP. Entre ellos, se destacan aspectos clave como los criterios que las empresas deben seguir para designar a un delegado de protección de datos personales, las circunstancias en las cuales las entidades responsables deben mantener un registro de las actividades de tratamiento, y, en términos generales, aborda cuestiones relacionadas con el consentimiento, las notificaciones de violaciones de seguridad y las evaluaciones de impacto.[24]

La sentencia 2064-14-EP/21, marcó un hito en la jurisprudencia constitucional de Ecuador estableciendo criterios de gran relevancia en el ámbito de la protección de datos personales, especialmente en el contexto de herramientas digitales y redes sociales.[25] La definición de parámetros para resolver casos específicos de acciones constitucionales reconoce la necesidad de un enfoque casuístico en asuntos que no admiten soluciones predefinidas y abstractas. La Corte enfatiza que estas decisiones deben estar respaldadas por estándares legales sólidos basados en la Constitución y los tratados internacionales de derechos humanos. La principal contribución de la sentencia es proporcionar una guía completa, vinculante y aplicable en la materia sobre la expectativa rasonable de privacidad.[26]

---

[22] Constitución de la República del Ecuador, R.O. 449, 20 de octubre de 2008, reformada por última vez R.O. Suplemento 181 de 15 de febrero de 2018.
[23] Constitución de la República del Ecuador, R.O. 25 de mayo de1967
[24] Decreto Ejecutivo 904, Presidencia de la República [Reglamento General de la Ley Orgánica de Protección de Datos Personales], Registro Oficial 435 de 07 de noviembre del 2023.
[25] Sentencia 2064-14-EP/21, Corte Constitucional del Ecuador, 27 de enero de 2021
[26] La expectativa razonable de privacidad es un concepto legal que se refiere a la idea de que una persona tiene derecho a esperar que ciertas áreas o aspectos de su vida no sean objeto de escrutinio público sin su permiso. La Sentencia 2064-14-EP/21 utiliza el razonamiento del caso United States vs. Katz, y explica que la expectativa razonable de privacidad, surge inicialmente como consecuencia del desarrollo jurisprudencial del derecho a la intimidad y privacidad efectuado por la Corte Suprema de los Estados

En relación a las normativas complementarias, el Código Orgánico Integral Penal aborda el delito de violación a la intimidad. Este delito se configura cuando una persona, sin contar con el consentimiento o la autorización legal pertinente accede o difunde datos personales por cualquier medio. En consecuencia, este acto ilícito conlleva una sanción de pena privativa de libertad que oscila entre uno y tres años.[27]

Si bien existen diversos enfoques internacionales en el ámbito de la regulación sobre protección de datos, el más influente para la creación de LOPDP es el Reglamento General de Protección de Datos, conocido como RGPD, que entro en vigor en 2016 en la Unión Europea.[28] En el ámbito internacional, el objetivo del reglamento es garantizar la protección de los datos personales de forma coherente y sin divergencias entre los países que conforman la Unión Europea, para promover la libre circulación de datos dentro del mercado interior. Un reglamento que pretende proporcionar seguridad jurídica y transparencia a las empresas, abarcando las necesidades de todos los operadores económicos, independientemente de su tamaño. El mismo incorpora excepciones proporcionales a las necesidades específicas de las microempresas y las pequeñas y medianas empresas, en lo que respecta a materia de registros para organizaciones con menos de 250 empleados. [29]

En los Estados Unidos existen una serie de leyes y regulaciones que protegen la privacidad y los datos de los individuos, pero no existe como tal un cuerpo legal a nivel nacional equivalente al de la Unión Europea. Este país tiene un enfoque sectorial y fragmentado. Algunos estados, como California, donde se implementó el *California Customer Privacy Act*, CCPA, obliga a todas las empresas a gestionar adecuadamente los datos personales del consumidor. Desde 1999, en Chile tienen la Ley N. 19.628, la cual ha sido objeto de fuertes críticas por quedarse desactualizada frente a los desafíos tecnológicos actuales.[30] En la actualidad, existe un proyecto de ley chileno que planea incorporar las reformas necesarias.

La Organización de los Estados Americanos, en adelante OEA, aprobó el 11 de noviembre de 2021, la publicación de los 13 principios actualizados sobre la privacidad

---

Unidos de América en el ya mencionado caso. En el la Corte Suprema decidió que el accionante tenía una expectativa razonable de privacidad, y que, por lo mismo, se vulneró su derecho a la intimidad.

[27] Código Orgánico Integral Penal, [COIP]. R.O. Suplemento 180 de 10 de febrero de 2014

[28] Reglamento (UE) 2016/679, *Unión Europea: Parlamento y Consejo Europeo*, 2016, deroga a la Directiva 95/46/EC, y entrará en vigencia desde el año 2018.

[29] Considerando 13, Reglamento (UE) 2016/679, 2016.

[30] "Comentarios al proyecto de ley chileno sobre protección de datos personales". *Revista Chilena de Derecho y Tecnología de la Universidad de Chile. Vol. 11 Núm. 1* (2022), 395-412

y la protección de datos personales. Este instrumento de soft law interamericano tiene la finalidad de identificar los elementos básicos de una protección efectiva, para fortalecer y armonizar los marcos jurídicos en la materia. Es una pieza clave para el desarrollo normativo en la región debido a que estandariza lo que se espera de los cuerpos legales producidos por los 35 países miembros de la Organización de los Estados Americanos.

5. El Derecho a la Intimidad frente al Derecho a la Protección de los Datos Personales

Históricamente, la idea moderna de la intimidad como ya se anunció en el inicio del presente trabajo se originó con el artículo *"The Right of Privacy"* de Brandeis y Warren, que influenció la percepción de la intimidad como un derecho suceptible de protección en los Estados Unidos.[31] El término *privacy* no tiene una traducción exacta al español en cuanto a sus características como derecho. Es común que en literatura se use "intimidad" y "privacidad" como sinónimos semánticos, o que se pierda el significado del mismo al momento de traducir al español los conceptos del common law.

Existen distinciones conceptuales y similitudes prácticas entre el concepto de privacidad e intimidad. Ambos buscan proteger ámbitos similares debido a que su vulneración implica la intromisión en la vida personal. Como lo señala el jurista argentino Germán J. Bidart en la lengua española la intimidad se refiere a la esfera donde la información no se encuentra en el conocimiento generalizado de un tercero, mientras que la privacidad abarca acciones que, aunque privadas, pueden ser conocidas por otros.[32]

En el common law existe una visión garantista del *right to privacy*, como bien jurídico protegido que asigna a cada individuo el derecho a decidir que información y hasta que punto puede ser compartida, la misma no depende de la naturaleza del contenido de la información ni de los medios empleados para su difusión, sino simplemente del consentimiento del individuo. Siendo este sistema solamente puede hacerse efectivo cuando se ocasiona un daño, que se debe resarcir. Debido a que no existe una lista taxativa de los posibles ataques contra la información personal.[33]

El derecho a la intimidad, se traduce en la protección que brinda *the right to privacy* en el sistema anglosajón. La mayoría de los Estados partidarios de la democracia han abordado la necesidad de regular el derecho a la intimidad a través de las normativas

---

[31] Andrea Villalba, "Reflexiones jurídicas sobre la protección de datos y el derecho a la intimidad en la autodeterminación informativa", *Foro: revista de derecho No.27 ISSN1390-2466* (Quito: 2021)
[32] Germán Bidart, "Derecho constitucional comparado" (Buenos Aires: Ediar, 1998)
[33] María Nieves Saldaña, " The right to privacy La génesis de la protección de la privacidad en el sistema constitucional norteamericano: El centenario legado de Warren y Brandeis", 195-240.

denominadas leyes de protección de datos personales.[34] Esto debido al debate jurídico, que considera que el derecho a la intimidad por sí solo es incapaz de proporcionar una protección completa e integra a las personas frente a los desafíos de la tecnología moderna y las nuevas formas de compartir información.[35] Situación que genera incertidumbre y ha sido clave para realizar varios estudios sobre el comportamiento humano como se describe a continuación.

La paradoja de la privacidad, es un concepto que nace de la supuesta contradicción entre las preferencias de los usuarios de proteger su privacidad, en contraposición con su comportamiento al compartir su información personal a cambio de beneficios.[36] Esto ocurre debido a que las personas también valoran los beneficios de las tecnologías digitales, como la posibilidad de conectarse con otros, mantenerse informados y acceder a servicios y productos.[37] Por lo que, a pesar de que los individuos quieren proteger sus datos personales varios estudios demuestran que su comportamiento no a alineado a esta idea.

Daniel J. Solove, señala que no es realmente una paradoja en el sentido estricto, ya que no implica una contradicción lógica en sí misma. Se trata de una situación donde las actitudes y comportamientos en relación con la privacidad se toman en contextos específicos y están influenciadas por varios factores, como la conveniencia, la presión social y la falta de conciencia sobre los riesgos. El argumento de la paradoja de la privacidad, es una aparente contradicción de acciones en la interpretación de las actitudes y de las personas con respecto a la privacidad en línea, que a menudo se malinterpreta y se utiliza de manera incorrecta en contra de la necesidad de regulaciones más estrictas en ámbito de la protección de datos personales.[38]

El derecho a la protección de datos personales en el Ecuador, a pesar de ser un derecho constitucionalmente protegido extiende las garantías que custodian al derecho a la intimidad, y comparte la visión de la autodeterminación informativa que es definida como la imperativa capacidad de los individuos de controlar la información relacionada

---

[34] Amalia Cobos, "El contenido del Derecho a la Intimidad", *Revista Mexicana de Derecho Constitucional No. 29*, (Ciudad de México: UNAM, 2013), 46

[35] Luis Ordoñez, "La protección de datos personales en los estados que conforman la Comunidad Andina: estudio comprado y precisiones para un modelo interamericano de integración", *Foro: Revista de Derecho* (Loja: UASB, 2021), 3

[36] Juan Pablo Carrascal et al., Su comportamiento de navegación para un big mac, *Actas del 22ª conferencia internacional sobre la World Wide Web* - WWW 13 (2013).

[37] Patricia Norberg, Daniel R. Horne y David A. Horne, "La paradoja de la privacidad: intenciones de divulgación personal versus comportamientos", *Journal of Consumer Affairs No. 41*, (2007), 100-126.

[38] Daniel J. Solove, "The Myth of the Privacy Paradox", *The George Washington Law Review*, (Washigton: 2020)

con ellos, y no solamente de intrusiones de terceros sino también de los nuevos riesgos tecnológicos a los que estan expuestos.[39] Para lograr una protección integral es fundamental delimitar qué datos, debido a su utilización, pueden poner en indefensión a sus titulares.

6. Datos Susceptibles de Protección ante la Ley

Los datos suceptibles de protección ante la ley son los datos personales, estos se encuentran definidos en el artículo 4 de la LOPDP, como aquellos datos que de forma natural, directa o indirecta, identifican o hacen identificable a una persona.[40] Esta definición se basa en la que incorpora el Reglamento (UE) 2016/679, y su vez es posible determinar que esta última basa sus parámetros en la opinión emitia por un grupo de expertos que trabajaron en 2007 en el Artículo 29. En la cual se delimitan los cuatro elementos escenciales de la definición de datos personales, los cuales son: cualquier información, relacionada con, identificada o identificable, una persona natural.[41]

Existen algunas excepciones.[42] El alcance de la ley aplica a datos personales en cualquier tipo de soporte, ya sea automatizado o no. Y salvo que exista el consentimiento del titular o alguna de la situaciones premeditadas por la ley, esta prohibido el tratamiento de datos sensibles para cualquier entidad.[43] Los datos sensibles incluyen etnia, identidad de género, religión, entre otros que pueden dar origen a una discriminación, debido a que el tratamiento de los mismos datos es propenso a infringir los derechos fundamentales se le concede una protección especial.

El Foro Económico Mundial estableció la diferencia entre datos voluntarios, inferidos y observados. Estos se diferencian entre sí por la forma en la que pueden obtenerse. En primer lugar, encontramos los datos voluntarios, que son creados y compartidos de manera específica por individuos, como los perfiles de redes sociales que revelan sus preferencias y actividades. En segundo lugar, se incluyen los datos observados, que son obtenidos a través del registro de las acciones de las personas, tales como la información de ubicación recopilada mediante el uso de dispositivos móviles.

---

[39] Lois Adamma, Vulneración del derecho a la autodeterminación informativa por la audencia de garantías legales, (Guayaquil: UCSG, 2021)
[40] Artículo 4, LOPDP.
[41] Article 29 Data Protection Working Party, "Opinion 4/2007 on the concept of personal data", web site of the European Commission, 01248/07/EN, disponible en: http://bit.ly/2PtGYnv.
[42] La ley no protege los datos para fines familiares o domésticos, de personas fallecidas, datos anonimizados, de actividades periodísticas, datos regulados por leyes especilizadas relacionadas con desastres naturales y seguridad del estado, y finalmente los datos utilizados por entidades estatales para asuntos penales.
[43] Artículo 26, LOPDP.

Por último, se consideran los datos inferidos, que se derivan de análisis sobre datos voluntarios y observados, como los puntajes de crédito que proporcionan una visión de la solvencia financiera de un individuo.[44]

La relevancia del concepto de datos personales radica en su influencia sobre la extensión de las normativas de protección que rigen su uso, es decir, su implementación y comprensión. Este concepto debe ser lo bastante amplio, adaptable y versátil para incorporar de manera efectiva las desafiantes situaciones que emergen en el entorno tecnológico actual en constante evolución.[45] La postura óptima sería la de promover una regulación de datos personales que equilibre la protección de la privacidad con la innovación y el uso legítimo de datos, alentando la transparencia, el consentimiento informado a partir de medidas de seguridad sólidas que incorporen las empresas.

Los datos personales deben ser recopilados con un objetivo específico y solo se pueden solicitar aquellos datos que sean esenciales para cumplir con dicho propósito, siempre que el titular de los datos haya otorgado su consentimiento previo, explícito, libre y bien informado, tema que se abordara en el decimo apartado de este trabajo.[46] Además, se debe entender que el intercambio abrupto de información que se da en la web no se limita a un espacio físico, por lo que es necesario delimitar el ámbito de protección con el que cuentan los datos personales. El alcance de este reguardo debe ser amplio, y debe incluir toda la información personal que se recopile, utilice o comparta, ya sea en línea o fuera de línea. Esto incluye información que se recopile de forma activa, como a través de formularios de registro, o de forma pasiva, como a través de cookies o rastreadores.[47]

7. Ámbito de Aplicación Territorial

La protección de datos es un derecho fundamental que busca resguardar la intimidad y privacidad de las personas naturales. La LOPDP en Ecuador parte del principio de territorialidad, y establece que la ley se aplica a todas las entidades y personas naturales que realicen el tratamiento de datos personales en cualquier parte del territorio ecuatoriano o que estén domiciliadas en el Ecuador.[48] La extraterritorialidad en el tratamiento de datos incorporado en la ley como herramienta, aborda el desafío de que

---

[44] Word Economic Forum, *Personal data: The emergence of a new asset class* (Ginebra, 2011), Disponible en http://bit.ly/2RD01sP

[45] Nadezhda Purtova, "La ley de todo: concepto amplio de datos personales y futuro de la legislación de protección de datos de la UE". *Derecho, Innovación y Tecnología* No. 10, (2018), 40-81. DOI: 10.1080/17579961.2018.1452176

[46] Artículo 10, LOPDP

[47] Francisco José García, "Las cookies en los principales cibermedios generalistas de España", *Miguel Hernández Comunication Journal No 4*, (Valencia: UV, 2013)

[48] Artículo 3, LOPDP.

los datos no están vinculados a una ubicación geográfica específica. Esto se refiere a la situación en la que una empresa, no basada en Ecuador, maneje información personal de ciudadanos que residen en el Ecuador, y es aplicable a las actividades relacionadas con la oferta de bienes o servicios, de forma gratuita u onerosa.[49]

En cuanto al ámbito de aplicación territorial la ley ecuatoriana tiene concordancias idénticas con el Reglamento (UE) 2016/679. Este se aplica en todos los establecimientos ubicados en la Unión Europea, independientemente de que el tratamiento de datos tiene o no lugar en la misma.[50] Lo que basicamente deja una gran parte de los datos personales del mundo occidental bajo el resguardo de la misma. Es un beneficio no solo comercial, sino también en terminos de protección de datos, ya que al alinear la ley ecuatoriana con el Reglamento (UE) 2016/679 en cuanto al alcance geográfico de su aplicación, se establece una normativa coherente y compatible con la Unión Europea.

Una normativa compatible en cuanto al ámbito de aplicación genera beneficios a la largo plazo ya que, facilita el comercio internacional, aumenta la confianza de los consumidores y simplifica la gestión de datos globales. Según la Organización para la Cooperación y el Desarrollo Económico, la cooperación de regulación internacional es crucial debido a su capacidad para abordar desafíos más allá de las fronteras nacionales, promover la eficiencia económica al reducir las barreras comerciales y mejorar la eficiencia administrativa al evitar la duplicación de esfuerzos en legislaciones incompatibles.[51]

8. Descripción del Mercado de Datos

El presente apartado define las características clave del mercado de datos personales de forma global, y posteriormente aborda las deficiencias más significativas en dicho mercado, los obstáculos existentes que impiden lograr un equilibrio adecuado entre la protección de la privacidad y datos personales de los individuos, y la presencia de incentivos para las empresas para fomentar la generación de valor adicional y la innovación a través del tratamiento de la información personal.

La evolución y difusión de la tecnología han ejercido un impacto significativo no solo en la reconfiguración de las bases estructurales de los mercados, sino también en la redefinición de los procesos de transacción y la dinámica subyacente de las relaciones

[49] Artículo 3, LOPDP.
[50] Artículo 3, RGPD
[51] OECD, *Cooperación Regulatoria Internacional*, (Paris: OECD Publishing, 2021)

comerciales. Las transacciones comerciales han experimentado una revolución con la digitalización, la automatización y la aparición de nuevos modelos de negocio en línea.[52]

Según la observación de Daniel Álvarez, la sociedad de la información, vinculada a la amplia disponibilidad de datos, ha ocasionado una transformación de gran magnitud en los ámbitos social, cultural y económico, superando incluso a la Revolución Industrial en su impacto. El mercado de datos personales se caracteriza porque los datos personales no reconocen fronteras geográficas.[53] Esta es una característica fundamental de que la comercialización de datos personales es intrínsecamente global. Las empresas tienen la capacidad de recopilar información de personas físicas que residen en cualquier parte del mundo, donde involucran un contrato internacional en el manejo de estos datos.

El mercado de datos personales es una dinámica constante que desafía a las empresas a mantener las últimas tendencias y tecnologías para garantizar la protección de la privacidad y el cumplimiento de los estándares. Simplificando los procesos de procesamiento de datos es posible decir que una parte significativa de la información que navega en internet se refiere a las preferencias, hábitos, características y comportamiento de individuos que pueden ser identicados o identificables. Las empresas recopilan y procesan estos datos mediante análisis computarizados de patrones para crear perfiles detallados de los usuarios.[54] Estos perfiles se utilizan con diferentes propósitos. Lo fundamental de esta situación es que la información tiene un valor económico intrínseco. Las compañías que prosesan datos generan mayores ganancias, debido a que optimizan el servicio al cliente, mejoran la eficiencia de sus operaciones y proporcionan una mayor rentabilidad a sus propietarios y accionistas.[55]

La premisa es simple, quienes más se benefician del uso de los datos personales son las empresas. Esta premisa resalta el desequilibrio de poder que existe entre las entidades y los consumidores en lo que respecta al uso de los datos personales. Las empresas tienen acceso a una gran cantidad de datos personales sobre los consumidores, y pueden utilizarlos para sus propios fines, a menudo sin el consentimiento o el conocimiento de los consumidores. Los consumidores, de bienes o servicios, por otro

---

[52] Haim Mendelson, "Modelos de negocio, tecnologías de la información y la empresa del futuro", *Reinventar la empresa en la era digital* (Madrid: BBVA, 2014)
[53] Daniela Alvarez, *La inviolabilidad de las Comunicaciones privadas*, (Santiago: LOM ediciones, 2019), 97 - 107
[54] Kean Brich, "Data as asset? The measurement, governance, and valuation of digital personal data by Big Tech". *Big Data & Society*, (SAGE, 2021)
[55] Carlos Reyes, "Data driven companies de ventaja competitiva a necesidad básica", *MIT Technology Review*, (Massachusetts: Opinno, 2021)

lado, tienen poco control sobre cómo se utilizan sus datos personales lo cual genera un mercado no eficiente.

9. Fallas del Mercado de Datos

Las fallas del mercado se definen como situaciones o elementos que obstaculizan la asignación eficiente de recursos en los mercados, cuestionando los fundamentos en los que se basa el equilibrio competitivo, tales como la competencia perfecta, la ausencia de externalidades o la disponibilidad de información completa.[56] Existen fallas que responden especificamente al mercado del uso de datos, entre las que se incluirá como objeto de estudio del presente trabajo, en pacticular a la existencia de asimetrías de información, las externalidades de datos y el abuso de posición dominate.

La asimetría de la información se refiere a una situación en la que una de las partes involucradas en una transacción o interacción posee más información que la otra, lo que crea desequilibrios y puede llevar a resultados no eficientes. En tales casos, la parte con información privilegiada puede tomar decisiones de ventajosas en detrimento de la parte con menos información, lo que genera problemas como la selección adversa y el riesgo moral. La teoría de la asimetría de la información resalta cómo estos desequilibrios informativos pueden afectar negativamente los mercados, los contratos, las relaciones comerciales y la toma de decisiones en diversas áreas, y sugiere la importancia de desarrollar mecanismos para mitigar estos problemas y promover la transparencia en las interacciones económicas.

En el contexto de la era digital y la economía de datos, esta asimetría de la información puede manifestarse por un lado, cuando las empresas que recopilan datos de usuarios, como gigantes tecnológicos y plataformas en línea, a menudo tienen una ventaja de información significativa sobre los individuos. Tienen acceso a datos personales, patrones de comportamiento en línea y preferencias, lo que les permite segmentar a los usuarios y dirigir estrategias de marketing o publicidad de manera más efectiva. Por otro lado, cuando los individuos, en su mayoría, tienen una comprensión limitada de cómo se utilizan sus datos y cuáles son los riesgos asociados con la privacidad y la seguridad de los mismos. Esta falta de conocimiento puede llevar a la toma de decisiones sesgadas o a la aceptación pasiva de prácticas de recopilación y uso de datos que pueden no ser beneficiosas para ellos.[57]

---

[56] Gregory Mankiw, *Principios de economia,* (Austria: Cengage Learning, 2012)

[57] José María Usategui, "Información asimétrica y mecanismos de mercado", *Ekonomiaz No. 45*, (Bilbao:UPV, 1999), 116 - 141

Según Gregory Mankiw, una externalidad se produce cuando las decisiones de compra y venta de un bien o servicio tienen un impacto en el bienestar de un tercero, que no recibe ninguna compensación o pago por este efecto. Los precios del mercado, en estas situaciones, no manifiestan los efectos adicionales vinculados a la producción o el consumo de estos bienes, lo que resulta en un equilibrio competitivo ineficiente para la sociedad en su totalidad.[58] La externalidad negativa ocurre cuando una actividad económica disminuye la calidad de vida de personas que no están directamente involucradas en el mercado, y estas personas no reciben ninguna compensación por los perjuicios que sufren. Estas actividades surgen como resultado de la recopilación, el intercambio y el uso de datos indiscriminado. Estas externalidades se manifiestan como efectos negativos que influyen en la violación de la privacidad, la discriminación de los individuos, la creación de perfiles sin el concentimiento de los usuarios, provocando que el mercado de datos sea ineficiente y solo beneficie a una parte de la relación.

Las externalidades negativas del mercado pueden crear un entorno en el que es más probable que se produzca el abuso del poder en el mercado. El abuso del poder en el mercado es una conducta que se encuentra definida en el Ecuador, en el artículo 9 de la LORCPM, como aquella siuación donde uno o varios agentes económicos, aprovechando su posición dominante, emplean cualquier método para obstaculizar, limitar, distorsionar la competencia o perjudiquen la eficiencia económica y el bienestar en general.[59]

La influencia o control que ejerce una empresa puede ser un elemento relevante a la hora de evaluar si la persona dio su consentimiento libremente para el procesamiento de datos, especialmente si este consentimiento está vinculado a la prestación de un servicio. Existe un caso reciente, del año 2019, que marco un precedente en la Unión Europea sobre el abuso de posición dominante de la empresa multinacional Facebook, ahora conocida como "Meta". Esta investigación fue llevada a cabo por la autoridad de competencia de Alemania, conocida como la *Bundeskartellamt*, la cual impuso una multa a Facebook por abusar de su posición dominante en el sector de las redes sociales al imponer términos y condiciones de privacidad que, según la entidad reguladora del mercado, perjudicaban el derecho de los usuarios a la protección de sus datos personales.[60]

---

[58] Gregory Mankiw, *Principles of Economics*, (Boston: Harcourt, 1997)
[59] Ley Orgánica de Regulación y Control del Poder de Mercado, [LORCPM]. R.O. Suplemento 555 de 13 de octubre de 2011.
[60] Sebastián Cañas, "El tortuoso romance entre datos y competencia: la mirada de la Corte Europea", CeCo, (Sanriago: UAI, 2023)

El *Bundeskartellamt* argumenta que el consentimiento obtenido por el proveedor que ostenta una posición dominante en el mercado, bajo condiciones en las cuales los usuarios no pueden elegir si desean que sus datos personales sean compartidos con terceros asociados a la plataforma, como WhatsApp o Instagram, no puede considerarse como genuinamente voluntario. Esto se debe a que el uso de Facebook está condicionado a la aceptación de sus términos y condiciones en relación con las políticas de privacidad, lo que expone a los usuarios a la publicidad dirigida basada en esta información y crea un efecto de bloqueo, conocido como *Lock in Effect*.[61] Este es un término que se utiliza para explicar una práctica en la que una empresa hace que sea extremadamente difícil para sus clientes abandonarlos o cambiar a un nuevo proveedor, incluso si el cliente así lo desea.

La determinación sobre si se aplican prohibiciones a estas conductas depende de la existencia de una posición de dominio por parte de la empresa, ya que las mismas conductas realizadas por una empresa que no ostente esta posición no tienen el mismo impacto en términos de competencia.[62] Según la Comisión Económica para América Latina y el Caribe, esto ha resultado en una marcada concentración de poder económico y político en un grupo reducido de aproximadamente veinte corporaciones con sede en dos o tres de las principales potencias mundiales. Estas empresas tienen un valor de mercado que se acerca o supera la cifra del billón de dólares.[63]

Lo relevante del caso es que no solo la autoridad de protección de datos alemana conocida como la Comisión Federal de Protección de Datos y Libertad de Información, en alemán *Bundesbeauftragte für den Datenschutz und die Informationsfreiheit*, es la única entidad encargada de velar por la protección de los datos personales, ya que las autoridades de competencia también pueden intervenir si consideran que la recopilación de datos está relacionada con prácticas anticompetitivas o abuso de posición dominante en el mercado.

Una vez determinadas algunas de las fallas más significativas del mercado de datos es necesario presentar un análisis de las posibles soluciones a las mismas utilizando mecanismos de control regulatorios y sancionatorios. Es razonable afirmar que se debería imponer una mayor carga de responsabilidad a aquellos que utilizan datos personales en beneficio de su crecimiento exponencial. Las soluciones públicas pueden ser una

---

[61] Markus Eurich, The Business-to-Consumer Lock-in Effect, Cambridge Service Alliance, (Zurich: University of Cambridge, 2014), 3

[62] OCDE, *Abuso de dominancia en los mercados digitales*, disponible en www.oecd.org/daf/competition/abuse-of-dominance-in-digital-markets-2020.pdf, (2020), 13.

[63] CEPAL, *Tecnologías Digitales para un nuevo futuro,* (Santiago: Naciones Unidas, 2021), 7

herramienta eficaz para abordar las externalidades del mercado de datos. Estas soluciones pueden adoptar diferentes formas, pero en general tienen como objetivo internalizar los costos de las externalidades, de modo que los agentes que las causan asuman la responsabilidad de los daños que producen.

10. Tratamiendo de Datos Personales

La lógica induce a pensar que las entidades o individuos que recopilan y utilizan información personal son quienes deben asumir la responsabilidad de garantizar que se cumplan las regulaciones y que se minimicen los riesgos de violación de la privacidad y el derecho a la autodeterminación informativa. El primer paso para subsanar las fallas existentes en el mercado de datos es la creación de regulaciones específicas en la materia que busquen precautelar los derechos de las personas sobre su información, en el caso ecuatoriano es el papel que cumple la LOPDP, donde se definen y delimitar ciertas definiciones que se trataran a continuación.

El tratamiento de datos personales es una actividad regulada con el propósito de proteger la intimidad y los derechos de las personas sobre su información. Este tratamiento de datos personales solamente es legítimo y lícito según la normativa ecuatoriana cuando cumple con las condiciones fundamentales que garantizan que el tratamiento de datos se realice de manera justa y conforme a la ley. El tratamiento de datos se refiere al conjunto de operaciones realizadas sobre datos personales, ya sea de forma automatizada o no automatizada. Este proceso abarca desde la recopilación y obtención de información personal hasta su utilización, posesión, comunicación y eventual eliminación. [64]

La importancia de este tema radica en la necesidad de garantizar la protección de los datos personales de los ciudadanos y el respeto de sus derechos fundamentales. Los principios que rigen este tratamiento son esenciales para mantener un equilibrio entre el uso legítimo de la información y la salvaguardia de la privacidad de las personas. Estos principios, como el de juridicidad, lealtad, transparencia, finalidad, seguridad y responsabilidad, juegan un papel crucial en la gestión adecuada de la información personal por parte de las empresas.[65]

Las empresas que gestionan datos personales tienen la responsabilidad de verificar que el consentimiento cumple con estos requisitos para ser considerado válido. El consentimiento en el tratamiento de datos es una manifestación de la voluntad del

[64] Artículo 7, LOPDP
[65] Artículo 10, LOPDP

titular que debe cumplir con requisitos específicos, se define de manera precisa en la LOPDP como "la manifestación de la voluntad libre, específica, informada e inequívoca" a través de la cual los titulares de los datos otorgan su autorización para el tratamiento de dicha información.[66] Además, es esencial destacar que los titulares tienen el derecho de revocar su consentimiento en cualquier momento, y las organizaciones deben proporcionar los canales adecuados para garantizar que este derecho se ejerza de manera efectiva.

Es aquí donde la figura del responsable de protección de datos adquiere protagonismo en este proceso, debido a que es él quien tiene la capacidad de prevenir riesgos de violación de privacidad de manera más eficiente y a un costo menor. Esto se alinea con la idea de que la entidad que tiene control sobre los datos personales es la que debe asumir la responsabilidad principal de proteger la privacidad de los individuos cuyos datos se están utilizando.[67] Se trata de la obligación de garantizar la protección de los datos personales desde la fase inicial de diseño y a lo largo de todo el proceso de tratamiento. En lugar de ser reactivos, se busca que los responsables adopten un enfoque preventivo y proactivo, integrando la seguridad de los datos desde el inicio, como en la creación de nuevos productos o servicios.[68]

La regulación del tratamiento de datos en un entorno de racionalidad limitada por parte de los usuarios que no tienen toda la información es un desafío importante. Para abordar las asimetrías de información en este contexto, se sugiere facilitar el acceso a la información y seleccionar la información relevante que debe ser comunicada a las personas sobre el uso que se le dara a sus datos. En encuesta realizada el 2019, por profesionales del derecho y la informática en de la Universidad de Illinois, se proporcionan pruebas contundentes sobre la conducta de los usuarios. En primer lugar, los usuarios no sólo no leen las políticas de privacidad, sino que probablemente no podrían entenderlas si lo hicieran debido a la asimetría de información entre los usuarios y los proveedores de servicios. [69] Una alternativa planteada es la implementación de una

---

[66] Artículo 4, LOPDP

[67] Catalina Frigerio Dattwyler, "Mecanismos de regulación de datos personales: Una mirada desde el análisis económico del derecho", *Revista Chilena de Derecho y Tecnología Vol. 7 No.* 2 (Santiago de Chile, 2018), 45-80

[68] Carlo Benussi, "Obligaciones de seguridad en el tratamiento de datos personales en Chile: Escenario actual y desafíos regulatorios pendientes", *Revista Chilena de Derechi y Tecnología Vol. 9 No. 1* (Santiago de Chile, 2020), 227-279

[69] Massoda Bashir, Carol Hayes, April Lambert y Jay Kesan, "Privacidad en línea y consentimiento informado: El dilema de la asimetría de la información", *Actas de la Asociación de Ciencia y Tecnología de la Información, vol. 52, núm*. (Illinois: UIUC, 2015), 1-10

calificación de servicio basada en estándares objetivos, similar a los sistemas utilizados en la industria alimentaria en algunos países.

Este trabajo de investigación plantea la idea de implementar un sistema de rotulación sobre el tratamiento de datos similar a la que utiliza el Reglamento de Etiquetado de Alimentos Procesados para Consumo Humano para etiquetar los alimentos, como se expondra a continuación.[70] Este sistema clasificaría las políticas de privacidad en categorías como baja, intermedia y alta, utilizando códigos de colores o números para notificar a los usuarios sobre las políticas de privacidad. Esta propuesta emerge como una solución efectiva para cumplir con las disposiciones del artículo 36 del Reglamento General de la Ley Orgánica de Protección de Datos Personales, y que el sistema de etiquetado serviria como prueba de las medidas de protección implementadas por la empresa. [71]

Si las plataformas o servicios que manejan los datos personales de manera riesgosa y poco transparente recibirían una etiqueta roja. Esto podría aplicarse a aquellos que comparten datos con terceros sin un consentimiento claro, tienen prácticas de seguridad deficientes o han experimentado brechas de seguridad significativas. Las plataformas con prácticas de protección de datos aceptables, pero que podrían mejorar, recibirían una etiqueta amarilla. Esto podría incluir servicios que recopilan datos con fines de publicidad dirigida, pero que cumplen con estándares de seguridad y proporcionan opciones claras de consentimiento. Las plataformas que cumplen con altos estándares de privacidad y seguridad, brindan transparencia en el manejo de datos y dan a los usuarios un control efectivo sobre su información, recibirían una etiqueta verde, estas servicios serán considerados como opciones seguras y respetuosas de la privacidad.

Esta clasificación basada en etiquetas de colores serviría como una herramienta visual y rápida para que los usuarios comprendan el nivel de riesgo asociado con el manejo de datos personales en una plataforma específica. Además, podría motivar a las empresas a mejorar sus prácticas de privacidad para alcanzar o mantener una etiqueta verde, demostrando su compromiso con la protección de la privacidad de los usuarios, y mejorando su reputación en el mercado. Los responsables y los respectivos encargados del tratamiento de datos tienen que contar con estrategias encaminadas al cumplimiento de sus obligaciones legales. La normativa entonces se alinea con la idea de que la entidad

[70] Reglamento de Etiquetado de Alimentos Procesados para Consumo Humano, [REAPCH]. R.O. Suplemento 318 de 25 de agosto de 2014.
[71] Artículo 36, RGLOPDP.

que tiene control sobre los datos personales es quien debe asumir la responsabilidad principal de proteger la privacidad de los individuos cuyos datos se están utilizando, por lo tanto es quien debe rendir cuentas sobre sus actividades.[72]

El diseño de un marco legal que aborde de manera efectiva las fallas del mercado de datos y garantice una protección integral a la intimidad y el derecho a la protección de datos es esencial en la era digital actual. Otra posible vía para subsanar las externalidades negativas del mercado de datos y el abuso de posición dominante de varias empresas es mediante la implementación de impuestos sobre datos. Estos impuestos podrían servir como herramienta para desincentivar la acumulación excesiva de información personal, promoviendo así la transparencia y responsabilidad por parte de las empresas como se desarrolla en el siguiente apartado.

11. Impuestos al Tratamiento de los Datos

A pesar de que actualmente Ecuador no aplique un impuesto específico sobre el tratamiento de datos, la idea de implementar tal gravamen se revela como una medida oportuna para tratar con las externalides negativas del mercado de datos. Estas eternalidades pueden tener efectos negativos sobre la privacidad, la competencia económica, y el proceso democrático. Una alternativa, recientemente explorada para subsanar las fallas del mercado de datos es gravar a las empresas que obtinenen beneficios del tratamiento de datos personales para evitar su sobreexplotación. Esta propuesta sugiere que los recolectores de datos deben ser gravados por la cantidad total de datos que recopilan, en lugar de evaluar impuestos sobre transacciones de datos individuales. [73]

La razón detrás de considerar un impuesto directo a los datos radica en la dificultad de transferir la carga tributaria directamente a los consumidores, ya que el beneficio de la recopilación de datos puede no distribuirse de manera equitativa entre los usuarios. En este enfoque, los datos pueden evaluarse en términos de una cantidad en dólares por el volumen total de datos recopilados. Por ejemplo, si un estado impone un impuesto de 1 dólar por gigabyte de datos recopilados, las empresas como Google tendrían que pagar impuestos sobre todos los datos recopilados de esa jurisdicción,

---

[72] Catalina Frigerio Dattwyler, "Mecanismos de regulación de datos personales: Una mirada desde el análisis económico del derecho", *Revista Chilena de Derecho y Tecnología Vol. 7 No.* 2, (Santiago de Chile,2018), 45-80

[73] Viktor Mayer-Schönberger, *Reinventing Capitalism in the Age of Big Data*, (London: Basic Books, 2018), 165

independientemente de la fuente específica de los datos. Este impuesto directo sobre los datos busca evitar que las empresas transfieran fácilmente el costo a los usuarios.[74]

Como alternativa para desincentivar la recopilación excesiva de datos, se plantea la idea de crear tramos impositivos marginales elevados más allá de ciertos niveles de datos. Esto podría ser una medida para desalentar la acumulación masiva de datos y fomentar prácticas más cuidadosas en la gestión de la información personal. Teniendo en cuenta estas dificultades, los datos pueden ser la mejor base impositiva o al menos un complemento viable en el futuro. Un impuesto al usuario y recopilador de datos basado en el volumen aliviaría la mayoría de los problemas que enfrentan los gobiernos modernos a la hora de recaudar ingresos, además de ayudar a disuadir algunas de las externalidades negativas que genera la recopilación de datos.

La preocupación sobre un impuesto como el descrito nace de la posible doble imposición, esto plantea un desafío importante en el contexto de la propuesta de gravar a las empresas que realizan el tratamiento de datos personales. La implementación de este nuevo impuesto, si no se aborda adecuadamente, podría dar lugar a situaciones de doble imposición, lo cual podría ser contraproducente y generar cargas fiscales adicionales tanto para las empresas como para las jurisdicciones involucradas. Es esencial tener en cuenta las consideraciones fundamentales de política tributaria para diseñar normas eficaces que eviten la doble imposición.[75]

Para garantizar que pequeñas empresas o usuarios no sean gravados de manera desproporcionada, se propone un umbral de exención que establece ciertos límites antes de aplicar el impuesto. Este umbral podría ser gradual para capturar rápidamente a aquellos que utilizan grandes cantidades de datos. Además, se sugiere que la tasa impositiva marginal pueda diseñarse como una función logarítmica para agilizar el impuesto a la recopilación de datos y evitar efectos acantilado.[76]

Este trabajo plantea además, la idea del establecimiento de beneficios fiscales basados en la implementación de prácticas avanzadas de seguridad y privacidad de datos. Antes de que el Estado de este beneficio tendría la empresa que certificarse con buenas

---

[74] Omri Marian, "Taxing Data", *Legal Studies Research Paper Series No. 2021-17*, (California: UCLA, 2021), 60

[75] Rocío Lasarte, Los desafíos fiscales de la economía digital: el impuesto provisional de la UE. ¿Nuevas medidas para que todas las empresas tributen de forma equitativa?, *Revista de Contabilidad y Tributación. CEF N.º 428* (Sevilla: US, 2018), 27

[76] Omri Marian, "Taxing Data", *Legal Studies Research Paper Series No. 2021-17*, (California: UCLA, 2021), 63

prácticas en protección de datos como lo estipula el artículo 52 del Reglamento General de la Ley Orgánica de Protección de Datos Personales.[77]

Las empresas que inviertan en tecnologías de cifrado robustas, medidas proactivas para prevenir brechas de seguridad y que adopten estándares internacionales de protección de la privacidad podrían recibir reducciones en sus obligaciones fiscales. Esto no solo motiva a las empresas a invertir en seguridad, sino que también destaca la importancia de la responsabilidad empresarial en la gestión de datos.

Los subsidios o prestamos preferenciales para fomentar la adopción de buenas prácticas es otra alternativa en beneficio de las empresas, ya que se podrían otorgar subsidios o préstamos preferenciales a empresas que demuestren un compromiso significativo con la protección de la privacidad y la innovación responsable. Estos fondos podrían destinarse específicamente al desarrollo de tecnologías centradas en la privacidad creadas en el Ecuador, la capacitación de empleados en cuestiones éticas de datos, o la implementación de infraestructuras seguras.

Al mismo tiempo, es crucial evaluar las sanciones existentes en el país, considerando el contexto ecuatoriano y evitando sanciones que puedan resultar excesivas, especialmente para las microempresas. Comparar el enfoque europeo y sus desafíos proporciona una perspectiva valiosa, permitiendo adaptar estrategias que se alineen con las particularidades de la realidad ecuatoriana y evitar consecuencias desproporcionadas para los actores del mercado.

12. Régimen Sancionatorio

En materia de sanciones hay una serie de obligaciones legales, técnicas y administrativas que las empresas deben cumplir. La Ley de Protección de Datos Personales en Ecuador ha establecido un marco regulatorio detallado para garantizar la seguridad y privacidad de los datos personales. Las entidades, ya sean públicas o privadas, que no respetan las disposiciones de esta ley enfrentan sanciones que varían según la naturaleza y gravedad de la infracción. Las infracciones se categorizan como leves o graves, con sus sanciones correspondientes que pueden ir desde multas basadas en salarios básicos unificados hasta porcentajes significativos del volumen de negocio anual.

Específicamente, las sanciones pueden alcanzar hasta el 1% del volumen de negocio del año anterior para las entidades privadas y entre 1 y 20 salarios básicos unificados para los servidores públicos.[78] Para determinar la sanción exacta, se consideran

[77] Artículo 52, RGLOPDP.
[78] Artículo 72, LOPDP.

varios factores, incluyendo la intención detrás de la infracción, si ha habido reiteración de faltas similares, el daño causado y si hay reincidencia.

A pesar de que han transcurrido dos años desde de la publicación oficial de la ley, aún no hay una autoridad designada que aclare su aplicación. A partir de mayo de 2023, sus obligaciones entraron en vigor. Por lo que, a partir de esa fecha corre el plazo de aplicación del régimen sancionatorio y las medidas correctivas en el caso de que se presenten incumplimientos. El desafío inherente para las empresas ecuatorianas radica en la disparidad económica que existe entre ellas, agravada por la falta de socialización y comprensión de las disposiciones del nuevo marco legal.

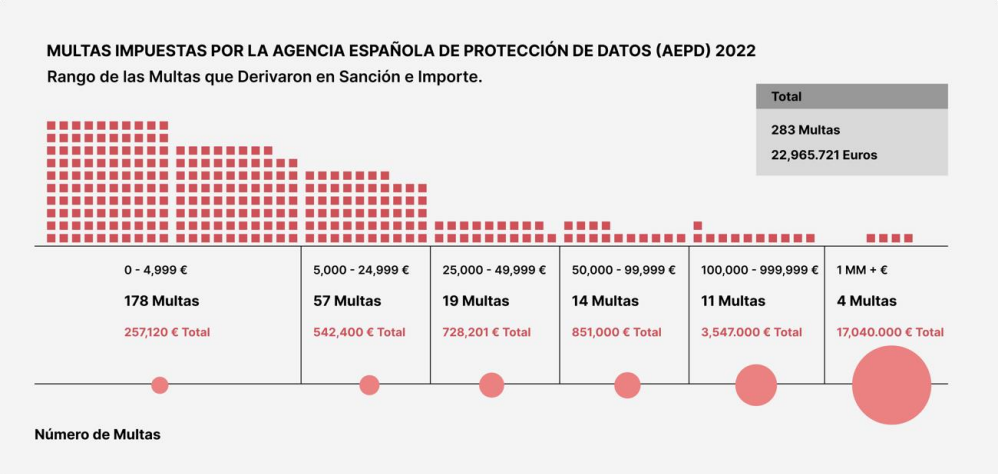
Según los datos emitidos por el Instituto Nacional de Estadística y Censos en el 2022, al categorizar las empresas por su magnitud, el Registro Estadístico de Empresas observa que las microempresas dominan con un 93,9% del total. En contraste, las empresas grandes solo constituyen el 0,5%, pero lideran en términos de ventas del 2021 y empleos registrados en 2022.[79] Por lo que, se espera que las organizaciones de mayor envergadura y dotadas de mayores recursos financieros experimenten una mayor facilidad en el cumplimiento de las exigencias y requisitos establecidos en contraposición a las microempresas.

En Europa, a pesar de la imposición de las altas multas sancionatorias se sigue con un número elevado de incumplimiento en toda la región, sobre todo por la incompatibilidad del reglamento con países fuera de la Unión Europea, y su desarrollo tecnológico como Estados Unidos, China o Rusia. La Comisión Europea está trabajando en la promoción de la cooperación internacional en materia de protección de datos. Esto incluiría la celebración de acuerdos con países fuera de la Unión Europea para garantizar que las empresas cumplan con el RGPD, y exista un sistema armónico en terminos de protección.

La Agencia Española de Protección de Datos, en adelante AEPD, es el organismo que controla el cumplimiento de la normativa. La misma lleva a cabo inspecciones, de oficio o por denuncia, y establece sanciones por incumplimiento.[80] En su memoria anual la AEPD indica que en el 2022 se impartió un total de 283 multas en España en el 2022, estas sanciones alcanzan 22, 965.721 millones de euros recaudados.

[79] Jacqueline Imbaquingo, Boletín Técnico No. 01-2023-REEM, (Ecuador: INEC, 2022), 9 - 10
[80] Memoria de Responsabilidad Social, Angencia española de Protección de Datos, (2022)

Gráfico No. 1 Multas impuestas por la AEPD en 2022



Fuente: Elaboración propia, a partir de memoria anual la AEPD de 2022.[81]

Las sanciones más elevadas impuestas por la AEPD en 2022 han sido dirigidas a las principales empresas tecnológicas que almacenan *Big Data.*[82] Es preciso mencionar la multa a Google, que ascendió a 10 millones de euros, la cual es la más alta que ha emitido la AEPD hasta ahora. Esta sanción se debe a la gestión inadecuada de las peticiones de derecho al olvido realizadas por los usuarios en su motor de búsqueda.[83] Derecho que la nueva ley ecuatoriana no incorporó en su regulación, pero si está protegido por la Unión Europea.

El riesgo que existe es sobre la imposición de sanciones desproporcionadas por el incumplimiento de la LOPDP. Ya que representa un desafío sustancial que afecta negativamente a la industria. Estas sanciones excesivas pueden resultar contraproducentes, especialmente para las microempresas que son el porcentaje mayoritario de empresas en el país, y estas pueden carecer de los recursos necesarios para cumplir plenamente con las multas. Además, estas medidas punitivas a menudo generan una carga financiera insostenible que puede poner en riesgo la supervivencia de estas empresas.

[81] Memoria de Responsabilidad Social, Angencia española de Protección de Datos, (2022)
[82] Big Data, se refiere a conjuntos de datos extremadamente grandes que, debido a su volumen, velocidad y variedad, no pueden ser procesados, analizados o gestionados de manera efectiva con herramientas tradicionales de bases de datos.
[83] Manuel G. Pascual, "Protección de Datos impone a Google una multa récord por no respetar el derecho al olvido", *EL PAÍS,* (28 de octubre 2022)

13. Conclusiones y Recomendaciones

La metodología de investigación, fundamentada en el análisis documental y comparativo, ha permitido explorar las corrientes teórico-jurídicas que han influido en la protección de datos desde su origen. El mercado de datos personales involucra a una amplia gama de actores, desde individuos que proporcionan sus datos personales, hasta empresas que los recopilan y utilizan, gobiernos que establecen regulaciones y organizaciones internacionales que establecen estándares. Esta complejidad se deriva de las múltiples partes interesadas y sus roles en la gestión de datos personales. Además, la complejidad se extiende a la necesidad de coordinación y colaboración entre diferentes partes interesadas para abordar cuestiones transfronterizas y garantizar un enfoque coherente para la protección de datos internacional.

Las empresas deben equilibrar la satisfacción de las demandas de los consumidores con el cumplimiento normativo de protección de la información. Es fundamental que las empresas desarrollen y mantengan manuales de protección de datos exhaustivos que aborden de manera clara y detallada las políticas y procedimientos para garantizar la seguridad y privacidad de la información. Las empresas deben asegurarse de comprender y cumplir con los estándares tanto a nivel nacional como internacional para evitar conflictos legales y garantizar un tratamiento uniforme y ético de la información personal en un contexto globalizado.

El mercado de datos tiene beneficios para las empresas como la facilidad para adaptarse a las necesidades de los consumidores y ofrecer servicios y productos más personalizados. La existencia de concordancias entre la LOPDP y el RGDP genera un impacto significativo para que las empresas ecuatorianas puedan participar con mayor fluidez en el mercado europeo. Bajo esta premisa las empresas ecuatorianas podrán gozar de eficiencia operativa y nuevas alianzas comerciales si se alinean a los parametros nacionales e internacionales de protección de datos. El RGLOPDP constituye la fuente primordial a la cual las empresas tendran que hacer referencia para delimitar el consentimiento de los usuarios, y además incluye el procedimiento de designación del delagado, lo que puede entender para las empresas.

El presente trabajo determina que bien es un beneficio comercial la logística detrás del tratamiento de datos, el problema ocurre cuando las grandes compañías de la información se aprovechan de su posición en el mercado, se crean asimetrías de la información entre usuarios y proveedores, y ocurren afectaciones a terceros. El examen profundo de los mecanismos más adecuados para abordar estas fallas del mercado de

protección de datos ha revelado la necesidad de incentivos que impulsen la adopción de prácticas éticas y la innovación responsable por parte de las empresas. Se ha evidenciado la importancia de la educación y concientización del consumidor para equilibrar el poder en el mercado de datos personales y subsanar la asimetría de la información, y se ha abordado la alternativa de rotulación del tratamiento de datos de parte de las empresas.

Además, se propone la creación de un impuesto que grave a las empresas, ya que son las responsables del tratamiento, que tenga la funcionalidad prevista de corregir las externalidades negativas al internalizar los costos asociados con la recopilación y uso de datos. Se ha destacado la importancia de un marco normativo que no solo impone sanciones, sino que también ofrece estímulos fiscales y reconocimientos para aquellas empresas que demuestren un compromiso significativo con la protección de la privacidad. En este contexto, es relevante destacar que, si bien el régimen sancionatorio de la Ley de Protección de Datos ha entrado en vigor a partir del 26 de mayo de 2023, la ausencia de una Superintendencia plenamente operativa genera incertidumbre en las empresas públicas y privadas, que ahora enfrentan la posibilidad de multas de hasta el 1% de su facturación por el inadecuado manejo de los datos personales de sus clientes y usuarios.

Finalmente, se concluye que la entidad estatal responsable del control debe ejercer su facultad sancionatoria de forma objetiva, con el objetivo de disuadir las conductas de incumplimiento de la ley de protección de datos personales. Para ello, debe evitar que el sistema sancionatorio se convierta en un sistema recaudatorio, y en su lugar, debe crear un sistema que capacite a las empresas sobre el tratamiento responsable de los datos personales. Además, se destaca la importancia de que la Autoridad de Protección de Datos tenga como objetivo primordial crear conciencia entre los consumidores acerca de este desequilibrio de poder, incentivando la toma de medidas para proteger su privacidad. En este contexto, el Estado debe intervenir para garantizar que los individuos conozcan sus derechos y se fomenten prácticas de información justa.