UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES

IMPLEMENTACIÓN DE MECANISMOS DE CONTROL Y REGULACIÓN EN EL TRATAMIENTO DE DATOS PERSONALES EN GUATEMALA

OSCAR DANILO ALLARA MARTÍNEZ

GUATEMALA, MAYO DE 2024

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES

IMPLEMENTACIÓN DE MECANISMOS DE CONTROL Y REGULACIÓN EN EL TRATAMIENTO DE DATOS PERSONALES EN GUATEMALA

TESIS

Presentada a la Honorable Junta Directiva

de la

Facultad de Ciencias Jurídicas y Sociales

de la

Universidad de San Carlos de Guatemala

por

OSCAR DANILO ALLARA MARTÍNEZ

Previo a conferírsele el grado académico de

LICENCIADO EN CIENCIAS JURÍDICAS Y SOCIALES

y los títulos profesionales de

ABOGADO Y NOTARIO

Guatemala, mayo de 2024

HONORABLE JUNTA DIRECTIVA
DE LA
FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES
DE LA
UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

DECANO:	M.Sc.	Henry Manuel Arriaga Contreras
VOCAL I:	Lcda.	Astrid Jeannette Lemus Rodríguez
VOCAL II:	Lic.	Rodolfo Barahona Jácome
VOCAL III:	Lic.	Helmer Rolando Reyes García
VOCAL IV:	Br.	Javier Eduardo Sarmiento Cabrera
VOCAL V:	Br.	Gustavo Adolfo Oroxom Aguilar
SECRETARIO:	Lic.	Wilfredo Eliú Ramos Leonor

TRIBUNAL QUE PRACTICÓ
EL EXAMEN TÉCNICO PROFESIONAL

Primera Fase:

Presidente:	Lcda.	Maida Elizabeth López Ochoa
Vocal:	Lcda.	Alba Jeanette González Aldana
Secretario:	Lic.	Dimas Camargo

Segunda Fase:

Presidente:	Lcda.	Silvia Patricia Hernández Montes
Vocal:	Lic.	Abraham Augusto Diaz Sánchez
Secretario:	Lic.	Edson Waldemar Bautista Bravo

RAZÓN: "Únicamente el autor es responsable de las doctrinas sustentadas y contenidas en la tesis" (Artículo 43 del Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público).

FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES
UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
SECRETARIA
GUATEMALA, C. A.

Facultad de Ciencias Jurídicas y Sociales, Unidad de Asesoría de Tesis. Ciudad de Guatemala, 09 de agosto de 2023.

Atentamente pase al (a) Profesional, **EDGAR ARMINDO CASTILLO AYALA,** para que proceda a asesorar el trabajo de tesis del (a) estudiante **OSCAR DANILO ALLARA MARTÍNEZ,** con carné 201601381 intitulado: **IMPLEMENTACIÓN DE MECANISMOS DE CONTROL Y REGULACIÓN EN EL TRATAMIENTO DE DATOS PERSONALES EN GUATEMALA.**

Hago de su conocimiento que está facultado (a) para recomendar al (a) estudiante, la modificación del bosquejo preliminar de temas, las fuentes de consulta originalmente contempladas; así como, el título de tesis propuesto.

El dictamen correspondiente se debe emitir en un plazo no mayor de 90 días continuos a partir de concluida la investigación, en este debe hacer constar su opinión respecto del contenido científico y técnico de la tesis, la metodología y técnicas de investigación utilizadas, la redacción, los cuadros estadísticos si fueren necesarios, la contribución científica de la misma, la conclusión discursiva, y la bibliografía utilizada, si aprueba o desaprueba el trabajo de investigación. Expresamente declarará que no es pariente del (a) estudiante dentro de los grados de ley y otras consideraciones que estime pertinentes.

Adjunto encontrará el plan de tesis respectivo.

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FAC. DE C.C. J.J. Y S.S.
UNIDAD DE ASESORIA DE TESIS
GUATEMALA, C. A.

CARLOS EBERTITO HERRERA RECINOS

Jefe (a) de la Unidad de Asesoría de Tesis

SAQO

Fecha de recepción 11 / 08 / 23. (f) _____

Asesor(a)
Edgar Armindo Castillo Ayala **(Firma y sello)**
Abogado y Notario

LIC. EDGAR ARMINDO CASTILLO AYALA 3ª AVENIDA 13-46 ZONA 1

Guatemala, 03 de octubre de 2023

Doctor
Carlos Ebertito Herrera Recinos
Jefe de Unidad de Asesoría de Tesis
Facultad de Ciencias Jurídicas y Sociales
Universidad de San Carlos de Guatemala

Doctor Herrera Recinos:

Respetuosamente me dirijo a usted con el objeto de informarle que, en mi calidad de Asesor de Tesis, procedí a asesorar al bachiller Oscar Danilo Allara Martínez, según nombramiento de fecha 09 de agosto de 2023, intitulada: "IMPLEMENTACIÓN DE MECANISMOS DE CONTROL Y REGULACIÓN EN EL TRATAMIENTO DE DATOS PERSONALES EN GUATEMALA". En virtud de lo analizado, me permito emitir el siguiente,

DICTAMEN:

a) En virtud de mis funciones como asesor, he evaluado el trabajo de investigación intitulado "IMPLEMENTACIÓN DE MECANISMOS DE CONTROL Y REGULACIÓN EN EL TRATAMIENTO DE DATOS PERSONALES EN GUATEMALA". Tras una revisión exhaustiva, se ha decidido mantener el título propuesto, ya que refleja con precisión el enfoque de la investigación.

b) El contenido de esta tesis aborda una cuestión de gran relevancia en la actualidad, analizando de manera detallada la legislación y las prácticas en el tratamiento de datos personales en Guatemala. Se identifican aspectos clave que impactan en la protección de la privacidad de los ciudadanos y se proponen recomendaciones concretas para mejorar la regulación en este ámbito.

c) En cuanto a los métodos de investigación empleados, el autor utilizó una combinación de métodos analíticos, sintéticos, inductivos y deductivos. Estos enfoques metodológicos permitieron un análisis profundo y una síntesis adecuada de la información recopilada, así como la generación de conclusiones basadas en una lógica sólida. En términos de técnicas de investigación, se utilizaron fichas bibliográficas y documentales. Estas técnicas facilitaron la recopilación y organización eficiente de la información relevante, asegurando la calidad y precisión de los datos utilizados en la investigación.

d) El informe final de la tesis se caracteriza por su claridad expositiva y su rigurosidad técnica. El bachiller ha demostrado un sólido dominio de las reglas ortográficas y una habilidad destacada para comunicar de manera efectiva los resultados de su investigación.

e) Esta tesis representa una contribución significativa al campo del derecho de datos personales en Guatemala y puede servir como referencia fundamental para futuros trabajos de investigación y para la formulación de políticas públicas en este ámbito.

f) En la sección de conclusiones, el bachiller presenta un análisis crítico de los hallazgos y formula recomendaciones concretas para mejorar la protección de datos personales en Guatemala. Estas recomendaciones son fundamentales para el fortalecimiento de la regulación en este campo.

g) La bibliografía utilizada en la investigación es pertinente y adecuada al tema, incluyendo fuentes tanto nacionales como internacionales de relevancia en el ámbito de la protección de datos personales.

h) El bachiller ha demostrado una actitud receptiva hacia las sugerencias y correcciones realizadas durante el proceso de asesoramiento, lo que ha contribuido significativamente a la calidad final del trabajo.

i) Declaro expresamente que cumplo con la indicación clara y precisa de que no existe grado de parentesco entre el bachiller OSCAR DANILO ALLARA MARTÍNEZ y el asesor que suscribe la presente.

Con base en lo anterior, confirmo que esta tesis cumple con todos los requisitos estipulados en el artículo 31 del Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales, y del Examen General Público, por lo que apruebo el trabajo de investigación, emitiendo para el efecto **DICTAMEN FAVORABLE** para que continúe con el trámite correspondiente.

Atentamente,

Licenciado Edgar Armindo Castillo Ayala
Abogado y Notario
Colegiado No. 6220
Cel: 3391-3595

Edgar Armindo Castillo Ayala
Abogado y Notario

USAC
TRICENTENARIA
Universidad de San Carlos de Guatemala

D.ORD. 236-2024

Decanatura de la Facultad de Ciencias Jurídicas y Sociales de la Universidad de San Carlos de Guatemala, siete de marzo de dos mil veinticuatro.

Con vista en los dictámenes que anteceden, se autoriza la impresión del trabajo de tesis del estudiante, **OSCAR DANILO ALLARA MARTÍNEZ**, titulado **IMPLEMENTACIÓN DE MECANISMOS DE CONTROL Y REGULACIÓN EN EL TRATAMIENTO DE DATOS PERSONALES EN GUATEMALA.** Artículos 31, 33 y 34 del Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público.

HMAC/JIMR

DEDICATORIA

A DIOS: Por guiarme en el camino hacia el logro de mis objetivos.

A MI MADRE: Flor de María. Por ser fuente de amor, paciencia, y sabiduría a lo largo de mi vida y su apoyo para la consecución de esta meta universitaria.

A MI HERMANA: Silvia María. Por ser mi compañera en los desafíos y apoyarme en cada obstáculo de este camino académico.

A MI PADRE: Silvio Danilo. Por sus consejos, su apoyo y el impulso para alcanzar mis metas.

A MI ABUELITA: Sonia Morales (Q.E.P.D). Con amor eterno, por compartirme de su incondicional cariño, provocarme sonrisas sinceras y creer en mis capacidades y habilidades para lograr mis metas.

A MI ABUELITO: Óscar Martínez (Q.E.P.D). Por ser una fuente inagotable de amor y de consejos, y por inspirarme con su ejemplo de perseverancia y sabiduría.

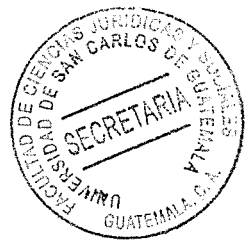
A MI TÍA: Mariela Martínez (Q.E.P.D.). Mujer ejemplar cuyo amor y sabiduría han dejado una huella imborrable en mi corazón.

A MI FAMILIA: Por el incondicional apoyo.

A MI NOVIA: Por su amor y apoyo incondicional.

A MIS AMIGOS: Quienes han sido fuentes inagotables de apoyo, risas y ánimo durante este viaje.

A: La Universidad de San Carlos de Guatemala, cuna de sabiduría.



PRESENTACIÓN

La presente tesis aborda la Implementación de mecanismos de control y regulación en el tratamiento de datos personales en Guatemala, con un enfoque en la protección de datos personales en el contexto guatemalteco. El sujeto de estudio abarca desde las autoridades gubernamentales encargadas de la regulación hasta las empresas, organizaciones y ciudadanos que gestionan datos personales.

Para llevar a cabo esta investigación, se utilizaron métodos analíticos y sintéticos, aplicando un enfoque deductivo para analizar las leyes y regulaciones pertinentes en Guatemala. Además, se adoptó un enfoque inductivo para comprender la percepción de las personas sobre la privacidad de datos y la eficacia de las regulaciones. La investigación se realizó principalmente en Guatemala, con un análisis minucioso de las políticas y regulaciones locales, incluyendo comparaciones con estándares internacionales de protección de datos para evaluar su eficacia.

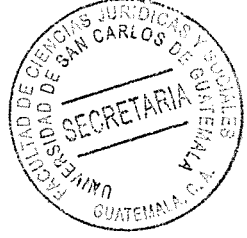
Esta tesis se centra en la protección de datos personales en Guatemala, explorando la implementación de mecanismos de control y regulación en los ámbitos del derecho públicos y privados, vinculados a la privacidad y la seguridad de la información. Los resultados de esta investigación son relevantes para comprender y mejorar la protección de datos en Guatemala, con posibles implicaciones para políticas públicas y prácticas empresariales.

HIPÓTESIS

La implementación efectiva de mecanismos de control y regulación en el tratamiento de datos personales en Guatemala, dentro del marco de los ámbitos legales y jurídicos, contribuirá a un aumento significativo en la protección de la privacidad de los ciudadanos al establecer estándares claros de manejo de datos y sanciones por su incumplimiento.

Además, al fomentar la confianza en el uso de servicios en línea, se reducirán las preocupaciones sobre la privacidad, lo que a su vez impulsará una mayor adopción de tecnologías digitales y la participación activa en la sociedad digital. Este proceso no solo beneficiará a los ciudadanos al proteger sus derechos de privacidad, sino que también fortalecerá la posición de Guatemala en el ámbito internacional al alinearse con los estándares de protección de datos aceptados a nivel mundial, lo que podría facilitar las relaciones comerciales y la cooperación en el ámbito digital con otros países.

COMPROBACIÓN DE LA HIPÓTESIS



La investigación confirma la hipótesis planteada al comprobar que la falta de una regulación sólida en protección de datos en Guatemala refuerza la necesidad crítica de establecer mecanismos de control y regulación. La revisión del marco legal guatemalteco destaca la urgencia de fortalecer la regulación existente y garantizar su aplicación efectiva para proteger los datos personales de posibles malas prácticas.

La comparación con experiencias internacionales subraya la importancia de regulaciones claras y eficientes para equilibrar la protección de datos con el desarrollo tecnológico. En conclusión, la investigación respalda la hipótesis al evidenciar que la carencia de regulación refuerza la necesidad imperativa de implementar mecanismos de control y regulación para garantizar la adecuada protección de la información personal en este entorno digital en constante evolución.

ÍNDICE

Pág.

CAPÍTULO III

Pág.

CAPÍTULO IV

Pág.

INTRODUCCIÓN

La implementación de mecanismos de control y regulación en el tratamiento de datos personales en Guatemala es un tema de creciente relevancia en la era digital, donde la recopilación, almacenamiento y procesamiento de información personal se ha vuelto omnipresente. Este enfoque surge de la necesidad de salvaguardar los derechos fundamentales de los individuos en la sociedad de la información, considerando implicaciones éticas y legales.

La hipótesis planteada consiste en que existe una ausencia de regulación efectiva de mecanismos de control y regulación en el tratamiento de datos personales en Guatemala, cuya existencia contribuiría a un aumento significativo en la protección de la privacidad de los ciudadanos al establecer estándares claros de manejo de datos y sanciones por su incumplimiento. Dicha hipótesis fue debidamente comprobada, pues se determinó la urgencia de fortalecer la regulación existente y establecer mecanismos que aseguren su aplicación efectiva, dada la exposición de los datos personales a posibles malas prácticas.

El objetivo central es analizar la situación actual de la protección de datos personales en Guatemala, evaluando la efectividad de los mecanismos de control y regulación existentes. Se busca comprender cómo el derecho informático, el tratamiento de datos personales, el derecho comparado y los mecanismos de control y regulación se entrelazan para garantizar la seguridad y privacidad de la información.

El primer capítulo de la investigación se enfoca en el derecho informático, explorando los fundamentos que respaldan la regulación de la información en la era digital. Se analizarán las leyes y normativas que establecen el marco jurídico para la protección de datos en Guatemala. El segundo capítulo abordará el tratamiento de datos personales, detallando los procesos, responsabilidades y derechos asociados a la gestión de información personal. En el tercer capítulo, se llevará a cabo un estudio comparativo. Este enfoque permitirá identificar mejores prácticas y posibles estrategias de mejora

para el contexto guatemalteco. El cuarto capítulo se centrará en los mecanismos de control y regulación existentes, evaluando su efectividad y proponiendo posibles ajustes o mejoras.

La metodología de investigación se basa en un enfoque método inductivo, para explorar las particularidades del contexto guatemalteco y un enfoque deductivo, para analizar cómo se aplican los principios generales de protección de datos. Además, se utilizó el método sintético para integrar la información recopilada e integral, buscando contribuir al desarrollo de políticas más efectivas que garanticen la privacidad y seguridad de los datos personales en el entorno digital guatemalteco.

CAPÍTULO I

1. Derecho informático

El derecho informático es una rama del derecho que se encarga de regular las relaciones entre las personas y las tecnologías de la información y la comunicación. Esta área del derecho aborda una amplia variedad de temas, desde la protección de datos personales y la privacidad en línea hasta la propiedad intelectual y el comercio electrónico[1].

Dicha rama del derecho es esencial en la actualidad debido a la creciente importancia de la tecnología en nuestras vidas diarias, y es necesaria para garantizar la protección de los derechos y libertades fundamentales en el entorno digital. A medida que la tecnología continúa evolucionando rápidamente, el derecho informático también debe adaptarse y desarrollarse para abordar los nuevos desafíos que surgen en este campo en constante cambio.

Tiene como objetivo principal proteger los derechos de las personas y las empresas en el entorno digital. En la actualidad, la mayoría de las actividades cotidianas, como la comunicación, el comercio, la banca, la educación y el entretenimiento, se realizan en línea. Por lo tanto, es importante que las leyes y regulaciones sean actualizadas y efectivas para asegurar que la privacidad, la seguridad y los derechos de propiedad intelectual estén protegidos en el mundo digital.

[1] https://www.ceupe.mx/blog/**que-es-el-derecho-informatico.html** (Consultado el 3 de junio de 2023).

1.1. Antecedentes

La seguridad siempre ha sido menester en la vida cotidiana del ser humano. El deseo de proteger la información de una manera segura no es una preocupación única de esta época; por el contrario, a lo largo de la historia el hombre ha usado diversos mecanismos para alcanzar esta tarea.

El derecho informático se originó a mediados de la década de 1960, cuando la tecnología de la información y la comunicación comenzó a avanzar rápidamente. Los primeros desarrollos en la tecnología de la información incluyeron el uso de sistemas informáticos para almacenar y procesar datos, y el uso de redes de computadoras para compartir información y recursos.

A medida que la tecnología avanzaba, surgieron nuevas cuestiones legales. En la década de 1970, los tribunales comenzaron a enfrentar casos relacionados con la propiedad intelectual en el ámbito de la tecnología, y se establecieron las primeras leyes de propiedad intelectual en el ámbito de la tecnología de la información[2]. En la década de 1980, surgieron los primeros casos de delitos informáticos, como la piratería informática y el robo de datos. Esto llevó a la creación de leyes y regulaciones específicas para abordar estos problemas[3].

[2] https://leyderecho.org/**propiedad-intelectual-en-informatica** (Consultado el 3 de junio de 2023).
[3] https://ogdi.org/**historia-del-cibercrimen**. (Consultado el 4 de junio de 2023).

A medida que la tecnología de la información continuaba avanzando, se desarrollaron nuevas áreas de derecho informático, como la privacidad en línea, la seguridad de la información, el comercio electrónico y la responsabilidad de los proveedores de servicios en línea.

Hoy en día, el derecho informático es una disciplina establecida que aborda una amplia variedad de cuestiones legales relacionadas con la tecnología de la información y la comunicación. Su importancia sigue creciendo a medida que la tecnología sigue avanzando y se vuelve cada vez más integrada en nuestras vidas diarias.

1.2. Definición

Para poder comprender qué es el derecho informático, su uso y ámbitos de aplicación, es necesario conocer diversos conceptos utilizados por estudiosos de la materia. La intersección de estos conceptos y su aplicación en la era digital plantea desafíos legales únicos que requieren un profundo entendimiento de las dinámicas tecnológicas y jurídicas.

El primer concepto de derecho informático fue acuñado en la Universidad de Regensburg de Alemania, por el profesor Dr. Wilhelm Steinmüller en los 70s. Sin embargo, no se trató de un concepto con una única interpretación. Steinmüller estudió

el concepto junto con otros términos como el derecho telemático, derecho de las nuevas tecnologías, derecho de la sociedad de la información, etcétera[4].

Aznit lo define como el conjunto de principios u normas que regulan los efectos jurídicos nacidos de la interrelación de sujetos en el ámbito de la informática y sus derivaciones, especialmente en el área denominada tecnología de la información. El concepto engloba la sociedad de la información, por lo que define una ecuación cuya resultante es el derecho informático: derecho + informática + sociedad de la información = derecho informático[5].

Ríos establece que el derecho informático es el conjunto de normas jurídicas que regulan la creación, desarrollo, uso, aplicación de la informática o los problemas que se deriven de la misma en las que exista algún bien que es o deba ser tutelado jurídicamente por las propias normas[6].

Manuel Cabanellas de Torres, reconocido jurista y autor del Diccionario Jurídico Elemental, define el derecho informático como: "la rama del derecho que se ocupa de las normas y principios que regulan la utilización de la informática y de las tecnologías de la información y la comunicación, así como de las relaciones jurídicas que surgen entre las personas físicas y jurídicas en el contexto de la sociedad de la información"[7].

[4] https://mexico.leyderecho.org/**derecho-informatico/** (Consultado el 4 de junio de 2023).
[5] Altmark, Daniel. **Tratado de derecho informático**. Pág. 37.
[6] Pérez, Enrique. **Manual de informática y derecho**. Pág. 23.
[7] Cabanellas, Guillermo. **Diccionario jurídico elemental.** Pág. 137.

Concatenando los elementos y perspectivas anteriores, podemos definir el derecho informático como: rama del derecho que se ocupa de las cuestiones legales relacionadas con el uso de la tecnología de la información y la comunicación, abordando temas como la propiedad intelectual digital, la privacidad y protección de datos personales, la seguridad en línea, el comercio electrónico, la responsabilidad legal de los proveedores de servicios en línea, la regulación de contenidos en línea, entre otras.

1.3. Derecho informático y seguridad informática

Las tecnologías de la información y comunicación están presentes en casi todas nuestras actividades cotidianas, por lo que el ser humano se encuentra expuesto a escenarios y contextos en los que sus derechos y seguridad misma están en peligro, debido al gran conjunto de información que se concentra en sistemas informáticos, los cuales se encuentran vulnerables.

El derecho informático y la seguridad informática son dos conceptos estrechamente relacionados en el ámbito de la tecnología de la información y la comunicación. El derecho informático se ocupa de las cuestiones legales relacionadas con el uso de la tecnología, mientras que la seguridad informática se refiere a las medidas que se implementan para proteger los sistemas y datos de las amenazas y ataques en línea. En este sentido, el derecho informático es fundamental para establecer las normas y regulaciones que permiten el uso seguro y responsable de la tecnología, mientras que

la seguridad informática es esencial para garantizar que los sistemas y datos estén protegidos contra posibles riesgos y amenazas.

La seguridad informática es la práctica de proteger los sistemas importantes y la información confidencial de los ataques digitales, protegiendo la información digital de acceso no autorizado, corrupción o robo en todo su ciclo de vida. Es un concepto que abarca todos los aspectos de la ciberseguridad, desde la seguridad física del hardware y los dispositivos de almacenamiento, así como la seguridad de las aplicaciones de software[8].

Según Álvaro Gómez, la seguridad informática es cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos puedan conllevar daños sobre la información, comprometer su confidencialidad, autenticidad o integridad, disminuir el rendimiento de los equipos o bloquear el acceso de usuarios autorizados al sistema[9].

El derecho informático establece las bases legales para proteger la privacidad y seguridad en línea, así como para regular el acceso, uso y distribución de la información en línea. Por otro lado, la seguridad informática se encarga de implementar las medidas técnicas y organizativas necesarias para proteger los sistemas y datos de posibles amenazas en línea, como virus, malware, ataques de hackers, robo de identidad, entre otros.

[8] https://www.ibm.com/ar-es/topics/**data-security** (Consultado el 5 de junio de 2023).
[9] https://www.ceupe.com/blog/**seguridad-informatica-y-proteccion-de-datos**.html (Consultado el 6 de junio de 2023).

La cuestión radica en encontrar la manera en que el derecho puede aportar a la administración de la seguridad de la información. Hay diversas maneras en que la intervención jurídica podría abordar esta cuestión, Una de las maneras en que la intervención jurídica puede abordar esta cuestión es estableciendo regulaciones específicas que impongan responsabilidades y estándares de seguridad a las organizaciones que manejan información sensible.

Estas regulaciones pueden abarcar desde la obligación de implementar medidas de seguridad específicas hasta la notificación de brechas de seguridad a las partes afectadas. Además, el derecho informático puede jugar un papel crucial al definir las consecuencias legales y sanciones para aquellos que violen la seguridad de la información, ya sea a través de acciones maliciosas o negligencia.

1.4. Naturaleza jurídica del derecho informático

El derecho informático es un campo relativamente nuevo que se ocupa de los aspectos jurídicos relacionados con el uso de la tecnología de la información y las comunicaciones. Su naturaleza jurídica es objeto de debate, ya que algunos expertos consideran que se trata de una rama del derecho autónoma con sus propios principios y normas, mientras que otros lo ven como una extensión de las disciplinas jurídicas tradicionales[10].

[10] Contreras, Víctor. **Sobre la naturaleza jurídica del derecho informático**. Pág. 4.

La naturaleza jurídica del derecho informático puede tener implicaciones importantes en la manera en que se desarrolla, aplica e interpreta el derecho en este campo. Por ello, es fundamental comprender las diferentes perspectivas y teorías sobre su naturaleza jurídica para poder aplicar adecuadamente las normas y principios jurídicos a los casos relacionados con la tecnología de la información y las comunicaciones.

El derecho informático puede ser considerado como una rama del derecho autónoma debido a su particularidad y complejidad. Aunque está relacionado con otras ramas del derecho, como el derecho civil, mercantil y penal, el derecho informático tiene sus propios principios, normas y conceptos jurídicos que lo diferencian de otras disciplinas jurídicas[11].

Asimismo, el derecho informático es un campo en constante evolución debido al rápido avance tecnológico, lo que significa que se enfrenta a desafíos y problemas únicos que requieren soluciones jurídicas específicas, constituyendo una rama autónoma del derecho y por ser una rama atípica del mismo está enmarcada tanto en el ámbito del derecho público como del privado.

1.4.1. El derecho informático como rama del derecho público

El derecho informático puede ser considerado como una rama del derecho público debido a su relación con el Estado y su función reguladora en la sociedad. En este sentido, el derecho informático tiene como objetivo establecer las normas y

[11] Piña, Libien. **El derecho informático y su autonomía como nueva rama del derecho**. Pág. 6.

regulaciones necesarias para garantizar el uso adecuado de la tecnología de la información y las comunicaciones por parte de los individuos y las organizaciones[12].

El derecho informático en su función pública puede estar involucrado en la regulación de actividades como la protección de datos personales, la seguridad de la información, la propiedad intelectual en la era digital, la lucha contra el ciberdelito y el acceso a la información. Además, puede regular las relaciones entre el Estado y los ciudadanos en relación con la tecnología de la información y las comunicaciones, como en el caso del comercio electrónico o la firma digital[13].

1.4.2. El derecho informático como rama del derecho privado

El derecho informático también puede ser considerado como una rama del derecho privado debido a su relación con los derechos y obligaciones de los particulares en el ámbito de la tecnología de la información y las comunicaciones, proporcionando un marco legal sólido para regular y resolver conflictos en el ámbito de la tecnología de la información y las comunicaciones.

Por ejemplo, el derecho informático regula temas como la propiedad intelectual en la era digital, la responsabilidad civil por el uso de la tecnología, el comercio electrónico y los contratos informáticos, entre otros. Estas áreas son relevantes para las relaciones

[12] https://gaceta.unadmexico.mx/septiembre-octubre-2022/133-**el-derecho-informatico-y-su-vinculacion-con-otras-ramas-del-derecho** (Consultado el 11 de junio de 2023).
[13] **Ibíd.**

privadas entre particulares y empresas y, por lo tanto, están dentro del ámbito del derecho privado[14].

Se puede decir que el derecho informático es una rama transversal que se relaciona con diversas ramas del derecho, tanto público como privado. Por ejemplo, en el ámbito del derecho privado, el derecho informático se relaciona con el derecho civil, comercial, laboral, entre otros. En este sentido, el derecho informático regula aspectos como la protección de datos personales, la propiedad intelectual, los contratos electrónicos, entre otros.

Por otro lado, en el ámbito del derecho público, el derecho informático se relaciona con el derecho administrativo, penal, constitucional, entre otros. En este sentido, el derecho informático regula aspectos como la seguridad informática, la ciberdelincuencia, la protección de los derechos fundamentales en el entorno digital, entre otros.

1.5. Fuentes del derecho informático

Las fuentes materiales del derecho informático son los hechos y circunstancias que han llevado a la creación y desarrollo de este campo del derecho. Estas incluyen, entre otras, los avances tecnológicos, la globalización de la información y las comunicaciones, los cambios en las formas de comunicación y la aparición de nuevos delitos y formas de violación de derechos.

[14] **Ibíd.**

Las fuentes formales del derecho informático son las normas jurídicas que regulan el uso de las tecnologías de la información y la comunicación. Estas incluyen leyes, reglamentos, jurisprudencia, tratados internacionales y principios generales del derecho. Son pilares fundamentales para la regulación y aplicación efectiva de las normas en el ámbito de la tecnología de la información y la comunicación.

Tal como indica Marcelo Menchaca Córdova, podemos definir las principales fuentes del derecho informático como:

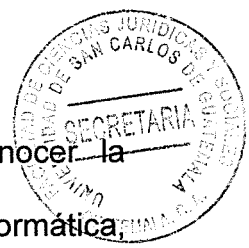
a) Los Actos: como resultado de un fenómeno directamente vinculado a la informática y provocado por el hombre.

b) Los Hechos: como resultado de un fenómeno aparejado a la informática imputable al hombre.

c) Jurisprudencia: en función de aquellos postulas emitidos por jueces, magistrados, tratadistas y estudiosos respecto al tema.

d) Las Normas: en virtud que integran la llamada política informática, la cual, según veremos posteriormente, presenta diferencias respecto a la legislación informática[15].

[15] Menchaca, Marcelo. **Derecho informático análisis, interpretación y adaptación de la teoría**. Pág. 139.



Esta clasificación refleja la complejidad del derecho informático al reconocer la interacción entre acciones humanas, eventos relacionados con la informática, decisiones judiciales y normativas específicas. La inclusión de la jurisprudencia resalta la importancia de la interpretación y evolución constante del derecho informático en respuesta a los desafíos emergentes en la era digital.

1.6. Clasificación del derecho informático

El derecho informático puede clasificarse en las formas siguientes: la informática y el derecho de la informática, las cuales se describen a continuación. En el ámbito de la informática, se enfoca en la aplicación de la tecnología de la información y los sistemas informáticos, abordando cuestiones cruciales como la propiedad intelectual de software, la protección de datos y la ciberseguridad. Por otro lado, el derecho de la informática se centra en las regulaciones legales específicas, como contratos electrónicos y privacidad en línea, estableciendo normas claras para garantizar transacciones seguras y abordar los desafíos éticos asociados con la tecnología de la información.

1.6.1. La informática

La informática jurídica, como hemos observado con el paso de los años, ha dejado sentir su influencia en prácticamente todas las áreas del conocimiento humano, incluido el campo del derecho. En este contexto, ha surgido lo que se conoce como informática jurídica, que puede definirse como el conjunto de aplicaciones informáticas en el ámbito legal.

En términos más amplios, la informática jurídica es una disciplina interdisciplinaria que se enfoca en el estudio e investigación de los principios generales de la informática aplicables a la recuperación de información legal, así como en la creación y uso de herramientas de análisis y procesamiento de datos legales necesarios para lograr dicha recuperación.

Inicialmente, en sus primeras etapas, la informática jurídica se centraba principalmente en la gestión documental de información de naturaleza legal, incluyendo leyes, jurisprudencia y doctrina jurídica, o cualquier dato relacionado con el ámbito jurídico. Sin embargo, con el tiempo, se comenzó a concebir la idea de que estos bancos de datos jurídicos no solo proporcionaban información, sino que, mediante programas especialmente diseñados, también podrían generar actos jurídicos reales, como certificaciones, atribuciones de jurisdicción y sentencias predefinidas[16].

la informática jurídica representa la integración de la informática en el ámbito legal, abarcando desde la recuperación de información jurídica hasta la creación de herramientas y procesos para la gestión de datos legales. A lo largo de su evolución, ha pasado de ser una disciplina centrada en la documentación jurídica a convertirse en una herramienta poderosa que puede generar actos jurídicos.

En síntesis, la informática jurídica fusiona la tecnología con el derecho, desde la recuperación de información hasta la automatización de actos legales. Su evolución

[16] Flores, Oswaldo. **El derecho informático y su autonomía como nueva rama del derecho**. Pág. 5.

simplifica procesos, agiliza el acceso a datos legales y mejora la eficiencia, beneficiando la toma de decisiones en el ámbito legal y facilitando la resolución de conflictos de manera más efectiva.

1.6.2. Derecho de la informática

La evolución tecnológica en las últimas décadas ha generado un profundo impacto en la sociedad, incluyendo un crecimiento exponencial en la dependencia de la tecnología de la información. Este fenómeno ha traído consigo desafíos legales que requieren atención y regulación. En este contexto, surge el derecho de la informática como una disciplina destinada a abordar estas cuestiones y a definir un marco legal adecuado para la era digital.

El derecho de la informática se puede definir como el conjunto de leyes, normas y principios que rigen los eventos y acciones relacionados con la informática. Este campo se enfoca en regular áreas emergentes, como la protección de datos personales, la propiedad intelectual, los delitos y contratos informáticos, y el comercio electrónico.

A pesar de su relativa novedad, su importancia es innegable debido a la falta de regulación en estos campos críticos de la sociedad digital.

Las fuentes del derecho de la informática son diversas. En el ámbito legislativo, existen ordenamientos jurídicos nacionales e internacionales que abordan específicamente cuestiones informáticas. Además, la jurisprudencia, la doctrina y la literatura

especializada contribuyen al desarrollo de esta disciplina, proporcionando interpretaciones y análisis fundamentales[17].

En resumen, el derecho de la informática surge como respuesta a la influencia de la tecnología de la información en la sociedad y busca establecer un marco legal sólido para la era digital. Su definición abarca un conjunto diverso de cuestiones legales, y su relevancia radica en la regulación de áreas que aún carecen de una legislación sólida. Este campo se posiciona como esencial para garantizar un entorno digital inclusivo, ético y jurídicamente sólido en la sociedad de la información.

1.7. Características del derecho informático

El derecho informático se destaca por ser único y esencial en la era digital, ya que afecta a diversas áreas legales como la privacidad, la propiedad intelectual, la ciberseguridad y el comercio en línea, debido a que la tecnología de la información y la comunicación están presentes en todas las partes de la sociedad y la economía moderna, lo que requiere normativas legales especializadas.

Tiene una serie de características que lo hacen una rama del derecho única y distinta de otras bifurcaciones. Algunas de las principales características del derecho informático, según Del Pozo, son las siguientes:

a) Su cronología de acción actúa antes de que ocurra el derecho vigente.

[17] **Ibíd.**

b) Su campo de investigación es internacional en la búsqueda de consensos aplicables en interacción con otros países y respetuoso, también, de leyes nacionales.

c) Su herramienta principal es el estudio de derecho comparado.

d) Sus fuentes de información generalmente no pueden ser los libros, porque su investigación se sitúa antes de que estos sean publicados. La mayoría de las veces serán sus fuentes de información las revistas especializadas o los documentos y memorias de los congresos en materia de derecho informático.

e) Su medio de conseguir información es siempre desarrollado con el manejo de otros idiomas además del español, debido a la cantidad necesaria de publicaciones leídas, para poder llegar a conclusiones sabias[18].

Otra característica fundamental del derecho informático es su constante evolución. La tecnología avanza a un ritmo vertiginoso, y el derecho informático debe mantenerse al día para abordar los nuevos desafíos y oportunidades que surgen en el entorno digital

[18] Del Pozo, Luz y Hernandez, Ricardo. **Informática en derecho**. Págs. 28 a la 33.

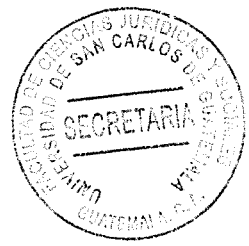
en constante cambio. Esto implica que las leyes y regulaciones deben ser interpretadas y adaptadas de manera flexible para mantener su relevancia y efectividad[19].

En síntesis, el derecho informático emerge como una disciplina legal única, desplegando características que lo diferencian de otras ramas jurídicas. Su capacidad de anticiparse a la normativa vigente, su enfoque internacional en la búsqueda de consensos, el uso primordial del derecho comparado, y la necesidad de acceder a fuentes de información especializadas, destacan su naturaleza singular.

La constante evolución del derecho informático se revela como un componente esencial, dada la acelerada velocidad del avance tecnológico. En este contexto dinámico, la flexibilidad en la interpretación y adaptación de leyes y regulaciones se convierte en un imperativo para abordar los nuevos desafíos y aprovechar las oportunidades que surgen en el entorno digital en constante cambio.

Así, el derecho informático se erige como una disciplina intrínsecamente ligada a la transformación tecnológica, exigiendo una continua actualización y adaptación para mantener su pertinencia y eficacia en la era digital.

[19] https://studylib.es/doc/710677/caracter%C3%A**Dsticas-fundamentales-del-derecho-informatico** (Consultado el 15 de junio de 2023).



CAPÍTULO II

2. Datos personales y tratamiento de datos personales

Los datos personales y su tratamiento son fundamentales en la era digital para garantizar la seguridad y protección de las personas. A continuación se describen algunos conceptos relevantes para el tema de la presente investigación.

2.1. Datos personales

Es importante distinguir entre información y datos, ya que, aunque son similares, no son lo mismo. William Ramírez describe el dato como: "el antecedente o noticia cierta que sirve como punto de partida para la investigación de la verdad y que aceptamos que se encuentra en un documento o soporte, físico o biológico, con la calidad de testimonio"[20]. Esto deja en claro que el dato es una información respaldada por documentos que se tiene certeza de su veracidad, mientras que la información en general no tiene una certeza exacta ni requiere un respaldo que pruebe el extremo expuesto.

Los datos personales son toda aquella información que permite identificar a una persona natural, ya sea directa o indirectamente, como por ejemplo el nombre, apellidos, número de identificación, dirección, teléfono, correo electrónico, fecha de nacimiento, género, entre otros. En la actualidad, con la digitalización de la información y el auge de las tecnologías de la información y la comunicación, el tratamiento de los

[20] Ramírez, William. **Libre acceso a la información, protección de datos y habeas data**. Pág.66.

datos personales se ha vuelto una cuestión clave para la protección de la privacidad y los derechos fundamentales de las personas.

En muchos países, existen leyes específicas que regulan el tratamiento de los datos personales, como la Ley de Protección de Datos Personales en la Unión Europea y la Ley de Protección de Datos Personales en México. Estas leyes establecen las obligaciones de las empresas y organizaciones que manejan datos personales, así como los derechos de los titulares de los datos, como el derecho de acceso, rectificación, cancelación y oposición (derechos ARCO).

2.2. Tratamiento de datos personales

El tratamiento de datos personales es un tema de creciente relevancia en la era digital. A medida que las tecnologías de la información avanzan, la recopilación, uso y protección de datos personales se ha convertido en un asunto fundamental tanto para individuos como para organizaciones.

Según el Manual de Protección de Datos Personales de Perú, el tratamiento de datos personales se puede definir como: "cualquier operación o proceso, automatizado o manual, que se realiza sobre los datos personales, tales como recopilación, grabación, registro, almacenamiento, conservación, uso, consulta, transferencia, modificación, supresión, bloqueo, entre otros"[21].

[21] Adjuntía en asuntos constitucionales de Perú. **Manual de protección de datos personales**. Pág. 14.

Actualmente, la información personal está al alcance de todos, y las preocupaciones sobre la seguridad y la privacidad son fundamentales. Las instituciones y empresas que gestionan datos personales deben abordar no solo los aspectos técnicos del almacenamiento y procesamiento, sino también las implicaciones éticas y legales asociadas. La transparencia en la recopilación de datos, el consentimiento de los individuos y la implementación de medidas de seguridad adecuadas son elementos esenciales en la protección y conservación de la información personal.

2.3. Derecho a la autodeterminación informativa

La protección de la privacidad y los datos personales (conocida como autodeterminación informativa) son derechos fundamentales estrechamente relacionados con la dignidad humana. El derecho a la privacidad implica principalmente proteger ciertos aspectos de nuestra vida personal y familiar de ser conocidos por otros, especialmente aquellos que deseamos mantener en privado.

En cambio, el derecho a la autodeterminación informativa tiene un alcance más amplio y se compone de elementos más complejos, abarcando una gama más amplia de aspectos en comparación a otros conceptos relativos a la protección de datos.

Según el autor Daniel López Carballo, la autodeterminación informativa se refiere a: "la capacidad de la persona para decidir, controlar y modificar la información que le

concierne y que está en poder de terceros, de tal forma que pueda determinar en qué medida y en qué condiciones esa información puede ser conocida por otros"[22].

La autodeterminación informativa se puede definir como la capacidad de una persona para controlar la divulgación y el uso de su información personal, y decidir lo que los demás pueden saber sobre su vida privada en cada momento. Este derecho es esencial para proteger los datos personales de los ciudadanos y les permite definir y ajustar su imagen pública y reputación.

Concisamente, la autodeterminación informativa otorga al individuo la autoridad para tomar decisiones sobre cuándo y en qué límites se debe compartir información sobre su vida privada, basándose en la idea de la autodeterminación.

2.4. Límites a la autodeterminación informativa

El derecho a la protección de los datos personales no es una norma absoluta, sino que, en ciertas situaciones, puede y debe ceder ante otros valores y derechos constitucionales. Al igual que cualquier otro derecho fundamental, esta libertad puede estar sujeta a limitaciones, que pueden derivar tanto de la Constitución de manera directa como de forma indirecta o mediata. Estas restricciones se justifican por la necesidad de salvaguardar no solo otros derechos consagrados en la Constitución, sino también otros intereses protegidos por esta.

[22] https://dlcarballo.com/2019/03/14/**analisis-de-la-normativa-nicaraguense-en-materia-de-proteccion-de- datos/** (Consultado el 30 de junio de 2023).

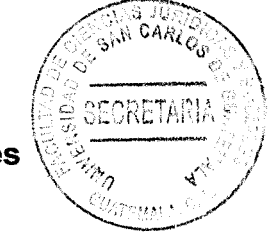
Si bien la autodeterminación informativa es un concepto fundamental para proteger la privacidad y los derechos individuales en el entorno digital, también existen algunos límites y consideraciones importantes que deben tenerse en cuenta. Además, la globalización y la transmisión de datos a través de las fronteras plantean desafíos en términos de jurisdicción y cumplimiento de las leyes de privacidad en diferentes países, lo que requiere acuerdos internacionales y estándares armonizados.

Según el Instituto Nacional de Transparencia, Acceso a la Información y Protección a los Datos Personales de México[23], este derecho, como cualquier otro, tiene límites: la seguridad nacional y pública, disposiciones de orden público, la salud pública y derechos de terceros.

La preservación de la autodeterminación informativa es esencial para resguardar la privacidad e individualidad en el entorno digital. Sin embargo, las limitaciones impuestas en determinadas situaciones subrayan la necesidad de tomar en cuenta estos derechos individuales con el bien común y la seguridad de la sociedad en su conjunto. En este delicado equilibrio, se busca establecer políticas que protejan tanto la libertad individual como el interés colectivo en un entorno digital siempre cambiante.

La promoción de una cultura de privacidad fomenta una mayor responsabilidad tanto en los usuarios como en las entidades que manejan datos, contribuyendo a un entorno digital más ético y respetuoso de los derechos fundamentales.

[23] https://micrositios.inai.org.mx/**guiastitulares/INAIvolumen01**/3.3.html (Consultado el 12 de julio de 2023).



2.5. Situaciones justificadas para la recopilación y uso de datos personales

La recopilación y uso de datos personales se justifican en diversas situaciones, principalmente cuando sirven para proporcionar y mejorar servicios, garantizar la seguridad, y cumplir con obligaciones legales y regulatorias. Es esencial que esta recopilación se realice de manera que garantice la seguridad y confidencialidad de los datos, evitando el acceso o uso no autorizado tanto de la información como del equipo utilizado para su tratamiento[24].

Estas prácticas encuentran su justificación en la necesidad de proporcionar experiencias adaptadas a las preferencias individuales, garantizar la seguridad en transacciones y prevenir fraudes, así como contribuir a avances en la investigación y desarrollo. No obstante, la gestión de datos personales también plantea desafíos éticos y de privacidad, subrayando la importancia de equilibrar la utilidad de la recopilación con la protección de los derechos individuales y el cumplimiento de obligaciones legales y regulatorias. En este contexto, exploraremos las razones legítimas que respaldan la recopilación y uso de datos personales, reconociendo la necesidad de prácticas responsables y transparentes en este ámbito:

a) Intereses legítimos y obligaciones legales: Las organizaciones pueden tener la obligación legal de recopilar y utilizar ciertos datos personales para cumplir con regulaciones específicas. Por ejemplo, en ciertos casos, las empresas pueden estar

[24] https://thedataprivacygroup.com/es/blog/2019-5-24-**gdpr-explained-the-6-legal-grounds-for-processing-personal-data-lawfully/** (Consultado el 15 de julio de 2023).

obligadas a recopilar información sobre sus clientes para fines fiscales o de seguridad.

b) Prevención de actividades ilícitas: En situaciones en las que exista un riesgo real de actividad criminal, como el terrorismo o el fraude, puede haber la necesidad de recopilar y compartir información personal para prevenir y abordar tales amenazas.

c) Intereses públicos: En algunos casos, la recopilación y el uso de información personal pueden ser justificados en interés del bienestar público. Por ejemplo, la recopilación de datos de salud pública puede ser necesaria para controlar brotes de enfermedades.

d) Investigaciones y cumplimiento de la ley: Las autoridades pueden requerir el acceso a cierta información personal como parte de investigaciones criminales o procesos judiciales.

e) Seguridad nacional: En situaciones que involucren la seguridad nacional, los gobiernos pueden justificar la recopilación y el acceso a ciertos datos personales para prevenir amenazas internas o externas.

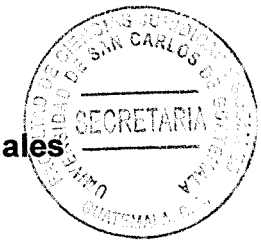
f) Protección de menores y personas vulnerables: Puede haber situaciones en las que se requiera recopilar información personal para proteger a menores de edad o personas vulnerables de daño o explotación.

Es importante encontrar un equilibrio entre la autodeterminación informativa y estas limitaciones legales y éticas. Las regulaciones y políticas de privacidad deben ser cuidadosamente diseñadas para proteger los derechos individuales y al mismo tiempo abordar las preocupaciones legales y de seguridad[25].

Es fundamental que las organizaciones identifiquen qué datos poseen y establezcan una base legal sólida para su recopilación y tratamiento. Esto implica documentar qué datos se conservan, dónde se almacenan y con qué finalidad se tratan. El cumplimiento de estas bases legales es esencial para proteger los derechos de privacidad de los individuos y evitar consecuencias graves[26].

La identificación precisa y documentación de los datos que poseen las organizaciones es un paso fundamental para garantizar la integridad y legalidad en la gestión de la información. Este proceso no solo implica conocer qué datos se almacenan, sino también comprender su ubicación y la finalidad específica para la cual se están utilizando. Establecer una base legal sólida para la recopilación y tratamiento de datos es esencial, ya que proporciona un marco normativo que respalda la legitimidad de estas prácticas.

[25] Domínguez, Ana Garriga. **Nuevos retos para la protección de datos personales en la era del big data y de la computación ubicua**. Pág. 135.
[26] **Ibíd.**



2.6. Fundamentos políticos y sociales de la protección de datos personales

El impacto de las tecnologías y las comunicaciones en la sociedad de la información, junto con el derecho a la intimidad, han llevado al reconocimiento del derecho a la protección de datos y a la creación progresiva de una cultura de protección de datos.

Esta cultura se caracteriza por una mayor conciencia sobre el valor de los datos personales y un mayor conocimiento sobre los derechos y medios de protección que el ordenamiento jurídico ofrece en este ámbito. La evolución de la tecnología y la conciencia sobre la importancia de la privacidad han sido fundamentales en el desarrollo del marco político y social de la protección de datos[27].

A lo largo de la historia, se pueden encontrar antecedentes del reconocimiento del derecho a la intimidad tal como lo entendemos actualmente. Un ejemplo es la Real Cédula emitida por Felipe II en 1592, que estableció el derecho al secreto de las comunicaciones relacionadas con la correspondencia. La cédula estableció que las cartas no podían ser abiertas ni examinadas sin el consentimiento del destinatario o el remitente.

Este antecedente puede ser considerado como un hito importante en la protección de la privacidad y la intimidad de las comunicaciones. Desde entonces, se han promulgado

[27] Zaballos, Emilia. **La protección de datos personales en España: evolución normativa y criterios de aplicación**. Pág. 34

leyes y regulaciones en todo el mundo para proteger la privacidad y seguridad de los datos personales[28].

2.7. Derecho a la intimidad, honor y privacidad

El derecho a la intimidad, honor y privacidad son derechos fundamentales reconocidos y protegidos jurídicamente en diversas legislaciones y documentos internacionales de derechos humanos. Estos derechos garantizan la protección de la esfera personal y privada de los individuos frente a interferencias indebidas por parte del Estado y de terceros.

El derecho al reconocimiento de la dignidad humana está expresamente reconocido y protegido en los primeros cinco artículos de la Constitución Política de la República. Estos artículos establecen la protección a la persona, los deberes del Estado, el derecho a la vida, la libertad de igualdad y la libertad de acción.

En cuanto a los derechos a la intimidad y la privacidad, la Corte ha señalado que se encuentran contenidos en los siguientes artículos constitucionales: la inviolabilidad de la vivienda, la inviolabilidad de correspondencia, documentos y libros, y el registro de personas y vehículos.

En relación al Artículo 31 de la Constitución, que se refiere al acceso a archivos y registros estatales, se reconoce parcialmente el derecho a la protección de datos

[28] **Ibíd**. Pág. 43.

personales o autodeterminación informativa. Este Artículo establece el derecho de toda persona a conocer la información que conste de ella en archivos, fichas u otras formas de registros estatales, así como la finalidad de dicha información. Además, se reconoce el derecho a la corrección, rectificación y actualización de la misma. Sin embargo, este derecho se limita a los datos personales que se encuentran en archivos y registros públicos, excluyendo aquellos contenidos en registros privados.

El jurista Cabanellas[29], en su sentido más general comenta que: "el derecho a la intimidad puede ser definido como aquel derecho humano por virtud del cual la persona individual, tiene el poder de excluir a las demás personas del conocimiento de su vida personal, sentimientos, emociones, datos biográficos, personales e imagen, determinando en qué medida esas dimensiones de la vida personal pueden ser legítimamente comunicados a otros".

El Artículo 11 de la Convención Americana sobre Derechos Humanos, conocida como el Pacto de San José consagra el derecho a la protección de la privacidad y la reputación de las personas. Este Artículo establece la salvaguardia de la dignidad humana y prohíbe cualquier interferencia arbitraria o abusiva en la esfera privada, familiar, domiciliaria y de la correspondencia de los individuos, así como los ataques ilegítimos a su honra o reputación.

La Convención Americana sobre Derechos Humanos, conocida como Pacto San José, es un tratado internacional que establece los derechos y libertades fundamentales de

[29] Cabanellas, Guillermo. **Diccionario enciclopédico de derecho usual.** Pág. 219.

las personas en el continente americano y fue adoptado en 1969 y entró en vigor en 1978.

El Artículo 11 establece lo siguiente: "Protección de la honra y de la dignidad:

1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad.

2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación.

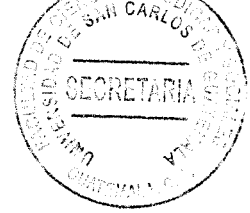
3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques".

El Estado, como parte de la Convención Americana sobre Derechos Humanos, tiene la obligación de asegurar la protección efectiva de estos derechos y adoptar medidas adecuadas para prevenir y sancionar las violaciones en este ámbito. Es importante resaltar que la libertad de expresión, protegida en el Artículo 13 del mismo instrumento legal, también está sujeta a los límites establecidos en el Artículo 11, evitando que se utilice como pretexto para difamar, insultar o atacar ilegalmente la reputación o la honra de las personas.

En el contexto del tratamiento de datos personales, el Artículo 11 del Pacto de San José implica que se reconoce el derecho de toda persona a la protección de su privacidad y dignidad. Este derecho se extiende a todas las etapas del tratamiento de datos, incluyendo la recopilación, uso, almacenamiento y divulgación de información personal. En este sentido, se prohíben las injerencias arbitrarias o abusivas en la vida privada de los individuos, lo cual engloba la salvaguardia de los datos personales recopilados.

Los Estados que son parte de la Convención Americana sobre Derechos Humanos tienen la obligación de establecer medidas legales y técnicas adecuadas para proteger la privacidad de las personas. Estas medidas deben incluir salvaguardias efectivas que impidan el acceso no autorizado, la divulgación indebida o el uso abusivo de los datos personales. Además, los Estados deben garantizar el derecho de las personas a acceder, corregir y suprimir sus datos personales cuando resulte necesario.

Es relevante destacar que el Artículo 11 del Pacto de San José, también establece límites en cuanto al uso de los datos personales. Los ataques ilegales a la honra o reputación de una persona a través de la difusión de información falsa o difamatoria pueden constituir una violación de este Artículo. En consecuencia, el tratamiento de datos personales debe realizarse de manera ética, respetando los derechos y la dignidad de las personas.



2.8. Acción de habeas data

El habeas data es un principio y un derecho fundamental en materia de protección de datos personales. Se refiere al derecho de las personas de acceder, conocer, actualizar y rectificar la información que se encuentra almacenada en bases de datos o registros de entidades públicas. El término habeas data proviene del latín, el primer vocablo hábeas significa: conserva o guarda y el segundo vocablo Data que significa: fecha o dato[30].

El habeas data tiene como objetivo principal garantizar el control y la autodeterminación de los individuos sobre sus datos personales. Este derecho busca proteger la privacidad y la intimidad de las personas, así como asegurar que la información que se almacena sea precisa, veraz, actualizada y utilizada de manera legítima. En Guatemala, el habeas data está reconocido y protegido por la Constitución Política de la República de Guatemala y la Ley de Acceso a la Información Pública (Decreto 57-2008).

El Artículo 31 de la Constitución establece que cualquier individuo tiene el derecho de conocer la información que se encuentre registrada sobre él en archivos, fichas u otras formas de registros estatales, así como la finalidad para la cual se utiliza dicha información. Además, se garantiza el derecho a corregir, rectificar y actualizar estos datos. Es importante destacar que está prohibido mantener registros y archivos que revelen la afiliación política de las personas, salvo aquellos que sean necesarios para el funcionamiento de las autoridades electorales y los partidos políticos.

[30] https://revistalex.org/index.php/**revistalex/article/view/97/228** (Consultado el 25 de julio de 2023).

CAPÍTULO III

3. Derecho comparado en materia de protección y tratamiento de los datos personales

A raíz de la ausencia de regulación de la materia en Guatemala, es de utilidad evaluar leyes existentes en otros países vecinos para tomar ideas que podrían ser funcionales adaptadas a nuestro contexto.

3.1. El derecho comparado

Según el Diccionario del español jurídico de la Real Academia Española, el derecho comparado es un método de estudio del derecho que se basa en la comparación de las distintas soluciones que ofrecen los diversos ordenamientos jurídicos para los mismos casos planteados[31].

El término derecho comparado se refiere a un análisis que compara las leyes, regulaciones y prácticas legales de diferentes países con el objetivo de identificar similitudes, diferencias y mejores prácticas en un área legal específica. En el caso de la protección de datos personales, este análisis comparativo es valioso para comprender cómo diferentes jurisdicciones abordan y regulan la privacidad de los datos personales.

[31] https://dpej.rae.es/lema/**derecho-comparado** (Consultado el 10 de agosto de 2023).

La protección de datos personales se ha convertido en un tema crucial en el entorno digital actual, ya que la creciente digitalización y recopilación de información plantean desafíos significativos para la privacidad y la seguridad de los individuos. A pesar de que Guatemala no cuenta con legislación específica en esta materia, es esencial considerar la experiencia de otros países de América Latina que han implementado regulaciones en protección de datos.

En América Latina, varios países han implementado leyes y regulaciones de protección de datos personales con el objetivo de salvaguardar la privacidad de los individuos y establecer estándares para la recopilación, el uso y la transferencia de datos personales.

Un análisis comparativo con países vecinos que tienen leyes de protección de datos podría proporcionar ideas sobre cómo estructurar una posible legislación en Guatemala. Además, puede ayudar a anticipar desafíos y consideraciones legales que podrían surgir al establecer regulaciones para la protección de datos personales en el país.

3.2. Legislación en materia de protección y tratamiento de datos personales en América Latina

En las últimas décadas, América Latina ha experimentado un importante avance en la regulación y protección de los datos personales en un mundo cada vez más digitalizado. Los países de la región han promulgado una serie de leyes y regulaciones que buscan salvaguardar la privacidad de los individuos y establecer pautas claras para

el manejo responsable de la información personal. Estas legislaciones reflejan el compromiso por equilibrar el avance tecnológico con la protección de los derechos fundamentales de privacidad, permitiendo a los ciudadanos tener mayor control sobre sus datos en un entorno en constante evolución.

Argentina, Chile, Costa Rica y Perú son algunos de los países que se destacan en la región por sus avances significativos en la innovación de las políticas de protección de datos personales.

3.2.1. Argentina

La Ley 25.326 de Protección de Datos Personales de Argentina establece una serie de disposiciones fundamentales para el tratamiento y protección de datos personales en el país. Algunos de los artículos más importantes de esta ley incluyen:

Artículo 5. Regula el consentimiento del titular para el tratamiento de sus datos, indicando que debe ser expreso, inequívoco y otorgado libremente.

Artículo 7. Establece que los datos sensibles (aquellos que revelan origen racial y étnico, opiniones políticas, religión, entre otros) solo pueden ser tratados con el consentimiento expreso del titular, salvo en excepciones previstas por la ley.

Artículo 9. Determina que los encargados de los archivos, registros y bancos de datos deben adoptar las medidas necesarias para garantizar la seguridad y confidencialidad de los datos.

Artículo 12. Regula la transferencia de datos personales a terceros países, asegurando que se cumplan los estándares adecuados de protección en dichos casos.

Artículo 14. Establece la creación de una base de datos con información de personas fallecidas, que deberá ser manejada de manera confidencial y respetuosa.

Artículo 16. Establece que el titular de los datos tiene derecho a acceder a su información personal y a solicitar su rectificación, actualización o supresión, conforme a lo dispuesto en la ley.

Artículo 26. Regula la creación de bases de datos con fines de evaluación crediticia y establece derechos específicos para los titulares de datos incluidos en dichas bases.

Artículo 31. Establece sanciones por incumplimiento de la ley, que pueden incluir multas y la suspensión de actividades relacionadas con el tratamiento de datos personales

Los Artículos del 13 al 20 establecen los derechos de los titulares de datos personales, incluyendo el derecho de acceso, rectificación, cancelación y oposición (derechos ARCO).

3.2.2. Perú

La Ley de Protección de Datos Personales de Perú, también conocida como Ley 29733, es una legislación fundamental que tiene como objetivo salvaguardar la privacidad y los derechos de los individuos en relación con sus datos personales. Promulgada en 2011 y posteriormente modificada en 2018, esta ley establece las bases para el manejo adecuado y responsable de la información personal en el país.

La ley abarca una serie de disposiciones que regulan diversos aspectos del tratamiento de datos personales. Entre los puntos clave se encuentran:

Artículo 28. Establece la obligación de notificar a la Autoridad Nacional de Protección de Datos Personales (APDP) sobre cualquier incidente de seguridad que pueda afectar los datos personales.

Artículo 32. Establece la creación de la Autoridad Nacional de Protección de Datos Personales, la cual es responsable de supervisar y hacer cumplir la ley.

Artículo 33. Regula el registro de bancos de datos ante la APDP, estableciendo los requisitos y procedimientos para su inscripción.

Artículo 37. Establece las sanciones por incumplimiento de la ley, que pueden incluir multas y otras medidas.

3.2.3. Chile

La Ley sobre Protección de la Vida Privada en Chile desempeña un papel fundamental al establecer regulaciones cruciales para el manejo y la seguridad de datos personales en el país. Esta legislación se centra en garantizar el respeto por la privacidad de los individuos y en proporcionar un marco legal que equilibre el uso legítimo de la información con la protección de los derechos fundamentales de las personas.

Uno de los aspectos destacados de esta ley es la creación de la Agencia de Protección de Datos Personales, una entidad autónoma encargada de supervisar y fiscalizar el cumplimiento de las disposiciones de la ley. Esta agencia desempeña un papel crucial al garantizar que las organizaciones y entidades que tratan con datos personales lo hagan de manera responsable y en línea con los principios establecidos en la ley.

Algunos de los Artículos importantes son los siguientes:

Artículo 6. Establece principios clave en la gestión de datos personales. En primer lugar, indica que los datos personales deben ser eliminados o cancelados si su almacenamiento no tiene un respaldo legal o si han caducado. Además, establece que, en caso de que los datos sean incorrectos, inexactos, equívocos o incompletos, deben ser modificados para reflejar la información correcta. Finalmente, subraya que es responsabilidad del encargado del banco de datos personales llevar a cabo la eliminación cuando sea necesario, garantizando así un manejo adecuado y ético de la información personal.

Artículo 17. Establece restricciones y condiciones para la comunicación de información por parte de los responsables de registros o bancos de datos personales. Según este Artículo, la divulgación de información está limitada a aspectos específicos relacionados con obligaciones de carácter económico, financiero, bancario o comercial.

3.2.4. Costa Rica

Costa Rica cuenta con una ley en materia de protección y tratamiento de datos personales. La ley se llama: Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales con asignación del número 8968. Fue aprobada en 2011 y establece las bases para el tratamiento de datos personales en el país, con el objetivo de proteger los derechos fundamentales de privacidad y autodeterminación de los ciudadanos.

A continuación, se mencionan algunos de los artículos más importantes de esta ley:

Artículo 7. Establece el derecho del titular a solicitar la cancelación de datos cuando no sean necesarios para el propósito original de su recolección.

Artículo 10. Establece que las entidades deben adoptar medidas de seguridad para proteger los datos personales contra pérdida, acceso no autorizado y otros riesgos.

Artículo 15. Establece la creación de la Agencia de Protección de Datos de los Habitantes, encargada de supervisar y hacer cumplir las disposiciones de la ley.

3.3 Legislación en materia de protección y tratamiento de datos personales en Europa

La rápida expansión de tecnologías de la información y la comunicación ha transformado la manera en que interactuamos, compartimos información y realizamos transacciones. Sin embargo, este progreso tecnológico ha llevado consigo preocupaciones significativas sobre la privacidad y seguridad de los datos personales.

Europa, en su enfoque proactivo hacia el amparo de los derechos individuales en la era digital, ha establecido un marco regulatorio pionero en la forma del Reglamento General de Protección de Datos (GDPR).

El GDPR es un cuerpo normativo que fue implementado en la Unión Europea (UE) y el Espacio Económico Europeo (EEE) el 25 de mayo de 2018[32]. Fue diseñada para abordar las crecientes preocupaciones sobre la privacidad y la seguridad de los datos personales en la era digital.

El GDPR establece un marco legal integral para el manejo y procesamiento de datos personales en los países de la Unión Europea (UE), así como en aquellos que tratan con datos de ciudadanos europeos. Algunos aspectos clave de la protección de datos personales en Europa bajo el GDPR incluyen:

[32] https://gdpr.eu/**what-is-gdpr/** (Consultado el 18 de agosto de 2023).

Artículo 5. Principios relativos al tratamiento de datos personales: Este Artículo establece los principios fundamentales para el tratamiento de datos personales, incluyendo la legalidad, la equidad, la transparencia, la limitación de la finalidad, la minimización de datos, la exactitud, la limitación del almacenamiento, la integridad y la confidencialidad.

Artículo 6. Base jurídica para el tratamiento. Este Artículo establece las bases legales en las que se puede basar el tratamiento de datos personales, como el consentimiento del interesado, la ejecución de un contrato, el cumplimiento de una obligación legal, la protección de intereses vitales, el ejercicio de funciones de interés público y el ejercicio de autoridad oficial.

Artículo 9. Tratamiento de categorías especiales de datos personales. Este Artículo regula el tratamiento de categorías especiales de datos personales, como datos de salud, origen étnico, creencias religiosas, etc. Estos datos en general están prohibidos, a menos que se aplique una excepción específica.

Artículo 12. Transparencia de la información, comunicación y modalidades para el ejercicio de los derechos del interesado. Establece que las organizaciones deben proporcionar información clara y comprensible sobre cómo se procesan los datos personales y cómo se pueden ejercer los derechos de los individuos, como el acceso, la rectificación y la eliminación de datos.

Artículo 17. Derecho al olvido y a la supresión. Este Artículo establece el derecho de los individuos a solicitar la eliminación de sus datos personales cuando ya no sean necesarios para los fines para los que fueron recopilados, cuando se retire el consentimiento o cuando se procesen de manera ilegal.

Artículo 20. Derecho a la portabilidad de los datos. Estipula el derecho de los individuos a recibir sus datos personales en un formato estructurado y legible por máquina, y a transmitir esos datos a otra organización si así lo desean.

Artículo 25. Protección de datos desde el diseño y por defecto. Establece la obligación de implementar medidas de protección de datos desde el inicio de cualquier proyecto que implique el tratamiento de datos personales, así como la adopción de medidas por defecto que respeten la privacidad de los usuarios.

Artículo 32. Versa sobre la seguridad del tratamiento. Este Artículo requiere que las organizaciones tomen medidas técnicas y organizativas adecuadas para garantizar la seguridad de los datos personales.

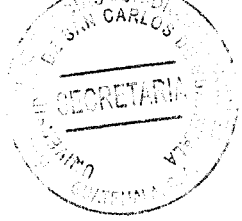
Artículo 35 dispone sobre la evaluación de impacto relativa a la protección de datos: Introduce la evaluación de impacto en la protección de datos (EIPD), que es un proceso para identificar y mitigar los riesgos para la privacidad en proyectos que impliquen un alto riesgo para los derechos y libertades de las personas.

Artículo 37 regula la designación de un delegado de protección de datos: Establece la obligación para algunas organizaciones de designar un delegado de Protección de Datos (DPO por sus siglas en inglés), un experto en privacidad que supervisa y asesora sobre cuestiones relacionadas con la protección de datos.

Comparar la legislación en materia de protección de datos personales entre Europa y Guatemala es esencial debido a varias razones fundamentales. En primer lugar, Europa ha establecido uno de los marcos legales más rigurosos y avanzados para la protección de datos personales a través del Reglamento General de Protección de Datos (GDPR).

Analizar la legislación en este contexto con la de Guatemala nos permite determinar si el país centroamericano garantiza un nivel adecuado de protección y está en concordancia con las normativas internacionales de privacidad.

Además, en un mundo donde muchas empresas operan globalmente y manejan datos de personas en diferentes jurisdicciones, las reglas para la transferencia de datos personales son cruciales. Europa tiene reglas estrictas en este sentido, lo que hace que comprender las diferencias entre las leyes de protección de datos en Europa y Guatemala sea esencial. Esto garantiza que las empresas que operan en ambos lugares cumplan con los requisitos legales al mover datos entre estas regiones.


SECRETARIA

CAPÍTULO IV

4. Implementación de mecanismos de control y regulación en el tratamiento de datos personales en Guatemala

Para garantizar una mayor seguridad jurídica y protección de la privacidad de las personas en Guatemala, es necesario que se implementen mecanismos de control y creación de una regulación jurídica en el tratamiento de datos personales.

4.1. Relevancia de la protección de datos personales en Guatemala

La relevancia de la protección de datos personales en Guatemala es un tema de gran importancia en la era digital actual. A medida que la tecnología y la digitalización se vuelven omnipresentes en la sociedad guatemalteca, la recopilación, el almacenamiento y el uso de datos personales se han convertido en una parte fundamental de la vida cotidiana[33].

La protección de datos personales garantiza que los ciudadanos guatemaltecos tengan el control sobre su información personal, permitiéndoles mantener su privacidad y tomar decisiones informadas sobre cómo y cuándo se recopilan y utilizan sus datos. Además, la falta de protección de datos puede llevar a la exposición de información personal sensible, lo que resulta en el robo de identidad, fraude y otros tipos de delitos

[33] https://thelawyermagazine.com/**la-proteccion-de-datos-en-guatemala/** (Consultado el 20 de agosto de 2023).

cibernéticos. En este sentido, una regulación sólida de protección de datos ayuda a crear un entorno digital más seguro y fomenta la confianza en el uso de servicios en línea.

Al adoptar regulaciones de protección de datos, Guatemala puede cumplir con estándares internacionales y facilitar la cooperación internacional y el intercambio de información en un contexto global. Este cumplimiento puede tener un impacto positivo en la economía, ya que las empresas que manejan datos personales de manera responsable y transparente ganan la confianza de los consumidores, lo que a su vez puede aumentar la demanda de servicios digitales y la innovación tecnológica[34].

4.2. Marco legal de la protección de datos personales en Guatemala

Aunque Guatemala no posee una ley específica de protección de datos personales a nivel nacional, cabe destacar que existen disposiciones legales y regulaciones que establecen principios y protecciones en este ámbito. Estas disposiciones se encuentran dispersas en diversas leyes y regulaciones sectoriales, evidenciando que la protección de datos en el país no cuenta con el respaldo de una legislación integral de privacidad de datos, como se observa en otros lugares de la región.

A pesar de esta ausencia de una normativa centralizada, el reconocimiento y abordaje de la importancia de la protección de datos personales en distintos sectores indican un

[34] **Ibíd.**

paso inicial hacia la consideración más detallada y específica de estos temas en el ámbito legal guatemalteco.

4.2.1. Constitución Política de la República de Guatemala

La Constitución Política de la República de Guatemala en su Artículo 24, reconoce el derecho a la inviolabilidad de la correspondencia, documentos y libros como derecho fundamental. Aunque no aborda específicamente la protección de datos personales, este derecho constituye la base para la protección de la privacidad de los ciudadanos en el territorio nacional.

Solo pueden ser revisados o incautados en virtud de una resolución firme dictada por un juez competente y con las formalidades legales. Este derecho también se encuentra protegido por tratados internacionales y se considera de jerarquía constitucional. La tutela de la inviolabilidad de la correspondencia tiende a impedir la intromisión y permanencia de terceros en un ámbito personal, siempre que no se cuente con autorización del titular del derecho.

4.2.2. Ley de Acceso a la Información Pública (Decreto 57-2008)

Esta ley establece procedimientos para el acceso a la información pública y puede tener implicaciones en la protección de datos cuando se trata de la divulgación de información gubernamental. Establece la obligación de las instituciones públicas de garantizar la confidencialidad de ciertos datos personales y limita la divulgación de

información que afecte la privacidad de los individuos. La ley reconoce el derecho de toda persona a solicitar y obtener información pública, sin necesidad de justificar su interés o finalidad.

4.2.3. Código Penal de Guatemala

El Código Penal de Guatemala contiene disposiciones relacionadas con delitos informáticos y el acceso no autorizado a sistemas y datos informáticos. Estos delitos pueden abordar cuestiones de seguridad de datos y la protección de la información personal. Por ejemplo, el Artículo 197.2 castiga tres comportamientos diferentes: Apoderarse, utilizar o modificar sin autorización datos reservados de carácter personal o familiar que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos o en cualquier otro tipo de archivo público o privado.

4.3. Derecho al olvido

El derecho al olvido es una facultad que tienen las personas físicas para solicitar que se eliminen de Internet los datos personales que les afecten y que consideren inadecuados, inexactos, irrelevantes o excesivos[35]. Este derecho surge como una respuesta a la necesidad de proteger la privacidad y la dignidad de las personas en el entorno digital, donde la información puede difundirse rápidamente y permanecer accesible indefinidamente. El derecho al olvido se basa en el principio de que las

[35] https://www.conceptosjuridicos.com/**derecho-al-olvido/** (Consultado el 25 de agosto de 2023).

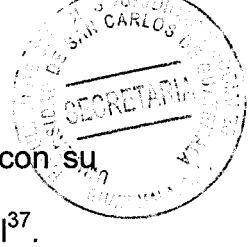
personas tienen derecho a controlar su propia imagen y reputación, y a decidir qué información personal quieren compartir o no con los demás.

El derecho al olvido tiene su origen en la jurisprudencia europea, especialmente en la sentencia del Tribunal de Justicia de la Unión Europea de 2014, conocida como: Sentencia Google Spain, que reconoció este derecho frente a los motores de búsqueda como Google. Posteriormente, el Reglamento general de protección de datos de la Unión Europea (RGPD) de 2018 estableció el derecho de supresión, que es similar al derecho al olvido, y la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD) de 2018 lo reguló específicamente en España. Algunos países fuera de la Unión Europea también han adoptado leyes parecidas, como Rusia, Turquía o Serbia[36].

El ejercicio del derecho al olvido implica un equilibrio entre el interés legítimo de las personas a proteger sus datos personales y el interés público en el acceso a la información. Por ello, no se trata de un derecho absoluto ni automático, sino que debe evaluarse caso por caso, teniendo en cuenta los criterios establecidos por la legislación y la jurisprudencia.

Así, el derecho al olvido no implica la eliminación total de la información de Internet, sino solo de los resultados de búsqueda asociados al nombre de la persona que lo

[36] **Ibíd.**



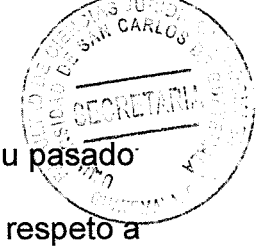
solicita. Tampoco afecta a la información publicada por el propio interesado o con su consentimiento, ni a la información que tenga relevancia histórica, cultural o social[37].

El derecho al olvido es un derecho que busca garantizar el respeto a la privacidad y la dignidad de las personas en el entorno digital, donde la información puede tener un impacto significativo en su vida personal y profesional. Sin embargo, este derecho no es ilimitado ni incondicional, sino que debe ponderarse con otros derechos e intereses legítimos, como la libertad de expresión, el acceso a la información y la memoria social. Por ello, es necesario contar con una regulación adecuada y unos mecanismos efectivos para ejercer este derecho.

El impacto en la privacidad del derecho al olvido es un tema complejo y controvertido, que implica un equilibrio entre el interés legítimo de las personas a proteger sus datos personales y el interés público en el acceso a la información. Puede ser positivo o negativo, dependiendo de las circunstancias y las consecuencias de cada caso[38].

Por un lado, el derecho al olvido puede favorecer la privacidad de las personas al permitirles borrar o limitar el acceso a información personal que pueda perjudicar su imagen, su reputación o su integridad. Por ejemplo, el derecho al olvido puede beneficiar a las víctimas de violencia, acoso o discriminación, que quieran evitar que se difunda su identidad o su historia; o a las personas que hayan cometido errores en el pasado, que hayan cumplido una condena penal o que hayan cambiado de opinión o de

[37] https://www.aepd.es/derechos-y-deberes/conoce-tus-derechos/**derecho-de-supresion-al-olvido** (Consultado el 25 de agosto de 2023).
[38] **Ibíd.**



conducta, y que quieran empezar una nueva vida sin ser estigmatizadas por su pasado. En estos casos, el derecho al olvido puede contribuir a la reinserción social, al respeto a la dignidad humana y al ejercicio de otros derechos fundamentales.

Por otro lado, el derecho al olvido puede afectar negativamente a la privacidad de las personas al suponer una injerencia en el derecho a la información y a la libertad de expresión de terceros. Por ejemplo, el derecho al olvido puede perjudicar el interés público en conocer información relevante para la democracia y el control ciudadano, como los antecedentes penales o políticos de un candidato o funcionario público; o el interés social en preservar la memoria histórica, cultural o científica, como los testimonios de supervivientes de una guerra o una catástrofe, o los avances médicos o tecnológicos.

En estos casos, el derecho al olvido puede suponer una censura, una manipulación o una distorsión de la realidad, que afecte al pluralismo informativo, al debate público y a la formación de una opinión crítica.

4.4. Políticas y procedimientos de control de datos

Las políticas y procedimientos de control de datos son un conjunto de directrices y reglas establecidas por una organización para regular la recopilación, el almacenamiento, el procesamiento y el uso de datos personales. Estas políticas definen

cómo se deben gestionar los datos personales y garantizan que se cumplan las normativas de privacidad y las leyes aplicables[39].

Son las consideraciones legales que se encargan de garantizar el cumplimiento de las leyes de privacidad y las regulaciones aplicables, así como las dimensiones éticas que subrayan la importancia de respetar la privacidad y los derechos de las personas cuyos datos están siendo tratados.

De manera conjunta, estas políticas y procedimientos constituyen una red de salvaguardias destinada a proteger información de carácter crítico y confidencial, asegurando su precisión y disponibilidad cuando sea necesaria, y cumpliendo con las obligaciones legales y éticas en la gestión de datos personales.

4.5. La protección de datos personales como bien económico

En las últimas décadas, el avance tecnológico ha sido exponencial, generando una vasta cantidad de información digital. Dispositivos como computadoras, teléfonos móviles y tabletas, junto con el acceso a Internet, están omnipresentes en nuestra vida diaria, creando grandes cantidades de datos. Este fenómeno, conocido como *big data*, se refiere a conjuntos masivos y complejos de información que no pueden ser gestionados eficazmente mediante métodos tradicionales de análisis.

[39] https://protecciondatos-lopd.com/empresas/**medidas-seguridad-proteccion-datos-personales/** (Consultado el 1 de septiembre de 2023).

Empresas líderes en tecnología, como Facebook, Google, Amazon y otras, se han sumado al aprovechamiento del *big data*. La información recopilada, que a menudo abarca preferencias, hábitos y comportamientos de individuos, se convierte en un activo valioso. El análisis de estos datos permite la creación de perfiles de usuarios y su aplicación en una variedad de aspectos de la vida individual y social, lo que tiene un gran valor económico al impulsar la innovación en la economía digital.

Una de las formas más comunes de utilizar datos personales para generar valor es la predicción del comportamiento con fines de marketing. Las empresas pueden organizar y analizar datos para segmentar a los consumidores y adaptar estrategias de mercado, lo que reduce los costos y mejora la eficiencia en la producción. Además, la combinación de datos personales de diversas fuentes da lugar a servicios innovadores que aumentan su valor. Por ejemplo, al cruzar registros de salud, se pueden realizar investigaciones importantes que conduzcan a descubrimientos significativos en el campo médico[40].

Los consumidores también se benefician de la masificación de la tecnología, ya que experimentan una personalización más eficiente en sus interacciones con el mercado. Por ejemplo, los bancos pueden detectar patrones de compra y prevenir transacciones fraudulentas. Sin embargo, a pesar de los beneficios económicos, los titulares de datos personales a menudo no reciben compensación directa por su uso. La protección de estos datos se ha centrado en el consentimiento otorgado por los usuarios, aunque en la práctica, este consentimiento puede ser limitado.

[40] Solove, Daniel. **Taxonomía de la privacidad**. Pág. 477.

La regulación es esencial, ya que los datos personales pueden caer en manos equivocadas o utilizarse de manera perjudicial. La falta de una definición única de privacidad complica la regulación, pero se asume que las violaciones de privacidad abarcan diversas actividades dañinas o problemáticas[41].

Esta explotación de datos personales plantea cuestiones éticas y legales. Los titulares de datos personales pueden tener preocupaciones sobre la privacidad y el control de su información. Esto ha llevado a un mayor énfasis en la protección de datos y la regulación de la privacidad en todo el mundo.

En resumen, el derecho a la privacidad y la protección de datos personales se considera cada vez más como un bien económico importante en la era digital, donde los datos personales tienen un valor tanto para las empresas como para los individuos, y donde es necesario equilibrar la explotación comercial con la protección de los derechos y la privacidad de las personas.

4.6. Retos éticos y morales

La ética y la moral son dos conceptos relacionados pero distintos que se centran en el comportamiento humano y en la diferenciación entre lo correcto y lo incorrecto. A continuación, se presentan definiciones de ambos términos:

[41] Solove, Daniel. **Conceptualizando la privacidad**. Pág. 1087.

La ética es una rama de la filosofía que se ocupa de estudiar y analizar la moral, es decir, las normas y principios que guían el comportamiento humano. La ética busca comprender las razones detrás de lo que se considera moralmente correcto o incorrecto y proporciona un marco teórico para tomar decisiones éticas. Examina cuestiones como la justicia, la igualdad, el deber y la responsabilidad, y busca establecer principios universales que guíen la conducta ética[42].

La moral se refiere a las normas, valores y creencias que rigen el comportamiento de las personas en una sociedad o comunidad. Estas normas morales determinan lo que se considera correcto o incorrecto en un contexto cultural específico. La moral es influenciada por factores como la religión, la cultura, la educación y las creencias individuales. En otras palabras, la moral es la aplicación práctica de los principios éticos en situaciones concretas.

En resumen, la ética es la reflexión teórica y filosófica sobre lo que es correcto o incorrecto, mientras que la moral se refiere a las normas y valores concretos que guían el comportamiento de las personas en la vida cotidiana. Ambos conceptos están interconectados y son fundamentales para la toma de decisiones éticas en diferentes contextos.

El tratamiento de datos personales plantea desafíos éticos y morales significativos en la sociedad contemporánea. Surgen de la necesidad de equilibrar el beneficio de la tecnología y la innovación con el respeto a los derechos individuales y la promoción de

[42] https://definicion.de/**etica/** (Consultado el 20 de septiembre de 2023).

prácticas éticas. Estos desafíos resaltan la importancia de abordar la protección de datos desde una perspectiva ética y moral sólida.

Uno de los retos más destacados es el consentimiento informado de las personas. Garantizar que las personas otorguen su consentimiento de manera consciente y libre para la recopilación y uso de sus datos es esencial. Sin embargo, las políticas de privacidad suelen ser extensas y complejas, lo que dificulta que las personas comprendan completamente a qué están dando su consentimiento[43].

La minimización de datos es otro desafío ético fundamental. Implica recopilar solo la información necesaria para el propósito específico, evitando así la recolección excesiva y el almacenamiento innecesario de datos personales. Este equilibrio entre recopilar lo necesario y evitar el exceso plantea interrogantes éticos sobre la gestión de la información personal[44].

La transparencia y el control son elementos cruciales para abordar los retos éticos en el tratamiento de datos. Las personas deben tener un control efectivo sobre sus datos personales y comprender cómo se utilizan. Las organizaciones tienen la responsabilidad ética de proporcionar información clara sobre el uso de datos y garantizar que las personas puedan ejercer sus derechos de control, como la eliminación o corrección de datos.

[43] https://datos.gob.es/es/noticia/**la-etica-en-la-gestion-de-los-datos**-0 (Consultado el 20 de septiembre de 2023)
[44] **Ibíd.**

La responsabilidad y la responsabilización en la protección y tratamiento de datos, son cuestiones éticas importantes. Determinar quién es responsable de qué aspectos del manejo de datos personales es esencial para garantizar la protección de los derechos individuales y la promoción de prácticas éticas[45].

La educación y la concienciación sobre la importancia de la protección de datos y los riesgos asociados son fundamentales para empoderar a las personas para que tomen decisiones informadas sobre su privacidad y comprendan los aspectos éticos relacionados con la gestión de datos[46].

En este contexto, es esencial desarrollar marcos éticos sólidos y prácticas responsables en el tratamiento de datos personales. La protección de la privacidad y la promoción de la autonomía individual deben ser prioridades, y las organizaciones y reguladores desempeñan un papel clave en garantizar que se respeten los derechos y valores éticos en la era digital. La ética en el tratamiento de datos personales es un imperativo no solo legal, sino también moral para una sociedad digital justa y equitativa.

4.7. Necesidad de la creación de una normativa en materia de protección de datos personales en Guatemala

En el contexto guatemalteco, la regulación del tratamiento de datos personales se presenta como una necesidad imperante en la era digital actual. Ante el vertiginoso

[45] https://ayudaleyprotecciondatos.es /2020/07/02/**etica-digital/** (Consultado el 20 de septiembre de 2023).
[46] **Ibíd.**

avance de la tecnología y la creciente interconexión de la sociedad, la protección de la privacidad y la seguridad de la información personal se convierten en pilares fundamentales.

Una normativa robusta en este ámbito no solo salvaguardaría los derechos individuales de los ciudadanos, sino que también promovería la confianza en las instituciones, así como fomentar el desarrollo de servicios digitales seguros. La creación de directrices claras y principios éticos en el tratamiento de datos personales se erige como un mecanismo esencial para armonizar la innovación tecnológica con el respeto a la privacidad, asegurando un equilibrio entre el progreso y la protección de los derechos fundamentales.

Una eventual normativa sobre protección de datos personales en Guatemala, fundada en la información recopilada y un exhaustivo análisis del derecho comparado, debería considerar los siguientes principios y aspectos para garantizar una legislación eficaz y acorde con las necesidades del contexto guatemalteco:

a) Definiciones claras. Se establecerán definiciones precisas de términos clave relacionados con el tratamiento de datos personales, asegurando una comprensión uniforme de los conceptos involucrados.

b) Principios de protección de datos. Se enunciarán principios fundamentales que guiarán el tratamiento de datos, incluyendo la legalidad, consentimiento, finalidad, proporcionalidad, calidad, seguridad y confidencialidad.

c) Consentimiento. Se detallarán los requisitos para obtener el consentimiento de los titulares de datos antes de procesar sus datos personales, definiendo los métodos y la posibilidad de retirar el consentimiento.

d) Derechos de los titulares de datos. Se establecerán claramente los derechos de los individuos sobre sus datos personales, incluyendo el acceso, rectificación, cancelación y oposición (derechos ARCO).

e) Transferencia internacional de datos. Se implementarán mecanismos para regular la transferencia de datos personales a países que no ofrezcan un nivel adecuado de protección de datos.

f) Registro de datos. Se definirán requisitos para la creación y mantenimiento de registros de tratamiento de datos personales por parte de las organizaciones.

g) Seguridad de datos. Se incluirán medidas de seguridad que las organizaciones deben implementar para proteger los datos personales contra accesos no autorizados, pérdida, destrucción, alteración o divulgación.

h) Notificación de brechas de seguridad. Se establecerán procedimientos para notificar a la autoridad de protección de datos y a los titulares de datos sobre cualquier violación de seguridad que pueda comprometer la privacidad de los datos.

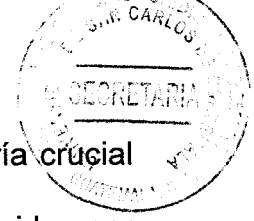
i) Responsabilidades del responsable y encargado del tratamiento. Se esclarecerán las responsabilidades y obligaciones de las organizaciones que tratan datos personales (responsables del tratamiento) y de aquellos que realizan el tratamiento en nombre del responsable (encargados del tratamiento).

j) Autoridad de protección de datos. Se definirán las funciones, facultades y procedimientos de la autoridad de protección de datos, así como las sanciones por incumplimiento.

k) Educación y concienciación. Se promoverán disposiciones para fomentar la educación y concienciación sobre la protección de datos entre las organizaciones y los individuos.

4.8. Creación de una institución especializada para la protección de datos en Guatemala

La creación de una institución independiente para la protección de datos personales en Guatemala es un paso esencial para establecer un marco regulatorio sólido en el tratamiento de información personal. Desde una perspectiva técnica, esta institución desempeñaría un papel central en la supervisión y regulación de las prácticas relacionadas con la recopilación, procesamiento y almacenamiento de datos personales en el país.



En términos de cumplimiento de estándares internacionales, la institución sería crucial para garantizar que Guatemala se adhiera a las normas y directrices establecidas por organizaciones y acuerdos internacionales relacionados con la protección de datos. Esto es de importancia fundamental para la cooperación internacional y el intercambio de información, especialmente en un entorno globalizado.

Desde una perspectiva técnica, esta institución sería responsable de establecer marcos normativos, directrices técnicas y procedimientos de supervisión que aseguren la protección de datos en todos los sectores, desde la atención médica y las finanzas hasta las comunicaciones y el comercio electrónico. Además, debería tener la capacidad de investigar y sancionar a las organizaciones que no cumplan con las regulaciones establecidas, lo que proporcionaría un mecanismo efectivo para prevenir abusos en el tratamiento de datos.

En definitiva, la creación de una institución independiente para la protección de datos personales en Guatemala sería un paso fundamental para garantizar la protección de los derechos individuales en el entorno digital, promover la ética en el tratamiento de datos y facilitar la cooperación a nivel nacional e internacional en asuntos relacionados con la privacidad y la protección de datos.

Esta entidad también juega un papel central en la supervisión y regulación de las prácticas de tratamiento de datos dentro del país, asegurando la conformidad con las leyes y regulaciones pertinentes. Además, es responsable de investigar y sancionar las

violaciones de estas regulaciones, lo que implica un aspecto fundamental en la imposición de sanciones y la preservación del estado de derecho.

En un contexto globalizado, esta institución garantiza la alineación con los estándares internacionales, lo que facilita la cooperación internacional y el flujo de datos transfronterizos. Esto es especialmente relevante en una era en la que la transferencia de datos es ubicua. La supervisión rigurosa y la regulación apropiada no solo son esenciales para prevenir abusos, sino también para fomentar una cultura ética en el tratamiento de datos.

La existencia de esta institución es crucial para asegurar un equilibrio apropiado entre la protección de los derechos individuales y la promoción de la innovación y la competitividad, salvaguardando así los intereses legales y éticos en el manejo de datos personales.

4.9. Creación de un registro simplificado de tratamiento de datos personales

En Guatemala, la gestión efectiva de datos personales se posiciona como una necesidad de suma importancia. La introducción de un registro simplificado para el tratamiento de datos surge como una solución práctica para afrontar los desafíos presentes. Este enfoque tiene como objetivo mejorar las actividades operativas de las organizaciones en Guatemala al reducir la carga administrativa, fomentando la transparencia y garantizar el cumplimiento de las normativas aplicables.

Este registro incluiría datos fundamentales, como la identificación de la persona a cargo del tratamiento, el propósito del procesamiento de datos y una visión general de las categorías de datos involucradas. Asimismo, se subrayará una sección destinada a registrar las medidas de seguridad adoptadas, fomentando prácticas seguras en la gestión de la información personal.

La implementación de un registro simplificado para el tratamiento de datos personales en Guatemala también podría ser impulsada por el reconocimiento de las tendencias internacionales en protección de datos. La adopción de este enfoque podría alinear a Guatemala con prácticas globales de gestión de información personal, fortaleciendo su posición en el escenario internacional.

Este paso esencial buscaría mejorar la eficiencia y ética en la gestión de datos, fortaleciendo la confianza en el tratamiento de información personal, esto en concordancia con estándares internacionales y el respeto a los derechos fundamentales.

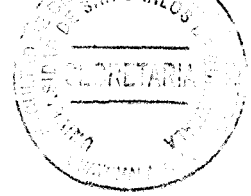

SECRETARIA

CONCLUSIÓN DISCURSIVA

La implementación de mecanismos de control y regulación en el tratamiento de datos personales en Guatemala es esencial para abordar los desafíos actuales en la protección de la privacidad y la seguridad de la información. Durante la investigación, se identificó un problema significativo relacionado con la falta de un marco regulatorio robusto y eficiente para supervisar la gestión de datos personales, lo cual ha dado lugar a posibles vulneraciones de la privacidad de los ciudadanos.

Una posible solución para este problema consiste en que el Estado guatemalteco, a través del Congreso de la República establezca una institución especializada encargada de supervisar y regular el tratamiento de datos personales. Esta entidad debería contar con los recursos necesarios y la autoridad para imponer sanciones significativas en caso de incumplimiento, garantizando así la responsabilidad de las organizaciones que manejan información personal, respaldado por una ley integral.

El objeto principal de estos mecanismos de control y regulación debe ser salvaguardar la privacidad de los individuos y proteger sus datos personales de posibles abusos. Esto implica establecer estándares claros para la recopilación, almacenamiento, procesamiento y transmisión de información personal, así como garantizar el consentimiento informado de los usuarios.



BIBLIOGRAFÍA

Cabanellas, Guillermo. **Diccionario jurídico elemental**. Ed. Heliasta, 2006.

Cabanellas, Guillermo. **Diccionario enciclopédico de derecho usual.** Ed. Heliasta, 2008.

Contreras, Víctor. **Sobre la naturaleza jurídica del derecho informático.** UNAM. 2019

Adjuntía en asuntos constitucionales de Perú. **Manual de protección de datos personales.** Defensoría de Perú. 2019

Altmark, Daniel. **Tratado de derecho informático**. Argentina. Ed. De Palma. 2006.

Del Pozo, Luz María y Hernández Jiménez, Ricardo. **Informática en derecho**. México: Ed. Trillas.1992.

Domínguez, Ana Garriga. **Nuevos retos para la protección de datos personales en la era del big data y de la computación ubicua**. Ed. Dykinson, S.L. 2016.

Flores, Oswaldo**. El derecho informático y su autonomía como nueva rama del derecho.** Unidad General de Asuntos Jurídicos. México. 2016.

https://ayudaleyprotecciondatos.es/2020/07/02/**etica-digital/** (Consultado el 20 de septiembre de 2023).

https://datos.gob.es/es/noticia/**la-etica-en-la-gestion-de-los-datos**-0 (Consultado el 20 de septiembre de 2023).

https://definicion.de/**etica/** (Consultado el 20 de septiembre de 2023).

https://dlcarballo.com/2019/03/14/**analisis-de-la-normativa-nicaraguense-en-materia-de-proteccion-de-datos/** (Consultado el 30 de junio de 2023).

https://dpej.rae.es/lema/**derecho-comparado** (Consultado el 10 de agosto de 2023).

https://gaceta.unadmexico.mx/septiembre-octubre-2022/133-**el-derecho-informatico-y-su-vinculacion-con-otras-ramas-del-derecho** (Consultado el 11 de junio de 2023).

https://gdpr.eu/**what-is-gdpr/.** (Consultado el 18 de agosto de 2023).

https://leyderecho.org/**propiedad-intelectual-en-informatica**. (Consultado el 3 de junio de 2023).

https://mexico.leyderecho.org/**derecho-informatico/** (Consultado el 4 de junio de 2023).

https://micrositios.inai.org.mx/**guiastitulares/INAIvolumen01/**3.3.html (Consultado el 12 de julio de 2023).

https://ogdi.org/**historia-del-cibercrimen**. (Consultado el 4 de junio de 2023).

https://protecciondatos-lopd.com/empresas/**medidas-seguridad-proteccion-datos-personales/**. (Consultado el 1 de septiembre de 2023).

https://revistalex.org/index.php/**revistalex/article/view/97/228** (Consultado el 25 de julio de 2023).

https://studylib.es/doc/710677/**caracter%C3%ADsticas-fundamentales-del-derecho-informatico** (Consultado el 15 de junio de 2023)

https://thedataprivacygroup.com/es/blog/2019-5-24-**gdpr-explained-the-6-legal-grounds-for-processing-personal-data-lawfully/** (Consultado el 15 de julio de 2023).

https://thelawyermagazine.com/**la-proteccion-de-datos-en-guatemala/** (Consultado el 20 de agosto de 2023).

https://www.aepd.es/derechos-y-deberes/conoce-tus-derechos/**derecho-de-supresion-al-olvido** (Consultado el 25 de agosto de 2023).

https://www.ceupe.mx/blog/**que-es-el-derecho-informatico**.html (Consultado el 3 de junio de 2023).

https://www.ceupe.com/blog/**seguridad-informatica-y-proteccion-de-datos**.html (Consultado el 6 de junio de 2023).

https://www.conceptosjuridicos.com/**derecho-al-olvido/** (Consultado el 25 de agosto de 2023).

https://www.ibm.com/ar-es/topics/**data-security** (Consultado el 5 de junio de 2023). **-informatico** (Consultado el 15 de junio de 2023).

Menchaca, Marcelo. **Derecho informático análisis, interpretación y adaptación de la teoría.** Creative Commons. Bolivia. 2014.

Pérez, Enrique. **Manual de informática y derecho**. España. Ed. Ariel S.A.1996.

Piña Libien, Hiram. **El derecho informático y su autonomía como nueva rama del derecho.** Unidad General de Asuntos Jurídicos de México. 2019

Ramírez, William. **Libre acceso a la información, protección de datos y habeas data**. Guatemala: Fundación Mirna Mack. 2003.

Solove, Daniel. **Conceptualizando la privacidad**. California. California Law Review. 2002.

Solove, Daniel. **Taxonomía de la privacidad**. Pensilvania. University of Pennsylvania Law Review. 2006.

Zaballos, Emilia. **La protección de datos en España: evolución normativa y criterios de aplicación.** Madrid: Facultad de Derecho de la Universidad Complutense de Madrid. 2013.

Legislación:

Constitución Política de la República de Guatemala, Asamblea Nacional Constituyente, Guatemala, 1986.

Ley de Acceso a la Información Pública, Decreto Número 57-2008. Congreso de la República de Guatemala, 2008.

Código Penal, Decreto número 17-73 del Congreso de la República de Guatemala.