Tabla de contenido

Orígenes del término “privacidad” y su relación con el concepto “datos personales”.

El término "privacidad" tiene orígenes etimológicos que se remontan al latín "privatus", que significa "separado del resto, particular". La noción de privacidad ha evolucionado a lo largo de la historia y ha adquirido diferentes connotaciones según el contexto cultural, social y tecnológico.

Introducción

En las sociedades griega y romana, la privacidad se entendía en términos de la distinción entre la vida pública y la vida privada. La vida privada era la esfera doméstica, mientras que la vida pública implicaba la participación en la vida cívica y política. En la Edad Media, la privacidad se relacionaba con el espacio físico del hogar y las actividades dentro de él. La privacidad personal y la confidencialidad también eran valoradas, especialmente en contextos religiosos y judiciales. Con la Ilustración y el surgimiento del individualismo, la privacidad comenzó a verse como un derecho fundamental. Filósofos como John Locke y John Stuart Mill argumentaron a favor de la autonomía personal y la libertad individual, conceptos ligados a la privacidad. Posteriormente con el avance de la tecnología y la aparición de internet, la privacidad adquirió una nueva dimensión. El fácil acceso a la información personal y la capacidad de recolectar, almacenar y analizar grandes cantidades de datos transformaron la privacidad en un tema crítico. La relación del concepto de "datos personales", se refiere a cualquier información relacionada con una persona física

identificada o identificable. Esto incluye, pero no se limita a, nombres, direcciones, números de teléfono, correos electrónicos, información biométrica, y datos de comportamiento en línea. La relación entre privacidad y datos personales es intrínseca. La protección de la privacidad en el contexto moderno implica la gestión y protección adecuada de los datos personales. Esto ha llevado al desarrollo de leyes y regulaciones específicas, como el Reglamento General de Protección de Datos (GDPR) en la Unión Europea, que establece estrictas normas sobre cómo deben ser manejados los datos personales para garantizar la privacidad de los individuos.

Evolución del derecho a la privacidad y protección de datos personales como derechos humanos.

La evolución del derecho a la privacidad y la protección de datos personales como derechos humanos ha sido un proceso gradual y multifacético, influenciado por cambios tecnológicos, sociales, legales y políticos. A continuación, se describe en detalle este proceso:

Orígenes y primeras manifestaciones (siglo XIX - mediados del siglo XX)

Siglo XIX: La noción de privacidad comenzó a tomar forma en el siglo XIX con el artículo de Samuel Warren y Louis Brandeis, "The Right to Privacy" (1890), publicado en la Harvard Law Review. Este artículo se considera uno de los primeros en argumentar la necesidad de un derecho a la privacidad, particularmente en respuesta a la creciente invasión de la vida privada por parte de los medios de comunicación.

Primera mitad del siglo XX: La privacidad fue ganando reconocimiento como un componente importante de la dignidad humana. En 1948, la Declaración Universal de los Derechos Humanos de la ONU, en su artículo 12, proclamó que "nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación".

Desarrollo durante la segunda mitad del siglo XX

Convenios y tratados internacionales: La Convención Europea de Derechos Humanos (1950) en su artículo 8 estableció el derecho al respeto de la vida privada y familiar. Este fue uno de los primeros instrumentos legales internacionales en abordar explícitamente el derecho a la privacidad.

Avances tecnológicos: La evolución tecnológica, especialmente con la llegada de los computadores y la informática en la década de 1960 y 1970, puso de relieve la necesidad de proteger la información personal. Este periodo vio el desarrollo de leyes específicas sobre protección de datos, como la Ley Federal de Protección de Datos de Alemania en 1970, la primera de su tipo en el mundo.

Años 80 y 90: Consolidación del marco legal

Directiva de Protección de Datos de la UE (1995): La Directiva 95/46/EC del Parlamento Europeo y del Consejo de la Unión Europea marcó un hito significativo al establecer un marco legal integral para la protección de datos personales en Europa. Esta directiva estableció principios y normas para la recolección, procesamiento y almacenamiento de datos personales, y subrayó la importancia del consentimiento informado.

Reconocimiento global: Durante este período, muchos países alrededor del mundo comenzaron a adoptar leyes de protección de datos inspiradas en el modelo europeo, reconociendo la privacidad como un derecho fundamental en un contexto de globalización y avances tecnológicos.

Siglo XXI: Respuestas a la era digital

Reglamento General de Protección de Datos (RGPD) (2018): La Unión Europea adoptó el RGPD, que reemplazó la Directiva de 1995. Este reglamento introdujo normas más estrictas y uniformes para la protección de datos personales en la UE, con un enfoque en el consentimiento explícito, el derecho al olvido, la portabilidad de datos y la notificación de violaciones de seguridad. Además, estableció sanciones significativas por incumplimiento.

Expansión global: Países fuera de la UE también comenzaron a fortalecer sus marcos legales de protección de datos, influenciados por el RGPD. Ejemplos incluyen la Ley de Privacidad del Consumidor de California (CCPA) en los Estados Unidos, y la Ley General de Protección de Datos (LGPD) en Brasil.

Desafíos modernos: La era digital ha presentado nuevos desafíos para la privacidad y la protección de datos, incluyendo el uso masivo de redes sociales, la vigilancia estatal, y la recopilación y análisis de grandes volúmenes de datos (big data). La inteligencia artificial y el Internet de las Cosas (IoT) también plantean riesgos significativos para la privacidad.

Fortalecimiento

Derecho emergente en derechos humanos: En 2020, la ONU adoptó una resolución sobre el derecho a la privacidad en la era digital, reafirmando la importancia de este derecho en el contexto de las tecnologías de la información y la comunicación.

Iniciativas y recomendaciones: Organizaciones como la Organización para la Cooperación y el Desarrollo Económicos (OCDE) y la Comisión Europea continúan emitiendo directrices y recomendaciones para mejorar la protección de datos y la privacidad a nivel global.

Derecho a la Intimidad

El derecho a la intimidad es uno de los pilares fundamentales de los derechos humanos y de la dignidad individual. Este derecho garantiza que cada persona pueda disfrutar de su vida privada sin interferencias indebidas, protegiendo aspectos personales y familiares frente a la injerencia del Estado, los medios de comunicación, y otras entidades o individuos. En este ensayo, exploraremos la importancia del derecho a la intimidad, su evolución a lo largo del tiempo, y los desafíos contemporáneos que enfrenta.

Definición y Fundamentos

El derecho a la intimidad se refiere a la protección de la vida privada y personal de los individuos, incluyendo sus datos personales, comunicaciones, y decisiones íntimas. Este derecho está consagrado en diversas declaraciones y convenciones internacionales, como la Declaración Universal de Derechos Humanos (artículo 12) y el Pacto Internacional de Derechos Civiles y Políticos (artículo 17). En muchas constituciones nacionales, también se reconoce y protege explícitamente.

Evolución Histórica

La concepción del derecho a la intimidad ha evolucionado considerablemente a lo largo del tiempo. En el siglo XIX, con el auge de la prensa y la fotografía, surgieron las primeras preocupaciones sobre la invasión de la privacidad. El famoso artículo “The Right to Privacy” de Samuel Warren y Louis Brandeis, publicado en 1890, sentó las bases para la discusión moderna sobre este derecho. Ellos argumentaron que la intimidad debía protegerse como un derecho inherente a la dignidad humana.

Legalidad y Protección de la Información

En el siglo XX, la expansión de las tecnologías de la información y la comunicación planteó nuevos desafíos. La aparición de internet y las redes sociales transformaron radicalmente la forma en que se recopila, almacena y comparte la información personal. En este contexto, surgieron leyes específicas para proteger la privacidad, como el Reglamento General de Protección de Datos (GDPR) en la Unión Europea, que establece estrictas normas sobre la recopilación y manejo de datos personales.

Importancia del Derecho a la Intimidad

El derecho a la intimidad es esencial para la libertad y la autonomía personal. Permite a los individuos tomar decisiones libres sobre su vida sin temor a la vigilancia o la coerción. La protección de la intimidad también es crucial para el desarrollo de relaciones personales y familiares auténticas, libres de intromisiones indebidas.

Además, la intimidad es fundamental para la protección de otros derechos y libertades. Sin una adecuada protección de la privacidad, derechos como la libertad de expresión, la libertad de asociación y el derecho a un juicio justo pueden verse comprometidos. Por ejemplo, en un entorno de vigilancia masiva, las personas pueden autocensurarse por temor a represalias, afectando negativamente el debate democrático y la participación ciudadana.

Desafíos

En la era digital, el derecho a la intimidad enfrenta numerosos desafíos. La recopilación masiva de datos por parte de empresas tecnológicas y gobiernos ha generado preocupaciones sobre el uso y abuso de esta información. Las filtraciones de datos, el seguimiento en línea y el uso de algoritmos para predecir comportamientos son solo algunos de los problemas que deben abordarse.

El avance de la inteligencia artificial y la biometría también plantea nuevas cuestiones. El reconocimiento facial, por ejemplo, puede ser utilizado para seguir y monitorear a las personas sin su consentimiento, lo que representa una amenaza significativa para la privacidad.

La Balanza entre Seguridad y Privacidad

Uno de los debates más intensos en torno al derecho a la intimidad es el equilibrio entre seguridad y privacidad. En un mundo donde las amenazas a la seguridad nacional y la

seguridad pública son reales, los gobiernos argumentan que ciertas medidas de vigilancia son necesarias para proteger a la sociedad. Sin embargo, estas medidas deben ser proporcionales y estar sujetas a una supervisión estricta para evitar abusos y garantizar que no se socaven los derechos fundamentales de las personas.

Decálogo del Derecho a la Intimidad

- Privacidad es un derecho fundamental: Toda persona tiene derecho a la privacidad de su vida personal, familiar y doméstica.
- Protección de datos personales: Tus datos personales son propiedad tuya y deben ser protegidos de accesos no autorizados o usos indebidos.
- Limitación de la vigilancia: La vigilancia debe estar justificada y ser proporcional, respetando siempre tu derecho a la privacidad.
- Comunicaciones privadas: Tus comunicaciones, ya sean telefónicas, electrónicas o postales, son privadas y deben ser respetadas.
- Espacios privados: Tu hogar, tu cuerpo y otros espacios privados son inviolables.
- Consentimiento informado: Nadie puede acceder a tu información privada sin tu consentimiento explícito.
- Protección de la reputación: Tu reputación es un aspecto importante de tu privacidad y debe ser protegida de difamaciones o calumnias.
- Acceso limitado a información: La información sobre tu vida privada debe ser limitada y solo accesible para aquellos con una necesidad legítima de conocerla.
- Derecho al olvido: En algunos casos, tienes derecho a que se elimine información obsoleta o perjudicial sobre ti.
- Remedios legales: Si tus derechos a la privacidad son violados, tienes derecho a buscar protección legal.

Derecho a la protección de los datos personales.

Concepto y Evolución del Derecho a la Protección de los Datos Personales

El derecho a la protección de los datos personales es un derecho fundamental que garantiza a los individuos el control sobre la información que les identifica o les hace identificables. Este derecho implica que las personas tienen la facultad de decidir sobre el uso y tratamiento de sus datos, asegurando que este manejo se realice de manera justa, transparente y segura.

El reconocimiento formal de este derecho ha evolucionado significativamente en las últimas décadas. En Europa, la Directiva 95/46/CE de 1995, también conocida como la Directiva de Protección de Datos, marcó un hito importante. Esta normativa fue reemplazada en 2018 por el Reglamento General de Protección de Datos (GDPR, por sus siglas en inglés), que ha establecido un marco robusto y detallado para la protección de datos personales en la Unión Europea. En otros lugares del mundo, países como México han implementado leyes específicas, como la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), que regula el tratamiento de datos personales en el ámbito privado.

Principios Rectores

La protección de los datos personales se fundamenta en una serie de principios clave:

- Licitud, lealtad y transparencia: Los datos deben ser tratados de manera lícita, leal y transparente en relación con el titular de los datos.
- Limitación de la finalidad: Los datos deben ser recogidos con fines determinados, explícitos y legítimos, y no ser tratados posteriormente de manera incompatible con dichos fines.
- Minimización de datos: Solo deben tratarse los datos personales que sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.
- Exactitud: Los datos personales deben ser exactos y, si fuera necesario, actualizados. Se deben tomar todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos.
- Limitación del plazo de conservación: Los datos personales deben ser mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento.
- Integridad y confidencialidad: Los datos personales deben ser tratados de manera que se garantice una seguridad adecuada, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental.

Desafíos

A pesar de los avances normativos, la protección de datos personales enfrenta numerosos desafíos. La rápida evolución tecnológica y la proliferación de dispositivos conectados han aumentado exponencialmente la cantidad de datos generados y recopilados. Las empresas y

organizaciones deben estar en constante adaptación para cumplir con las normativas y proteger los datos de posibles brechas de seguridad.

Además, la globalización y la naturaleza transfronteriza de internet plantean problemas adicionales en la protección de datos. La transferencia de datos personales entre países con diferentes niveles de protección jurídica requiere acuerdos y mecanismos que garanticen la seguridad y privacidad de la información.

Otro reto significativo es la concienciación y educación de los individuos sobre sus derechos en materia de protección de datos. Varias personas no saben la cantidad de información que comparten y cómo puede usarse. Fomentar una cultura de protección de datos es esencial para que los individuos puedan ejercer sus derechos de manera efectiva.

Decálogo del Derecho a la Protección de Datos Personales

- Tus datos te pertenecen: Tú tienes el control sobre tu información personal. Nadie puede utilizarla sin tu consentimiento.
- Informa y consiente: Antes de que una empresa o institución recolecte tus datos, debe informarte claramente sobre cómo los utilizará y pedirte tu autorización.
- Datos mínimos: Solo se deben recolectar los datos estrictamente necesarios para el fin que se persigue.
- Veracidad: La información que proporcionas debe ser veraz y actualizada.
- Acceso y rectificación: Tienes derecho a conocer qué información se tiene sobre ti y a solicitar que se corrija si es errónea.
- Supresión: Puedes pedir que se eliminen tus datos cuando ya no sean necesarios.
- Limitación: Puedes solicitar que se limite el uso de tus datos en determinadas circunstancias.
- Oposición: Puedes oponerte al tratamiento de tus datos en cualquier momento.
- Seguridad: Tus datos deben estar protegidos contra accesos no autorizados, alteraciones o destrucciones.
- Transparencia: Las empresas y organizaciones deben ser transparentes sobre cómo manejan tus datos.

Resolución 509 del Consejo de Europa de 1968 sobre protección de datos

Legalidad y Protección de la Información

La Resolución 509 del Consejo de Europa, adoptada en 1968, marca un hito significativo en la evolución de la protección de datos en Europa. Este documento refleja una conciencia emergente sobre la necesidad de proteger la privacidad y los datos personales en una era en la que las tecnologías de la información comenzaban a transformar la sociedad. A través de esta resolución, se establecieron principios fundamentales que sentarían las bases para la legislación futura en el ámbito de la protección de datos.

Contexto Histórico

En la década de 1960, el mundo se encontraba en medio de una revolución tecnológica. La computación y la capacidad de procesamiento de datos estaban avanzando rápidamente, lo que permitió a las organizaciones públicas y privadas recolectar, almacenar y analizar grandes cantidades de información sobre individuos. Aunque estos avances ofrecían beneficios, también preocupaban la privacidad y la seguridad de los datos personales. Fue en este contexto que el Consejo de Europa decidió abordar la cuestión a través de la Resolución 509.

Contenido de la Resolución 509

La Resolución 509 enfatiza la importancia de proteger la privacidad de los individuos contra el uso indebido de sus datos personales. Entre los aspectos más destacados de la resolución se encuentran:

- Definición y Alcance: La resolución proporciona una definición inicial de "datos personales", refiriéndose a cualquier información relacionada con una persona identificada o identificable. Esto sentó las bases para una comprensión más precisa y universal de lo que constituye datos personales.

- Principios de Tratamiento de Datos: Se establecieron principios básicos para el tratamiento de datos, incluyendo la necesidad de recolectar datos de manera justa y legal, y utilizar los datos solo para los fines especificados al momento de su recolección. Además, se resaltó la importancia de garantizar la exactitud y la actualización de los datos.

- Derechos del Individuo: La resolución reconoció los derechos fundamentales de los individuos en relación con sus datos personales. Estos derechos incluían el acceso a

la información recolectada, la posibilidad de corregir errores y la protección contra el uso no autorizado de sus datos.

- Seguridad de los Datos: Se subrayó la necesidad de implementar medidas adecuadas para proteger los datos personales contra el acceso no autorizado, la alteración y la destrucción.

Impacto y Evolución Posterior

La Resolución 509 no tenía carácter vinculante, pero su influencia fue profunda y duradera. Sirvió como un marco de referencia para muchos países europeos que comenzaron a desarrollar sus propias leyes de protección de datos. Además, inspiró debates y colaboraciones internacionales que eventualmente llevaron a la creación de acuerdos más formalizados y robustos.

Uno de los desarrollos más significativos fue la Convención 108 del Consejo de Europa, adoptada en 1981, que se convirtió en el primer instrumento legal vinculante a nivel internacional en el ámbito de la protección de datos. Esta convención amplió y profundizó los principios establecidos en la Resolución 509, adaptándolos a un contexto global en rápida evolución.

Relevancia

Hoy en día, la protección de datos es un componente esencial de la legislación en la mayoría de los países del mundo. Instrumentos como el Reglamento General de Protección de Datos (RGPD) de la Unión Europea, adoptado en 2016, se basan en los principios fundamentales articulados por primera vez en la Resolución 509.

El RGPD, por ejemplo, no solo amplía los derechos de los individuos y fortalece las obligaciones de las organizaciones, sino que también introduce conceptos avanzados como el derecho al olvido y la portabilidad de los datos. Estas disposiciones reflejan una evolución continua y una adaptación a los desafíos emergentes en la era digital.

Decálogo de la Resolución 509 del Consejo de Europa de 1968

Esta resolución, pionera en su época, sentó las bases para la protección de datos personales en el ámbito digital. A continuación, te presento sus principios clave en un formato conciso:

- Veracidad y precisión: La información personal debe ser exacta y mantenerse actualizada.
- Finalidad legítima: Los datos solo pueden recopilarse y utilizarse para fines específicos y legítimos.
- Limitación del almacenamiento: La información personal no debe conservarse más tiempo del necesario para cumplir los fines para los que fue recogida.
- Confidencialidad: Los datos personales deben tratarse de forma confidencial y protegerse contra cualquier acceso no autorizado.
- Seguridad: Se deben implementar medidas técnicas y organizativas adecuadas para proteger los datos personales contra cualquier pérdida, alteración o destrucción accidental o ilícita.
- Derechos del individuo: Las personas tienen derecho a acceder a sus datos personales, corregirlos si son inexactos y oponerse a su tratamiento en determinadas circunstancias.
- Prohibición de ciertos datos: Queda prohibida la recopilación y el tratamiento de datos sensibles, como aquellos relacionados con el origen racial, las opiniones políticas, las creencias religiosas, la salud o la vida sexual.
- Consentimiento: El tratamiento de datos personales debe basarse, en general, en el consentimiento libre e informado de la persona interesada.
- Responsabilidad: Los responsables del tratamiento de datos son responsables de cumplir con los principios establecidos en esta resolución.
- Cooperación internacional: Los Estados deben cooperar entre sí para garantizar la protección de los datos personales a nivel internacional.

Ley de Privacidad (Privacy Act)

La Ley de Privacidad, conocida como el “Privacy Act”, es una pieza fundamental en la protección de la información personal de los individuos en diversas jurisdicciones, especialmente en los Estados Unidos, donde se promulgó en 1974. Esta ley establece un marco legal para la gestión y protección de los datos personales recopilados por agencias

gubernamentales, garantizando ciertos derechos a los individuos en relación con la información que se almacena sobre ellos.

Orígenes y Contexto Histórico

La Ley de Privacidad surgió en un contexto de creciente preocupación por la protección de la privacidad en la era de la informática. A medida que las tecnologías de la información avanzaban, también lo hacía la capacidad de recopilar, almacenar y analizar grandes cantidades de datos personales. La década de 1970 vio una mayor conciencia pública sobre cómo el gobierno y otras entidades podían potencialmente abusar de esta información, lo que llevó a un movimiento por mayores protecciones legales.

La Ley de Privacidad fue una respuesta directa a estos temores, inspirada en parte por el escándalo del Watergate, que reveló hasta qué punto las agencias gubernamentales podían espiar a los ciudadanos. Esta ley fue una de las primeras en establecer principios de protección de datos que más tarde influirían en legislaciones similares en todo el mundo.

Principios Fundamentales de la Ley de Privacidad

La Ley de Privacidad de 1974 se basa en varios principios clave que buscan equilibrar la necesidad del gobierno de recopilar información con el derecho de los individuos a la privacidad:

- Transparencia: Las agencias gubernamentales deben informar a los individuos sobre la recopilación de datos personales. Esto incluye la naturaleza de la información recopilada, el propósito de su recolección y el uso que se le dará.

- Acceso y Corrección: Los individuos tienen derecho a acceder a la información que las agencias gubernamentales tienen sobre ellos. Además, pueden solicitar la corrección de datos inexactos o incompletos.

- Consentimiento y Notificación: Las agencias deben obtener el consentimiento de los individuos, cuando sea posible, antes de recopilar información personal y deben notificar cualquier uso secundario de los datos que no haya sido previamente informado.

- Seguridad: Las agencias están obligadas a implementar medidas de seguridad adecuadas para proteger la información personal contra accesos no autorizados, uso indebido o divulgación.

- Limitación de Recopilación y Uso: La recopilación de datos personales debe limitarse a lo que es necesario para cumplir con los propósitos especificados. Además, el uso de esta información debe restringirse a los fines para los cuales fue recolectada, a menos que se obtenga un consentimiento adicional del individuo.

Desafíos

La Ley de Privacidad ha tenido un impacto significativo en la forma en que las agencias gubernamentales gestionan la información personal. Ha establecido un estándar para la protección de datos que ha sido emulado por otras leyes y regulaciones en todo el mundo. Sin embargo, la implementación de la ley no ha estado exenta de desafíos.

Uno de los principales problemas es la creciente cantidad de datos y la sofisticación de las tecnologías de recopilación y análisis de información. Las agencias gubernamentales, al igual que las empresas privadas, han ampliado su capacidad para recopilar datos a través de medios digitales, lo que plantea nuevas preguntas sobre la eficacia de las protecciones actuales. Además, el equilibrio entre la seguridad nacional y la privacidad individual sigue siendo un tema de debate constante, especialmente en el contexto de la lucha contra el terrorismo y la delincuencia.

Tendencia

Desde su promulgación, la Ley de Privacidad ha sido enmendada varias veces para adaptarse a los cambios tecnológicos y sociales. Sin embargo, muchos expertos argumentan que se necesita una revisión más completa para abordar los desafíos modernos de la privacidad en la era digital.

El futuro de la Ley de Privacidad puede ver una mayor armonización con otros marcos legales internacionales, como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea, que ofrece protecciones más robustas y un enfoque más global de la privacidad de los datos. Además, la integración de nuevas tecnologías, como la inteligencia artificial y el big data, requerirá enfoques innovadores para garantizar que la privacidad individual siga siendo una prioridad en un mundo cada vez más interconectado.

Decálogo de la Ley de Privacidad

- Consentimiento Informado: Toda recopilación y uso de datos personales requiere el consentimiento explícito y voluntario del individuo. Este consentimiento debe ser informado, es decir, la persona debe conocer claramente el propósito de la recopilación y cómo se utilizarán sus datos.
- Finalidad Específica: La información personal solo puede recopilarse y utilizarse para los fines declarados y legítimos al momento de la recopilación. Cualquier cambio de propósito debe ser notificado al individuo y, en algunos casos, requerir un nuevo consentimiento.
- Limitación de Datos: La recopilación de datos personales debe ser adecuada, relevante y limitada a lo necesario para cumplir con los fines declarados. No se pueden recopilar datos excesivos o innecesarios.
- Precisión: Los datos personales deben ser exactos, completos y actualizados. El individuo tiene derecho a acceder a sus datos y solicitar su corrección en caso de errores.
- Seguridad: Los responsables del tratamiento de datos personales deben implementar medidas de seguridad técnicas y organizativas adecuadas para proteger los datos contra el acceso no autorizado, la pérdida, la alteración o la destrucción.
- Transparencia: Los responsables del tratamiento de datos deben ser transparentes en cuanto a sus prácticas de privacidad. Deben proporcionar información clara y accesible sobre cómo se recopilan, utilizan, comparten y protegen los datos personales.
- Acceso y Portabilidad: Los individuos tienen derecho a acceder a sus datos personales, conocer cómo se utilizan y solicitar una copia de los mismos. También tienen derecho a la portabilidad de los datos, a solicitar que sus datos se transfieran a otro responsable del tratamiento.
- Oposición y Supresión: Los individuos tienen derecho a oponerse al tratamiento de sus datos personales en determinadas circunstancias, como cuando se utilizan con fines de marketing directo. También tienen derecho a solicitar la supresión de sus datos cuando ya no sean necesarios para los fines recogidos.
- Responsabilidad: Los responsables del tratamiento de datos son responsables de cumplir con la ley de privacidad. En caso de incumplimiento, pueden enfrentar sanciones administrativas o judiciales.

- Protección de Datos de Menores: Los datos de los menores de edad requieren una protección especial. Se suelen aplicar requisitos adicionales de consentimiento parental y medidas de seguridad reforzadas.

Bibliografía

Díaz, María. (2024). Inteligencia artificial generativa y los retos en la protección de los datos personales. Estudios en Derecho a la Información. 179-205. 10.22201/iij.25940082e.2024.18.18852.

Piña Libien, Hiram & Uribe Arzate, Enrique. (2020). La protección de datos personales ante el ejercicio de los derechos político-electorales en México. Estudios en Derecho a la Información. 65-92. 10.22201/iij.25940082e.2021.11.15300.

Díaz Santana, Karla & Santos, Julio. (2023). Términos abusivos en avisos de privacidad, su registro como mecanismo para garantizar el derecho a la protección de los datos personales. Internaciones. 10. 173-190. 10.32870/in.v10i25.7259.

Ambrona, Pilar. (2010). Vulneración mediática del derecho a la intimidad. CEFLegal. Revista práctica de derecho. 145-180. 10.51302/ceflegal.2010.12969.

Martínez, Silvia. (2019). Nuevos pasos para la protección de datos personales y los derechos digitales. COMeIN. 10.7238/c.n85.1907.

Guerrero, Manuel. (2022). El derecho a conocer los algoritmos utilizados en la toma de decisiones. Aproximación desde la perspectiva del derecho fundamental a la protección de datos personales. Teoría y Realidad Constitucional. 141-171. 10.5944/trc.49.2022.33847.

Ordóñez Pineda, Luis. (2022). Los derechos a la igualdad y no discriminación como bienes jurídicos del derecho fundamental a la protección de datos personales. Revista de Cultura de Paz. 5. 191-204.

Carvajal, Ángela & Estrada, Jenny. (2020). Vulneración del derecho a la intimidad personal y familiar en las redes sociales. Crítica y Derecho, Revista Jurídica. 1. 51-63. 10.29166/criticayderecho.v1i1.2447.

Falcón, Carol. (2020). DERECHO A LA INTIMIDAD EN EL ÁMBITO LABORAL ¿Privacidad del empleado o salvaguarda del empleador?. Revista de Direito do Trabalho, Processo do Trabalho e Direito da Seguridade Social. 1. 10.35987/laborjuris.v1i1.32.

Peña Pérez, Pascal. (2020). La protección de los datos personales como derecho fundamental: su autonomía y vigencia propia en el ordenamiento jurídico estatal. Revista de la Facultad de Derecho de México. 70. 915. 10.22201/fder.24488933e.2020.278-2.77065.