EL DATO LA INFORMACIÓN Y LA IA COMO NOCIONES JURÍDICAS

INTRODUCCIÓN

Oportunidad y necesidad de la IA

La inteligencia artificial, como la máquina de vapor o la electricidad en el pasado, está cambiando nuestra vida, sociedad y empresas. Esto se debe a que las computadoras son más poderosas, hay mucha información disponible y los programas informáticos son mejores. La inteligencia artificial es muy importante en este siglo. La forma en que tratemos este tema afectará cómo será nuestro mundo. En una competencia global intensa, Europa necesita tener reglas claras sobre la inteligencia artificial.

Necesidad de un marco ético y jurídico

- Mejorar la capacidad tecnológica e industrial de la Unión Europea y promover el uso de la IA en todas las áreas de la economía, tanto en empresas privadas como en el sector público.
- Prepararse para los cambios sociales y económicos causados por la IA, incluyendo la modernización de la educación y la formación, el fomento del talento, la anticipación de cambios en el mercado laboral y el apoyo a las transiciones laborales, así como la adaptación de los sistemas de protección social.
- Garantizar el establecimiento de un marco ético y jurídico apropiado, basado en los valores de la Unión y en consonancia con la Carta de los Derechos Fundamentales de la UE. Esto incluye orientaciones sobre la responsabilidad por productos defectuosos relacionados con la IA y la colaboración con diferentes partes interesadas en una Alianza europea de la IA para desarrollar directrices éticas en este ámbito. Es preciso que, en relación con el desarrollo y la utilización de la IA, se cree un entorno de confianza y se establezca la obligación de rendir cuentas

Directrices para una IA fiable

La fiabilidad de la inteligencia artificial (IA) se basa en tres cosas importantes que deben ser ciertas durante toda la vida de la IA:

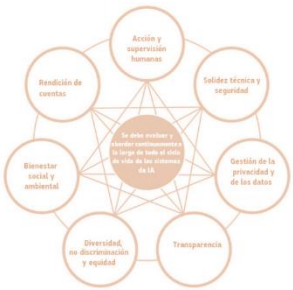
a. La IA debe seguir todas las leyes y reglas, como si fuera una persona obediente y buena.
b. La IA ha de ser ética, de modo que se garantice el respeto de los principios y valores éticos.
c. La IA debe ser fuerte y resistente, tanto en términos técnicos como sociales. Esto es importante porque incluso si la IA intenta hacer cosas buenas, podría causar problemas accidentales si no es fuerte y estable.

Principios y requisitos de la IA

Principios:

I. Respeto de la autonomía humana
II. Prevención del daño
III. Equidad
IV. Explicabilidad.

Requisitos:



Marco de los aspectos éticos de la inteligencia artificial, la robótica y las tecnologías conexas

El Marco Ético de la Inteligencia Artificial, la Robótica y las Tecnologías Relacionadas, propuesto por el Parlamento Europeo en 2020, abarca diversos aspectos importantes:

- Inteligencia artificial antropocéntrica y antropogénica: La inteligencia artificial debe centrarse en beneficios humanos y ser desarrollada por seres humanos, evitando la autonomía completa de las máquinas.
- Evaluación de riesgos: Se deben evaluar y abordar los riesgos asociados con la inteligencia artificial y la robótica de manera adecuada.
- Características de seguridad, transparencia y rendición de cuentas: Las tecnologías deben ser seguras, transparentes y sus creadores deben rendir cuentas por su uso.
- Sin sesgo y sin discriminación: La inteligencia artificial no debe mostrar sesgos injustos o discriminar a personas por ningún motivo.

- Responsabilidad social y paridad de género: Debe promoverse la responsabilidad social en el desarrollo de la inteligencia artificial, y se debe garantizar la igualdad de género en su aplicación.
- Medio ambiente y sostenibilidad: Se debe considerar el impacto ambiental y promover la sostenibilidad en el desarrollo y uso de estas tecnologías.
- Protección de la intimidad y reconocimiento biométrico: Debe respetarse la privacidad de las personas, especialmente en relación con el uso de datos biométricos.
- Buena gobernanza: Se deben establecer prácticas de gobierno sólidas para regular y supervisar la inteligencia artificial.
- Empleo, derechos de los trabajadores, competencias digitales y lugar de trabajo: Se deben abordar los impactos en el empleo, los derechos laborales, las habilidades digitales y las condiciones de trabajo relacionadas con estas tecnologías.
- Autoridades nacionales de control: Es importante contar con autoridades nacionales que supervisen y regulen el uso de la inteligencia artificial.
- Coordinación a escala de la Unión: Debe haber coordinación a nivel de la Unión Europea para garantizar una implementación coherente y efectiva de estas políticas.
- Cooperación internacional: La cooperación internacional es esencial para abordar los desafíos globales relacionados con la inteligencia artificial y la robótica.

LOS CONCEPTOS DE INFORMACIÓN Y DATO A EFECTOS JURÍDICOS Y ÉTICOS

Los datos y la información

Los términos “dato” e “información” se suelen usar como sinónimos. Sin embargo, existe diferencia entre estos términos.

Dato: unidad de significación simple (hechos crudos, no procesados, sin contexto específico que pueden consistir en números, letras, símbolos, sonidos, imágenes…). Se considera como un elemento descriptivo y objetivo que por sí solo puede carecer de significado.

Información: conjunto de datos que han sido procesados de manera que tienen un significado o propósito o se les da un contexto, lo que implica actividades de interpretación, conexión, relevancia y estructura de datos.

Tradicionalmente: dato < información < conocimiento.

La importancia del desarrollo de este marco jurídico no es una cuestión reciente, pero sí actual

Dentro de la Unión Europea (UE), hay un plan importante llamado "Brújula Digital 2030", que es la forma en que Europa quiere abordar la próxima década digital. Este plan se enfoca en varias áreas:

- Ciudadanos con capacidades digitales y profesionales del sector digital muy cualificados: La UE quiere que las personas sepan cómo usar la tecnología y también quiere tener muchos expertos en tecnología.
- Infraestructuras digitales sostenibles que sean seguras y eficaces: Quieren construir sistemas tecnológicos que funcionen bien, sean seguros y no dañen el medio ambiente.
- Transformación digital de las empresas: Las empresas deben adaptarse a la tecnología para seguir siendo competitivas.
- Digitalización de los servicios públicos: Los servicios que ofrece el gobierno deben estar disponibles en línea y ser fáciles de usar.

Además, la UE también está trabajando en lo que llaman "Una Estrategia Europea de Datos". Esto significa que están planeando cómo usar y compartir información en toda Europa. Aquí hay algunas cosas importantes que quieren hacer:

- Un marco de gobernanza intersectorial para el acceso a los datos y su utilización: Quieren establecer reglas para cómo las personas y las empresas pueden acceder y usar datos.
- Catalizadores: Quieren invertir en tecnología para almacenar y usar datos de manera más eficiente y hacer que los datos funcionen bien juntos.
- Competencias: Quieren que las personas tengan las habilidades necesarias para usar datos y quieren ayudar a las pequeñas empresas a hacer lo mismo.
- Espacios comunes europeos de datos en sectores estratégicos y en ámbitos de interés público: Quieren crear lugares donde la información importante esté disponible para todos en Europa en áreas que son muy importantes.

¿Cómo se ha organizado jurídicamente la información?

La información siempre ha sido importante, pero su valor ha aumentado debido al avance del conocimiento y la tecnología, que hacen más fácil usar y gestionar la información. Desde una perspectiva legal, se han abordado dos enfoques diferentes respecto a la información:

- Enfoque Instrumental: La información se ve como un medio para lograr otros objetivos. Por ejemplo, en el contexto de un curso, la información se utiliza para comunicar conocimientos a los estudiantes.
- Enfoque como Cosa o Activo: Aquí, la información se considera como un recurso con el cual se puede negociar o tratar de diversas formas.

La información vista como un recurso tiene características interesantes:

- Es inmaterial: No puedes tocarla, es una idea o datos.
- Se puede reproducir fácilmente: Puedes hacer copias de la información con facilidad.
- No se consume con su uso: Usar la información no la destruye, puedes seguir usándola una y otra vez.
- Tiene valor en muchas dimensiones: La información puede ser valiosa de muchas maneras, desde el conocimiento que proporciona hasta su utilidad en la toma de decisiones.
- Tiene un significado: Usar la información requiere ciertas habilidades y conocimientos para comprender su significado y aplicarla de manera efectiva.

El Derecho ha establecido un marco del manejo/uso de la información

En algunas ocasiones, ciertas cuestiones relacionadas con la información se fundamentan en la Constitución o el Derecho Europeo. Aquí se presentan algunos ejemplos:

- Libertad de creación de información: Este derecho se refiere a la libertad de expresión, creación y producción de información. Está respaldado por la Constitución Española (Artículo 20) y los artículos 11 y 13 del Tratado de Funcionamiento de la Unión Europea.
- Protección de la información personal: Esto involucra aspectos como la intimidad, el secreto de las comunicaciones y la protección de datos personales. Está respaldado por el Artículo 18 de la Constitución Española y los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea. También se aplica a la información oficial, que puede estar sujeta a consideraciones de publicidad, seguridad y secreto.
- Derecho a usar y disfrutar la información como cualquier otro bien: Este derecho establece que las personas tienen el derecho de utilizar y beneficiarse de la información de la misma manera que lo harían con cualquier otro recurso. Está respaldado por el Artículo 33 de la Constitución Española y el Artículo 17 del Tratado de Funcionamiento de la Unión Europea.
- Configuración de un orden público / economía de la información que puede limitar su utilización: Esto significa que, en ciertas situaciones, el gobierno puede establecer reglas y restricciones en el uso de la información en aras del orden público o para regular la economía de la información. Estas restricciones pueden afectar cómo se utiliza la información en determinados contextos.

Derecho de acceso a la información

Si bien no existe un derecho de acceso a la información expresamente reconocido en todas las circunstancias y para cualquier tipo de información, el derecho reconoce situaciones en las que sí existe este derecho.

- Derecho a la información (pública o privada) disponible en el mercado de la información: Este derecho se refiere a la posibilidad de acceder a información, ya sea pública o privada, que esté disponible en el mercado de la información. Esto significa que, si la información está a la venta o de alguna manera accesible, se reconoce el derecho a acceder a ella (Artículo 20.1.d de la Constitución Española).
- Derecho a la información pública: En general, se reconoce el derecho a acceder a la información pública (Artículo 105.b de la Constitución Española). Sin embargo, este derecho tiene límites en situaciones que involucran la investigación de delitos o la seguridad del Estado. Además, la legislación de transparencia y reutilización de la información pública ha ampliado significativamente este derecho y establecido reglas específicas para su ejercicio.

Límites del manejo de información

Existen diferentes aspectos relacionados con el derecho a la privacidad y la protección de datos, tanto en el ámbito del derecho privado como en el derecho público:

- En el ámbito del derecho privado:
  - Derivado del DERECHO DE PROPIEDAD: Este derecho se basa en la propiedad, que es el derecho a disfrutar y disponer de algo, sujeto a las restricciones establecidas por las leyes. En el contexto de la información, esto se aplica a la propiedad intelectual y la propiedad industrial.
  - Derivados de un CONTRATO: Los contratos son acuerdos que son obligatorios siempre que cumplan con ciertas condiciones esenciales para su validez. En el ámbito de la privacidad, esto puede incluir cláusulas de confidencialidad y secreto, tanto en acuerdos independientes como parte de relaciones profesionales, como el deber de secreto profesional.
- En el ámbito del derecho público:
  - Deber de secreto: El deber de secreto puede derivar del ejercicio de funciones públicas y también estar relacionado con la materia, como en la legislación de secretos oficiales. Esto significa que las personas que trabajan en el ámbito público están obligadas a mantener la confidencialidad en ciertas situaciones.
  - Límites de derecho privado aplicables a la Administración Pública: Los límites establecidos en el derecho privado también pueden aplicarse a la Administración Pública en ciertos casos.
- Límites derivados de la dignidad de la persona: La dignidad de la persona es un principio fundamental y, en el ámbito público, esto se refleja en el derecho a la intimidad (protegido por el artículo 18 de la Constitución Española) y en la protección de datos personales (también protegido por el artículo 18.4 de la Constitución Española).
  - Privacidad y Protección de datos: Estos son aspectos clave en el ámbito público y privado. La privacidad se refiere al derecho de las personas a mantener su vida privada y sus asuntos personales alejados de la observación pública no deseada, mientras que la protección de datos se centra en garantizar que la información personal se maneje de manera adecuada y segura, de acuerdo con la legislación vigente.

Escenario de gobernanza derivado del DUE y del Derecho Español

El escenario de gobernanza en España se deriva tanto del Derecho de la Unión Europea (DUE) como del Derecho Español. Este marco legal se ha ido desarrollando a lo largo del tiempo con varios antecedentes, que incluyen:

- Normativa sobre protección de datos personales: Esto se refiere a las leyes y regulaciones relacionadas con la privacidad y el manejo de datos personales, en conformidad con el Reglamento General de Protección de Datos (RGPD) de la Unión Europea.
- Privacidad en los servicios de comunicaciones electrónicas: Normativas específicas que abordan la privacidad en el contexto de los servicios de comunicaciones electrónicas, como las comunicaciones por Internet y teléfono.
- Circulación de datos no personales: Reglas relacionadas con el intercambio y el flujo de datos que no son de carácter personal
- Reutilización de información pública: Normativas que establecen cómo se puede reutilizar la información que es de dominio público.
- Acceso a los documentos públicos: Reglas sobre cómo acceder a documentos gubernamentales y de organismos públicos.
- Servicios de la sociedad de la información: Regulaciones que rigen los servicios en línea y la actividad digital.
- Protección de redes y sistemas de información: Normativas que se enfocan en la seguridad y protección de las redes y sistemas de información contra amenazas cibernéticas.

Recientemente, se ha aprobado normativa adicional que se centra en la gobernanza de los datos. Esto incluye la regulación de cómo se manejan y gestionan los datos en diversos contextos.

Además, se ha propuesto una regulación específica en relación con los mercados disputables y la inteligencia artificial. Estas propuestas buscan establecer reglas y directrices para abordar los desafíos y oportunidades que surgen en estos ámbitos en constante evolución.

El concepto jurídico de dato

El Derecho de la Unión Europea (UE) define el término "dato" como toda representación digital de actos, hechos o información, así como su recopilación, incluso como grabación sonora, visual o audiovisual.

Además, el Derecho de la UE también define el término "fichero" como todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica.

Es importante destacar que los datos se consideran como información y, como tal, están sujetos a regulación tanto como un objeto en sí mismos como un instrumento que puede ser utilizado o manejado de diversas formas, de acuerdo con las leyes y regulaciones de protección de datos de la UE.

Datos y privacidad

El Reglamento General de Protección de Datos (RGPD) establece definiciones clave relacionadas con datos y privacidad:

- Datos personales: Se refiere a toda información sobre una persona física identificada o identificable, a quien se llama "el interesado". Se considerará identificable a cualquier persona cuya identidad pueda determinarse, ya sea directa o indirectamente. Esto puede lograrse mediante un identificador, como un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos que caracterizan la identidad física, fisiológica, genética, psicológica, económica, cultural o social de esa persona (según el artículo 4.1 del RGPD).
- Datos: Este término se refiere a la información que no cumple con la definición de datos personales según el artículo 4, punto 1 del RGPD. En otras palabras, son datos que no están relacionados con una persona física identificada o identificable de ninguna manera.

Es importante tener en cuenta esta distinción, ya que el RGPD se aplica principalmente a la protección de datos personales y establece reglas específicas para su manejo y procesamiento, mientras que los datos no personales están fuera del alcance de este reglamento en particular.

Tipos de datos relevantes en relación con la protección de datos

Existen varios tipos de datos relevantes en relación con la protección de datos, cada uno de los cuales se trata de manera especial según las normativas de privacidad:

- Datos Personales Especiales o Sensibles (Artículo 9 del RGPD): Estos son datos que revelan información delicada, como el origen étnico o racial, opiniones políticas, creencias religiosas o filosóficas, afiliación sindical, datos genéticos, datos biométricos utilizados para identificar de manera única a una persona, datos de salud o información sobre la vida sexual u orientación sexual de una persona. Estos datos están sujetos a reglas de protección más estrictas debido a su naturaleza sensible.
- Datos Relacionados con Condenas Penales y Delitos (Artículo 10 del RGPD): Esta categoría incluye datos personales relacionados con condenas criminales, infracciones penales o medidas de seguridad relacionadas con delitos. También están sujetos a normativas específicas de protección.
- Datos de Menores: Los datos de menores de edad, especialmente en el contexto de servicios en línea, están sujetos a normativas específicas de protección para garantizar su seguridad y privacidad.
- Datos con Reglas de Menor Protección o que no se Consideran Datos Personales: Algunos datos, como los datos anonimizados, ya no se consideran datos personales si se han desvinculado correctamente de una persona física identificable. Además, los datos pseudonimizados se tratan de manera especial, ya que se desvinculan de la identidad del interesado, pero aún se pueden relacionar utilizando información adicional que se guarda de forma separada y está protegida por medidas técnicas y organizativas.

Estas categorías de datos tienen diferentes niveles de protección y requisitos legales para su tratamiento, diseñados para garantizar la privacidad y la seguridad de los individuos cuyos datos se están procesando.

Debe tenerse en cuenta que el RGPD

Es importante tener en cuenta que el Reglamento General de Protección de Datos (RGPD) es una norma que regula el uso de los datos personales, pero no prohíbe su uso. El RGPD establece claramente su objetivo en el artículo 1.1, que es "establecer las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y las normas relativas a la libre circulación de tales datos".

En otras palabras, el RGPD no otorga la propiedad de los datos a la persona a la que se refiere como el "interesado". En cambio, lo que le preocupa principalmente a esta norma es la responsabilidad de quienes realizan el tratamiento de datos, es decir, los Responsables y Encargados del tratamiento.

Esta normativa se enfoca en asegurar que quienes manejan y procesan datos personales lo hagan de manera adecuada y cumplan con ciertas obligaciones y estándares de seguridad para proteger los derechos y la privacidad de las personas cuyos datos se están utilizando. En resumen, el RGPD no prohíbe el uso de datos personales, pero sí establece reglas y responsabilidades estrictas para garantizar su tratamiento adecuado y seguro.

Derecho de la UE

- Art. 16 del Tratado de Funcionamiento de la Unión Europea.
  - 1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.

- 2. El Parlamento Europeo y el Consejo establecerán, con arreglo al procedimiento legislativo ordinario, las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos. El respeto de dichas normas estará sometido al control de autoridades independientes.
- Las normas que se adopten en virtud del presente artículo se entenderán sin perjuicio de las normas específicas previstas en el artículo 39 del Tratado de la Unión Europea.

- Art 8 (Protección de datos de carácter personal) Carta de los Derechos Fundamentales de la Unión Europea:
  - 1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.
  - 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación.
  - 3. El respeto de estas normas estará sujeto al control de una autoridad independiente.

Datos no personales

Los datos no personales son un aspecto importante en la regulación de la circulación de datos. En este contexto, es esencial comprender a quiénes se refieren estas normativas y cómo se definen los sujetos involucrados:

- RDNP (Reglamento sobre Datos No Personales): Este reglamento busca eliminar obstáculos para la libre circulación de datos que no sean de carácter personal.

Sujetos involucrados:

- Usuario de Datos: Se refiere a cualquier persona física o jurídica que tiene acceso legítimo a ciertos datos, ya sean personales o no personales, y tiene el derecho de usarlos con fines comerciales o no comerciales. Esto incluye el acceso a datos personales y no personales, y este derecho está respaldado por el Reglamento (UE) 2016/679 en el caso de los datos personales (según la definición del artículo 3.9 del RDNP).
- Usuario: Este término se aplica a cualquier persona física o jurídica, incluyendo autoridades y organismos públicos, que utiliza o solicita un servicio de tratamiento de datos según lo dispuesto por el RDNP (según la definición del artículo 3.7 del RDNP).
- Usuario Profesional: Se refiere a una persona física o jurídica, incluyendo autoridades y organismos públicos, que utiliza o solicita un servicio de tratamiento de datos para fines relacionados con su actividad comercial, negocio, oficio, profesión o función (según la definición del artículo 3.8 del RDNP).

Estas definiciones son fundamentales para entender cómo se aplican las regulaciones sobre datos no personales y cómo se involucran diferentes actores en la circulación y uso de esta información.

Régimen jurídico de los datos

El régimen jurídico que rige los datos se basa en diversas normas fundamentales, tanto a nivel nacional como de la Unión Europea. Estas normas establecen las bases legales para la protección y regulación de los datos. Entre las normas fundamentales destacan las siguientes:

Normas Fundamentales:

- Constitución Española (CE): En la Constitución Española se contemplan varios artículos relacionados con la protección de datos, como los artículos 18 (derecho a la intimidad), 20 (derecho a la libertad de expresión) y 105 (acceso a documentos públicos).
- Derecho de la Unión Europea (UE): El Derecho de la UE juega un papel esencial en la regulación de los datos, especialmente en el contexto del mercado único y la protección de datos personales (PD).

Derecho de la UE:

- Reglamento (UE) 2022/868: Este reglamento, adoptado el 30 de mayo de 2022, se refiere a la gobernanza europea de datos y modifica el Reglamento (UE) 2018/1724 (Reglamento de Gobernanza de Datos). Establece directrices y normativas para la gestión de datos a nivel europeo.
- Reglamento (UE) 2018/1725: Adoptado el 23 de octubre de 2018, este reglamento se ocupa de la protección de datos personales por parte de las instituciones, órganos y organismos de la Unión Europea, así como de la libre circulación de estos datos. Deroga el Reglamento (CE) n.° 45/2001 y la Decisión n.° 1247/2002/CE, y establece estándares claros para el tratamiento de datos por parte de las instituciones de la Unión Europea.

Estas normativas constituyen la base legal que rige la gestión y protección de los datos en el ámbito de la Unión Europea y en España, asegurando el respeto de los derechos fundamentales y la armonización de las regulaciones en todo el mercado único europeo.

Titularidad y disposición de la información y del dato

La titularidad y disposición de la información y los datos son conceptos importantes en el contexto de la regulación de la privacidad y la protección de datos. Aquí se explica cómo se abordan estos aspectos:

- En lo que respecta a la información, la titularidad depende en gran medida de la autoría o generación de esa información. Por ejemplo, en el artículo 20.1 de la Constitución Española se establece el derecho a la libertad de expresión y, por lo tanto, se reconoce la autoría y generación de información por parte de los individuos.
- En relación con los datos, se hace una distinción entre el titular y el usuario. El titular de los datos se refiere a la persona física identificada o identificable, es decir, "el interesado", cuya identidad puede determinarse directa o indirectamente a través de identificadores como un nombre, un número de identificación, datos de localización, identificadores en línea u otros elementos relacionados con su identidad física, fisiológica, genética, psicológica, económica, cultural o social (según el artículo 4.1 del RGPD).
- Por otro lado, el "titular de datos" se refiere a cualquier persona física o jurídica, incluyendo organismos del sector público y organizaciones internacionales, que, de acuerdo con el Derecho de la Unión o la legislación nacional aplicable, tiene el derecho de otorgar acceso o compartir ciertos datos personales o no personales (según el artículo 3.8 del RDNP).

Ambos, el titular de los datos y el titular de datos, tienen cierto poder de disposición sobre el uso de los datos, ya sea en términos de acceder a ellos o compartirlos, y están sujetos a regulaciones específicas destinadas a garantizar la protección de la privacidad y la seguridad de la información.

Uso y gestión: reutilización

El uso y la gestión de datos, en particular en el contexto de la reutilización de información pública, se definen y regulan de la siguiente manera:

- Reutilización: Se refiere a la utilización de datos que están en posesión de organismos del sector público por parte de personas físicas o jurídicas. Esta reutilización puede tener fines comerciales o no comerciales y se realiza para propósitos distintos de aquellos para los que se produjeron originalmente estos datos en el marco de la misión de servicio público (según el artículo 2.2 del RGD). Sin embargo, existe una excepción para el intercambio de datos entre organismos del sector público en el desempeño de sus actividades de servicio público.
- Permiso: Este término se refiere a la concesión otorgada a los usuarios de datos para el tratamiento de datos no personales (según el artículo 2.6 del RGD).
- Licencia Tipo: Se trata de un conjunto de condiciones de reutilización predefinidas en formato digital, preferiblemente compatibles con licencias modelo públicas disponibles en línea. Estas licencias tipo facilitan el proceso de reutilización de datos al proporcionar condiciones claras y estándar para su uso.
- Requisito de Localización de Datos: Hace referencia a cualquier obligación, prohibición, condición, restricción u otro requisito establecido en las disposiciones legales, reglamentarias o administrativas de los Estados miembros, o derivado de prácticas administrativas generales y coherentes en un Estado miembro y en organismos de Derecho público. Estos requisitos pueden imponer el tratamiento de datos en el territorio de un Estado miembro específico o dificultar el tratamiento de datos en otro Estado miembro (según el artículo 3.5 del RDNP).

Estas definiciones y regulaciones son fundamentales para establecer un marco claro y coherente para la reutilización de datos en el contexto de la información pública, al tiempo que garantizan la protección de los derechos y la privacidad de las personas.

Uso y gestión: intercambio

El uso y la gestión de datos, específicamente en el contexto del intercambio de datos, se definen de la siguiente manera:

- Intercambio de Datos: Este término se refiere a la facilitación de datos por parte de un interesado o titular de datos a un usuario de datos, ya sea de forma directa o a través de un intermediario. Este intercambio se lleva a cabo en virtud de un acuerdo voluntario o en cumplimiento del Derecho de la Unión o de la legislación nacional. El propósito del intercambio es permitir el uso compartido o individual de dichos datos, ya sea mediante licencias abiertas o mediante licencias comerciales, ya sean de pago o gratuitas.

- Servicio de Intermediación de Datos: Se trata de cualquier servicio cuyo objetivo sea establecer relaciones comerciales para facilitar el intercambio de datos entre un número indeterminado de interesados y titulares de datos, por un lado, y usuarios de datos, por otro. Esto se logra a través de medios técnicos, jurídicos u otros. Sin embargo, hay ciertos servicios que se excluyen de esta definición:
    a) Servicios que obtienen datos de titulares de datos, los agregan, enriquecen o transforman para agregarles un valor sustancial y otorgan licencias a los usuarios de datos para utilizar los datos resultantes sin establecer una relación comercial entre los titulares de datos y los usuarios de datos.
    b) Servicios dedicados a la intermediación de contenido protegido por derechos de autor.
    c) Servicios utilizados exclusivamente por un único titular de datos para permitir la utilización de los datos en su posesión, así como aquellos utilizados por múltiples personas jurídicas en un grupo cerrado o en relaciones contractuales específicas, incluyendo aquellos destinados a garantizar las funcionalidades de objetos y dispositivos conectados a la Internet de las Cosas.
    d) Servicios de intercambio de datos ofrecidos por organismos del sector público sin la intención de establecer relaciones comerciales.

Estas definiciones son esenciales para comprender cómo se regula y facilita el intercambio de datos, ya sea en un contexto comercial o no comercial, y cómo se establecen las relaciones entre los interesados, los titulares de datos y los usuarios de datos en este proceso.

Elementos subjetivos relacionados con la gestión y explotación de los datos

Los elementos subjetivos relacionados con la gestión y explotación de los datos, especialmente en lo que respecta al tratamiento de datos personales, se definen de la siguiente manera:

- Titular e Interesado: Estos términos se utilizan de forma intercambiable y se refieren a la persona física identificada o identificable cuya información personal está siendo tratada. El interesado o titular de datos tiene ciertos derechos y control sobre cómo se utilizan sus datos personales (según el Reglamento General de Protección de Datos - RGPD).
- Usuario de Datos: Se trata de cualquier persona física o jurídica que tenga acceso legítimo a datos, ya sean datos personales o no personales, y que tenga el derecho de usarlos con fines comerciales o no comerciales. Este acceso legítimo se rige por el RGPD en el caso de datos personales (según el artículo 3.9 del RGD).
- Usuario: Se refiere a una persona física o jurídica, incluyendo autoridades y organismos de Derecho público, que utiliza o solicita un servicio de tratamiento de datos (según el artículo 3.7 del RDNP).
- Usuario Profesional: Este término se aplica a una persona física o jurídica, incluyendo autoridades y organismos de Derecho público, que utiliza o solicita un servicio de tratamiento de datos con fines relacionados con su actividad comercial, negocio, oficio, profesión o función (según el artículo 3.8 del RDNP).

Estos elementos subjetivos son esenciales para definir quiénes están involucrados en la gestión y explotación de datos, ya sea para fines comerciales o no comerciales, y para establecer las responsabilidades y derechos de cada parte en el tratamiento de datos personales y no personales.

Datos e información en procesos de reutilización

En el contexto de los procesos de reutilización de datos e información, se utilizan ciertos términos clave para definir los tipos de documentos y datos involucrados. Aquí están las definiciones relevantes:

- Documento: Un documento se refiere a cualquier contenido, independientemente del soporte en el que se encuentre, ya sea en forma escrita en papel o almacenado en formato electrónico, o incluso como grabación sonora, visual o audiovisual. Esto puede incluir cualquier parte de ese contenido (según el DRISP).
- Datos Dinámicos: Los datos dinámicos son documentos en formato digital que están sujetos a actualizaciones frecuentes o en tiempo real. Esto se debe a su volatilidad o rápida obsolescencia. Los datos generados por sensores, por ejemplo, a menudo se consideran datos dinámicos.
- Datos de Investigación: Estos son documentos en formato digital que se distinguen de las publicaciones científicas. Los datos de investigación se recopilan o elaboran durante actividades de investigación científica y se utilizan como prueba en el proceso de investigación. También son ampliamente aceptados en la comunidad investigadora como necesarios para validar las conclusiones y resultados de la investigación.
- Conjuntos de Datos de Alto Valor: Se refieren a documentos cuya reutilización está asociada con beneficios significativos para la sociedad, el medio ambiente y la economía. Esto se debe a su capacidad para crear servicios de valor añadido, aplicaciones y empleos nuevos, dignos y de calidad. La

importancia de estos conjuntos de datos también se relaciona con el número de posibles beneficiarios de los servicios de valor añadido y aplicaciones basados en ellos.

Estas definiciones son esenciales para comprender la diversidad de datos e información que pueden ser objeto de reutilización en diversos contextos y cómo dichos datos pueden generar beneficios significativos para la sociedad y la economía.

Normas armonizadas para un acceso justo a los datos y su utilización (Ley de Datos)

Trata de *la puesta a disposición de los datos generados por el uso de un producto o servicio relacionado para el usuario de dicho producto o servicio, sobre la puesta a disposición de datos por parte de los titulares de datos para los destinatarios de datos, y sobre la puesta a disposición de datos por parte de los titulares de datos para organismos del sector público o instituciones, organismos y órganos de la Unión, cuando exista una necesidad excepcional, para el desempeño de una misión realizada en interés público.*

Estructura subjetiva pLD

La estructura subjetiva del pLD (Proyecto de Ley de Datos) comprende los siguientes elementos:

- Usuario: Una persona física o jurídica que posee, alquila o arrienda un producto o recibe un servicio.
- Titular de Datos: Una persona física o jurídica que tiene el derecho o la obligación, según lo establecido en el pLD, el Derecho de la Unión aplicable o la legislación nacional que implementa el Derecho de la Unión, de poner a disposición ciertos datos. En el caso de datos no personales, también puede ser el titular de datos aquel que, a través del control del diseño técnico de un producto o servicios relacionados, tiene la capacidad de poner a disposición determinados datos.
- Destinatario de Datos: Una persona física o jurídica que actúa con un propósito relacionado con su actividad comercial, empresa, oficio o profesión. Este destinatario es diferente del usuario del producto o servicio relacionado y recibe los datos que el titular de datos pone a disposición. Esto puede incluir a terceros que acceden a los datos a solicitud del usuario, del titular de datos o en cumplimiento de una obligación legal de acuerdo con el Derecho de la Unión o la legislación nacional que implementa el Derecho de la Unión.
- Empresa: Una persona física o jurídica que, en el contexto de los contratos y prácticas regulados por el pLD, opera con fines relacionados con su actividad comercial, empresa, oficio o profesión.

Estos elementos definen quiénes son los actores involucrados en el contexto del pLD y establecen las relaciones y responsabilidades entre ellos en lo que respecta a la gestión y utilización de datos.

Gobernanza de los datos

La gobernanza de los datos se refiere a la regulación y gestión de la reutilización de ciertas categorías de datos protegidos que están en manos de organismos del sector público. Aquí se describen los aspectos clave de la gobernanza de los datos:

- Reutilización de Datos Protegidos: Se prohíben acuerdos de exclusividad, condiciones restrictivas de reutilización y tasas para promover un acceso más abierto y equitativo a estos datos. Además, se establecen mecanismos de supervisión y control para garantizar el cumplimiento de estas normativas, así como la transparencia en el proceso.
- Servicios de Intermediación de Datos: Se definen tres tipos de servicios de intermediación de datos:
    a) Servicios que facilitan la interacción entre los titulares de datos y los potenciales usuarios, incluyendo la creación de plataformas para el intercambio de datos.
    b) Servicios que actúan como intermediarios entre los interesados que desean compartir sus datos personales o datos no personales y los posibles usuarios de esos datos. Esto incluye el apoyo al ejercicio de los derechos de los interesados según el Reglamento (UE) 2016/679.
    c) Servicios ofrecidos por cooperativas de datos.
- Estatuto de los Servicios de Intermediación: Estos servicios deben cumplir con ciertos requisitos, incluida la notificación a la autoridad competente, condiciones de utilización que respeten los regímenes específicos de datos, y estarán sujetos a la supervisión de las autoridades de control. Esto garantiza que los servicios de intermediación operen de manera transparente y cumplan con las regulaciones.
- Cesión Altruista de Datos: Se promueve la cesión altruista de datos a través de registros públicos de organizaciones reconocidas por su gestión de datos con fines altruistas, es decir, organizaciones sin ánimo de lucro e independientes. Estos registros deben cumplir con requisitos específicos y códigos normativos, y estarán sujetos a supervisión. Se establece un formulario europeo para la cesión altruista de datos para facilitar este proceso.

En resumen, la gobernanza de los datos busca regular la reutilización de datos protegidos del sector público, promoviendo la transparencia, la equidad en el acceso y la gestión responsable de estos datos a través de servicios de intermediación y la promoción de la cesión altruista de datos.

Elementos subjetivos (intermediación)

Los "servicios de cooperativas de datos" se refieren a los servicios de intermediación de datos proporcionados por una estructura organizativa que está formada por interesados, empresas individuales o pequeñas y medianas empresas (pymes) que forman parte de esta estructura. El propósito principal de estas cooperativas de datos es brindar apoyo a sus miembros en el ejercicio de sus derechos relacionados con ciertos datos. Esto incluye ayudar a los miembros a tomar decisiones informadas antes de otorgar su consentimiento para el tratamiento de datos, facilitar el intercambio de opiniones sobre los propósitos del tratamiento de datos y las condiciones que mejor representen los intereses de sus miembros en relación con esos datos, y negociar las condiciones contractuales para el tratamiento de datos en nombre de sus miembros antes de autorizar el tratamiento de datos no personales o de dar su consentimiento para el tratamiento de datos personales. En resumen, estas cooperativas de datos actúan como intermediarios para proteger los derechos e intereses de sus miembros en relación con los datos.

Gobernanza de los datos

La gobernanza de los datos se rige por una serie de regulaciones y directivas en la Unión Europea, que incluyen:

- Reglamento (UE) 2022/868 del Parlamento Europeo y del Consejo, de 30 de mayo de 2022, que se refiere a la gobernanza europea de datos y modifica el Reglamento (UE) 2018/1724 (Reglamento de Gobernanza de Datos). Este reglamento aborda la reutilización de ciertas categorías de datos protegidos que están en manos de organismos del sector público y establece requisitos para los servicios de intermediación de datos.
- Directiva (UE) 2019/1024 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, relacionada con datos abiertos y la reutilización de información del sector público. Esta directiva se enfoca en la apertura y reutilización de datos del sector público.
- Reglamento (UE) 2018/1807 del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, que establece un marco para la libre circulación de datos no personales en la Unión Europea. Este reglamento se ocupa de la circulación de datos que no son de naturaleza personal en la Unión Europea.

Estas regulaciones y directivas forman parte del marco legal que rige la gestión y reutilización de datos en la Unión Europea, y establecen las pautas y requisitos para garantizar un uso adecuado y responsable de los datos en diferentes contextos.

Servicios de datos

Los servicios de datos están regulados en la Unión Europea a través de varias normativas, que incluyen:

- Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre mercados disputables y equitativos en el sector digital, comúnmente conocida como "Ley de Mercados Digitales". Este proyecto de reglamento tiene como objetivo establecer un marco para garantizar la competencia justa y equitativa en el sector digital.
- Reglamento (UE) 2019/1150 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, que se centra en el fomento de la equidad y la transparencia para los usuarios profesionales de servicios de intermediación en línea. Esta normativa se enfoca en garantizar que los servicios de intermediación en línea sean justos y transparentes para los usuarios profesionales.

Estas regulaciones buscan promover un entorno equitativo y competitivo en el sector digital y asegurar que los servicios de datos en línea sean justos y transparentes para todos los usuarios, en particular para los profesionales que los utilizan.

Reglamento sobre mercados disputables y equitativos en el sector digital

El Reglamento sobre mercados disputables y equitativos en el sector digital tiene como objetivo principal promover el adecuado funcionamiento del mercado único europeo. Esto se logra mediante la creación de normas armonizadas que aseguren la equidad y la competencia en el sector digital, especialmente en aquellos segmentos donde existen actores dominantes que ejercen un control significativo sobre el acceso a servicios y recursos digitales. Esta regulación tiene como finalidad beneficiar tanto a los usuarios profesionales como a los usuarios finales, garantizando un entorno comercial justo y competitivo en toda la Unión Europea.

Mercados disputables

Los "guardianes de acceso" en el contexto de los mercados disputables se refieren a empresas que cumplen con los siguientes criterios:

- Tienen un impacto significativo en el mercado interior.

- Operan una plataforma de servicios básicos que funciona como una puerta importante para que los usuarios profesionales alcancen a los usuarios finales.
- Mantienen una posición sólida y duradera en sus operaciones o se espera que alcancen esa posición en el futuro cercano.

Estas empresas están sujetas a regulaciones destinadas a garantizar la equidad y la competencia en el mercado. Esto incluye la prohibición de prácticas que limiten la competencia o sean desleales. Además, se pueden establecer obligaciones específicas para estas empresas, y se implementan mecanismos de control y respuesta para supervisar su actividad y tomar medidas adecuadas cuando sea necesario para mantener la competencia justa en el mercado.

Procesos de uso y gestión: intermediación

En el contexto de los procesos de uso y gestión de datos, se utilizan los siguientes términos:

- Intermediación se refiere a cualquier uso de datos de acuerdo con requisitos técnicos, legales u organizativos específicos, sin necesidad de transmitir o descargar los datos.
- Cesión altruista de datos hace referencia a un intercambio voluntario de datos que se basa en el consentimiento de los interesados para el tratamiento de sus datos personales o en el permiso de los titulares de datos para el uso de sus datos no personales. Este intercambio se realiza sin la intención de obtener o recibir una recompensa que supere la compensación de los costos incurridos al proporcionar los datos. El propósito de esta cesión altruista de datos es promover el interés general, como la atención médica, la lucha contra el cambio climático, la mejora de la movilidad, el desarrollo y difusión de estadísticas oficiales, la mejora de los servicios públicos, la formulación de políticas públicas o la investigación científica de interés general, según lo establezca la legislación nacional.

NOCIÓN JURÍDICA DE INTELIGENCIA ARTIFICIAL

Inteligencia Artificial y Datos

En el contexto de la inteligencia artificial y los datos, es esencial definir el concepto de inteligencia artificial, a pesar de su complejidad. Se entiende como un "Sistema de inteligencia artificial (sistema de IA)" al software que se desarrolla utilizando una o varias de las técnicas y estrategias detalladas en el anexo I. Este software tiene la capacidad de generar información de salida, como contenidos, predicciones, recomendaciones o decisiones que pueden influir en los entornos con los que interactúa.

El anexo I especifica las estrategias utilizadas en la inteligencia artificial, que incluyen:

- Estrategias de aprendizaje automático, que abarcan el aprendizaje supervisado, no supervisado y por refuerzo, utilizando una amplia variedad de métodos, como el aprendizaje profundo.
- Estrategias basadas en la lógica y el conocimiento, que incluyen la representación del conocimiento, la programación lógica inductiva, las bases de conocimiento, los motores de inferencia y deducción, así como los sistemas expertos y de razonamiento simbólico.
- Estrategias estadísticas, que abarcan la estimación bayesiana, métodos de búsqueda y optimización, entre otros.

Estas estrategias y técnicas son utilizadas por los sistemas de inteligencia artificial para cumplir con los objetivos definidos por seres humanos y generar resultados que tienen un impacto en los entornos en los que operan.

Otras unidades – procesos de información relevantes

En el contexto de otros procesos de información relevantes, se definen los siguientes términos:

- Sistema de reconocimiento de emociones: Este sistema de inteligencia artificial tiene como objetivo detectar o inferir las emociones o intenciones de personas físicas utilizando datos biométricos.
- Sistema de categorización biométrica: Se trata de un sistema de inteligencia artificial diseñado para asignar a personas físicas a categorías específicas, como género, edad, color de cabello, color de ojos, tatuajes, origen étnico, orientación sexual o política, basándose en sus datos biométricos.
- Sistema de identificación biométrica remota: Este sistema de IA se emplea para identificar a personas físicas a distancia al comparar sus datos biométricos con los que se encuentran en una base de datos de referencia. Es importante destacar que el usuario del sistema de IA no sabe de antemano si la persona en cuestión estará en esa base de datos ni si podrá ser identificada.

- Sistema de identificación biométrica remota "en tiempo real": Este sistema de identificación biométrica remota permite la recopilación de datos biométricos, la comparación y la identificación sin una demora significativa. Esto abarca desde la identificación instantánea hasta demoras mínimas limitadas, con el objetivo de evitar elusión.
- Sistema de identificación biométrica remota "en diferido": Se refiere a cualquier sistema de identificación biométrica remota que no funcione en tiempo real, es decir, no proporciona resultados de identificación de manera instantánea.

Estas definiciones son relevantes para comprender los sistemas y procesos que utilizan datos biométricos en diferentes contextos, desde el reconocimiento de emociones hasta la identificación de individuos a distancia.

Tipología de datos relevante a los efectos de su aplicación

Se definen distintas categorías de datos relevantes en el contexto de su aplicación:

- Datos de entrenamiento: Estos datos se utilizan para entrenar un sistema de inteligencia artificial mediante el ajuste de sus parámetros entrenables, que pueden incluir los pesos de una red neuronal.
- Datos de validación: Los datos de validación se emplean para proporcionar una evaluación del sistema de inteligencia artificial que ha sido entrenado. También se utilizan para adaptar los parámetros no entrenables del sistema y su proceso de aprendizaje, con el fin de evitar el sobreajuste. El conjunto de datos de validación puede ser independiente o formar parte del conjunto de datos de entrenamiento, ya sea como una división fija o variable.
- Datos de prueba: Estos datos se utilizan para llevar a cabo una evaluación independiente del sistema de inteligencia artificial que ha sido entrenado y validado. Su propósito principal es confirmar que el sistema funciona según lo previsto antes de su introducción en el mercado o su puesta en servicio.
- Datos de entrada: Son los datos que se proporcionan a un sistema de inteligencia artificial o que el sistema obtiene directamente. Estos datos se utilizan como base a partir de la cual el sistema genera información de salida.
- Datos biométricos: Esta categoría incluye datos personales que se obtienen mediante un tratamiento técnico específico y que están relacionados con las características físicas, fisiológicas o conductuales de una persona física. Estos datos permiten o confirman la identificación única de dicha persona e incluyen ejemplos como imágenes faciales o datos dactiloscópicos.

Estas definiciones son esenciales para comprender cómo se utilizan diferentes tipos de datos en el contexto de la inteligencia artificial y cómo contribuyen al entrenamiento, validación y prueba de sistemas de IA.

Sujetos relevantes (pRIA)

Se definen distintos sujetos relevantes en el contexto del Reglamento sobre sistemas de inteligencia artificial (pRIA):

- Operador: Este término abarca varias categorías de actores en el ámbito de los sistemas de IA, incluyendo al proveedor, al usuario, al representante autorizado, al importador y al distribuidor.
- Proveedor: Se refiere a cualquier persona física o jurídica, autoridad pública, agencia u organismo que desarrolla un sistema de IA con la intención de introducirlo en el mercado o ponerlo en servicio, ya sea de manera remunerada o gratuita.
- Proveedor a pequeña escala: Este término engloba a los proveedores que son microempresas o pequeñas empresas, conforme a la definición de la Recomendación 2003/361/CE de la Comisión de la Unión Europea.
- Representante autorizado: Designa a una persona física o jurídica establecida en la Unión Europea que ha recibido un mandato por escrito de un proveedor de un sistema de IA para cumplir con las obligaciones y llevar a cabo los procedimientos establecidos en el reglamento en representación de dicho proveedor.
- Importador: Se refiere a cualquier persona física o jurídica establecida en la Unión Europea que introduce en el mercado o pone en servicio un sistema de IA que lleva el nombre o la marca comercial de una persona física o jurídica establecida fuera de la Unión.
- Distribuidor: Designa a cualquier persona física o jurídica que forma parte de la cadena de suministro y que comercializa un sistema de IA en el mercado de la Unión Europea sin influir sobre sus propiedades.
- Usuario: Este término engloba a todas las personas físicas o jurídicas, autoridades públicas, agencias u organismos que utilizan un sistema de IA bajo su propia autoridad, a menos que dicho uso se enmarque en una actividad personal que no sea de carácter profesional.

Estas definiciones son esenciales para establecer roles y responsabilidades claros en relación con los sistemas de inteligencia artificial y para garantizar el cumplimiento de las regulaciones establecidas en el reglamento.

Uso y gestión: inteligencia artificial

Se definen varios términos relevantes en el contexto del uso y gestión de sistemas de inteligencia artificial (IA):

- Finalidad prevista: Se refiere al propósito para el cual un proveedor concibe un sistema de IA, lo cual incluye el contexto y las condiciones específicas de uso. Esta finalidad se determina a partir de la información proporcionada por el proveedor en las instrucciones de uso, materiales, declaraciones de promoción y venta, así como en la documentación técnica.
- Uso indebido razonablemente previsible: Este término hace referencia a la utilización de un sistema de IA de una manera que no corresponde a su finalidad prevista, pero que puede resultar de un comportamiento humano o de una interacción con otros sistemas y que es razonablemente previsible.
- Componente de seguridad de un producto o sistema: Se trata de un componente que forma parte de un producto o sistema y que desempeña una función de seguridad para dicho producto o sistema. Además, cualquier fallo o defecto en el funcionamiento de este componente puede poner en peligro la salud y la seguridad de las personas o los bienes.

Estas definiciones son esenciales para comprender las circunstancias relacionadas con el uso de sistemas de IA y garantizar la seguridad y la integridad tanto de las personas como de los bienes en el contexto de la inteligencia artificial.