TEMA 2. PROTECCIÓN DE DATOS PERSONALES Y NO PERSONALES

Datos personales Según el RGPD, cuyo propósito del RGPD es proteger los datos personales y regular su libre circulación. Los "datos personales" son información que identifica o hace identificable a una persona física, ya sea directa o indirectamente, a través de identificadores como nombres, números de identificación u otros elementos de la identidad.

Datos no personales Según el Reglamento (UE) 2018/1807, los "datos" se refieren a la información que no califica como datos personales según la definición del RGPD. El Reglamento (UE) 2018/1807 se enfoca en garantizar la libre circulación de datos no personales en la Unión Europea y establecer normas relacionadas con la localización de datos y su disponibilidad para las autoridades competentes y la portabilidad de datos para usuarios profesionales.

Tratamiento cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

Motivación para la protección

Destaca la preocupación histórica sobre la protección de datos personales, su inclusión en la legislación constitucional, y cómo el flujo legal de datos es fundamental para el desarrollo del mercado único y la economía digital. Además, se menciona la creciente consideración del dato como un activo económico y su relación con conceptos como la transparencia, el gobierno abierto y el mercado de datos. También se resalta la relevancia del Reglamento General de Protección de Datos (RGPD) en la investigación y desarrollo de la inteligencia artificial.

Derecho UE en la Protección de Datos

El Derecho de la Unión Europea en cuanto a la protección de datos personales se basa en el Derecho Originario y el Derecho Derivado. El **Derecho Originario** incluye los artículos 16 del Tratado de Funcionamiento de la Unión Europea y el artículo 8 de la Carta Europea de los Derechos Fundamentales, que reconocen directamente el derecho a la protección de datos y principios relacionados.

El **Derecho Derivado** (más importante) se compone del Reglamento (UE) 2016/679, conocido como el Reglamento General de Protección de Datos, la Directiva (UE) 2016/680 y el Reglamento (UE) 2018/1725.

En **España**, el régimen constitucional se basa en el artículo 18.4 de la Constitución Española, y la Ley Orgánica 3/2018 de Protección de Datos Personales y Garantía de los Derechos Digitales es un componente fundamental. Además, la Ley Orgánica 7/2021 se centra en la protección de datos personales en el contexto de la prevención, detección e investigación de infracciones penales, y el Real Decreto 1720/2007 establece el reglamento de desarrollo de la Ley Orgánica 15/1999, que también trata la protección de datos de carácter personal.

Aplicación

1. **Ámbito material:** Se aplica al tratamiento total o parcialmente automatizado de datos personales y al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero.

2. **Ámbito territorial:** Se aplica cuando las actividades son realizadas por un establecimiento del responsable o del encargado en la Unión Europea (UE). Si no existe un establecimiento en la UE, aún se aplica si se ofrece bienes o servicios a personas en la UE o si se controla su comportamiento en la UE.
3. **Exclusiones:** Hay exclusiones de la aplicación del RGPD, como actividades personales o domésticas, tratamientos para procedimientos judiciales o de seguridad, tratamientos de datos de personas fallecidas, y la normativa sobre protección de materias clasificadas. Además, ciertas actividades generales tienen su propia normativa específica.

Principios del RGPD

1. Licitud, lealtad y transparencia.
2. Finalidad.
3. Minimización de datos.
4. Exactitud.
5. Limitación del plazo de conservación.
6. Integridad y confidencialidad.
7. Responsabilidad proactiva.

Licitud del tratamiento de datos

Los **supuestos** para el tratamiento de datos incluyen el consentimiento del interesado, la necesidad de tratamiento para la ejecución de un contrato, el cumplimiento de una obligación legal, los intereses vitales, el cumplimiento de una misión en interés público, o la satisfacción de intereses legítimos, siempre que no prevalezcan los intereses o derechos fundamentales del interesado. Y en los casos de tratamiento sin consentimiento debe estar clara la base jurídica.

El **consentimiento** debe ser libre, informado, inteligible y claro. Si está condicionado al acceso a un servicio, debe ser congruente con la finalidad del servicio. Existen regímenes especiales de consentimiento para niños y categorías especiales de datos.

Derechos de los interesados

Derechos de Información: Contenido mínimo de la información incluye: identidad del responsable, datos de contacto del delegado de protección de datos, fines del tratamiento, justificación si los datos no se han obtenido con el consentimiento, destinatarios o categorías de destinatarios de los datos, intención de transferencia internacional.

Derecho a la Transparencia: se debe informar sobre el plazo de conservación, la existencia del derecho de acceso, rectificación o supresión, revocabilidad del consentimiento, derecho a presentar una reclamación, existencia de decisiones automatizadas (incluidos perfiles), si es obligatorio y las consecuencias de no proporcionar los datos.

Derecho de Acceso: El derecho a obtener del responsable del tratamiento una confirmación de si se están procesando datos personales y, en caso afirmativo, obtener acceso a esos datos y cierta información relacionada con el tratamiento.

Derecho a la Rectificación: El derecho a que se corrijan los datos personales inexactos sin dilación indebida.

Derecho a la Supresión (o Derecho al Olvido): El derecho a que se borren los datos personales cuando se cumplan ciertas condiciones, como que los datos ya no sean necesarios para los fines para los que se recopilaron.

Derecho a la Limitación del Tratamiento: El derecho a limitar el procesamiento de datos personales en ciertas circunstancias, como cuando se está verificando la precisión de los datos o se ha impugnado la legitimidad del tratamiento.

Derecho a la Portabilidad de los Datos: El derecho a recibir los datos personales en un formato estructurado, de uso común y lectura mecánica, y transmitirlos a otro responsable del tratamiento, siempre que el tratamiento se base en el consentimiento o en un contrato.

Derecho de Oposición: El derecho a oponerse al procesamiento de datos personales, a menos que el responsable del tratamiento demuestre razones legítimas para el procesamiento que prevalezcan sobre los intereses, derechos y libertades del interesado.

Derecho a no ser objeto de Decisiones Automatizadas: El derecho a no estar sujeto a decisiones basadas únicamente en el procesamiento automatizado, incluida la elaboración de perfiles, que produzcan efectos jurídicos o tengan un impacto significativo.

Derecho a Retirar el Consentimiento: Si el procesamiento se basa en el consentimiento del interesado, este tiene el derecho a retirar su consentimiento en cualquier momento.

Derecho a Presentar una Reclamación ante una Autoridad de Control: El derecho a presentar una queja ante la autoridad de control de protección de datos en su país si considera que el tratamiento de sus datos personales infringe la RGPD.

<u>Limitaciones</u>

Se establecen limitaciones al tratamiento de datos en situaciones que incluyen la seguridad del Estado, la defensa, la seguridad pública, la prevención y enjuiciamiento de infracciones penales, y otros objetivos importantes de interés público.

<u>Responsable del tratamiento</u>

El **responsable del tratamiento** es la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros.

Por Estatuto tiene la carga de demostrar que el tratamiento se adecua al RGPD, políticas de PD = posibilidad de acudir a Códigos de conducta. Así como contar con una protección de datos desde el diseño y por defecto

<u>Encargado del tratamiento</u>

El **Encargado del Tratamiento** es la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento. Es el representante del responsable del tratamiento

Debe demostrar capacidad técnica y organizativa para garantizar la seguridad y legalidad del tratamiento de datos personales. El encargado está sujeto a un acuerdo de encargo por escrito, debe seguir las instrucciones del responsable del tratamiento y garantizar la confidencialidad

en el uso de los datos por parte de terceros. Además, debe colaborar activamente con el responsable para garantizar el cumplimiento del RGPD, proporcionando asistencia, ayuda y documentación cuando sea necesario. Al finalizar el encargo, el encargado debe eliminar o devolver los datos al responsable. También se le permite recurrir a subencargados, pero esto debe hacerse con el consentimiento previo del responsable y asegurando que los subencargados cumplan con las mismas obligaciones de protección de datos.

Responsabilidad del tratamiento

La responsabilidad del tratamiento según el RGPD implica llevar un registro de las actividades de procesamiento, que debe estar disponible para la autoridad de control cuando lo solicite.

- El responsable/encargado del tratamiento, contenido: responsable, fines del tratamiento, categorías de interesados y de datos personales, categorías de destinatarios, supuestos de transferencia de datos, plazos previstos para supresión de cada categoría de datos, medidas técnicas y de seguridad del tratamiento.
- El encargado del tratamiento: encargado, y del delegado de protección de datos, categorías de tratamiento por cada responsable, transferencias de datos, medidas técnicas y de seguridad de los tratamientos

Además, el principio de seguridad del tratamiento exige notificar cualquier violación de la seguridad de los datos a la autoridad de control y comunicar estas violaciones a los interesados.

También, es esencial llevar a cabo evaluaciones de impacto en la protección de datos cuando exista un alto riesgo para los derechos y libertades de las personas en ciertas circunstancias, como tratamientos automatizados con efectos jurídicos, tratamiento de categorías especiales de datos u observación sistemática a gran escala en áreas de acceso público. Estas evaluaciones deben describir las operaciones, evaluar la necesidad y proporcionalidad, identificar riesgos y medidas para mitigarlos, y garantizar la seguridad de los datos.

Por último, el principio de responsabilidad involucra la consulta con la autoridad de control sobre las medidas a tomar para evitar o reducir riesgos en el procesamiento de datos que lo requiera.

Delegado de protección de datos

El delegado de protección de datos (DPD) debe ser designado en ciertos supuestos, como en el caso de organismos públicos o actividades de tratamiento que requieren una observación habitual y sistemática de interesados a gran escala o el tratamiento de categorías especiales de datos. El DPD debe cumplir con requisitos específicos de conocimientos especializados en derecho y práctica en protección de datos.

El DPD tiene una posición relevante, con derechos y deberes específicos. Debe desempeñar sus funciones de manera independiente y tiene la responsabilidad de informar y asesorar al responsable del tratamiento, supervisar el cumplimiento del RGPD, asesorar en la Evaluación de Impacto de Protección de Datos (EIPD) y cooperar con la autoridad de control, siendo el punto de comunicación con esta última. Además, el DPD debe mantener la confidencialidad de los datos y garantizar la compatibilidad de su función con otras responsabilidades.

Códigos de conducta y certificaciones

Los **códigos de conducta** son instrumentos destinados a promover el cumplimiento del Reglamento General de Protección de Datos (RGPD) en sectores o ámbitos específicos. Estos códigos se aplican a un colectivo que los adopta y buscan establecer buenas prácticas en relación con la protección de datos. Para su aprobación, se requiere la aprobación de una Autoridad de Control, y deben ser supervisados por un organismo con pericia e independencia adecuada, que evalúa el cumplimiento y resuelve reclamaciones.

Por otro lado, las **certificaciones** son marcas o sellos que acreditan el cumplimiento del RGPD y son de iniciativa privada. Estas certificaciones son voluntarias y se obtienen a través de procedimientos transparentes y temporales. Su otorgamiento no limita la responsabilidad del responsable de tratamiento de datos y debe contar con garantías adecuadas para asegurar su cumplimiento, siendo posible retirar la certificación. Las certificaciones son emitidas por organismos de certificación.

Transferencias internacionales de datos

Las transferencias internacionales de datos en el contexto del Reglamento General de Protección de Datos (RGPD) se rigen por el principio general de mantener el mismo régimen de protección de datos en relación con los principios y garantías previstos en la Unión Europea (UE). Para lograrlo, se utilizan diferentes fórmulas, que incluyen:

- **Decisión de adecuación**: Se refiere a la determinación de que un país o territorio extranjero proporciona un nivel de protección de datos equivalente al de la UE.
- **Garantías adecuadas**: Esto implica el uso de mecanismos de garantía que aseguren un nivel adecuado de protección de datos, como decisiones de autorización por parte de la Autoridad de Control, instrumentos jurídicamente vinculantes entre organismos públicos, normas corporativas vinculantes, cláusulas tipo de protección de datos, códigos de conducta y mecanismos de certificación.
- **Autorización de la Autoridad de Control**: En algunos casos, se requiere la autorización expresa de una Autoridad de Control para llevar a cabo una transferencia internacional de datos.
- **Cláusulas contractuales:** Estas son disposiciones contractuales específicas incorporadas a acuerdos entre las partes involucradas en la transferencia internacional de datos.
- **Disposiciones incorporadas a acuerdos administrativos:** Algunas transferencias de datos pueden basarse en acuerdos administrativos que contienen disposiciones específicas sobre protección de datos.

Normas corporativas vinculantes

Las **Normas Corporativas Vinculantes** son reglas obligatorias establecidas por un grupo empresarial para cumplir con el Reglamento General de Protección de Datos (RGPD). Para que sean válidas, deben cumplir con ciertas condiciones: ser obligatorias, otorgar derechos que los interesados puedan exigir, y aprobarse de acuerdo con las pautas del RGPD.

El contenido aborda aspectos como las transferencias de datos, el reconocimiento de los derechos de los interesados, el cumplimiento de las responsabilidades del responsable y el encargado del tratamiento, la forma de informar a los interesados, la designación de un delegado de protección de datos (DPO), los procedimientos para presentar reclamaciones, los

mecanismos de verificación y cómo se debe informar a la autoridad de control. Deben ser aprobadas por la autoridad de control correspondiente para garantizar su cumplimiento con los estándares del RGPD.

Autoridades de control

Las **autoridades de control** son entidades responsables de garantizar el cumplimiento del Reglamento General de Protección de Datos (RGPD) en cada Estado miembro de la Unión Europea (UE). Estas autoridades pueden ser designadas por cada Estado miembro o por la Autoridad de Control representante a nivel de la UE.

Las autoridades de control tienen diversas funciones, que incluyen la aplicación coherente del RGPD. Para ejercer estas funciones de manera efectiva, las autoridades de control deben cumplir con requisitos importantes, como la independencia y contar con la capacidad técnica y los recursos necesarios. La autoridad de control principal juega un papel crucial en la gestión de asuntos transfronterizos relacionados con la protección de datos. Cooperación y coherencia:

Cooperación: Se refiere a la colaboración activa y el trabajo conjunto entre la Autoridad de Control Principal y las demás Autoridades de Control interesadas en la UE. Esto es especialmente importante en casos que involucran organizaciones multinacionales que operan en varios países de la UE. La cooperación implica compartir información, coordinar investigaciones y tomar decisiones en conjunto para garantizar que las organizaciones cumplan de manera consistente con el RGPD en todos los países donde operan.

Coherencia: La coherencia se logra mediante un "Mecanismo de Coherencia", que busca asegurar que las decisiones tomadas por las diferentes Autoridades de Control en la UE sean coherentes y uniformes en situaciones que involucran a organizaciones que operan en múltiples países miembros. El mecanismo de coherencia implica la emisión de dictámenes por parte del Comité Europeo de Protección de Datos (CEPD), la resolución de conflictos y la facilitación del intercambio de información entre las Autoridades de Control. Esto evita la fragmentación y asegura una aplicación uniforme de las leyes de protección de datos en toda la Unión Europea. Europeo de Protección de Datos.

Protección de Datos no Personales

Libre Circulación de Datos no Personales (RDNP)

El Reglamento (UE) 2018/1807 del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, relativo a un marco para la libre circulación de datos no personales en la Unión Europea, establece las reglas para garantizar la libre circulación en la Unión de datos que no sean personales. Su objetivo es eliminar las barreras para la circulación de estos datos y fomentar su disponibilidad y portabilidad para usuarios profesionales.

Dato no personal: Se refiere a los datos que no son datos personales según la definición del Reglamento (UE) 2016/679. Esto incluye conjuntos de datos mixtos, en los que algunos datos son personales y otros no.

Territorial: La normativa se aplica a los datos utilizados en la prestación de servicios a residentes o establecidos en la Unión Europea, así como a los prestadores establecidos en la UE.

Principios de RDNP

1. **Prohibición de requisitos para la localización de datos:** En principio, se prohíben los requisitos que exijan que los datos no personales se almacenen o procesen en un lugar específico. Sin embargo, se pueden establecer excepciones.

2. **Disponibilidad para autoridades competentes**: El reglamento garantiza la disponibilidad de datos no personales para las autoridades competentes, lo que es esencial para cumplir con la normativa y la supervisión.

3. **Portabilidad de datos**: El RDNP promueve la portabilidad de datos, lo que significa que los usuarios profesionales tienen el derecho de acceder a los datos, garantizar su disponibilidad, y recibirlos en un formato estructurado y legible automáticamente.

Regulación de la Gobernanza de Datos (RGD)

El Reglamento (UE) 2022/868 establece la regulación de la gobernanza de datos en la Unión Europea, abordando aspectos como la **reutilización** de ciertas categorías de datos públicos, la **notificación** y supervisión de **servicios de intermediación** de datos, la inscripción voluntaria de entidades que manejan datos con fines altruistas y la creación de un Comité Europeo de Innovación en materia de Datos. Importante hay que destacar que esta regulación no reemplaza las normativas existentes sobre reutilización de datos públicos, protección de datos, legislación de competencia, seguridad y defensa, sino que complementa estas áreas para promover una adecuada gestión de datos en la Unión Europea. La **RGD** introduce aspectos relacionados con:

Reutilización de Datos en Posesión de Organismos Públicos: Este ámbito de aplicación se refiere a datos protegidos por motivos como confidencialidad comercial, estadística, propiedad intelectual o protección de datos (siempre que el RGPD no sea aplicable). Se permiten excepciones datos en poder de empresas públicas, organismos públicos de radiodifusión, centros culturales o de enseñanza, datos protegidos por motivos de seguridad pública o defensa nacional, datos ajenos a la misión de servicio público.

- Se **prohíben los acuerdos de exclusividad**, excepto por necesidad de cumplimiento de la misión de servicio o producto de interés general.
- **Condiciones de reutilización.**
- **Garantías**

Condiciones, estas condiciones deben ser no discriminatorias, transparentes, proporcionadas y adecuadas a las categorías de datos, sin restringir la competencia. El acceso a estos datos se realiza a través de un punto único. Se requiere preservar la protección de la información mediante requisitos como la anonimización de datos personales, imponer medidas de control de sistemas de acceso y reutilización a distancia, o se permite el acceso en locales propios.

Garantías, que el acceso no compromete la seguridad de los tratamientos de datos, se establece un deber de confidencialidad en la reutilización, se brinda asistencia por parte de organismos del sector público en casos de prohibición y para la transferencia de datos a terceros estados.

Servicios de Intermediación de Datos, tienen como objetivo establecer relaciones comerciales para el intercambio de datos entre diversas partes interesadas, incluyendo propietarios de datos, usuarios y partes interesadas. Estos servicios pueden implicar medios técnicos, legales u otros, y pueden incluir servicios relacionados con el ejercicio de los derechos de los interesados en los datos, excluyendo ciertos servicios específicos. Son **excluidos** los siguientes:

- Servicios que agregan, enriquecen o transforman datos.
- Servicios de intermediación de contenido con derechos de autor.
- Servicios utilizados exclusivamente por un único propietario de datos o por múltiples entidades legales en un grupo cerrado.
- Servicios de intercambio de datos ofrecidos por organismos del sector público sin la intención de establecer relaciones comerciales.

La regulación sobre servicios de intermediación de datos establece varias categorías de servicios sujetos a notificación y proporciona un procedimiento de notificación detallado:

Servicios de Intermediación de Datos Sujetos a Notificación: Estos servicios incluyen:

- Servicios de intermediación entre los titulares de datos y los usuarios de datos, facilitando el intercambio de datos.
- Servicios de intermediación entre interesados que deseen facilitar datos personales o no personales y potenciales usuarios de datos.
- Servicios de cooperativas de datos, que son ofrecidos por estructuras organizativas compuestas por interesados, empresas unipersonales o pymes.

1. **Procedimiento de Notificación:** Los proveedores de servicios de intermediación de datos deben presentar una notificación a la autoridad competente antes de comenzar su actividad, incluyendo información sobre su organización y una descripción del servicio. Esta notificación permite al proveedor ofrecer servicios de intermediación de datos en toda la Unión Europea y se comunica a la Comisión Europea para su registro.

2. **Condiciones de Prestación de Servicios de Intermediación de Datos:**
    - El acceso a los servicios debe ser equitativo, transparente y no discriminatorio para los propietarios y usuarios de datos.
    - Los datos recopilados de los usuarios solo pueden utilizarse para el servicio proporcionado.
    - Deben evitarse prácticas fraudulentas o abusivas.
    - Deben establecerse medidas para garantizar la continuidad de los datos en caso de insolvencia, especialmente cuando se involucra el almacenamiento de datos.
    - Se debe mantener el formato de los datos, a menos que se realicen mejoras.
    - Los datos deben ser interoperables mediante estándares abiertos de uso común.

Cesión Altruista de Datos

La Cesión Altruista de Datos implica una regulación estatal para facilitar estas operaciones, junto con la creación de Registros Públicos de Organizaciones Reconocidas de Gestión de Datos con Fines Altruistas, establecidos por autoridades competentes y la Comisión. Las condiciones

para la inscripción en estos registros requieren que las organizaciones operen sin ánimo de lucro, de manera jurídicamente independiente, y cumplan con un código normativo.

Estatuto de la Organización de Cesión Altruista de Datos (ORGDFA)

- Transparencia: Se lleva un registro de las personas que han permitido el tratamiento de sus datos, la duración del tratamiento, la finalidad y las tasas abonadas.
- Protección de Derechos e Intereses de los Titulares de Datos: Incluye el deber de información, tratamiento para fines de interés general consentidos, información sobre transferencia, acceso o utilización no autorizada.
- Código Normativo: Se debe elaborar y aprobar un código normativo por la Comisión

Garantías de la Gobernanza de Datos

El RDNP establece una serie de garantías generales relacionadas con la gobernanza de datos, que incluyen:

Garantías del Uso Altruista de Datos:

- **Autoridad Competente**: Cada Estado miembro tiene una autoridad competente y debe comunicar esto a la Comisión Europea.
- **Supervisión de Cumplimiento**: La autoridad competente tiene la competencia para recabar información, notificar observaciones, ordenar el cese de infracciones y cancelar el registro con pérdida de la posibilidad de uso del título ORGDFA. En caso de competencia territorial, se establece un procedimiento de cooperación.
- **Formulario Europeo de Consentimiento para la Cesión Altruista de Datos**: Se utiliza un formulario específico para obtener el consentimiento de la cesión altruista de datos.

Garantías Generales sobre la Gobernanza de Datos:

- **Autoridades Competentes**: Deben ser independientes, transparentes, coherentes y facilitar la competencia legal y la no discriminación. Deben ser económicamente autosuficientes y proporcionar información.
- **Comité Europeo de Innovación en Materia de Datos**: Compuesto por expertos, autoridades competentes y representantes de interesados. Cumple funciones de asesoramiento y asistencia a la Comisión en la materia, propone directrices, facilita la cooperación entre Estados y emite informes en casos previstos en el RGD.
- **Acceso y Transferencia Internacionales**: Se prohíbe generalmente la transferencia a terceros países, con excepciones bajo ciertas condiciones, incluyendo la minimización de datos e información al afectado.