

Riesgo, seguridad y legislación en Sistemas de Información (04MBID).



Universidad
Internacional
de Valencia

Tema 4: Medidas de Protección de Datos de Carácter Personal

Principio de Privacidad Universal a los Derechos Personales

El origen legal del ***derecho a la privacidad*** está en la Declaración Universal de Derechos Humanos de 1948. Dicho texto otorga a una persona el derecho a proteger su intimidad, familia, domicilio o reputación de cualquier intromisión ilegítima.

¿Hasta donde llega la libertad de una persona?

Marco jurídico Español

España el Art. 10 Constitucional señala:

“1. La dignidad de la persona, los derechos inviolables que le son inherentes, el libre desarrollo de la personalidad, el respeto a la ley y a los derechos de los demás son fundamento del orden político y de la paz social.

2. Las normas relativas a los derechos fundamentales y a las libertades que la Constitución reconoce se interpretarán de conformidad con la Declaración Universal de Derechos Humanos y los tratados y acuerdos internacionales sobre las mismas materias ratificados por España.”

Art. 18: Garantiza el derecho al honor, a la intimidad personal y familiar y a la imagen; la condición de inviolabilidad del domicilio personal; la inviolabilidad de las comunicaciones; y establece los límites al uso de la informática.

“4. La Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.”

Protección de Datos

El marco jurídico aplicable a proyectos Big Data empezaría por el conjunto de normas que regulan el **uso y tratamiento de datos personales**.

1. **Reglamento General de Protección de Datos de la UE (RGPD)**, de 27 de abril de 2016, publicado en mayo de 2016 y aplicable desde el 25 de mayo de 2018. Norma de aplicación directa en la Unión Europea, relativa a la protección de datos personales y su libre circulación, de las personas físicas de la UE.
2. En España la **Ley Orgánica sobre Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD)**, del 5 de diciembre de 2018, que *deroga la Ley 15/1999 (LOPD) y su reglamento de desarrollo 1720/2007*.

Portal de la Agencia Española de Protección de Datos: <https://www.aepd.es/es>

Si añadimos LSSICE y LGT tenemos:

- **Ley de servicios de la sociedad de la información y de comercio electrónico (LSSICE).**
Ley 34/2002, de 11 de julio.
- **Ley General de Telecomunicaciones (LGT).**
Ley 11/2022, de 29 de junio de 2022

¿Qué es un DATO de carácter personal?

Para la Agencia Española de Protección de Datos (AEPD). Los datos de carácter personal son cualquier información referente a personas físicas identificadas o identificables, pudiendo ser identificable toda persona cuya identidad pueda determinarse mediante un identificador (por ejemplo, un nombre, un número de identificación, datos de localización o un identificador en línea) o mediante el uso de uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de las personas.

Tipos de DATOS de carácter personal

.- **Identificativos** (nombre, apellidos, número de documento de identidad -en España DNI-, correo electrónico, foto), referidos a la situación laboral (No. de Seguridad Social), financiera (Cta. bancaria, tarjeta de crédito, Iban, Swift) o de salud (tarjeta sanitaria, registros médicos).

Tipos de DATOS de carácter personal. Categorías especiales

También existen las **categorías especiales de datos**, en los que además de los datos de salud, se encuentran los que puedan revelar:

- ☐ origen étnico o racial,
- ☐ opiniones políticas,
- ☐ convicciones religiosas o fisiológicas,
- ☐ afiliación sindical,
- ☐ datos genéticos, biométricos,
- ☐ vida sexual u orientación sexual

Donde se suministran los DATOS de carácter personal

- .- Cuando te registras en un hotel.
- .- Si solicitas una hipoteca.
- .- Cuando te suscribes a algún tipo de servicio a través de internet.
- .- Si te das de alta en un servicio de correo electrónico.
- .- En los centros de salud, hospitales, clínicas.
- .- En tú trabajo.
- .- Cuando te das de alta en una red social.

Tema 4 Medidas de Protección de Datos de Carácter Personal

Cuando es aplicable la normativa

La normativa de protección de datos sólo será de aplicación cuando los proyectos impliquen el tratamiento de datos personales, entendiéndose estos como cualquier información concerniente a personas físicas identificadas o identificables.

- Dicha condición se refiere a que una persona pueda ser identificada por un dato o por la combinación de información de diversas fuentes.
- **Cuando no sea posible la identificación de la persona** o esta requiera esfuerzos desproporcionados, **no será de aplicación** la normativa de protección de datos, igual en caso de datos no personales, como por ejemplo, datos relativos al tráfico, la contaminación o al clima.

Principios rectores del RGPD

.- Principio de licitud, lealtad y transparencia.

Cuando se recaban datos de carácter personal deben ser tratados de manera lícita, leal y transparente, este principio excluye que los datos personales puedan ser tratados de forma desleal o sin proporcionar toda la información necesaria sobre el objeto y fines del tratamiento, así como sus consecuencias y posibles riesgos.

.- Principio de limitación de la finalidad.

Los datos personales deben ser recogidos para fines determinados, explícitos y legítimos, y no serán tratados de manera incompatible con otros fines, la finalidad del tratamiento de los datos personales ha de estar claramente definida.

.- Principio de minimización de datos.

Los datos personales serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.

Principios rectores del RGPD

.- Principio de exactitud.

Los datos personales serán exactos y si fuera necesario actualizados, adoptándose medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos respecto a los fines para los que se tratan.

.- Principio del plazo de conservación.

Los datos personales serán mantenidos de forma que se permita la identificación de los interesados por un plazo de tiempo no superior al necesario para cumplir con los fines del tratamiento, una vez cumplidas las finalidades, los datos deben ser borrados o, al menos, desprovistos de todo elemento que permita identificar a los interesados.

.- Principio de integridad y seguridad.

Los datos personales serán tratados de manera que se garantice su adecuada seguridad, incluyendo la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental.

.- Principio de responsabilidad proactiva.

Los responsables y encargados del tratamiento de datos deben ser capaces de demostrar el cumplimiento de la normativa establecida.

Ámbito Aplicación de la LOPD

LOPD(-GDD): protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos.

Aplica a cualquier **tratamiento** total o parcialmente automatizado de **datos personales**, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero

La Agencia Española de Protección de Datos (AEPD): Informa sobre contenido, principios, y las garantías de los derechos regulados en la LOPD

- ❑ Ayuda al **ciudadano** a **ejercer** sus derechos
- ❑ **Tutela** al ciudadano en el ejercicio de sus derechos cuando no han sido adecuadamente atendidos por los responsables de los ficheros
- ❑ **Garantiza** el cumplimiento investigando actuaciones contrarias a los principios de la LOPD-GDD (y otras). Impone en su caso la correspondiente sanción

Figuras RGPD: Responsable del tratamiento

Una organización que va a diseñar y/o implementar tecnología Big Data será, a efectos de la normativa de protección de datos el **responsable del tratamiento**:

“persona física o jurídica, autoridad pública, servicio u otro organismo, que determine los fines y medios del tratamiento”

Quien fija la finalidad del tratamiento y decide sobre la externalización del mismo y en qué grado delega las actividades de tratamiento a otra organización.

Figuras RGPD: Encargado del tratamiento

La norma define “**encargado del tratamiento**” como:

“persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento”

Para el desarrollo del análisis masivo de información, se acude a **proveedores** que tengan la consideración de **encargados de tratamiento**.

Únicamente se deberán contratar empresas que tengan la condición de encargado del tratamiento **cuando ofrezcan garantías suficientes para aplicar medidas técnicas y organizativas adecuadas de manera que el tratamiento sea conforme al RGPD**

Figuras RGPD: Responsable y encargado del tratamiento - Contrato

Tanto la normativa nacional como europea establecen que la realización de tratamientos por cuenta de terceros que realiza el encargado de tratamiento deberá estar regulada en un **contrato por escrito**, u otro acto jurídico, **que vincule al encargado respecto del responsable** y establezca el *objeto, la duración, la naturaleza y la finalidad del tratamiento, así como el tipo de datos personales, categorías de interesados y las obligaciones y derechos del responsable*.

Figuras RGPD: Corresponsable del tratamiento

Como novedad, el RGPD ha introducido la figura del “**corresponsable del tratamiento**” en los casos en los que dos o más responsables determinen conjuntamente los objetivos y los medios del tratamiento, estos deben determinar cuáles son las responsabilidades compartidas y cuales individuales, y poner a disposición del interesado los aspectos esenciales del acuerdo.

Figuras RGPD: **DPD** Delegado de Protección de Datos

Persona encargada del correcto cumplimiento de la normativa de protección de datos, desempeñando las tareas:

- a) Informar y asesorar al **responsable** o al **encargado** del tratamiento y a los **empleados** que se ocupen del tratamiento de las obligaciones que les incumben en virtud del presente Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros;
- b) Supervisar el cumplimiento de lo dispuesto en el presente **Reglamento**, de otras **disposiciones** de protección de datos de la Unión o de los Estados miembros y de las **políticas** del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de **responsabilidades**, la **concienciación** y **formación** del personal que participa en las operaciones de tratamiento, y las **auditorías** correspondientes;
- c) Ofrecer el asesoramiento que se le solicite acerca de la **evaluación de impacto** relativa a la protección de datos y supervisar su aplicación;
- d) Cooperar con la autoridad de control. En el caso de España, con la **Agencia Española de Protección de Datos**;
- e) Actuar como punto de contacto de la autoridad de control para resolver cuestiones y consultas relativas al tratamiento de los datos.

Figuras RGPD: **DPD** delegado de protección de datos

El Reglamento obliga a las organizaciones cuyas actividades principales consistan en tratamientos que requieran una **observación habitual y sistemática de los ciudadanos a gran escala**, también en el **tratamiento importante de categorías especiales de datos personales** o de datos relativos a **condenas e infracciones penales**, a designar un DPD.

Se **notificará** la designación a la AEPD para su inclusión en el Registro Público de Delegados de Protección de Datos.

En el resto de los supuestos, la designación de un DPD será *voluntaria*.

Tema 4 Medidas de Protección de Datos de Carácter Personal

Licitud

Será **lícito** tratar datos si se cumplen al menos una de las siguientes condiciones:

- a) El interesado dio **consentimiento** para el tratamiento de sus datos para uno o varios fines específicos.
- b) El tratamiento es **necesario para la ejecución de un contrato** en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales.
- c) El tratamiento es **necesario para el cumplimiento de una obligación legal** aplicable al responsable del tratamiento.
- d) El tratamiento es necesario para **proteger intereses vitales del interesado o de otra persona física**.
- e) El tratamiento es necesario para el cumplimiento de una misión realizada en **interés público o en el ejercicio de poderes públicos** conferidos al responsable del tratamiento.
- f) El tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, **siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño**.

Responsabilidad Activa

La AEPD alude a la responsabilidad de las organizaciones en la implantación de **medidas que garanticen el cumplimiento** de los **principios** y **obligaciones** en materia de protección de datos, así como el establecimiento de mecanismos internos y externos para **evaluar su fiabilidad y demostrar su efectividad cuando se solicite por las autoridades de control**.

- El nombramiento de un **Delegado de Protección de Datos**, que será la persona que se encargue del correcto cumplimiento de la normativa.
- En caso de fuga de información o cualquier otra amenaza sobre los datos, el Reglamento exige a la organización responsable la **notificación** a la autoridad de control (en el caso de España la AEPD).

<https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento>

<https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/otros-mecanismos/codigos-de-conducta>

Derechos de los interesados

El RGPD establece los siguientes derechos de protección a los interesados:

Art. 15: Derecho de acceso del interesado

Art. 16: Derecho de rectificación

Art. 17: Derecho de supresión (derecho al olvido)

Art. 18: Derecho a la limitación del tratamiento

Art. 19: Derecho de información sobre la rectificación

Art. 20: Derecho a la portabilidad de los datos

Art. 21: Derecho de oposición

Art. 22: Derecho a la no elaboración de perfiles

Estos derechos son ratificados en la LOPDPGDD (Arts. 12 al 18)

Tema 4 Medidas de Protección de Datos de Carácter Personal

Cuando los datos personales no se hayan obtenidos del interesado, el responsable del tratamiento facilitará la siguiente información

- a. La identidad y los datos de contacto del responsable y, en su caso, de su representante.
- b. Los datos de contacto del Delegado de Protección de Datos.
- c. Los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento.
- d. Los intereses legítimos del responsable o de un tercero.
- e. Los destinatarios o las categorías de destinatarios de los datos.
- f. La intención del responsable de transferir datos personales a un tercer país u organización internacional.
- g. El plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar dicho plazo.

Tema 4 Medidas de Protección de Datos de Carácter Personal

Cuando los datos personales no se hayan obtenidos del interesado, el responsable del tratamiento facilitará la siguiente información

- h. La existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos y su rectificación o supresión.
- i. La existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada.
- j. El derecho a presentar una reclamación ante una autoridad de control.
- k. Si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de no facilitar los mismos.
- l. La existencia de decisiones automáticas, como la elaboración de perfiles, y las consecuencias previstas de dicho tratamiento para el interesado.

Principios que rigen la Privacidad desde el diseño

1. **Proactivo no reactivo; preventivo no correctivo:** la privacidad desde el diseño suele caracterizarse por tomar **medidas proactivas en lugar de reactivas**. Se anticipa y previene la pérdida de privacidad de la información antes de que suceda.
2. **La Privacidad por Defecto:** consiste ofrecer el máximo grado de privacidad para asegurar que los **datos personales están protegidos automáticamente** en cualquier sistema informático o dentro de las buenas prácticas. Sin necesidad de actuación por parte del cliente o proveedor, la protección de su información y su privacidad se mantiene intacta, ya que está integrado en el sistema por defecto.
3. **La privacidad embebida en el diseño:** la protección de la información debe estar embebida en la infraestructura TI y en los procesos de la empresa. No debe ser considerado como un añadido sino como un **componente esencial del núcleo** como parte integral del sistema sin que por ello se disminuya la funcionalidad.
4. **Funcionalidad completa** - Se trata de garantizar que se cubren todas las funcionalidades y necesidades de los distintos implicados, pero sin afectar a la privacidad. Privacidad desde el diseño evita la pretensión de falsas dicotomías, como la privacidad frente a la seguridad. **No tiene sentido pensar en la privacidad sin la seguridad ni en la seguridad sin la privacidad.**

Principios que rigen la Privacidad desde el diseño

5. **Seguridad punto-a-punto - Protección completa del ciclo de vida de los datos:** desde el momento de su recolección, la protección se extiende a través de todo el ciclo de vida de los datos involucrados. De esta manera, **todos los datos se conservan y destruyen de forma segura**, asegurando la gestión del ciclo de vida seguro de la información, punto a punto.
6. **Visibilidad y transparencia** - Mantenerlo abierto: garantizar a todos los interesados que, sean cuales sean las prácticas de negocio o la tecnología utilizadas, funcionarán de acuerdo con los compromisos y los objetivos establecidos, y que estarán sujetos a una **verificación independiente**. De esta forma los componentes y operaciones permanecen **visibles y transparentes, a los usuarios y proveedores** por igual.
7. **El respeto a la privacidad del usuario** - Mantenerla **centrada en el usuario**: la privacidad desde el diseño requiere que los desarrolladores y operadores del sistema mantengan por encima de todo el interés de las personas, ofreciendo unas medidas de protección fuertes en sus valores predeterminados de privacidad, con avisos apropiados, y fortalecer las opciones para que sean fáciles de usar.

La anonimización y seudonimización

La **anonimización** de datos es un método para eliminar información de identificación personal de un conjunto de datos y así proteger la privacidad de la persona o empresa de la que se recopilaron los datos.

Con el uso creciente de análisis de datos en Big Data, el uso de conjuntos de datos anónimos debería ser fuente de estudio en profundidad.

La anonimización supone que no será posible identificar a la persona con datos o con información de diversas fuentes, teniendo en cuenta todos los medios que puedan ser **razonablemente** utilizados para su identificación.

<https://www.aepd.es/sites/default/files/2019-09/guia-orientaciones-procedimientos-anonimizacion.pdf>

La anonimización y seudonimización

El objetivo de la **anonimización** es la protección de la **privacidad** y el **cumplimiento** de la ley.

- Implica la modificación de los conjuntos de datos para que no quede información personal identificable.
- Como resultado, los datos pueden ser utilizados y transferidos sin que las identidades de los individuos sean reveladas involuntariamente.

Pero la verdadera anonimización es difícil de lograr.

La **seudonimización** consiste en reemplazar un atributo en un registro por otro, por lo que sigue permitiendo identificar indirectamente a cualquier persona, y no se puede equiparar a la **anonimización**, queda por tanto dentro del ámbito del régimen jurídico de la protección de datos.

La anonimización y seudonimización

La **seudonimización** es una excelente forma de **reducir los riesgos** derivados del tratamiento de datos de carácter personal en proyectos Big Data y ayuda a las organizaciones a cumplir sus obligaciones de protección de los datos.

Pero no se debe perder de vista que *utilizando estas técnicas una persona aún puede ser identificable*, por lo que cada organización deberá tomar las medidas adicionales necesarias.

Si lo que se pretende es **anonimizar** los datos, se deberá garantizar que la identificación sea *irreversible*.

Tema 4 Medidas de Protección de Datos de Carácter Personal



DERECHO DE ACCESO

Faculta al interesado a dirigirse al responsable del tratamiento para **conocer** si está tratando o no sus datos personales y, en caso afirmativo **obtener información** sobre:

- Copia de los datos personales que son objeto de tratamiento.
- Fines del tratamiento.
- Categorías de datos personales de que se trate.

DERECHO DE OPOSICIÓN

Este derecho ofrece la posibilidad al interesado de solicitar al responsable el **cese** concreto de **un tratamiento concreto** sobre sus datos personales.



DERECHO DE RECTIFICACIÓN

Este derecho faculta al interesado obtener sin dilación indebida del responsable del tratamiento la rectificación de sus datos personales **inexactos**.



DERECHO DE SUPRESION

Conocido como «**el derecho al olvido**» permite al interesado la supresión de sus datos de carácter personal cuando concorra alguna de las siguientes circunstancias:

- Los datos personales ya **no sean necesarios** en relación con los fines para los que fueron recogidos o tratados de otro modo;
- El interesado **retire el consentimiento**, siempre que el citado tratamiento no se base en otra causa que lo legitime;
- El interesado ejerce el derecho de **oposición**;
- Los datos personales hayan sido tratados **ilícitamente**;
- Los datos personales deban **suprimirse** para el **cumplimiento** de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento;
- Los datos personales se hayan obtenido en relación con la oferta de **servicios de la sociedad de la información** mencionados en el **artículo 8, apartado 1 del RGPD**.

DERECHO A LA LIMITACIÓN DEL TRATAMIENTO

Este derecho faculta al interesado a obtener del responsable del tratamiento la limitación del tratamiento de los datos cuando se cumpla alguna de las condiciones siguientes:

- El interesado impugne la exactitud de los datos personales, durante un plazo que permita al responsable verificar la exactitud de los mismos;
- El tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso;
- El responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones;
- El interesado se haya opuesto al tratamiento en virtud del artículo 21 del RGPD mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado.

DERECHO A LA PORTABILIDAD DE LOS DATOS

La finalidad de este derecho es reforzar el control que tienen las personas, de forma que cuando el tratamiento se efectúe por medios automatizados, **reciba sus datos personales en un formato estructurado**, de uso común, de lectura mecánica e interoperable, y pueda transmitirlos posteriormente a otro responsable del tratamiento, siempre que el tratamiento se legitime en base al consentimiento o en el marco de la ejecución de un contrato

<https://help.twitter.com/es/managing-your-account/how-to-download-your-twitter-archive>

<https://www.aepd.es/es/derechos-y-deberes/conoce-tus-derechos/derecho-la-portabilidad>

DERECHO A NO SER OBJETO DE DECISIONES INDIVIDUALIZADAS

Este derecho tiene mucho impacto en proyectos Big Data, pretende garantizar a las personas que no sean objeto de una decisión basada únicamente en el tratamiento de sus datos, incluida la elaboración de **perfiles**.

Como elaboración de perfiles entendemos toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física.

Véase art. 4.4 del RGPD

DERECHO DE INFORMACIÓN

Cuando se recaban datos de carácter personal, el responsable del tratamiento debe cumplir con el derecho de información.

Para dar cumplimiento a este derecho, la AEPD recomienda que esta información se facilite por **capas o niveles** de manera que:

- Se te facilite una **información básica en un primer nivel**, de forma resumida, en el mismo momento y en el mismo medio en que se recojan datos personales.
- Y, por otra parte, se te remita el resto de la información, en un medio más adecuado para su presentación, compresión y, si se desea, archivo.

<https://www.aepd.es/es/derechos-y-deberes/conoce-tus-derechos/derecho-de-informacion>

Conclusiones

A los usuarios que nos facilitan sus datos hay que darles **transparencia**

- ¿qué información se recolecta, cómo se procesa, con qué finalidades y si será transferida a terceros?

La transparencia es un punto vital del análisis de conjuntos de datos utilizando Big Data, y es el primer paso para que **cada persona tenga el control sobre sus datos**.

En la práctica *la transparencia no es algo fácil*, muchas organizaciones se escudan en el **secreto industrial** para obviar el "cómo" por razones de confidencialidad comercial.

Conclusiones

Es muy importante Obtener el **consentimiento expreso**.

Una vez que la persona ha sido debidamente informada de forma clara y transparente se deberá obtener su consentimiento en relación con el uso de información personal para fines concretos de análisis y de creación de perfiles.

libre, específico,
inequívoco, informado
y explícito

Conclusiones

Respetar el principio de **calidad** de los datos y la **minimización** de los mismos.

La recolección y el tratamiento masivo de datos se deberá limitar única y exclusivamente a los **datos necesarios** para los fines, debidamente informados y que sean necesarios para el propósito legítimo que se pretende.

Conclusiones

Se deberá contemplar y respetar los **derechos de los ciudadanos**.

Los derechos otorgados en las diferentes normativas de protección de datos son la gran baza que tienen todas las personas para tener un control efectivo sobre sus datos personales.

Conclusiones

Realizar una **evaluación de impacto en la privacidad**, especialmente cuando el análisis del Big Data implica **usos novedosos o inesperados** de los datos personales.

Las evaluaciones de impacto de privacidad son parte integral de la adopción de un enfoque de **privacidad por diseño** y son una herramienta que permite identificar y reducir los riesgos sobre la **privacidad** de los ciudadanos.

Además ayuda a diseñar procesos más eficientes y efectivos en el manejo de datos

- [Guía Práctica de Análisis de Riesgos en los Tratamientos de Datos Personales sujetos al RGPD](#)
- [Herramienta FACILITA](#)







Conclusiones

Anonimizar los datos personales permite mejorar la protección de la privacidad.

La anonimización puede ayudar a mitigar los riesgos asociados con el análisis en Big Data en el caso de brecha o quiebra de seguridad, pero sólo si la anonimización está diseñada y gestionada apropiadamente.

La solución óptima para anonimizar los datos de un conjunto debe decidirse caso por caso, posiblemente utilizando una combinación de técnicas.

Adaptación al RGPD – Sector privado

-  — **1.** Designación del **DELEGADO DE PROTECCIÓN DE DATOS (DPD)** si es obligatorio para la empresa o si lo asume voluntariamente. En caso de no ser necesario designar un DPD, identificar a la/s persona/s responsables de **COORDINAR LA ADAPTACIÓN**
-  — **2.** Elaborar el **REGISTRO ACTIVIDADES DE TRATAMIENTO** teniendo en cuenta su finalidad y la base jurídica
-  — **3.** Realizar un **ANÁLISIS DE RIESGOS** (*guía práctica*)
-  — **4.** Revisar **MEDIDAS DE SEGURIDAD** a la luz de los resultados del análisis de riesgos tanto para garantizar la integridad, confidencialidad y disponibilidad de los datos como para salvaguardar los derechos y libertades de las personas
-  — **5.** Establecer mecanismos y procedimientos necesarios para realizar la **NOTIFICACIÓN DE QUIEBRAS DE SEGURIDAD**
-  — **6.** A partir de los resultados del análisis de riesgos, realizar, en su caso, una **EVALUACIÓN DE IMPACTO EN LA PROTECCIÓN DE DATOS** (*guía práctica*)

Actuaciones simultáneas a los pasos anteriores:



— Adecuar los **FORMULARIOS** *derecho de información*



— Adaptar los **MECANISMOS Y PROCEDIMIENTOS** para el ejercicio de derechos utilizando servicios web siempre que sea posible



— Valorar si los **ENCARGADOS** ofrecen garantías y *realizar la adaptación de sus contratos al RGPD*



— Elaborar / Adaptar **POLÍTICA DE PRIVACIDAD**

En todo caso, es imprescindible documentar todas las actuaciones realizadas para poder acreditar la diligencia en el *cumplimiento del RGPD*.

Tema 4 Medidas de Protección de Datos de Carácter Personal

Interesante las nuevas cláusulas de transferencias internacionales de datos UE

https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en)

Volvemos sobre ello al final del tema

Publicidad

Limitación de la actividad publicitaria de las empresas: las “listas Robinson”

Los ciudadanos pueden registrarse en los sistemas de exclusión publicitaria (las conocidas como “Listas Robinson” www.listarobinson.es) para evitar la publicidad no deseada a través de los canales postal, telefónico o electrónico.

Los ciudadanos registrados en las Listas Robinson solo recibirán publicidad de las empresas que hayan autorizado.

Como ejercicio se propone que os inscribáis en la lista Robinson

Lecturas recomendadas

[Introducción al Hash como técnica de seudonimización de datos personales](#)

En el documento se analizan las fuentes de riesgo de reidentificación en la aplicación de técnicas de hash y se establece la necesidad de realizar un análisis objetivo de estos riesgos para determinar la adecuación de este como técnica de seudonimización o incluso anonimización

[Guía de Privacidad desde el diseño](#)

El objetivo es que la protección de datos esté presente desde las primeras fases de desarrollo y no sea una capa añadida a un producto o sistema. La privacidad debe formar parte integral de la naturaleza de dicho producto o servicio.

[LOPD: Novedades para el Sector Privado](#)

Recopilación de novedades para el sector privado de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales

Ojo: Partimos de la base de que si los datos personales son de personas físicas europeas (aunque la empresa que los trate no lo sea), se tratan en algún Estado miembro de la UE o la organización es europea, se aplica el RGPD.

Origen de esta normativa:

La **Organización para la Cooperación y el Desarrollo Económicos (OCDE)**, fue la primera en adoptar un documento con implicaciones internacionales en materia de protección de datos personales y privacidad en los 80.

Las directrices de la OCDE constituyen un referente, tanto en la Unión Europea como en otras latitudes alrededor del mundo que incluyen países tales como Israel, Japón, Australia, Canadá, Chile, México, Estados Unidos ...

En Europa se adopta el **Convenio 108 del Consejo de Europa**, del 28 de enero de 1981 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. En Europa veremos dos épocas: Directiva y Reglamento.

Ojo: Partimos de la base de que si los datos personales son de personas físicas europeas (aunque la empresa que los trate no lo sea), se tratan en algún Estado miembro de la UE o la organización es europea, se aplica el RGPD.

En Europa veremos dos épocas:

- La Unión Europea adoptó la **Directiva** 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.
- Posteriormente, en 2016: **REGLAMENTO** (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (RGPD)- **Vigente**

Organización de Estados Americanos (OEA):

Desde el año 1996 la Asamblea General de la OEA resoluciones sobre protección de datos personales. El Comité Jurídico Interamericano (CJI) en 2000 presentó un documento sobre “El Derecho de la información: acceso y protección de la información y datos personales en formato electrónico.” En 2012 el CJI “Propuesta de Declaración de Principios de Privacidad y Protección de Datos Personales en las Américas” y en 2015, la “Guía Legislativa sobre la Privacidad y la Protección de Datos Personales en las Américas”. El 9 de abril de 2021, el CJI aprobó los Principios Actualizados sobre la Privacidad y la Protección de Datos Personales, con Anotaciones, que reconocen la importancia de promover el desarrollo y la armonización jurídica en el continente en esta temática, así como la transparencia en el tratamiento de estos datos, la rendición de cuentas por parte de los controladores y encargados, la seguridad de los datos sensibles, la agilización del comercio nacional e internacional y el empoderamiento de los ciudadanos respecto del tratamiento de sus datos personales.

América latina: observatorio legislativo ciber: <https://observatoriolegislativocele.com/documentacion/>

Brasil: [LEI Nº 13.709, DE 14 DE AGOSTO DE 2018](#). Inspiración del RGPD, entró en vigor en enero del 2021, sanciones a partir de agosto del 2021.

- Regula la transferencia de datos. Si bien cuando se trata de un tercer Eº no especifica las excepciones debiendo acudir a su Autoridade Nacional de Proteção de Dados. Ciertamente es que, se basa en los Ppos del RGPD
- Control por los ciudadanos de sus datos personales: exige **consentimiento explícito** para obtención y tratamiento, y contempla derechos ARCO.
- En cuanto al tratamiento de datos de menores la norma brasileña establece la protección en la mayoría de edad (No en el tope mínimo europeo de 13 /España 14)
- prevé multas pecuniarias por valor del 2% de la facturación nacional con un techo máximo de 50 millones de reales, aproximadamente 7,8 millones € (RGPD hasta 20 millones de euros para infracciones muy graves, la cuantía podría ascender al 4% de la facturación internacional).
- Respecto a la notificación de brechas de seguridad la norma es ambigua, no especifica un plazo concreto como sí hace el RGPD (72h máximo).

Chile: [ley de protección de datos personales \(ley 19.628\)](#) norma de 1999 por lo que carente de la cultura de protección de datos actual. Si bien alguna de las funciones de protección de datos han recaído en el [Consejo para la Transparencia](#)

Es por ello **que se prevé una nueva norma** que sí se adapta a los Principios de: licitud del tratamiento, finalidad, proporcionalidad; calidad, responsabilidad, seguridad, transparencia e información y confidencialidad. Que contempla los derechos ARCO+portabilidad

Se basa en el consentimiento expreso como norma general y las excepciones a esa base legal serían (que también hacen lícito el tratamiento): fuentes de acceso

público; tratamiento de datos relativos a obligaciones de carácter económico, bancario o comercial; tratamiento de datos sea necesario para la formulación, ejercicio o defensa de un derecho ante los tribunales de justicia (Como sucede con el RGPD y la LOPDygd).

Prevé infracciones en leves, graves y gravísimas: sancionables con amonestación escrita o multa de 1 a 100 UTM, las graves con multa de 101 a 5.000 UTM y las gravísimas con multa de 5.001 a 10.000 UTM respectivamente.

Colombia: normativa principal: art 15 Constitución Política de Colombia, la [Ley 1581 de 2012](#): Ley de Protección de Datos Personales el [Decreto 1377 de 2013](#): Reglamento de desarrollo Ley, el [Decreto 1074 de 2015](#) (Sector Comercio, Industria y Turismo).

Recoge derechos ARCO

Principios: legalidad, finalidad, consentimiento, veracidad, calidad, transparencia, acceso y circulación restringida, seguridad, confidencialidad.

Clasificación de los datos en públicos, privados, semiprivados, sensibles y aquellos que están relacionados con los niños, niñas y adolescentes.

Las sanciones previstas son de hasta 2.000 salarios mínimos mensuales legales vigentes

Ampliar información:

<https://repository.ucatolica.edu.co/bitstream/10983/23060/1/La%20Ley%20De%20Protecci%C3%B3n%20De%20Datos%20En%20Colombia.pdf>

Guatemala:

Artículos 24 y 31 la Constitución Política de la República de Guatemala

[Ley de Libre Acceso a la Información Pública](#), 2009.

Información sobre la normativa previa: https://www.ipandetec.org/wp-content/uploads/2019/01/EDP_Guatemala.pdf

[Proyecto de Ley de Protección de Datos Personales – 2021](#): adecuación al ámbito europeo de protección de datos que se sustenta en el Habeas data, la responsabilidad, tal y como venimos estudiando.

Regla general: Consentimiento (escrito/electrónico). Excepción: existencia de autorización judicial, investigación, estudios estadísticos, encuestas o conocimiento de interés público.

Derechos: ARCO

Principios: seguridad, confidencialidad, calidad de datos

Ecuador:

Art. 66.19 Constitución de Ecuador (Protección de datos)

LOPD: vigor en 26 mayo 2021; sanciones a partir de los 2 años de la entrada en vigor mayo 2023.

Influencia europea pretende garantizar los derechos de los ciudadanos respecto de sus datos personales.

Principios del tratamiento de datos personales: juridicidad, lealtad y transparencia, legitimidad, finalidad, pertinencia y minimización de los datos personales, así como la proporcionalidad del tratamiento, consentimiento, confidencialidad, calidad, conservación y seguridad.

principio de responsabilidad proactiva y demostrada el que constituya el eje central de la normativa.

Principio que requiere no sólo una actitud diligente por parte de las organizaciones a la hora de cumplir con lo establecido, sino también estar en todo momento en disposición de acreditar la implementación de mecanismos efectivos para la protección de los datos personales que les han sido encomendados.

Derechos: Arco+ portabilidad+ actualización, limitación, consulta + no decisiones únicamente automatizadas+ **educación digital**

Vulneración de seguridad, se fija un plazo de **tres días** desde su detección para notificar a la Autoridad de Protección de Datos Personales y a la Agencia de Regulación y Control de las Telecomunicaciones.

Sanciones: entre el **0.7% y el 1%** volumen de negocios, ejercicio económico anterior

México:

[Ley Federal De Protección De Datos Personales en Posesión de los Particulares](#) de 2017

[Reglamento de desarrollo.](#)

[Otra normativa](#)

Principios: licitud, consentimiento, información, calidad (exactos, completos, pertinentes, correctos y actualizados); finalidad, lealtad, proporcionalidad (necesarios, adecuados y relevantes) y responsabilidad.

Derechos: ARCO – No portabilidad o desindexación (olvido)

Quien se encarga de su garantía es el [Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales](#) ("INAI")

- [Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales](#)
- [Guías de PDP emitidas por el INAI](#)
- [Documentos y guías para sector privado emitidas por INAI](#)
- [Diccionario Protección Datos Personales publicado por el INAI.](#)

Perú:

Art. 2.6 Constitución de Perú.

[Ley N° 29733 LPDP](#) y su reglamento aprobado por Decreto Supremo N° 03-2013-JUS
<https://diariooficial.elperuano.pe/pdf/0036/ley-proteccion-datos-personales.pdf>

Principios: legalidad, consentimiento (Libre, expreso, previo e informado), finalidad, proporcionalidad, calidad, seguridad.

Derechos: información , ARCO,

[Más información sobre normativa sectorial](#)

Guías: <https://www.gob.pe/institucion/anpd/informes-publicaciones/460307-material-informativo>

La transferencia de datos en ESTADOS UNIDOS

- .- Ley Federal de Privacidad de 1974.
- .- Ley Federal CAN-SPAM (Controlling the Assault of Non-Solicited Pornography And Marketing Act) de 2003.

La transferencia de datos UE- terceros Estados

Como sabemos en UE la protección de datos es considerado un Derecho fundamental: goza de especial protección legal.

En la UE el **RGPD** es el marco normativo de **referencia y exige** que los datos de carácter personal sean transferidos bajo **estándares de protección similares**: no se trata de prohibir la transferencia de datos sino de garantizar los Derecho de las personas.

Sin embargo **no define qué hemos de atender por nivel adecuado de protección** siendo el TJUE y las instituciones europeas las que tratan de definir este concepto indeterminado.

[Art 45 RGPD](#)- La realidad establece que se cumple si existen decisión de la Comisión, certificaciones, normas empresariales/códigos de conducta...

Esta situación derivó en las dos sentencias [Schrems I](#) y [Schrems II](#)

1º Safe Harbor- puerto seguro- Schrems I

2º Privacy Shield- escudo de privacidad- Schrems II

Actualmente: Marco Transatlántico de Protección de Datos

No parte como en Europa o América Latina del habeas data (de considerar la protección de datos como derecho fundamental), sino del Principio de Responsabilidad. Debemos acudir a las normas de los distintos estados para conocer la protección específica

OJO DEROGADO (en teoría el escudo no funciona, la práctica es otra cosa)

La Comisión: Decisión de Ejecución (UE) 2016/1250 de 12 de julio de 2016 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo sobre la adecuación de la protección conferida por un nuevo esquema denominado **“Escudo de Privacidad UE-EEUU-Privacy Shield”**: Se basaba en un **sistema de auto certificación** por el que **las entidades estadounidenses se comprometen a cumplir** una serie de principios de protección de la vida privada establecidos por el Departamento de Comercio de Estados Unidos. [Guía del escudo de privacidad de la AEPD](#)

Previamente [Puerto seguro-Safe Harbor: acuerdo](#) que permite transferencia internacional de datos UE-USA de finales de los '90- Schrems I invalidación del acuerdo por no proteger USA los datos de los ciudadanos europeos, ¿os suena Snowden y los programas USA de espionaje?

La transferencia de datos UE- USA

Schrems I - Safe Harbor- puerto seguro

TJUE confirmó que USA participaba en una vigilancia masiva indiscriminada de los ciudadanos europeos y que el Safe Harbor no proporcionaba un nivel adecuado de protección, permitía la injerencia en los derechos fundamentales de los ciudadanos europeos por parte de las autoridades norteamericanas y la existencia de una falta de control jurisdiccional por parte de USA frente a la protección de datos

La transferencia de datos UE- USA

Tras Schrems I se hicieron varias **reformas-Escudo de Privacidad**:

Ámbito de aplicación: las transferencias internacionales de carácter comercial como al acceso de las autoridades públicas de USA. a los datos transferidos desde la UE, incluso por causas de seguridad nacional.

Los operadores bajo el **Escudo de Privacidad** se encontraban sujetos a compromisos con respecto a los **límites de retención de datos, derechos de acceso, publicidad de políticas de privacidad**, etc.

Respecto al funcionamiento de los poderes públicos estadounidenses, la adhesión a ***los principios se limita a lo estrictamente necesario para satisfacer las exigencias de seguridad nacional, interés público o aplicación de la ley.***

El Gobierno estadounidense creó el ***Defensor del Pueblo***, un mecanismo de supervisión de las injerencias con fines de seguridad nacional, dentro del Departamento del Estado, y era responsable de ***la investigación de los casos presentados por las autoridades europeas en protección de datos.***

No parte como Europa o América Latina del habeas data (de considerar la protección de datos como derecho fundamental), sino del Principio de Responsabilidad.

OJO DEROGADO-EN TEORÍA EL ESCUDO NO FUNCIONA, LA PRÁCTICA ES OTRA COSA

Schrems II: El 16 de julio de 2020, el **Tribunal de Justicia de la Unión Europea (TJUE)** emitió una [sentencia](#) declarando como **'inválida'** la **Decisión 2016/1259**. En cambio, declara que la **Decisión 2010/87** de la Comisión, relativa a **las cláusulas contractuales** tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, **es válida**. (cláusulas contractuales estándar adoptadas por la Comisión Europea para realizar transferencias internacionales de datos entre un responsable establecido en la Unión Europea y un encargado del tratamiento fuera de la UE.

Se permite seguir realizando las [transferencias internacionales con garantías](#) por parte del receptor de dichos datos (USA), siempre y cuando el Gobierno americano no realice una intromisión, en cuyo caso el contrato sería declarado nulo.

No parte como Europa o América Latina del habeas data (de considerar la protección de datos como derecho fundamental), sino del Principio de Responsabilidad.

Marco Transatlántico de Protección de Datos

El 25/Mar. 22 la Unión Europea y los Estados Unidos, anunciaron nuevo acuerdo sobre el marco legal de las transferencias de datos personales entre ambos territorios.

El nuevo marco marca un compromiso sin precedentes por parte de Estados Unidos para aplicar **reformas que reforzarán las protecciones de la privacidad y las libertades civiles aplicables a las actividades de inteligencia de señales de Estados Unidos**. En virtud del Marco Transatlántico de Privacidad de Datos, Estados Unidos establecerá nuevas salvaguardias para garantizar que las actividades de vigilancia de señales **sean necesarias y proporcionadas para la consecución de los objetivos de seguridad nacional definidos**, establecerá un **mecanismo de reparación independiente de dos niveles** con autoridad vinculante para dirigir las medidas correctoras, y mejorará **la supervisión rigurosa y por niveles de las actividades de inteligencia** de señales para garantizar el cumplimiento de las limitaciones de las actividades de vigilancia.

Cada Estado tiene su propia normativa.

5 Estados se han adecuando al RGPD el 1º California

California: [Ley de Privacidad para Consumidores de California](#) (California Consumer Privacy Act, "CCPA") **en vigor desde el 2020**. Aplica a empresas con 25 millones de dólares en ingresos o que almacenan los datos de al menos 50.000 consumidores.

(Espíritu europeo).

Principios que incorpora: Información, consentimiento, finalidad...

Derechos: ARCO + portabilidad

Introduce obligaciones del consentimiento paterno para menores 13.

Prevé multas de hasta 7.500\$ (6.750€) **por cada archivo afectado**.

El 3-11-2020 se aprobó la [Ley de derechos de privacidad de California](#), «The California Privacy Rights Act Of 2020» (CPRA), que entrará en vigor el 1 de febrero de 2023.

Esta nueva ley introduce diversas enmiendas a la CCPA con las que incrementa los derechos de los consumidores y establece un nuevo organismo de ejecución, la Agencia de Protección de la Privacidad de California. Al fortalecer las normas de privacidad, parece buscar la alineación del sistema de protección en California al de la Unión Europea, para facilitar las transferencias de datos

La transferencia de datos UE- USA, terceros Estados

Art 45.2 RGPD. Al evaluar la adecuación del nivel de protección, **la Comisión** tendrá en cuenta, en particular, los siguientes elementos:

a) **El Estado de Derecho**, el respeto de los derechos humanos y las libertades fundamentales, la legislación pertinente, tanto general como sectorial, incluida la relativa a la seguridad pública, la defensa, la seguridad nacional y la legislación penal, y el acceso de las autoridades públicas a los datos personales, así como la aplicación de dicha legislación, **las normas de protección de datos**, las normas profesionales y las **medidas de seguridad**, incluidas las normas sobre transferencias ulteriores de datos personales a otro tercer país u organización internacional observadas en ese país u organización internacional, la jurisprudencia, así como el reconocimiento a los interesados cuyos datos personales estén siendo transferidos de derechos efectivos y exigibles y de recursos administrativos y acciones judiciales que sean efectivos;

La transferencia de datos UE- USA, terceros Estados

Art 45.2 RGPD. Al evaluar la adecuación del nivel de protección, la Comisión tendrá en cuenta, en particular, los siguientes elementos:

- b) **La existencia y el funcionamiento efectivo de una o varias autoridades de control independientes** en el tercer país o a las cuales esté **sujeta una organización internacional**, con la responsabilidad de garantizar y hacer cumplir las normas en materia de protección de datos, incluidos poderes de ejecución adecuados, de asistir y asesorar a los interesados en el ejercicio de sus derechos, y de cooperar con las autoridades de control de la Unión y de los Estados miembros, y
- c) Los **compromisos internacionales** asumidos por el tercer país u organización internacional de que se trate, u otras obligaciones derivadas de **acuerdos o instrumentos jurídicamente vinculantes**, así como de su participación en sistemas multilaterales o regionales, en particular en relación con la protección de los datos personales.

La transferencia de datos UE- USA

¿Por qué seguimos con la vista en USA?

La seguridad nacional USA: la [Clarifying Lawful Overseas Use of Data Act o Cloud Act, 2018, HR 4943](#) permite el acceso de las autoridades norteamericanas a datos almacenados en servidores de sus empresas situados en el extranjero, al amparo de una orden judicial pero sin cumplir normativa nacional en la que se encuentran los datos

La transmisión generalizada e indiferenciada de datos por parte de los proveedores de servicios de comunicaciones electrónicas para su comunicación a las agencias de seguridad e inteligencia excede los límites de lo necesario y resulta contrario a la Carta de los Derechos Fundamentales de la Unión Europea

Ello hace que las STJUE se muestren contrarias a las prácticas norteamericanas:

- STJUE de 6 de octubre de 2020, Privacy International, C-623/17. EU:C:2020:790, apdos. 76-82.
- Sentencia del TJUE de 6 de octubre de 2020, La Quadrature du Net y otros, C-511/18, C-512/18 y C-520/18. EU:C:2020:791, apdos. 175 y 176.

La transferencia de datos UE- USA

El resultado de todo lo anterior nos lleva nuevamente a considerar la fuerza centrípeta del RGPD a nivel global incidiendo en empresas y Estados (California)

Estandarización como respuesta a la pluralidad normativa

Un ejemplo sobre la estandarización : [Microsoft](#)

[Garantías para las transferencias de datos personales a terceros países u organizaciones internacionales](#)

... no hay mejor camino para hallar la felicidad,
que el conocimiento.



Universidad
Internacional
de Valencia

