TEMA 5. LA PROTECCIÓN DE DATOS PERSONALES

I- LAS AGENCIAS DE PROTECCIÓN DE DATOS

- **Agencia Española de Protección de Datos:** la autoridad pública independiente encargada de velar por la privacidad y la protección de datos de los ciudadanos.

- La AEPD protege los derechos de acceso, rectificación, limitación, oposición, supresión ("derecho al olvido"), portabilidad y oposición al tratamiento de decisiones automatizadas.
- Antes de interponer una reclamación sobre derechos ante la AEPD, es necesario dirigirse al responsable por un medio que permita acreditarlo y ejercerlos.

https://www.aepd.es/

- **Autoritat Catalana de Protecció de Dades:** organisme independent que vetlla per garantir, en l'àmbit de les competències de la Generalitat, els drets a la protecció de dades personals i d'accés a la informació que hi està vinculada. Des d'aquest organisme, s'informa sobre quins són els drets en aquesta matèria, com s'exerceixen i què s'ha de fer si no es respecten. L'APDCAT també informa i assessora sobre les obligacions que preveu la legislació i controla que les entitats les compleixin.

http://apdcat.gencat.cat/ca/inici

L'àmbit d'actuació de l'Autoritat Catalana de Protecció de Dades comprèn els fitxers i els tractaments que duen a terme:

- *Les institucions públiques.*

- *L'Administració de la Generalitat.*
- *Els ens locals.*
- *Les entitats autònomes, els consorcis i les altres entitats de dret públic vinculades a l'Administració de la Generalitat o als ens locals, o que en depenen.*
- *Les entitats de dret privat que compleixen, com a mínim, un dels tres requisits següents amb relació a la Generalitat, als ens locals o als ens que en depenen:*
    - *El seu capital pertany majoritàriament als ens públics esmentats.*
    - *Els seus ingressos pressupostaris provenen majoritàriament dels ens públics esmentats.*
    - *En els seus òrgans directius, els membres designats per aquests ens públics són majoria.*
- *Les altres entitats de dret privat que presten serveis públics per mitjà de qualsevol forma de gestió directa o indirecta, si es tracta de fitxers i tractaments vinculats a la prestació d'aquests serveis.*
- *Les universitats públiques i privades que integren el sistema universitari català, i els ens que en depenen.*
- *Les persones físiques o jurídiques que compleixen funcions públiques amb relació a matèries que són competència de la Generalitat o dels ens locals, si es tracta de fitxers o tractaments destinats a exercir aquestes funcions i el tractament es duu a terme a Catalunya.*
- *Les corporacions de dret públic que compleixen les seves funcions exclusivament en l'àmbit territorial de Catalunya, als efectes del que estableix aquesta llei.*

II.- EL REGLAMENTO EUROPEO 2016/679 , DE 27 DE ABRIL DE 2016, GENERAL DE PROTECCIÓN DE DATOS (RGPD)

1) Origen del RGPD y aplicabilidad directa

- El 25 de mayo de 2016 entró en vigor el Reglamento General de Protección de Datos (RGPD), y que comenzó a aplicarse el 25 de mayo de 2018. Este periodo de dos años tuvo como objetivo permitir que los Estados de la Unión Europea, las Instituciones y también las empresas y organizaciones que tratan datos fueran preparándose y adaptándose para el momento en que el Reglamento fuera aplicable.

- El Reglamento europeo es directamente aplicable, por lo que a diferencia de la Directiva 95/46 no necesita ser transpuesto al ordenamiento jurídico español.

- Este reglamento atiende a nuevas circunstancias provocadas fundamentalmente por el aumento de los flujos transfronterizos de los datos personales como consecuencia de la actividad del mercado interior, teniendo en cuenta que la rápida evolución tecnológica y la globalización han provocado que esos datos sean un recurso fundamental para la sociedad de la información. Ante esta situación, han aumentado los riesgos inherentes a que las informaciones sobre los individuos se hayan multiplicado de forma exponencial siendo más accesibles y más fáciles de procesar, al tiempo que se ha hecho más difícil el control de su uso y destino.

2) Derechos que el RGPD otorga al ciudadano

- El Reglamento otorgó nuevos derechos para el ciudadano que son los siguientes:

- acceso,
- rectificación,
- oposición,
- supresión (“derecho al olvido”),
- limitación del tratamiento,
- portabilidad
- y de no ser objeto de decisiones individualizadas

- **El derecho al olvido:**
  El derecho al olvido se presenta como la consecuencia del derecho que tienen los ciudadanos a solicitar, y obtener de los responsables, que los datos personales sean suprimidos cuando, entre otros casos, estos ya no sean necesarios para la finalidad con la que fueron recogidos, cuando se haya retirado el consentimiento o cuando estos se hayan recogido de forma ilícita. Asimismo, según la sentencia del Tribunal de Justicia de la Unión Europea de 13 de mayo de 2014, que reconoció por primera vez el derecho al olvido recogido ahora en el Reglamento europeo, supone que el interesado puede solicitar que se bloqueen en las listas de resultados de los buscadores los vínculos que conduzcan a informaciones que le afecten que resulten obsoletas, incompletas, falsas o irrelevantes y no sean de interés público, entre otros motivos.

- **El derecho a la portabilidad** implica que el interesado que haya proporcionado sus datos a un responsable que los esté tratando de modo automatizado podrá solicitar recuperar esos datos en un formato que le permita su traslado a otro responsable. Cuando ello sea técnicamente posible, el responsable deberá trasferir los datos directamente al nuevo responsable designado por el interesado.

3) ¿A qué empresas u organizaciones se aplica el RGPD?

El Reglamento se aplica a responsables o encargados de tratamiento de datos establecidos en la Unión Europea, y se amplía a responsables y encargados no establecidos en la UE siempre que realicen tratamientos derivados de una oferta de bienes o servicios destinados a ciudadanos de la Unión o como consecuencia de una monitorización y seguimiento de su comportamiento.

Para que esta ampliación del ámbito de aplicación pueda hacerse efectiva, esas organizaciones deberán nombrar un representante en la Unión Europea, que actuará como punto de contacto de las Autoridades de supervisión y de los ciudadanos y que, en caso necesario, podrá ser destinatario de las acciones de supervisión que desarrollen esas autoridades. Los datos de contacto de ese representante en la Unión deberán proporcionarse a los interesados

entre la información relativa a los tratamientos de sus datos personales.

Esta novedad ha supuesto una garantía adicional a los ciudadanos europeos. En la actualidad, para tratar datos no es necesario mantener una presencia física sobre un territorio, por lo que el Reglamento pretende adaptar los criterios que determinan qué empresas deben cumplirlo a la realidad del mundo de internet.

Ello permite que el Reglamento sea aplicable a empresas que, hasta ahora, podían estar tratando datos de personas en la Unión y, sin embargo, se regían por normativas de otras regiones o países que no siempre ofrecen el mismo nivel de protección que la normativa europea.

4) **¿A qué edad pueden los menores prestar su consentimiento para el tratamiento de sus datos personales?**

El Reglamento establece que la edad en la que los menores pueden prestar por sí mismos su consentimiento para el tratamiento de sus datos personales en el ámbito de los servicios de la sociedad de la información (por ejemplo, redes sociales) es de 16 años. Sin embargo, permite rebajar esa edad y que cada Estado miembro establezca la suya propia, estableciendo un límite inferior de 13 años. En el caso de España, ese límite continúa en 14 años. Por debajo de esa edad, es necesario el consentimiento de padres o tutores.

En el caso de las empresas que recopilen datos personales, es importante recordar que el consentimiento tiene que ser verificable y que el aviso de privacidad debe estar escrito en un lenguaje que los niños puedan entender.

5) **¿Qué implica la responsabilidad activa recogida en el Reglamento?**

Uno de los aspectos esenciales del Reglamento es que se basa en la prevención por parte de las organizaciones que tratan datos. Es lo que se conoce como responsabilidad activa. Las empresas deben adoptar medidas que aseguren razonablemente que están en condiciones de cumplir con los principios, derechos y garantías que el Reglamento establece. El Reglamento entiende que actuar sólo cuando ya se ha producido una infracción es insuficiente como estrategia, dado que esa infracción puede causar daños a los

interesados que pueden ser muy difíciles de compensar o reparar. Para ello, el Reglamento prevé una batería completa de medidas:

- Protección de datos desde el diseño

- Protección de datos por defecto

- Medidas de seguridad

- Mantenimiento de un registro de tratamientos

- Realización de evaluaciones de impacto sobre la protección de datos

- Nombramiento de un delegado de protección de datos

- Notificación de violaciones de la seguridad de los datos

- Promoción de códigos de conducta y esquemas de certificación.

* El Reglamento supone un mayor compromiso de las organizaciones, públicas o privadas, con la protección de datos. Pero ello no implica necesariamente ni en todos los casos una mayor carga.

En primer lugar, algunas de las medidas que introduce el Reglamento son una continuación o reemplazan a otras ya existentes, como es el caso de las medidas de seguridad o de la obligación de documentación y, hasta cierto punto, la evaluación de impacto y la consulta a Autoridades de supervisión.

Otras constituyen la formalización en una norma legal de prácticas ya muy extendidas en las empresas o que, en todo caso, formarían parte de una correcta puesta en marcha de un tratamiento de datos, como pueden ser la privacidad desde el diseño y por defecto, la evaluación de impacto sobre protección de datos en ciertos casos o la existencia de un delegado de protección de datos.

En todos los casos, el Reglamento prevé que la obligación de estas medidas, o el modo en que se apliquen, dependerá de factores tales como el tipo de tratamiento, los costes de implantación de las medidas o el riesgo que el tratamiento presenta para los derechos y libertades de los titulares de los datos.

Por ello, es necesario que todas las organizaciones que tratan datos realicen un análisis de riesgo de sus tratamientos para poder determinar qué medidas han de aplicar y cómo hacerlo. Estos análisis pueden ser operaciones muy simples en entidades que no llevan a cabo más que unos pocos tratamientos sencillos que no impliquen, por ejemplo, datos sensibles, u operaciones más complejas en entidades que desarrollen muchos tratamientos, que afecten a gran cantidad de interesados o que por sus características requieren de una valoración cuidadosa de sus riesgos.

Las Autoridades de protección de datos europeas de forma colectiva, y la Agencia Española ofrecen herramientas que facilitan la identificación y valoración de riesgos y en recomendaciones sobre la aplicación de medidas, especialmente en relación con pymes que realizan los tratamientos de datos más habituales en la gestión empresarial.

6) Importancia del consentimiento

Una de las bases fundamentales para tratar datos personales es el consentimiento. El Reglamento pide que el consentimiento, con carácter general, sea libre, informado, específico e inequívoco. Para poder considerar que el consentimiento es inequívoco, el Reglamento requiere que haya una declaración de los interesados o una acción positiva que indique el acuerdo del interesado. El consentimiento no puede deducirse del silencio o de la inacción de los ciudadanos.

Las empresas han tenido que revisar la forma en la que obtenían y registraban el consentimiento. Prácticas que se encuadraban en el llamado consentimiento tácito y que antes eran aceptadas en la anterior normativa han dejado de serlo con el RGPD.

Además, el Reglamento prevé que el consentimiento tiene que ser explícito en algunos casos, como puede ser para autorizar el tratamiento de datos sensibles. Se trata de un requisito más estricto, ya que el consentimiento no podrá entenderse como concedido implícitamente mediante algún tipo de acción positiva. Así, será preciso que la declaración u acción se refieran explícitamente al consentimiento y al tratamiento en cuestión.

Hay que tener en cuenta que el consentimiento tiene que ser verificable y que quienes recopilen datos personales deben ser capaces de demostrar que el afectado les otorgó su consentimiento.

Por ello, es importante revisar los sistemas de registro del consentimiento para que sea posible verificarlo ante una auditoría.

7) ¿Qué información deben recoger los avisos de privacidad a la luz del RGPD?

El Reglamento prevé que se incluyan en la información que se proporciona a los interesados una serie de cuestiones que anteriormente con la Directiva y muchas leyes nacionales de trasposición no eran necesariamente obligatorias.

Por ejemplo, es necesario explicar la base legal para el tratamiento de los datos, los períodos de retención de los mismos y que los interesados puede dirigir sus reclamaciones a las Autoridades de protección de datos si creen que hay un problema con la forma en que están manejando sus datos.

Es importante recordar que el Reglamento exige de forma expresa que la información que se proporcione sea fácil de entender y presentarse en un lenguaje claro y conciso.

8) ¿En qué consiste el sistema de 'ventanilla única'?

Este sistema está pensado para que los responsables establecidos en varios Estados miembros o que, estando en un solo Estado miembro, hagan tratamientos que afecten significativamente a ciudadanos en varios Estados de la UE tengan una única Autoridad de protección de datos como interlocutora.

También implica que cada Autoridad de protección de datos europea, en lugar de analizar una denuncia o autorizar un tratamiento a nivel estrictamente nacional, a partir de la aplicación del Reglamento valorará si el supuesto tiene carácter transfronterizo, en cuyo caso habrá que abrir un procedimiento de cooperación entre todas las Autoridades afectadas buscando una solución aceptable para todas ellas. Si hay discrepancias insalvables, el caso puede elevarse al Comité Europeo de Protección de Datos, un organismo de la Unión integrado por los directores de todas las Autoridades de protección de datos de la Unión. Ese Comité resolverá la controversia mediante decisiones vinculantes para las Autoridades implicadas.

Este nuevo sistema no supone que los ciudadanos tengan que relacionarse con varias Autoridades o con Autoridades distintas de la del Estado donde residan. Siempre pueden plantear sus

reclamaciones o denuncias ante su propia Autoridad nacional (en el caso español, la Agencia Española de Protección de Datos). La gestión será realizada por esa Autoridad, que será también responsable de informar al interesado del resultado final de su reclamación o denuncia.

La ventanilla única, en todo caso, no afectará a empresas que sólo estén en un Estado miembro y que realicen tratamientos que afecten sólo a interesados en ese Estado.