

Actividad: Tratamiento de datos personales. Estudio de caso sobre el cáncer de mama

Objetivos

- Comprender el concepto y el alcance de los datos relativos a la salud, así como su régimen jurídico específico según el RGPD y la legislación nacional aplicable.
- Identificar los aspectos legales, éticos y técnicos que se deben tener en cuenta en el tratamiento de datos personales relativos a la salud con fines de investigación.
- Aplicar los principios y las garantías del RGPD y la legislación nacional aplicable al caso práctico propuesto, proponiendo soluciones adecuadas y razonadas.

Pautas de elaboración

Analiza y resuelve un caso práctico relacionado con el RGPD y los datos de salud, aplicando los conceptos y principios aprendidos. El caso práctico plantea una situación hipotética en la que se produce un tratamiento de datos personales relativos a la salud con fines de investigación. Se te pide que identifiques los aspectos legales, éticos y técnicos implicados, así como las medidas de protección que se deberían adoptar. A continuación, se presenta un ejemplo de caso práctico:

Caso práctico 1: Investigación sobre el cáncer de mama

Un equipo de investigadores de una universidad pública solicita al hospital de referencia de su zona el acceso a los datos personales de las pacientes que han sido diagnosticadas de cáncer de mama en los últimos cinco años, con el fin de realizar un estudio sobre los factores de riesgo y la eficacia de los tratamientos aplicados. El hospital accede a facilitar los datos, siempre que se cumplan las condiciones establecidas por el RGPD y la legislación nacional aplicable.

Preguntas:

1. *¿Qué tipo de datos personales se tratan en este caso?*

En el caso presentado en la actividad nos encontramos con dos tipos de datos personales. Por un lado, aunque no se indica explícitamente, el equipo de

investigadores requiere de **datos personales identificativos** tales como el nombre y apellidos, el DNI, datos de contacto como el teléfono o email, dirección, número de la tarjeta sanitaria, etc. estos, como su nombre indica, nos permiten identificar directamente a una persona. Por este motivo su tratamiento exige de especial precaución. Por otro lado, el grupo requiere de **datos personales relativos a la salud** para la investigación a realizar. Este tipo de datos puede ser:

- El propio diagnóstico de cáncer de mama
- Evolución de la enfermedad
- Fecha del diagnóstico
- Tratamiento recibido y respuesta a este
- Resultados de las pruebas realizadas, así como biopsias, imágenes médicas
- Factores de riesgo asociados tales como los antecedentes familiares, los hábitos de vida, las condiciones en las que se encuentra el paciente, etc.

Este último tipo de datos se consideran especialmente sensibles según el Reglamento General de Protección de Datos (RGPD) y por eso están dentro de una categoría especial.

2. ¿Qué base legal se podría utilizar para el tratamiento de los datos personales con fines de investigación?

Según el RGPD, existen varias bases legales que se pueden utilizar para el tratamiento de estos datos personales con fines de investigación científica, como es el caso de este estudio sobre el cáncer de mama.

En primer lugar, con respecto al tratamiento de datos personales en general, nos encontramos con el **artículo 6** del RGPD. En el cual se recoge que será lícito el tratamiento de datos si cumple al menos una de las siguientes condiciones:

- Hay un **consentimiento del interesado**. Es decir, la persona cuyos datos son tratados consiente de forma libre, informada de forma específica e inequívoca el trato de los mismos.

- Se requiere del **cumplimiento de una obligación legal** del responsable del tratamiento, en el caso de que este tratamiento sea como resultado un proceso legal.
- El tratamiento de estos datos responde a un **interés público**. En este caso podemos poner de ejemplo el propio caso práctico pues la investigación sobre el cáncer de mama es un tema de interés patente en nuestro día a día. Por lo tanto, este puede ser el punto más interesante a la hora de solicitar este tipo de tratamiento de datos.
- Hay un interés **legítimo del responsable del tratamiento de datos** o de un tercero. Siempre y cuando este interés no entre en conflicto con los derechos y libertades fundamentales del interesado que requieran la protección de sus datos personales. En este caso, como el grupo de investigadores pertenecen a una entidad pública, como lo es la universidad, existen ciertas restricciones adicionales.
- Hay un **interés vital del interesado** o de otras personas físicas. En este caso el fin del estudio no responde a una urgencia vital de ningún interesado, sino a una mayor comprensión de los factores de riesgo y la eficacia del tratamiento aplicado. Pero pudiera darse el caso de que una de las personas con dicho tratamiento, u otra ajena al experimento, pero en condiciones similares, requiriese de un análisis profundo y urgente de estos datos para una correcta aplicación del tratamiento (o simplemente para el hecho de empezarlo o no) con el fin de mejorar sus condiciones de vida o para llegar a salvarla, dependiendo de la gravedad del caso.

Si bien existen otras condiciones en las que se puede dar esta licitud de la solicitud del tratamiento de datos, no considero que sean relevantes para este caso en concreto, ya que no parece que se plantee la idea de ningún contrato firmado por ninguna de las partes.

Por otra parte, el tratarse de datos especialmente sensibles y, por lo tanto, encontrarse dentro de categorías especiales de datos del RGPD, podemos recurrir al **artículo 9** del mismo. En este artículo se recogen varias condiciones en las que el tratamiento de **datos relativos a la salud** es lícito. Por el contexto del Caso 1

considero que las condiciones más relevantes a tratar son las siguientes (aun cuando el resto están abiertas a debate):

- El interesado dio su **consentimiento explícito** para el tratamiento de los datos. A igual que nos encontrábamos en el artículo 6.
- El tratamiento es necesario y responde a un **interés público**. Como expliqué en el artículo 6, este puede ser un punto muy interesante a tratar en este caso.
- El tratamiento es necesario para fines de **medicina preventiva o laboral**. En el caso concreto de los datos personales relativos a la salud, este puede ser una condición muy importante. Creo que en el Caso 1 nos encontramos que los requerimientos del grupo de investigación responden a este caso en particular, ya que el fin del estudio es comprender los factores de riesgo y la eficacia de un tratamiento, lo cual podíamos considerar como medicina preventiva.
- El tratamiento es necesario con **fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos**. Por el contexto podemos ver claramente que el tratamiento de estos datos se va a dar con fines de investigación científica. Esto no está reñido con la idea de que pueda, a su vez, tratarse con otros fines como la medicina preventiva.

Al igual que comenté en el caso del artículo 6, existen más condiciones por las que se puede hacer lícito el tratamiento de estos datos, pero no los considero relevantes para el caso a tratar.

3. *¿Qué derechos tienen las pacientes cuyos datos personales se tratan con fines de investigación?*

Todos los derechos que tienen los pacientes cuyos datos personales se tratan con fines de investigación se recogen en el RGPD y, en el ámbito nacional, la **Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD)**. En este caso, al tratarse de un estudio sobre el cáncer de mama, es decir un estudio científico, existen algunas limitaciones específicas de estos derechos. Dentro del RGPD encontramos una serie de artículos (artículos del 15 al 22) que

describen estos derechos y que por la inicial del nombre de cada derecho se conocen como derechos SOPLAR. Estos mismos derechos se recogen en la LOPDGDD, cambiando el orden del artículo. Atendiendo al orden descrito en el RGPD son los siguientes:

- **Derecho al acceso (artículo 15):** describe el derecho a saber si sus datos están siendo tratados. También el de conocer información sobre su finalidad, la duración del tratamiento, sus destinatarios y demás información relevante.
- **Derecho a la rectificación (artículo 16):** permite al paciente corregir datos inexactos o erróneos.
- **Derecho a la supresión (artículo 17):** se conoce como “derecho al olvido” y se trata del derecho a pedir que eliminen sus datos. Este derecho puede ser limitado en caso de investigación científica si la eliminación de ciertos datos puede impedir los objetivos del estudio, como se describe en el propio artículo.
- **Derecho a la limitación del tratamiento (artículo 18):** el paciente limita el uso de sus datos. Este derecho también puede presentar limitaciones en el caso de investigaciones científicas.
- **Derecho a la portabilidad (artículo 20):** consiste en el derecho de cambiar de responsable del tratamiento de datos. Considero que en el caso tratado este derecho no se encuentra muy vigente ya que no existe otra entidad a parte del grupo de investigación que se nos presente con el objetivo de realizar el estudio, pero me parece reseñable mencionarlo ya que es uno de los derechos principales.
- **Derecho a la oposición (artículo 21):** se encarga de la posibilidad de oponerse al tratamiento de los datos. Esta oposición puede ser limitada en el caso de demostrarse un interés público o científico justificado.
- **Derecho a no ser objeto de decisiones automatizadas (artículo 22):** por último, podemos agregar este derecho en el caso de que el sistema de tratamiento de datos sea automatizado. Cualquier respuesta derivada del tratamiento de estos datos que sea automatizada puede ser desechada si

no ha habido intervención humana en el proceso. Este derecho también puede ser limitado en ciertos casos.

Las limitaciones a los derechos por tratarse de una investigación científica podemos encontrarlos en el **artículo 89** del RGPD. En este artículo se indica que se puede limitar ciertos derechos siempre que se cumplan una serie de condiciones tales como que **el tratamiento sea exclusivamente con fines científicos**, se apliquen ciertas **garantías** (pseudonimización, minimización de datos, medidas técnicas y organizativas), que **la aplicación de estos derechos imposibilite o dificulte gravemente la investigación**.

4. *¿Qué medidas de protección se deberían adoptar para garantizar la seguridad y la confidencialidad de los datos personales?*

En el contexto de un estudio sobre el cáncer de mama los datos tratados son datos personales de salud, por lo tanto, las medidas de protección son cruciales ya que son datos especialmente sensibles tanto para el sentido común como para el RPPD. Por este motivo se ha de considerar una serie de medidas para garantizar la confidencialidad y la seguridad de los datos personales, en la medida de lo posible. Algunas de ellas las he mencionado en preguntas anteriores, pero existen otras a tener en cuenta:

- Los datos identificatorios directos se pueden sustituir por códigos (Por ejemplo, nombres por un código) para que no se puedan identificar directamente a la persona sin conocer información adicional, es decir, se **pseudonimizan**. Este cambio por códigos puede ser irreversible para que nunca se puedan vincular estos datos a personas. En ese caso se considera que ha habido una **anonimización** de los datos.
- El acceso a los datos debe ser **limitado a personas autorizadas y necesarias**.
- Los datos en reposo y tránsito deben ser **cifrados**. Esto es especialmente importante habiendo un flujo regular entre el grupo de investigación y el hospital.
- Antes de realizar el tratamiento debemos considerar los riesgos de su trato y minimizar las posibles consecuencias. Esta **evaluación de impacto** es obligatoria cuando se trata de datos de salud a gran escala.

- Se debe tener un **registro de las actividades** del tratamiento en el que se indiquen qué datos se tratan, su fin, qué medidas se aplican y quién accede a ese tratamiento.
- Se debe recopilar y tratar solo aquellos datos **estrictamente necesarios**.
- Debe de haber **contratos y acuerdos de confidencialidad** entre el hospital y la universidad.
- Tiene que haber un **delegado de protección de datos**. Al tratarse de entidades públicas, este punto es de obligatorio cumplimiento.
- Se debe dar **formación a todo el personal** que va a tratar los datos para la protección y seguridad de la información.
- En el caso de cometerse fallos, o producirse una violación de la seguridad, se debe contar con un **plan de actuación** y notificarse a la agencia española de protección de datos (AEPD), en menos de 72 horas si la violación conlleva riesgo para los derechos de las personas.

Estas son las principales medidas a considerar en el caso descrito.

5. *¿Qué papel desempeñan el responsable, el encargado y el delegado de protección de datos en este caso?*

En primer lugar, debemos considerar quién es el responsable, el encargado y el delegado en el caso tratado para poder definir su rol. En el marco de una universidad que solicita al hospital de referencia el acceso a datos de pacientes podemos distinguir los tres roles de la siguiente manera:

- **El responsable del tratamiento:** en este caso considero tanto al hospital como a la universidad como corresponsables del tratamiento de los datos. Su función es la de **determinar los fines y medios del tratamiento de los datos**. Es el responsable de **garantizar que se respeten los principios del RGPD y de la LOPDGDD**, que se apliquen las **medidas técnicas y organizativas adecuadas**, de **informar a los pacientes**, y **demostrar el cumplimiento** de todo lo anterior dicho. Si bien puede que corresponda al hospital la mayoría de estas acciones, puede que la universidad también deba tomar parte a la hora de garantizar, por ejemplo, que se apliquen medidas técnicas y organizativas adecuadas. Por este

motivo podemos considerar al hospital como el responsable o a los dos como corresponsables.

- **Encargado del tratamiento:** en este caso podemos considerar a la universidad como la encargada de realizar el tratamiento de datos. Sus funciones la de **tratar los datos por cuenta del responsable** y este **no decide la finalidad ni los medios esenciales**. Deben firmarse **contratos** en los que se regulen las **condiciones de acceso, la confidencialidad, la seguridad**, etc. Aunque en el enunciado del caso práctico no se menciona, puede que el tratamiento de los datos se externalice a una empresa si la universidad no tiene los medios necesarios para ello. En ese caso el encargado del tratamiento también sería esa empresa.
- **Delegado de protección de datos:** es de obligado nombramiento por parte de cualquier entidad pública y, al tratarse de un hospital y una universidad pública, según el RGPD y la LOPDGDD, debe nombrarse un delegado que cumpla las siguientes funciones:
 - **Supervisar** si se están **cumpliendo las normativas del RGPD y la LOPDGDD**.
 - **Asesorar** en el proceso del tratamiento de datos tanto al responsable como al encargado.
 - Actuar como **nexo entre el responsable y encargado y la AEPD**. Colaborando con esta en caso de fallos o consultas.
 - Debe **participar en la evaluación de impacto** mencionada en la pregunta anterior.

Todos estos roles están abiertos a debate, pero dado el caso presentado, considero que esta es la forma correcta de verlos.