Trabajo Fin de Máster

Dictamen elaborado por

Javier Turón Hernández

Con objeto de

La protección de datos de carácter personal en el ámbito sanitario

Dirigida por

José Félix Muñoz Soro

Facultad de Derecho
Diciembre de 2021

ÍNDICE

I. INTRODUCCIÓN

Como se indica en el Reglamento de los Trabajos de fin de Grado y de Master en la Universidad de Zaragoza, el objeto del presente trabajo es poner de manifiesto los conocimientos, habilidades y aptitudes adquiridas por el estudiante a lo largo de la titulación.

He de confesar que para mí ha supuesto un remarcado desafío frente a una modalidad más teórica y menos práctica a la que venía acostumbrado a dar respuesta, ya que se me plantea la situación futuro profesional del ejercicio de la abogacía de resolver un supuesto. La importancia radica, y es lo que he procurado con el presente Dictamen, en ofrecer una respuesta fundamentada en Derecho y exhaustiva de mis clientes, y finalmente en las conclusiones cristalizar todo el Trabajo de manera numerada y ordenada de los aspectos tratados.

En cuanto a la temática del presente TFM desarrollado a continuación, he deseado aventurarme en una materia sobre la cuál hemos recibido pequeñas pinceladas y que atrae mi atención hasta el punto de querer cursar estudios posteriores sobre la misma, y prácticamente focalizar mi actividad profesional en dicho ámbito.

El Derecho Digital se encuentra en boga y cada vez adquiere una mayor relevancia en el panorama jurídico actual, debido a la irrupción de las nuevas tecnologías y fenómenos como el *big data*, criptomonedas, inteligencia artificial, etc.

La implantación de las nuevas tecnologías ha conllevado un giro radical en el modo de transmisión de los datos personales, como consecuencia directa de ello se ha generado la necesidad de diseñar nuevos modelos de tutela que se enfoquen en dicho ámbito de privacidad.

Con el objeto de acotar el amplio elenco de conceptos que lo integran he decidido centrar mi atención en el planteamiento de un supuesto que versa sobre la fuga de datos personales de un hospital, el cual afecta a miles de personas de distintos rangos de edades, sexo, nacionalidad y raza.

La protección de datos de carácter personal cada vez cobra más importancia en la formación del jurista, muchos de los delitos hoy cometidos se producen en la red y, por ende, se requiere de profesionales cualificados que sepan solucionar dichas cuestiones. Por desgracia, seguimos hallando que muchos de estos profesionales desconocen dicha relevancia, y por ello, los profesionales no son tan numerosos ni cualificados.

Es tal su relevancia que su normativa se encuentra en constante estudio para poder dar respuesta a los distintos supuestos que se originen, hasta el punto de existir un Grupo de Trabajo de la Unión Europea especializado en materia de protección de datos como es el Comité Europeo de Protección de Datos (Anteriormente el Grupo de Trabajo del Artículo 29) y una entidad a nivel nacional de reconocidas competencias como la Agencia Española de Protección de Datos.

Cierto es que en este Trabajo me voy a centrar en datos de carácter sanitario, la legislación vigente en materia sanitaria busca el máximo respeto a la dignidad de la persona y a la libertad individual, y garantizar la salud como derecho inalienable de la población.

La protección de datos de carácter personal tiene un ámbito tan extenso que confluye con la actividad del jurista, siendo un deber del mismo la correcta conservación de los datos de carácter personal de sus clientes.

Si dicho profesional no cumple con lo debido puede incurrir en una vulneración del secreto profesional recogida en el Estatuto General de la Abogacía Española en su capítulo IV, siendo este un principio fundamental a seguir por el abogado con graves consecuencias como la suspensión e inhabilitación del ejercicio, en caso de que normativa específica no recoja la correspondiente sanción.

Para resolver el presente supuesto trataré temas como los principios fundamentales de protección de datos, las figuras del encargado de tratamiento y responsable de tratamiento, las medidas de seguridad que deben adoptar, cómo debieron haber actuado ante la violación de datos de carácter personas y sus consecuencias legales.

Sin olvidar por supuesto a la parte más débil, y la cual ha sufrido un mayor perjuicio, los afectados. Indicaré cuáles son las distintas vías para obtener el resarcimiento de daños y cómo pueden lograr que sus datos de carácter personal se desvinculen de las distintas URL en los que han sido publicados y se eliminen.

DICTAMEN

DICTAMEN que, a petición de Don Juan García Ferrer y Doña María José Martínez Amor emite el Letrado Don Javier Turón Hernández, sobre la posible vulneración de datos de carácter personal por parte del Hospital Santa María del Pilar, el día 13 de julio de 2021, en la ciudad de Zaragoza.

I. ANTECEDENTES DE HECHO

Todos los datos que aparecen aquí reflejados se obtuvieron a partir de la documentación trasladada, escrita, por parte de Don Juan García Ferrer y María José Martínez Amor[1].

PRIMERO: En fecha de junio de 2021 un grupo de quinientos pacientes del Hospital Nuestra Señora de la Salud, situado en Zaragoza (España) observaron que aparecían reflejados en varios portales web como Revisatusalud.com, Consultatussíntomas.com o Descrubretupatología.com, datos de carácter personal, sin consentimiento alguno de dichos pacientes, siendo conocedores que las publicaciones constan en estos portales web desde el año 2019.

SEGUNDO: Los datos de carácter personal publicados de los pacientes versaban sobre todo su historial clínico, desde documentación relativa a la hoja clínicoestadística, hoja de ingreso, órdenes médicas, su evolución, hasta informes de quirófano y anatomías patológicas, ya sean de este Hospital u otro.

[1] Habiendo sido modificados los datos y fechas para no afectar a la verdadera identidad de los implicados.

TERCERO: El Hospital Nuestra Señora de la Salud niega en todo momento haber proporcionado dichos datos de carácter personal a los portales web y alega que los acontecimientos se han sucedido a raíz de una intromisión ilegítima en sus ficheros de datos de carácter personal de los pacientes, habiendo adoptado el Hospital las medidas de seguridad pertinentes reflejadas en la legislación aplicable.

CUARTO: Entre los datos publicados del historial clínico de los pacientes en los portales web anteriormente mencionados, aparecen datos de todos los rangos de edades, incluyendo menores de edad especialmente protegidos. Entre los afectados se encuentra Francisco García Martínez, de 13 años de edad, hijo de Don Juan García Ferrer y María José Martínez Amor, siendo estos los denunciantes de la infracción.

QUINTO: En el caso que nos ocupa El Hospital Nuestra Señora de la Salud ejerce la figura del responsable del tratamiento de datos, cuya función se basa en conservar, proteger y permitir el ejercicio de los derechos relacionados con los datos de carácter personal depositados por los pacientes, en el momento que estos solicitan un tratamiento médico por parte del Hospital. Del mismo modo que se encarga de la llevanza de un registro de actividades del tratamiento.

SEXTO: A su vez el Hospital ha contratado a un encargado de tratamiento que, mediante contrato suscrito con el responsable del tratamiento, tiene encomendado que estos datos de carácter personal sean conservados y protegidos por cuenta del responsable del tratamiento.

SÉPTIMO: Una vez fueron conocedores tanto el encargado del tratamiento como el responsable del tratamiento, respectivamente, de la violación de datos de carácter personal, no es, hasta pasados tres meses, el 15 de abril de 2021, cuando deciden ponerse en contacto con el Delegado de Protección de Datos del Hospital y la Agencia Española de Protección de datos, sin haber documentado dicha violación.

OCTAVO: Existe constancia de que se han producido varios intentos de comunicación por parte del Delegado de Protección de Datos con el responsable y el encargado del tratamiento donde se les comunica que no están adoptando las medidas

que se les detalla en el informe de auditoría y que ello conlleva un gran riesgo para los datos contenidos en los archivos, sin recibir respuesta alguna.

NOVENO. Ni el encargado del tratamiento de datos ni la responsable del tratamiento de datos adoptaron medida de seguridad técnica u organizativa suficientes, previa la violación de datos, para evitar una mayor fuga o la supresión de los datos publicados en los portales web.

DÉCIMO. El encargado de tratamiento niega en todo momento ser conocedor de dicha violación de datos de carácter personal y alega no haber suscrito ningún contrato o acto jurídico previo donde se determine cómo debe actuar frente a la presente situación.

UNDÉCIMO: Por su parte la responsable del tratamiento de datos menciona haber notificado la vulneración a la Agencia Española de Protección de Datos tan pronto como fue conocedor de esta, en concreto el 15 de abril de 2021 actuando acorde a la normativa de protección de datos, y haber ordenado al encargado adoptar las medidas de seguridad técnicas y organizativas oportunas para reducir los daños ocasionados, así como de poseer en su poder una copia del contrato firmado por el encargado de protección de datos, sin aportar esta como medio de prueba.

DUODÉCIMO. Los afectados por la violación de datos de carácter personal, solicitan que se les informe de las medidas legales oportunas a ejercer para la supresión de la información publicada en los portales web anteriormente mencionados.

DECIMOTERCERO: Los afectados en ningún momento han recibido comunicación alguna de dicha violación de datos de carácter personal, ni el encargado de tratamiento, ni responsable, han dado señal alguna de haber llevado a cabo actividades destinadas a identificar a los afectados para que puedan ejercer las medidas legales pertinentes de manera individual o colectiva, a través de un tercero.

DECIMOCUARTO: La falta de notificación a los afectados se debe a que tanto, el encargado del tratamiento, como la responsable del tratamiento del Hospital Nuestra

Señora de la Salud alegan la imposibilidad de ponerse en contacto de una manera rápida y eficaz con todos los afectados, dado su gran número.

DECIMEQUINTO: A su vez tampoco indican a los denunciantes de dicha vulneración las acciones legales que tienen a su disposición para denunciar esta conducta, probar y cuantificar los daños y solicitar la indemnización en la vía civil.

DECIMOSEXTO: A día de hoy siguen los datos personales de los afectados en Revisatusalud.com, Consultatussíntomas.com, Descrubretupatología.com, sin haber signos de que se hayan puesto en contacto con dichas páginas para que supriman estos datos, ni haberse explicado a los afectados las opciones procesales para que se desvinculen los ficheros con las URLS, como la opción de formulario de Google.

II. CUESTIONES JURÍDICAS PLANTEADAS.

PRIMERO. Determinación de los principios de protección de datos vulnerados y tratamiento de dato sanitarios.

SEGUNDO. Importancia y funciones de la figura del responsable y encargado del tratamiento.

TERCERO. Causas de legitimación del tratamiento afectadas.

CUARTO. Necesidad de adopción de las medidas de seguridad técnicas y organizativas con carácter previo al tratamiento de datos

QUINTO. Sujetos responsables de la adopción de las medidas de seguridad técnicas y organizativas del tratamiento.

SEXTO. Consecuencias de la inexistente comunicación a la Agencia Española de Protección de Datos como autoridad de control.

SÉPTIMO. Obligación de notificación de la violación de datos de carácter personal a los afectados.

OCTAVO. Idea de reparación del daño y supresión de los datos publicación en las URLS.

NOVENO. Determinación de las infracciones cometidas por el encargado del tratamiento y responsable de tratamiento de protección de datos, y las sanciones aplicables.

DÉCIMO. Responsabilidad civil del responsable y encargado del tratamiento

UNDÉCIMO. Modo de ejercicio de los de los interesados frente a la Agencia Española de Protección de datos

DUODÉCIMO Reclamación por vía judicial de los derechos de los afectados.

1. NORMATIVA APLICABLE

1. 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 (Reglamento general de protección de datos)
2. Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales.
3. Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.
4. Constitución Española de 1978
5. Real Decreto de 24 de julio de 1889 por el que se publica el Código Civil.
6. Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.
7. Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil.

8. Real Decreto 135/2021, de 2 de marzo, por el que se aprueba el Estatuto General de la Abogacía Española.

2. JURISPRUDENCIA

1. STSJ Madrid de 19 de julio de 2001
2. SAN (Sala de lo Contencioso-administrativo, Sección 1) 29 de noviembre de 2019. (ECLI:ES:AN:2019:4627),
3. STJUE 13 de mayo de 2014. Asunto C-131/12 (ECLI:EU:C:2014:317).
4. STS, Sala de lo Civil, de 5 de julio de 2019. (ECLI:ES:TS:2019:7376A)
5. SAN, de 20 de diciembre de 2019. (ECLI:ES:AN:2019:4735).
6. SAN(Sala de lo Contencioso-administrativo, Sección 1) 29 de noviembre de 2019. (ECLI:ES:AN:2019:4627)
7. STC, de 30 de noviembre del 2000. (ECLI:ES:TC:2000:29)
8. STC (Pleno), 25 de septiembre de 2014, ECLI ES:TC:2014:151.
9. STS, 17 de abril de 2007, RJ 2007, 3295
10. SAN, 19 de noviembre de 2003, JUR 2004, 53695
11. SAN, 10 de julio de 2014, JUR 2014, 203639
12. STS, 5 de julio de 2019. ECLI:ES:TS:2019:7376ª
13. SJPI, 12 de enero de 2018, JUR 2018\18466

3. FUNDAMENTOS DE DERECHO

FUNDAMENTO PRIMERO. OBLIGACIONES RELATIVAS AL TRATAMIENTO

PRIMERO. Principios de protección de datos y su estrecha relación con el tratamiento de datos sanitarios.

El tratamiento de datos en el ámbito sanitario debe respetar los principios de protección de datos que se recogen en la normativa europea y estatal, independientemente de la normativa sectorial que exista en el ámbito concreto.

Los sujetos encargados del cumplimiento de estos principios se tratan del Hospital Nuestra Señora de la Salud como responsable del tratamiento, y Dataprotector como encargado.

En el momento en el que se produjo la violación de datos de carácter personal se vulneraron varios de los principios que aparecen reflejado en la LOPDGDD y RGPD, ello se debe a que Nuestra Señora de la Salud y Dataprotector no obraron con la diligencia debida.

Para ello es preciso que previamente conozcamos cuáles son estos principios, y después precisemos cuáles se han visto vulnerados, centrándonos en estos. Estos se ubican en el Capítulo II del RGPD en los artículos 5 a 11. Los principios son los de: responsabilidad activa, transparencia e información, seguridad y confidencialidad, limitación del pleno de conservación de datos, limitación de la finalidad, minimización de datos, exactitud y licitud y lealtad[2].

En primer lugar, han faltado al *principio de integridad y confidencialidad* de artículo 5.1 del RGPD. En el tratamiento de los datos personales se deberá garantizar,

[2] Estos principios aparecen en una tabla del libro de ALVÁREZ HERNÁNDEZ, J. *Practicum Protección de Datos 2021*, Thomson Routers, Pamplona (Navarra), 2021, p. 160

mediante medidas técnicas u organizativas, una seguridad adecuada que los proteja del tratamiento no autorizado o ilícito y que evite su pérdida, su destrucción y que sufran daños accidentales.

Es primordial el respeto de la confidencialidad de los datos del tratamiento por parte tanto del Hospital Nuestra Señora de la Salud como responsable del tratamiento de datos como Dataprotector, como encargado del tratamiento (artículo 5.1 LOPGDD) evitando que se origine una brecha de seguridad y se filtren dichos datos.

Justo lo que ha sucedido al haberse producido una intromisión ilegítima en los ficheros del Hospital Nuestra Señora de la Salud faltando a este principio básico de protección de datos.

Este deber de confidencialidad ya aparecía reflejado en la anterior normativa de protección de datos, Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal como declaró el Tribunal Superior de Justicia de Madrid en su Sentencia de 19 de julio de 2001: "El deber de guardar secreto del artículo 10 queda definido por el carácter personal del dato integrado en el fichero, de cuyo secreto sólo tiene facultad de disposición el sujeto afectado, pues no en vano el derecho a la intimidad es un derecho individual y no colectivo. Por ello es igualmente ilícita la comunicación a cualquier tercero, con independencia de la relación que mantenga con él la persona a que se refiera la información (...)".

Por otro lado, el Hospital Nuestra Señora de la Salud y Dataprotector tienen la obligación de rendir cuentas en caso de que se produzca una violación de datos de carácter personal como la sucedida en sus ficheros. Esta obligación de rendir cuentas se cristaliza en el *principio de responsabilidad proactiva* del artículo 5.2 del RGPD.

El Hospital debería haber realizado una evaluación de impacto del tratamiento de datos de carácter personal que poseen en sus ficheros, con el fin de determinar las medidas a aplicar para garantizar que los datos personales están conformes a las exigencias legales, recogidas en el artículo 35 del RGPD. Este artículo se centra en los supuestos en los que el uso de nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas,

siendo este el derecho a la intimidad constitucionalmente reconocido en la Carta Magna en su artículo 18.4.

Por ello, si hubieran actuado correctamente, el encargado del tratamiento y el responsable del tratamiento deberían haber evaluado de forma previa los riesgos que entraña la protección de datos personales, derivado de su tratamiento. El Hospital debe poseer un registro de actividades en el que se describan los tratamientos de datos personales que lleven a cabo en el marco de sus actividades, el cual convendría solicitar que aporte Nuestra Señora del Pilar para poder así conocer qué tuvieron en cuenta para evitar que se produjera la presente violación de datos de carácter personal.

Por ende, desconocemos cuál es el protocolo de actuación de Nuestra Señora del Pilar frente a una violación de la seguridad de los datos que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales, o la comunicación o acceso no autorizado a dichos datos, siendo esta la definición recogida en el art.4.12 del RGPD. Dichas violaciones deberán documentarse y se adoptarán medidas para solventar y paliar los posibles efectos negativos para los interesados.

Habiendo determinado cuáles son los principios de datos de carácter personal. y habiendo precisado cuáles se han visto vulnerados debemos centrar nuestra atención en el *tratamiento específico* de datos personales ante el cual nos encontramos. Los datos que se han visto revelados a partir de la brecha de seguridad se tratan de datos de carácter especial como establece el artículo 9 del RGPD al tratarse de datos relativos a la salud de los pacientes. En esta categoría de datos especiales inciden tanto el legislador comunitario como el nacional, siendo conscientes que no todos los datos referidos a una persona física inciden de igual forma en su intimidad[3].

La Carta Magna en su artículo 43 reconoce el derecho a la protección de la salud y a la atención sanitaria de todos los ciudadanos, ello implica que el tratamiento afecta tanto a la propia asistencia sanitaria que reciban los pacientes como la investigación científica. El sector sanitario presenta importantes singularidades al hablar del tratamiento de datos personales, al estar en juego categorías especiales de datos y que

[3] FERNÁNDEZ LÓPEZ, J. M, «El derecho fundamental a la protección de los datos personal. Obligaciones que derivan para el personal sanitario», Dialnet, Extraordinario XI Congreso Derecho y Salud, p. 42

sea la normativa sectorial sanitaria la que regule los derechos y obligaciones de los pacientes y usuarios[4].

El RGPD define los datos de salud, genéticos y biométricos en los apartados 13 a 15 del artículo 4. En el presente supuestos los datos que se han visto comprometidos a partir del tratamiento son los datos relativos a la salud, y el Considerando 35 dice que tienen la consideración de datos relativos a la salud: el estado de salud física o mental pasado, presente o futuro de una persona, asistencia sanitaria, número o símbolo asignado a una persona, información de pruebas o exámenes, enfermedades, discapacidades, historial médico, etc.

Como se ve reflejado en los antecedentes de hecho es en las URLS indicadas donde se ha visto publicado todo el historial clínico de los pacientes del Hospital Nuestra Señora de la Salud, dejando claramente evidenciado el incorrecto tratamiento de datos de carácter personal llevado a cabo por responsable y encargado del tratamiento.

Tal es la importancia de los datos de carácter personal el en el ámbito sanitario que tiene su propia normativa, la Ley 41/2002, la LBAP, en relación a la autonomía del paciente y los derechos que a estos se le confieren cuando se vea afectado su historial clínico.

El derecho a la intimidad del paciente se ve recogido en su artículo 7, haciendo alusión al derecho vulnerado por parte del responsable y encargado respectivamente, de que se respete el carácter confidencial de los datos referentes a su salud y que nadie acceda a ellos sin previa autorización amparada por la Ley. Del mismo modo, también fallan a su punto segundo al no haber adoptado el centro sanitario las medidas oportunas para garantizar los derechos a los que se refiero el artículo 7.1 LBAP.

Para conocer la gravedad de la violación de datos de carácter personal conviene aclararles a Don Juan García Ferrer y Doña María José Martínez Amor qué comprende el contenido de la historia clínica para así abarcar toda su afectación, siendo esta trascendental para el conocimiento veraz y actualizado del estado de salud del paciente.

[4] ALVÁREZ HERNÁNDEZ, J. *Practicum Protección...* cit, p. 160

Su contenido mínimo, conforme al artículo 15 de la LBAP comprende:

a) La documentación relativa a la hoja clínicoestadística.
b) La autorización de ingreso.
c) El informe de urgencia.
d) La anamnesis y la exploración física.
e) La evolución.
f) Las órdenes médicas.
g) La hoja de interconsulta.
h) Los informes de exploraciones complementarias.
i) El consentimiento informado.
j) El informe de anestesia.
k) El informe de quirófano o de registro del parto.
l) El informe de anatomía patológica.
m) La evolución y planificación de cuidados de enfermería.
n) La aplicación terapéutica de enfermería.
ñ) El gráfico de constantes.
o) El informe clínico de alta

Pedro Laín Entralgo, en una de sus máximas obras ofreció una definición de historia clínica, útil para los afectados, definiéndolo como: «el documento fundamental y elemental del saber médico, en donde se recoge la información confiada por el enfermo al médico, para obtener su diagnóstico, tratamiento y la posible curación de su enfermedad»[5].

El Hospital Nuestra Señora de la Salud debería haber conservado la documentación clínica en unas condiciones que garantizaran su correcto mantenimiento y seguridad como se indica en el artículo 17 LBAP, con una custodia activa y diligente de las historias clínicas, artículo 19 LBAP.

[5] LAÍN ENTRALGO, P., "La historia clínica, historia y teoría del relato patográfico", Madrid, 1998 (reimpresión del original de 1950)", pp. XVi, 668.

No obstante, han permitido que se produzca una intromisión ilegítima en sus ficheros produciendo la fuga de datos de carácter personal de quinientos pacientes, entre los que se encuentran los de mis defendidos Don Juan García Ferrer y Doña María José Martínez Amor.

Inclusive existen unos Principios Éticos de la Sanidad en la Sociedad de la Información del 30 de julio de 1999, sin valor legal, elaborados por el Grupo Europeo de Ética de la Ciencia y de las Nuevas Tecnologías, que poseen un carácter asimilado al recogido en la normativa de protección de datos, y que realizan una enumeración, siendo estos: la recogida de datos, control y disposición de los datos de salud por el propio interesado, derecho de oposición de sus datos cuando la finalidad no se corresponda con la de recogida y justificación de la utilización de los datos personal en la proyección social de la salud.[6]

SEGUNDO. Importancia y funciones de la figura del responsable y encargados del tratamiento.

Con carácter preferente debemos distinguir cuáles son las figuras del responsable de tratamiento de datos y el encargado de tratamiento, así como sus principales funciones, ya que asumen un papel crucial en el tratamiento de los mismos y poseen un régimen sancionador al que atenerse en caso de que se cometa una infracción de las reflejadas en la LOPDGDD o RGPD.

Por un lado, la definición de figura del *responsable de tratamiento de datos*, en este caso, el Hospital Nuestra Señora de la Salud, la encontramos recogida en la legislación europea en el RGPD en su artículo 4.7. Se trata de la persona, física o jurídica, la cual determina los fines y medios del tratamiento.

Los fines y medios específicos del tratamiento por parte del responsable versarían sobre el tratamiento de los datos de salud concernientes a los pacientes que acuden al Hospital Nuestra Señora de la Salud, permitir el correcto ejercicio de los derechos que les concierne a los interesados, en este caso los afectados por el tratamiento y llevar a

[6]MERINO MARTÍN, J, **"**Los datos personales relativos a la salud y la Historia Clínica", Revista Aranzadi Doctrinal Num.10/2019, p. 15

cabo una correcta conservación de datos de carácter personal contenidos en el historial clínico en sus ficheros, durante el tiempo que legalmente se establezca en la legislación.

Por otro lado, el *encargado del tratamiento*, siendo este Dataprotector, encuentra su definición en la misma normativa, en el artículo 4.8. Este es aquel que trata datos personales por cuenta del responsable del tratamiento, es decir realiza, a través de un contrato o acto jurídico suscrito entre ambas partes, las actividades que le encomiende en responsable en materia de tratamiento de datos de carácter personal.

Estas actividades son las de conservar y proteger frente a cualquier posible violación de datos de carácter personal los datos depositados por los pacientes en el Hospital Nuestra Señora de la Salud, así como, en caso de que se produjera una situación de violación de datos de carácter personal, que se les comunicara a los afectados cuáles son los derechos que puedan ejercer frente a dicha situación.

Entre ambos se debe dilucidar si existe o no un contrato u acto jurídico, dado que el artículo 28.3 RGPD obliga que este exista entre el encargado y responsable de tratamiento. Este contrato suscrito entre el Hospital y Dataprotector debería haber incluido: el objeto, duración, naturaleza y finalidad del tratamiento, especificar que se trata de datos de la salud de categoría especial, la obligación del encargado del tratamiento de tratar los datos únicamente como se precise a través de instrucciones documentadas del responsable, y la asistencia al responsable[7].

A tener de lo observado en el supuesto, y sin haber realizado todavía medidas de averiguación, parece no existir un contrato o acto jurídico entre el Hospital y Dataprotector. Si no existe una formalización previa del contrato o acto jurídico con el contenido en el artículo 28.3 del RGPD, Laura Gracia habría incurrido en una infracción, tipificada como grave, por el artículo 73.k de la LOPDGDD y debería hacer frente a un procedimiento sancionador con la consiguiente multa o apercibimiento.

Dataprotector alega no haber suscrito ningún contrato previo al desarrollo a la actividad de tratamiento de datos, siendo que este, aparte de haberse suscrito tendría que

[7] ALVÁREZ HERNÁNDEZ, J. *Practicum Protección...* cit, p. 402

haber constado por escrito, inclusive en formato electrónico como indica el artículo 28 apartado 9 RGPD.

El Tribunal Supremo, en su Sentencia de 17 de abril de 2007[8], haciendo alusión al artículo 12 de la derogada LOPD, incide en la necesidad no solo de que esté por escrito, sino que quede claramente especificado su contenido. Del mismo modo la Sentencia de la AN de 19 de noviembre de 2003[9] hace hincapié en la obligatoriedad de que este contrato se encuentre por escrito, ya que de otro modo nos encontraríamos ante una cesión ilícita de datos.

No haber suscrito el contrato entre ambas partas no exime completamente a Dataprotector de la responsabilidad derivada de la intromisión ilegítima en los ficheros del Hospital, y del cumplimiento de la normativa de protección de datos. Sin olvidar que como encargado de tratamiento es conocedor de cómo debería actuar un encargado y que debería haber formalizado un contrato antes de que comenzara el tratamiento.

Otro aspecto adicional que debe ser abordado es la necesidad del Hospital Nuestra Señora de la Salud de contar con un *Delegado de Protección de Datos* (en adelante DPD) en relación al tratamiento de datos de carácter personal, recogido en los artículos 34 a 37 del RGPD y cuya función es la de informar a la entidad responsable o el encargado del tratamiento sobre sus obligaciones legales en materia de protección de datos, y velan el cumplimiento normativo al respecto.

El Hospital Nuestra Señora de la Salud ha decidido confiar la función de DPD en Antonio Marcuello que, tal y como se recoge en el artículo 39 RGPD y 36.1 y 36.2 LOPDGDD tiene encomendadas las siguientes funciones: función de información y asesoramiento normativo, supervisión del cumplimiento normativo, cooperación y enlace con la autoridad de control, y atención a los interesados e intermediación en caso de reclamación.

Antonio Marcuello ha actuado diligentemente informando y asesorando al Hospital Nuestra Señora de la Salud de las obligaciones normativas en la protección de datos

[8] STS, 17 de abril de 2007, RJ 2007, 3295
[9] SAN, 19 de noviembre de 2003, JUR 2004, 53695

que les incumben (artículo 37.5 RGPD), y de la evaluación de impacto relativa. No obstante, es el Hospital de Nuestra Señora de la Salud o Dataprotector los que toman las decisiones que estimen, ya sea teniendo o no en cuenta, las recomendaciones del DPD[10].

En cuanto a la función de supervisión del cumplimiento normativo, el DPD ha emitido varias recomendaciones al Hospital y a Dataprotector acerca de las medidas de seguridad que deberían haber adoptado para evitar la violación de datos de carácter personal. Tan pronto como este fue conocedor de esta vulneración de datos, lo documentó y se lo comunicó al responsable del tratamiento (artículo 39 RGPD), aunque como se menciona en los antecedentes de hecho no recibió respuesta alguna

La designación de Antonio Marcuello como DPD tiene un carácter obligatorio, el artículo 37.1.C del RGPD indica que será obligatorio en el caso de que las actividades principales del responsable o encargado consistan en el tratamiento a gran escala de categorías de datos especiales. De hecho, se establece como ejemplos del tratamiento a gran escala el tratamiento de datos de pacientes en el desarrollo normal de la actividad de un hospital.[11] Ello se debe a que atendiendo a la naturaleza, alcance y fines del Hospital Nuestra Señora de la Salud requiere una observación habitual y sistemática de interesados a gran escala. En el presente caso se han vulnerado datos de 500 afectados, pero el volumen de afectados podría haber sido mucho mayor al tratar con cientos y cientos diariamente de pacientes el Hospital.

No solo el RGPD determina esta obligación, la LOPDGDD en su artículo 34.1.l también determina la necesidad de designación de un delegado de protección de datos, al tratarse de un centro sanitario legalmente obligados al mantenimiento de las historias clínicas de los pacientes.

[10] ALVÁREZ HERNÁNDEZ, J. *Practicum Protección...* cit, p.333
[11] GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29. *Directrices sobre los delegados de protección de datos* (DPD)» cit., Página 9 y ALVÁREZ HERNÁNDEZ, J. *Practicum Protección...* cit, p. 339.

Para ello debe contar con unos recursos necesarios facilitados por el responsable o encargado con los que no ha contado, al no habérsele facilitado la actividad del tratamiento[12].

En definitiva, el Hospital Nuestra Señora de la Salud es la figura que determina los fines y objeto del tratamiento, por ello no se puede culpabilizar a Antonio Marcuello (DPD) de la brecha de seguridad acaecida al haber cumplido este correctamente su función de: asesorar, supervisar, informar y controlar los diversos procedimientos, políticas, normativas y demás elementos necesarios para desarrollar las acciones de tratamiento. Lo correcto hubiera sido que tanto responsable como encargado del tratamiento hubieran seguido estas recomendaciones que suponen una gran herramienta para que los responsables y encargados puedan desempeñar su actividad con mayor tranquilidad[13].

TERCERO. Causas de legitimación del tratamiento afectadas. **Consentimiento del interesado**

Aunque no se trata de un principio de datos de carácter personal, sino de una de las posibles causas de legitimación del tratamiento, el *consentimiento* es uno de los pilares esenciales que configuran la estructura del derecho fundamental a la protección de datos.

La definición de consentimiento del interesado la hallamos en el artículo 4.11 del RGPD, así como el artículo 3 y 6 LOPGDD y este se define como: "toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen". Este consentimiento se plasma en el momento que los pacientes del Hospital, acorde a los requisitos del artículo 4.11 RGPD, consienten que sus datos de carácter sanitarios se traten por los profesionales del Hospital.

[12] GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29. *Directrices sobre los delegados…* p. 26

[13] MESSIA DE LA CERDA BALLESTEROS, J. A. "Consideraciones y perspectivas del delegado de protección de datos". Revista Aranzadi de Derecho y Nuevas Tecnologías num.47, 2018, p. 15 y 18

Para que este consentimiento sea válido, este debe haberse otorgado para una finalidad concreta, para cualquier tratamiento presente y futuro que puedan recibir los pacientes en el Hospital. No obstante, los pacientes no otorgaron su consentimiento para que este sea usado como modo de resolución de consultas en URLS de internet.

Es importante remarcar que el consentimiento debe ser informado, es decir, el afectado debe conocer y ser plenamente consciente, ya antes de que comience el tratamiento, para qué se van a destinar dichos datos. Si el responsable del tratamiento no proporciona información accesible al afectado, este consentimiento no constituirá una base jurídica válida para el tratamiento de datos[14]. Esta idea se refleja en la LBAP, en su artículo 8.1.

En el Procedimiento Nº: PS/00104/2021 se cristaliza esta idea del consentimiento informado, con el objeto de que, en el momento de que este se otorgue para el tratamiento de datos por parte del titular de mismo, estos se destinen a un fin determinado. La entidad obligaba a los usuarios a aceptar un tratamiento de datos personales, siendo estas imágenes grabadas de alumnos menores de edad, para otros fines ajenos a los inicialmente destinados, como era la publicación en redes sociales de sus actividades deportivas.

Todos los interesados afectados por la brecha de seguridad deben conocer que el consentimiento es tan fácil retirarlo como otorgarlo como indica el artículo 7.3 RGPD, y este interesado podrá retirar su consentimiento en cualquier momento[15].

De hecho, trayendo a colación la Sentencia de la AN de 29 noviembre de 2019[16], que presenta ciertas similitudes con el caso aquí discutido, castiga como infracción grave la revelación de datos relativos a la salud de afectados en el atentado del 11 de marzo ocurrido en Madrid. No se contaba con el consentimiento expreso e informado de los afectados, prevaleciendo el derecho a la intimidad.

[14] ALVÁREZ HERNÁNDEZ, J. *Practicum Protección...* cit, p. 173
[15] GARROS FONT, I "Las categorías especiales de datos personales y su régimen aplicable". Revista Aranzadi Doctrinal, num.2, 2021, p. 8
[16] SAN (Sala de lo Contencioso-administrativo, Sección 1), 29 de noviembre de 2019

Esta idea de legitimación del tratamiento se refleja en la Sentencia del Tribunal Constitucional del año 2000 en su Fundamento de Derecho Séptimo[17]-→ "…consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para PERIODICO.1, pudiendo oponerse a esa posesión o uso.

Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos, se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular (...)."

En contraposición a esto existen opiniones que indican que el tratamiento de datos de categorías especiales no debe pivotar tanto sobre el consentimiento del interesado, sino sobre el principio de legalidad, en virtud de la obligación constitucional del Estado de proteger la vida. Es decir, no recae sobre Don Juan García Ferrer y Doña María José Martínez Amor como interesados al otorgar su consentimiento, sino sobre el Estado y que este adopte las medidas de naturaleza normativas suficientes[18].

A raíz de la brecha se seguridad acaecida se han visto publicados en los portales web datos de carácter personal de menores especialmente protegidos en la normativa europea de protección de datos. El RGPD en su artículo 8 indica unas Condiciones aplicables al consentimiento del niño en relación con los servicios de la sociedad de la información.

Francisco García Martínez, hijo de Don Juan García Ferrer y Doña María José Martínez Amor, cuenta a día de hoy con una edad de 13 años. Ello implica que

[17] STC, 30 de noviembre de 2000
[18] TRONCOSO REIGADA, A. "Las categorías especiales de datos personales en el Reglamento General de Protección de Datos de Unión Europea", *El Derecho.com*, Lefebvre 2019.

conforme al artículo 7 de la LOPDGDD párrafo segundo, al ser su edad inferior a 14 años el consentimiento solo será lícito si fue autorizado por las personas que ostenten la patria potestad del menor.

En relación con dichas autorizaciones conviene traer a colación lo dispuesto en el artículo 156 del Código Civil, que dispone que:

"La patria potestad se ejercerá conjuntamente por ambos progenitores o por uno solo con el consentimiento expreso o tácito del otro. Serán válidos los actos que realice uno de ellos conforme al uso social y a las circunstancias, o en situaciones de urgente necesidad".

No consta por escrito, ni de manera verbal que existiera un consentimiento inequívoco de sus respectivos padres, Don Juan García Ferrer y Doña María José Martínez Amor, quienes, en ningún momento, autorizaron por escrito el uso divulgativo del historial clínico de los menores afectados en el ámbito públicos y en las páginas Revisatusalud.com, Consultatussíntomas.com, Descrubretupatología.com, sino solamente para los tratamientos clínicos que pudiera recibir el menor ya sea periódicamente o de manera puntual.

La AEPD contiene varias resoluciones en materia de menores cuando se ven publicados en portales web, redes sociales u otros medios, imágenes o información del menor sin consentimiento de quienes ostenten la patria potestad del menor.

La AEPD en uno de sus Procedimientos[19] realiza un apercibimiento a una Escuela de Danza por la publicación en un portal web de imágenes e información de menores de edad pudiendo identificar completamente de quien se trata, incumpliendo las condiciones del consentimiento necesarias del artículo 7 del RGPD. En su Fundamento de Derecho II se refleja como, en el impreso de matrícula, no se establece ningún precepto que refleje la cesión de la imagen para los fines de envío publicitario y mercadotecnia. Por ello no se ajusta a la base legitimadora del consentimiento ni al RGPD.

[19] Procedimiento AEPD Nº: PS/00046/2019

En otra ocasión la AEPD[20] sancionó a un club de esquí por una vulneración del artículo 7 del RGPD, por publicar datos de carácter personal mediante el formato vídeo, de una menor hija de la denunciante esquiando, sin otorgar la madre de dicha hija su consentimiento para que se publiquen en las redes sociales.

Si extrapolamos este Procedimiento al supuesto del presente Dictamen, Don Juan García Ferrer y Doña María José Martínez Amor, cuando rellenaron el formulario relativo a los datos de Francisco García Martínez fue con el objeto de crear un perfil en el fichero del Hospital Nuestra Señora del Pilar para que en el caso de que este necesitara cualquier tratamiento médico fuera atendido del modo más eficaz. Mientras que cuando prestaron este consentimiento en ningún momento fue para que se publicaran los datos de su progenitor en los portales web: Revisatusalud.com, Consultatussíntomas.com, Descrubretupatología.com.

CUARTO. Obligación de adopción de las medidas de seguridad técnicas y organizativas con carácter previo al tratamiento de datos.

Previo a la violación de datos personales sucedida, el responsable del tratamiento o el encargado, deberían haber adoptado las respectivas medidas técnicas, organizativas con el objeto de garantizar un nivel de seguridad adecuado como se refleja en el artículo 32 del RGPD. Es obligación del responsable realizar una evaluación de riesgos para poder determinar qué medidas de seguridad son las apropiadas para garantizar un nivel de seguridad de la información tratada y los derechos de las personas afectadas.

Se exige a cualquier organización a disponer de un elenco de medidas técnicas de seguridad en el tratamiento de datos personales, conforme al artículo 24.1 RGPD. La Sentencia de la AN de 10 de julio de 2014[21] confirmó una sanción impuesta a la AEPD en la cual se obligaba a la entidad recurrente a adoptar las medidas técnicas y

[20] Procedimiento AEPD Nº: PS/00104/2021
[21] SAN, 10 de julio de 2014

organizativas necesarias que impidieran el acceso no autorizado de terceras personas a los datos personales conservados en sus ficheros.

Estas medidas de seguridad de carácter técnico, indicadas a continuación, cumplen con el objeto de orientar al responsable y encargado del tratamiento para que las adopten y así se reduzca el daño causado, o bien en siguientes ocasiones no vuelvan a cometer el mismo error. Por ejemplo, una actualización permanente de los parches de seguridad de los dispositivos con los que se accede a los datos de carácter personal, llevar a cabo pruebas de penetración para encontrar vulnerabilidades, medidas de seguridad para los ficheros temporales, y medidas dirigidas a evitar la sustracción, pérdida o acceso indebido a la información durante su transporte[22].

En cuanto a las medidas de seguridad de carácter organizativo, también es obligatoria su adopción por parte del responsable del tratamiento o encargado, estableciendo protocolos y determinando estas medidas en la entidad, con el fin de observar el principio de responsabilidad proactiva del RGPD[23]. Unos ejemplos de las políticas de seguridad y de normativas para los empleados y usuarios de los sistemas de información de la entidad que podrían haber adoptado son: control de accesos, actualización del software, políticas de almacenamiento en la red corporativa, equipos de trabajo o nube, política de contraseñas, etc.[24]

La finalidad de la adopción de estas medidas técnicas y organizativas es proteger los derechos y libertades de las personas físicas con respecto al tratamiento de datos personales.

Las medidas de seguridad a adoptar se determinarán y aplicarán teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, artículo 24 RGPD.

[22] ALVÁREZ HERNÁNDEZ, J. *Practicum Protección...* cit, p. 594 y 595.
[23] ALVÁREZ HERNÁNDEZ, J. *Practicum Protección...* cit, p. 601
[24] ALVÁREZ HERNÁNDEZ, J. *Practicum Protección...* cit, p. 602

Las medidas técnicas y organizativas serán las que resulten apropiadas para garantizar un nivel de seguridad adecuado al riesgo.

El artículo 32.1 RGPD enuncia que: "teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros":

a) la seudonimización y el cifrado de datos personales;
b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;
c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;
d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento[25].

Debería existir constancia de la existencia de un inventario de soportes, donde queden registradas las entradas y salidas de todo soporte físico. Así como, que cualquier incidencia de seguridad sea notificada a través del parte de notificación y registro de incidencias que puedan afectar a un fichero que contenga datos personales.

Aunque el RGPD incide, como hemos podido apreciar, en la crucial importancia de adoptar unas medidas técnicas y organizativas suficientes para evitar que se ocasione una violación de datos de carácter personal, la normativa no establece cuáles son estas medidas.

Por ello convendría conocer, para la resolución del presente Dictamen, si el Hospital Nuestra Señora del Pilar, ya sea a través del encargado del tratamiento o del responsable del tratamiento pudiera responder a las siguientes cuestiones que ya

[25] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Directrices para la elaboración de contratos entre responsables y encargados del tratamiento*, p. 9.

deberían tener resueltas mediante el informe de auditoría de protección de datos que realizaran en su momento.

En cuanto a los datos archivados en formato papel al ser ya conocedores de que la violación se ha producido mediante una intromisión ilegítima en sus archivos vía Internet no revisten de una especial atención, siendo relevante dilucidar las medidas de seguridad adoptadas por el Hospital Nuestra Señora de la Salud y Dataprotector.

Cierto es que ni la RGPD, ni la LODGDD expresan literalmente la obligación de realizar una auditoría de protección de datos, lo que sí hacen es, en el artículo 24 del RGPD indicar que existe la obligación de evaluar la eficacia de las medidas de técnicas y organizativas implantadas deberán ser revisadas y actualizadas "cuando sea necesario".

Relacionando la idea de la necesidad de adoptar medidas de seguridad técnicas y organizativas, a continuación, voy a mencionar a modo de check list, unos aspectos que tendrían que haber tenido en consideración para el tratamiento de datos.

Por un lado, el nivel de seguridad de las contraseñas con el que se acceden a los ficheros del Hospital y si estas se suelen cambiar de forma periódica y se almacenan de forma que puedan ser recuperadas por el administrador de sistemas o la persona designada.

Por otro lado, qué mecanismos usan que permitan identificar cada usuario que acceda a los sistemas de tratamiento, la fecha y hora en la que tenga acceso, aquellos ficheros a los que accede y el tratamiento de los datos que lleva a cabo.

El tercer aspecto es el desarrollo de un perfilamiento de roles dentro del Hospital para limitar el acceso de personal a los tratamientos imprescindibles para realizar su trabajo y una política de control de accesos, identificación y autenticación de usuarios.

En función de las medidas técnicas y organizativas que hayan adoptado el Hospital Nuestra Señora de la Salud como responsable del tratamiento y Dataprotector como

encargado del tratamiento la sanción correspondiente será mayor o menor y lo mismo sucederá con la infracción cometida.

Es el Hospital Nuestra Señora de la Salud como responsable del tratamiento el que debería haber adoptado medidas de seguridad tales como: reducir al máximo el tratamiento de datos personales, seudonimizar lo antes posible los datos personales, dar transparencia a las funciones y el tratamiento de datos personales, entre otras como indica el Considerando 78 del RGPD.

No es esgrimible el argumento alegado por el responsable del tratamiento de datos, contra el encargado, haciendo mención a la falta de comunicación entra ambos, puesto que al no existir contrato o acto jurídico, aquí sería donde se hubiera descrito qué medidas técnicas y organizativas deben adoptar con carácter previo[26]. No obstante, como no hay contrato Dataprotector desconocía cómo actuar exactamente.

Como se puede apreciar Dataprotector, encargado del tratamiento no ha adoptado medidas de seguridad suficientes para prevenir la violación de datos de carácter personal, independientemente de que este indique que no se le haya notificado en ningún momento por parte del responsable del tratamiento acerca de cómo debía actuar, este es un experto en la materia que seguro conocía unas medidas de seguridad standard a adoptar en estos casos.

A su vez, las medidas técnicas y organizativas, la notificación de violaciones de seguridad a la autoridad de protección de datos y, en su caso, a los interesados, u otras que sean aplicables, se adoptarán por el responsable del tratamiento.

Por ende, la propia Guía de Directrices para la elaboración de contratos, útil a modo de título orientativo, entre responsables y encargados del tratamiento de la AEPD especifica que en el acuerdo suscitado entre ellos se debe contener la obligación del

[26] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Directrices para la elaboración…* cit., p. 11

encargado de adoptar todas las medidas de seguridad necesarias, de conformidad con lo establecido en el artículo 32 del RGPD[27].

No consta que el responsable haya llevado a cabo ninguna acción que cumpla con este precepto, ni tampoco el encargado que, hubieran debido evaluar los posibles riesgos derivados del tratamiento, teniendo en cuenta los medios utilizados que se encuentren a su disposición y otras circunstancias que puedan incidir en la seguridad.

FUNDAMENTO SEGUNDO. OBLIGACIONES Y RESPONSABILIDAD DERIVADAS DEL INCIDENTE DE SEGURIDAD

PRIMERO. Consecuencias de la inexistente comunicación a la Agencia Española de Protección de Datos como autoridad de control de la violación de datos de carácter personal.

No es lo mismo la notificación a la autoridad de control que la notificación a los interesados para que estos ejerzan sus derechos, por ello distinguiré claramente ambas con la remisión normativa pertinente. En el Considerando 85 del RGPD deja claro que el objetivo de la notificación es limitar los daños y perjuicios ocasionados en los afectados.

El Hospital Nuestra Señora del Pilar tiene la obligación de documentar y notificar cualquier violación de seguridad de los datos personales a la autoridad de control, siendo esta la Agencia Española de Protección de Datos conforme al artículo 33 del RGPD.

Podría plantearse la duda de cuándo se considera que tiene constancia, el responsable del tratamiento, de la violación de datos de carácter personal. El GT29 considera que esta se da cuando se tiene un grado razonable de certeza de que se ha

[27] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Directrices para la elaboración*… cit., p. 8

producido un suceso que compromete datos personales[28] y así notificar a la autoridad sin una dilación indebida.

En el presente supuesto el Hospital no ha notificado dicha vulneración en el plazo de 72 horas como legalmente se establece en el artículo 33 del RGPD en su apartado 1, de hecho, ha sido tres meses después, con base en el principio de responsabilidad proactiva. Esta notificación se trata de una parte esencial de la gestión de la seguridad de la información.

Si se hubiera llevado a cabo la notificación, para que esta fuera correcta, de acuerdo al artículo 33.3 RGPD esta debería haber descrito la naturaleza de la violación de seguridad de los datos personales, datos del contacto del delegado de protección de datos, posibles consecuencias de la violación de la seguridad de los datos personales y las medidas propuestas o adoptadas por el responsable del tratamiento para poner remedio a dicha violación.

Como se refleja en las *"Directrices sobre la notificación de las violaciones de la seguridad de los datos personales de acuerdo con el Reglamento 2016/679" del Grupo de Trabajo sobre Protección de Datos del Artículo 29*, el responsable del tratamiento debería disponer de procesos internos para poder detectar y subsanar una violación, adoptando medidas técnicas como analizadores de flujo de datos y de registro, por ejemplo.

Asimismo, el responsable del tratamiento está obligado a actuar frente a cualquier alerta inicial, siendo esta la notificación de varios de los afectados al Hospital de la publicación de sus datos en varios portales web. Es por ello, que al no actuar de manera rápida y eficiente frente a dicha violación nos encontramos ante una falta de notificación con base en el artículo 33 del RGPD.

Es el responsable el que conserva la responsabilidad general de la protección de datos personales, pero el encargado asume un papel importante para que este pueda

[28] GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29, *Directrices sobre la notificación de las violaciones de la seguridad de los datos personales acuerdo con el Reglamento 2016/*679 p. 11.

cumplir sus obligaciones debiendo ayudarle a garantizar el cumplimiento de las obligaciones de los artículos 32 a 36 RGPD, indicado en el artículo 28.3.F RGPD.

El artículo 33.2 RGPD establece claramente que, si el responsable recurre a un encargado del tratamiento, este debe notificar cualquier brecha de seguridad al responsable sin dilación indebida. Dataprotector en su función de encargado del tratamiento no notificó al responsable que los datos de los pacientes habían sido publicados en Internet, impidiendo una comunicación temprana a la AEPD por parte del Hospital Nuestra Señora de la Salud incurriendo en una infracción grave de la LOPDGDD.[29]

Las recomendaciones que establece el GT29 y que debería haber seguido Dataprotector son, aparte de la comunicación sin demora, ir facilitando de forma gradual información al responsable acerca del estado de la violación de datos de carácter personal. De este modo el responsable puede cumplir de manera eficaz el requisito de notificación a la autoridad de control en el plazo de setenta y dos horas, y adoptar las medidas de seguridad técnicas y organizativas pertinentes para reducir los daños[30].

Independientemente de que el encargado del tratamiento haya o no notificado dicha violación al responsable del tratamiento, ninguno de los dos adoptó ninguna medida para disminuir o suprimir los efectos negativos de dicha violación, debiendo asumir las consecuencias por ello.

Podemos llegar a comprender que la notificación, por su naturaleza de datos de categoría especial y por la magnitud de los afectados, exija una investigación continuada para poder esclarecer todos los hechos del incidente, pero ello no le exime de su comunicación temprana.

El artículo 33.4 RGPD menciona que, si no fuera posible facilitar la información simultáneamente, esta se podrá facilitar de manera gradual y sin dilación indebida.

[29] ALVÁREZ HERNÁNDEZ, J. *Practicum Protección...* cit, p. 771
[30] GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29. *Directrices sobre la notificación…* cit., p.15.

Dataprotector no realizó ninguna comunicación al responsable avisándole de dicha violación, sino que, como aparece mencionado en los hechos, fue el responsable de protección de datos la que se dio cuenta de ello.

El problema radica en que se ha producido una excesiva dilación en el tiempo en la notificación, ya que, cierto es que se ha experimentado múltiples violaciones de confidencialidad en un corto periodo temporal, pero en ningún momento encargado o responsable ha presentado una notificación "agrupada" dentro del plazo previsto en la normativa, concerniente al mismo tipo de datos personales afectados,

Es decir, la AEPD, aun siendo la notificación tardía le hubiera permitido notificar posteriormente dicha violación con el objeto de aunar al mayor número de afectados, aun así, no se notificó y mis clientes quedaron totalmente desamparados.

El modo en el que debería haber notificado la quiebra de seguridad a la AEPD sería a través de su sede electrónica, exigiéndose certificado electrónico. Para ello hay que cumplimentar un formulario indicando: datos del DPD, responsable y encargado del tratamiento, información relativa a la brecha de seguridad y los datos afectados, quiénes han sido lo sujetos afectados y la consecuencia de ello[31].

SEGUNDO. Obligación de notificación de la violación de datos de carácter personal a los afectados.

Del mismo modo que se comunica la violación de seguridad por parte del responsable o el encargado a la AEPD, estos deben del mismo modo comunicárselo al interesado que se haya visto afectado por dicho acontecimiento, al ser sus datos de carácter personal los que se han visto publicados.

A tenor de este último párrafo cabe explicar la comunicación al interesado. El artículo 34.1 RGPD indica que, si la violación de la seguridad de datos personales entraña un alto riesgo para los derechos y libertades de las personas físicas, el responsable la deberá comunicar al interesado sin dilación indebida. Esta comunicación

[31] ALVÁREZ HERNÁNDEZ, J. *Practicum Protección...* cit, p. 772.

permitirá que los afectados, si no lo conocían, conozcan que se ha producido dicha brecha y puedan ejercer los derechos que la normativa de protección de datos les reconoce frente a tales situaciones.

Una definición totalmente válida de interesado sería la de aquella persona física cuyos datos se han visto afectados por una brecha, comprometiendo la confidencialidad, integridad y/o disponibilidad de esos datos, y quien puede sufrir esas consecuencias[32].

Con ello se pretende que los sujetos afectados puedan adoptar las medidas oportunas para protegerse. Como observamos a ninguno de los afectados se les ha comunicado la violación de datos de carácter personal, sino que fueron estos los que realizando búsquedas por Internet en, Revisatusalud.com, Consultatussíntomas.com, Descrubretupatología.com, los que localizaron en sus datos personales.

Esta comunicación a los interesados debería haber descrito en un leguaje claro y sencillo la naturaleza de la violación de datos sufrida por el Hospital Nuestra señora de la Salud, artículo 34.2 RGPD. También debería haberles descrito las posibles consecuencias de la violación, y la descripción de las medidas adoptadas o propuestas por el Hospital Nuestra Señora de la Salud para poner remedio a la violación de la seguridad de los datos personales[33].

Esta obligación de comunicación aporta un valor añadido de transparencia a las personas que son objeto del tratamiento, permitiéndoles conocer si sus datos han podido ser revelados a terceros. Aunque cierto es que, si el responsable no lleva a cabo la comunicación de manera voluntaria, la AEPD previa valoración de que esta violación entraña un alto riesgo le podrá exigir que comunique a los afectados dicha violación[34].

Aunque no existe un plazo determinado para que se produzca dicha comunicación con los afectados se aplica la misma condición que cuando se trata de la comunicación

[32] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Guía para la notificación de brechas de datos personales*, 2021 p. 26
[33] GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29. *Directrices sobre la notificación…* cit., p. 23 y ALVÁREZ HERNÁNDEZ, J. *Practicum Protección...* cit, p. 773.
[34] ALVÁREZ HERNÁNDEZ, J. *Practicum Protección...* cit, p. 773.

encargado-responsable de tratamiento, es decir, sin la dilación indebida. Conforme al artículo 34 del RGPD debería haber sido el Hospital en su consideración de responsable del tratamiento que tenía que haberlo comunicado a los interesados.

No resulta acertado el argumento alegado por el responsable del tratamiento al indicar que, debido al número de afectados, resultaba imposible comunicarse con ellos. En caso de que esta comunicación suponga un esfuerzo desproporcionado con relación a los riesgos para las libertades pueden hacer uso de blogs corporativos, o comunicados de prensa[35]. En Internet también se encuentran modelos fácilmente localizables de comunicación de una quiebra de seguridad a un afectado, pudiendo enviar el mismo modelo a todos los afectados.

Tanto la no notificación por parte del encargado del tratamiento al responsable, como la no notificación a la autoridad competente son conductas sancionables por la LOPDGDD, y esta sanción será posteriormente determinada.

TERCERO. Reparación del daño

Como hemos ido analizando a lo largo del presente Dictamen los tratamientos de datos personales pueden generar riesgos que deriven daños y perjuicios, si no se actúa diligentemente. Precisamente la producción de un daño derivado de un tratamiento es la que permite al afectado ejercer varias acciones para su resarcimiento.

Para la satisfacción de esta indemnización el RGPD, en su artículo 82 establece una acción orientada a obtener la indemnización de daños y perjuicios sufridos por la conducta del responsable o encargado del tratamiento.

Si los afectados desean que prospere una acción de responsabilidad civil (artículo 82 RGPD) el reclamante debe acreditar que concurren los siguientes requisitos: condición de responsable o encargado del reclamado, infracción de la normativa de

[35] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Guía para la notificación…* cit., p. 28

protección de datos del RGPD, daños y perjuicios efectivamente ocasionados y que existe relación de causalidad entre la infracción y el resultado.[36]

Determinar el sujeto ante el cual se exige la responsabilidad civil ya sea responsable o del encargado del tratamiento no tiene mayor complicación para los afectados, será la persona con la que esté vinculado contractualmente en el momento que el afectado otorgó su consentimiento para el tratamiento (artículo 99.2 RGPD).

Por consiguiente, para que se materialice esta indemnización el afectado deberá probar que la violación de datos de carácter personal es imputable al responsable o encargado del tratamiento, a este aspecto puede ayudar la AEPD si publica una decisión que declara la existencia de la infracción.

En tercer lugar, los afectados deberán probar la existencia, alcance y la cuantificación de los daños sufridos, que pueden ser tanto patrimoniales como no patrimoniales[37]. Los daños sufridos son claramente probables, para ello tienen que acudir a los motores de búsqueda y buscar sus nombres, en ese momento se les remite a las páginas web mencionadas en los antecedentes de hechos y ahí se puede ver todos sus datos de carácter personal.

En cuarto lugar, los afectados deberán acreditar una existente relación de causalidad entre la infracción denunciada y el daño sufrido. Esta relación de causalidad se trata en profundidad en el apartado CUARTO del Fundamento Segundo Obligaciones y responsabilidades derivadas del incidente de seguridad[38].

Por otro lado, a los afectados por la violación de datos de carácter personal del Hospital Nuestra Señora de la Salud se les confiere una serie de derechos reconocidos tanto en la normativa de protección de datos a nivel europeo como estatal que les

[36] RUBÍ PUIG, A. "Daños por infracciones del derecho a la protección de datos personales El remedio indemnizatorio del artículo 82 RGPD." Revista de Derecho Civil, vol. V, núm. 4, octubre-diciembre de 2018; p. 57

[37] RUBÍ PUIG, A. "Problemas de coordinación y compatibilidad entre la acción indemnizatoria del artículo 82 RGPD y otras acciones en derecho español", Mimeo, Universitat Pompeu Fabra, 2018, pp. 1-34

[38] RUBÍ PUIG, A. "Daños por infracciones del…" cit; p. 59

permiten exigir al Hospital y a Dataprotector que se reparen los daños causados por su grave negligencia en el tratamiento de datos. Es el responsable del tratamiento el que tiene que facilitar información acerca del procedimiento y de estos derechos de una manera clara y sencilla.

El Hospital como responsable del tratamiento tiene encomendada esta función conforme al artículo 12 del RGPD, deberían haber facilitado información, sobre el ejercicio del *derecho al olvido* que les permite reparar el daño ocasionado, suprimiendo de las URLS los datos de carácter personal publicados.

Esta obligación de notificación de los derechos de los interesados se aprecia en el Procedimiento de la AEPD[39] en el cual un paciente de la entidad MEDICINA PSICO-ORGÁNICA, S.L recibe un tratamiento sin obtener, en ningún momento del mismo, información de los derechos a ejercer. A raíz de esta falta de notificación en su Fallo, se apercibe a la entidad por la comisión de una infracción del artículo 13 del RGPD.

Este motivo justifica la total incertidumbre en la que se hallan Juan García Ferrer y María José Martínez Amor, del mismo modo que el resto de los afectados, para poder ejercer sus derechos y exigir la reparación del daño.

A título adicional, la AEPD, a través de una de sus guías[40], en materia de pacientes y usuarios de la sanidad reconoce la obligación de atender a los derechos de los afectados en el plazo de un mes, e importante, con carácter gratuito, tratándose de unas cuestiones comunes al ejercicio de todos los derechos.

El TC ha reconocido en su marcada jurisprudencia el ejercicio de este derecho, en una de sus sentencias, de análoga aplicación al presente supuesto, en su Fundamento de Derecho Sexto reconoce que la persona afectada puede solicitar en cualquier momento el ejercicio de los derechos de acceso, rectificación, cancelación y oposición

[39] Procedimiento AEPD, Nº: PS/00288/2019, 938-051119
[40] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Guía para pacientes y usuarios de la sanidad*, 2019, p. 9

dirigiéndose con un escrito a la persona titular de la gerencia del Servicio Navarro de Salud.[41]

La AEPD nos explica que su ejercicio tiene carácter gratuito y debe ser resuelto en el plazo de un mes, prorrogable como máximo dos meses más. No es necesario que la solicitud se presente por medios físicos, si lo desean los afectados pueden presentarla por medios electrónicos y pueden ejercer sus derechos directamente o mediante representante legal o voluntario[42].

Los derechos de los interesados reconocidos en los artículos 15 a 22 del RGPD son personalísimas, es decir, es el interesado el que de manera personal e individual puede ejercerlos frente al responsable. Ello no obsta a, si varios afectados lo desean puedan ejercerlo por medio de representante legal o voluntario (artículo 12.1 LOPDGDD), que debe ser expresamente designado y con poder específico para el ejercicio de ese derecho[43].

Debemos partir de que los afectados por la violación de datos de carácter personal tienen, independientemente de que se hubiera producido o no la violación, pueden acceder a aquellos datos que hubieren facilitado al Hospital Nuestra Señora de la Salud en cualquier momento del tratamiento. Tampoco se les puede negar que el responsable no les indique el fin del tratamiento ni los destinatarios a los que se les ha comunicado los datos personales. Esto es lo que se conoce como Derecho de Acceso y se encuentra recogido en el artículo 15 del RGPD y 13 de la LOPDGDD.

La cuestión más relevante para el presente caso de los distintos derechos a ejercer por los afectados por la brecha de seguridad es el derecho de supresión o "derecho al olvido" que se recoge en el artículo 17 RGPD y 15 LOPDGDD. Este derecho de supresión está estrechamente vinculado con la salvaguardia del derecho fundamental a la protección de datos personales frente al uso de la informática[44].

---

[41] STC (Pleno) 25 de septiembre de 2014

[42] https://www.aepd.es/es/derechos-y-deberes/conoce-tus-derechos Consulta día 11/11/2021

[43] ALVÁREZ HERNÁNDEZ, J. *Practicum Protección...* cit, p. 441

[44] ALVÁREZ HERNÁNDEZ, J. *Practicum Protección...* cit, p. 482

Ejerciendo este derecho Juan García Ferrer y María José Martínez Amor, al igual que el resto de afectados, permite que sus datos sean suprimidos, sin dilación indebida, por parte del responsable del tratamiento si concurre alguna de las circunstancias del artículo 17.1 RGPD

Dichas circunstancias se encuentran numeradas y el presente supuesto podría englobarse en varias de ella. Por una parte, podría ser discutible si el uso de datos se está destinando a fines de marketing directo, cuyo caso entraría dentro del artículo 17.1.c al poder obtener un lucro las URLS por resolver las consultas. También por un tratamiento ilícito del 17.1.d al haber sido estos datos tratados ilícitamente y destinarse a un fin distinto al original[45].

Gracias a este derecho de supresión se podrá solicitar que, en los enlaces en los que aparece los datos personales de los afectados, no figuren en los resultados de una búsqueda en Internet realizada por tu nombre. Así evitarán que sus datos personales sigan en Revisatusalud.com, Consultatussíntomas.com, Descrubretupatología.com.

Los motores de búsqueda también se encuentran sometidos a la normativa de protección de datos, como reflejó el TJUE en una Sentencia[46] la cual sentó jurisprudencia para el ejercicio de supresión de datos de carácter personal que obren en poder de dichos motores. En su Considerando 36 relativo a la cuestión prejudicial, presentado por el Gobierno de España, reconoce que los motores de búsqueda desempeñan un papel decisivo en la difusión global de dichos datos en la medida en que facilita su acceso a todo internauta que lleva a cabo una búsqueda a partir del nombre del interesado.

También se reconoce en el Considerando 39 de la misma Cuestión Prejudicial como GOOGLE, en su función de motor de búsqueda, afecta al derecho fundamental de la vida privada del internauta, y en la determinación de los fines y objetos del tratamiento debe adecuarse al RGPD. Esta Sentencia impide que se difunda información personal a

[45] ALVÁREZ HERNÁNDEZ, J. *Practicum Protección...* cit, p. 492
[46] STJUE (Gran Sala), 13 de mayo de 2014.

través de Internet si las publicaciones no cumplen con los requisitos de adecuación y pertinencia[47].

El Tribunal Supremo también se pronunció en una de sus Sentencias[48] en la cual se presenta un interés casacional objetivo para la formación de jurisprudencia en relación al derecho al olvido. En esta Sentencia se plantea la cuestión de determinar si el derecho fundamental a la protección de datos de carácter personal del reclamante ante la AEPD debe prevalecer sobre el derecho de acceso de los internautas a los datos publicados en unas plataformas de quejas facilitado por Google.

En su Fundamento de Derecho Cuarto se aprecia como reconoce que, por una supuesta lesión del derecho al honor, intimidad y propia imagen, los afectados están legitimados para fundamentar una acción de reclamación ante la entidad proveedora de los servicios de motor de búsqueda o ante la AEPD.

No obstante, los afectados no tienen la necesidad de acudir exclusivamente contra el Hospital en su función de responsable del tratamiento para que estos datos se supriman de Internet, si lo desean pueden ejercer este derecho "al olvido" contra los motores de búsqueda, es decir, contra GOOGLE directamene.

Este formulario fácilmente accesible en el motor de búsqueda de GOOGLE permite solicitar que se retiren determinados resultados de búsqueda de Google devueltos en consultas que incluyen tu nombre. Google actúa como responsable del tratamiento de los datos personales a la hora de determinar los resultados que se encuentran en sus búsquedas[49].

A la hora de cumplimentar los datos deberán identificarse de manera individual Juan García Ferrer y María José Martínez Amor, o cualquiera de los afectados que lo desee, incluyendo una dirección de correo electrónico y su país de origen.

---

[47] https://www.aepd.es/es/areas-de-actuacion/internet-y-redes-sociales/derecho-al-olvido Consulta día 11/11/2021

[48] STS, 5 de julio de 2019

[49] https://www.google.com/webmasters/tools/legal-removal-request?complaint_type=rtbf&visit_id=637663615838423141-2500234284&hl=es&rd=1 Consulta día 12/11/2021

No será necesario que actúen en nombre de ninguna de otra persona a la hora de presentar la solicitud, únicamente en nombre de su hijo Francisco García Martínez, como sujetos de la patria potestad al no estar este capacitado legalmente.

A pesar de ello, si desean ser asistidos de asistencia letrada pueden hacerlo indicándolo en dicho formulario, y justificando después la relación legal con la persona en cuyo nombre presenta la solicitud.

Continuando con la cumplimentación después deberán indicar que los URLS de los que desean retirar información son: Revisatusalud.com, Consultatussíntomas.com, Descrubretupatología.com.

En cuanto a los motivos de la eliminación deben indicar claramente que han sido víctimas de una violación de datos de carácter personal originada por una brecha de seguridad del Hospital de Nuestra Señora de la Salud, y que a raíz de ello obran en poder de estas tres páginas web (Revisatusalud.com, Consultatussíntomas.com, Descrubretupatología.com.) información confidencial acerca de todo su historial clínico, desde documentación relativa a la hoja clínicoestadística, hoja de ingreso, órdenes médicas, su evolución, hasta informes de quirófano y anatomías patológicas, ya sean de este Hospital u otro.

Finalmente deberán indicar el nombre que escriben en el buscador que les redirecciona a las páginas web donde se ve reflejada sus datos de carácter personal y su firma.

El motivo por el cual se ejerce el derecho contra el motor de búsqueda es que este realiza una función de difusión universal, sumado a que la búsqueda en Internet se puede realizar por el nombre, puede suponer un ataque a su intimidad desproporcionado.

De hecho, la Audiencia Nacional ya se ha pronunciado en varias ocasiones acerca de la desvinculación de datos de carácter personal reflejado en un motor de búsqueda.

Por ejemplo, la Sentencia de la Audiencia Nacional[50] relativa a tutela de los derechos resuelve sobre una reclamación de tutela de derechos a Google Inc para que el nombre del interesado no se vincule a una determinada URL. En su Fundamento de Derecho TERCERO se refleja el derecho de toda persona a que de los motores de búsqueda en Internet eliminen de las listas de resultados, a raíz de una búsqueda, aquellos datos que sean inadecuados, inexactos o no pertinentes.

A su vez la AEPD se ha pronunciado en varias ocasiones en distintos procedimientos estimando solicitudes del recurrente en relación a la eliminación de búsqueda de distintos enlaces. Por ejemplo, en uno de sus recursos[51] se estima la reclamación de un afectado, consistente en la eliminación de los resultados de búsqueda de cuatro enlaces referidos a la publicación de candidaturas a elecciones generales del año 2003 y 2004 en los cuales se mencionaban datos de carácter personal acerca de sus votaciones a candidatos.

En particular al supuesto aplicable cabe citar una Resolución[52] de la AEPD que liga perfectamente con la situación actual en las que se encuentran los afectados. En esta Resolución se solicita que se elimine de Internet ciertos enlaces que afectan a la vida privada del afectado que no tienen relevancia pública y que además son obsoletos. La AEPD decide suprimir dichos enlaces respaldándose en la argumentación que dichos afectan a la vida privada del afectado, sin tratarse este de un personaje público.

En España desde la sentencia del STJUE anteriormente nombrada del año 2014 hasta enero de 2020, Google, a través de su portal de "transparencia", ha recibido 83554 solicitudes de eliminación de información, de las cuales solamente se han visto desestimado un 46,1%. Además, tiene un carácter gratuito.

[50]SAN, 20 de diciembre de 2019, ECLI:ES:AN:2019:4735
[51] Recurso AEPD nº 389/2018
[52] Resolución AEPD nº252/2018

CUARTO. Determinación de las infracciones cometidas por el encargado del tratamiento y responsable de tratamiento de protección de datos, y la consiguiente sanción.

La violación de datos de carácter personal se ha originado a raíz de una serie de infracciones cometidas por el responsable del tratamiento y el encargado que convienen determinar, con el fin de tipificar su conducta y determinar el régimen sancionador aplicable. Son responsable y encargado del tratamiento los *sujetos pasivos del régimen sancionador*, como se indica en el artículo 83.4 del RGPDA y 70 LOPDGDD.

Para ello es necesario probar la existencia de una *relación de causalidad* entre el daño cuyo resarcimiento se pretende y la conducta imputada al agente del daño, derivada del incumplimiento de derechos y obligaciones que recaen sobre el responsable y encargado del tratamiento[53]. El *nexo causal* se da claramente al quedar probado que es, a raíz de la negligencia cometida por el responsable y encargado del tratamiento, el motivo por el que se ha originado la brecha de seguridad.

El hecho de que concurra actuaciones de terceros con actuaciones negligentes del responsables o encargados del fichero no exime de la responsabilidad pertinente al encargado o responsable del tratamiento. Por lo que en este supuesto en el que se han incumplido los deberes de seguridad de los ficheros de datos, no son desconocedores de que la actuación de un tercero ajeno al fichero es un rasgo típico que puede darse[54].

En primer lugar, El Hospital Nuestra Señora de la Salud como responsable del tratamiento asumirá la responsabilidad que le corresponda por las infracciones cometidas por cualquier tratamiento de datos, ya que esta debe quedar establecida, ya sea realizado por ella mismo o como en el presente supuesto a través de Dataprotector, encargado de tratamiento como observamos en el Considerando 74 del RGPD.

[53] BUSTO LAGO, J. M "La Responsabilidad Civil de los responsables de ficheros de datos personales y de los encargados de su tratamiento". Revista Doctrinal Aranzadi Civil-Mercantil num.5, 2006

[54] BUSTO LAGO, J. M "La Responsabilidad Civil de los responsables de ficheros…" cit. p. 31

Por otro lado, Dataprotector, encargado de tratamiento, no ha cumplido con su obligación de avisar al responsable del tratamiento de la violación de datos de carácter personal, desde que este fue conocedor de la misma.

Para cumplir con su obligación debería haber descrito la naturaleza de la violación de la seguridad de los datos personales, incluyendo, si fuera posible, el número aproximado de interesados afectados, así como el número de registros de datos personales afectados, una descripción de las posibles consecuencias de la violación de la seguridad de los datos personales y una descripción de las medidas adoptadas o propuestas para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos[55].

Las Partes responderán separadamente de la responsabilidad que, en su caso, les fuera exigible a las mismas, manteniendo indemne a la otra parte siempre y cuando la responsabilidad exigible se derivara de una acción u omisión de cada una de ellas que hubiera producido algún daño a la otra conforme a la legislación de protección de datos aplicable.

Las infracciones que puedan cometer responsable y encargado del tratamiento se encuentran recogidas en la normativa sobre protección de datos en el artículo 83 RGPD y en los artículos 71 a 74 LOPDGDD.

El artículo 71 de la LOPDGDD hace una remisión directa a la normativa europea de protección de datos indicando que constituyen infracciones los actos y conductas de los apartados 4, 5 y 6 del Artículo 86 del RGPD.

Las infracciones perciben una diferenciación en función de si se trata de infracciones de carácter muy grave, grave o leve, conforme a la LOPDGDD en los artículos 72, 73 y 74.

[55] AGENCIA ESPAÑOLA PROTECCIÓN DE DATOS. *Guía para la notificación de brechas..*, cit, p. 22.

En el presente caso se han visto afectados principios básicos de la protección de datos del artículo 5 del RGPD, en particular el *principio de confidencialidad*, por ello resultaría aplicable el artículo 72 de la LOPDGDD considerándose una infracción muy grave. En concreto, se ha visto vulnerado el principio de confidencialidad, siendo este la piedra angular sobre la que orbita la protección de datos.

Otra infracción muy grave es la de *no notificar a los afectados los derechos* que se le confieren en materia de protección de datos recogidos en los artículos 13, 14 y 15 RGPD, como se especifica en el artículo 73.h LOPDGDD.

Entrando en la categoría de infracciones graves recogidas en el artículo 72 LOPDGDD también son varias las infracciones cometidas por parte del Hospital y Dataprotector.

En materia de las *medidas de seguridad técnicas y organizativas* anteriormente descritas considero que la infracción cometida debe ser asumida por el Hospital como responsable del tratamiento. La explicación es que Dataprotector al no pactar ningún contrato desconocía la existencia de dichas medidas y su adopción. El artículo 72 f) tipifica como falta grave: "la falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento, en los términos exigidos por el artículo 32.1 del Reglamento (UE) 2016/679".

Para ser más precisos esta *falta de formulación previa del contrato con el encargado* supone a su vez la comisión de otra infracción grave, la de encargar el tratamiento de datos a un tercero sin la previa formalización de un contrato u otro acto jurídico escrito con el contenido exigido por el artículo 28.3 del Reglamento (UE) 2016/679, artículo 73.K LOPDGDD.

Siguiendo con la comisión de las infracciones graves, Dataprotector debería *haber notificado al responsable del tratamiento la violación de datos de carácter personal*, tan pronto como fue conocedora de esta, esto se tipifica como una infracción grave del artículo 73.q LOPDGDD.

Es parte de la *responsabilidad proactiva de los responsables del tratamiento*, o encargados, notificar las brechas de datos personales ante la Autoridad de Control. Esta notificación no implica una sanción, sino que sirve para demostrar que han actuado con la diligencia debida a la hora de ejecutar la obligación de responsabilidad proactiva del RGPD[56].

Del mismo modo que el responsable del tratamiento ha infringido el deber de comunicar, en el plazo de setenta y dos horas (artículo 33 RGPD) la violación de datos de carácter personal a la autoridad competente, artículo 73.r LOPDGDD.

Sin olvidar que responsable y encargado del tratamiento respectivamente han incurrido en otra infracción al hacer *caso omiso de las recomendaciones realizadas por Antonio Marcuello*, DPD del Hospital Nuestra Señora de la Salud.

Habiendo determinado ya las infracciones cometidas por el responsable y el encargado conforme al RGPD y la LOPDGDD conviene orientar a Don Juan García Ferrer y Doña María José Martínez Amor, aplicable al resto de afectados, el régimen sancionador al que se someterían el encargado y el responsable del tratamiento.

Las *sanciones* que se impongan deberán ser efectivas, proporcionadas y disuasorias. Para cumplir con este mandato se habilita que, en todos los Estados miembros, la Autoridad de control (AEPD) tenga la posibilidad de imponer sanciones por vulneraciones del reglamento, atendiendo a las circunstancias concretas de cada supuesto[57].

Existen varios tipos de sanciones extraíbles de la lectura de lo artículos 83 y 84 del RGPD, por un lado, las sanciones económicas o multas administrativas, y, por otro lado, otro tipo de sanciones elegibles por los Estados miembros, que respeten los principios de proporcionalidad y disuasión, como pueden ser sanciones penales. Estas multas se impondrán, adicionalmente, o de forma sustitutiva con las medidas contempladas en los

[56] AGENCIA ESPAÑOLA PROTECCIÓN DE DATOS. *Guía para la notificación de brechas…* cit., p. 45.
[57] ALVÁREZ HERNÁNDEZ, J. *Practicum Protección...* cit, p. 894

artículos 58.2.a LOPDGDD y 83.2 RGPD[58]. Un ejemplo de estas medidas adicionales se trata del apercibimiento cuando ya se ha cometido la infracción, pero también puede ser que se requiera de una especial atención al ejercicio de los derechos, etc.

Cierto es que la experiencia nos indica que la AEPD, antes de imponer una sanción por vulneración de datos de carácter personal suele apercibir al presunto infractor a que tome las medidas necesarias para que se cese en esta actividad infractora. Es en caso de que haga caso omiso de este aviso cuando impone la sanción correspondiente. En el presente supuesto debido a la gravedad de la violación de datos de carácter personal estimo oportuna una sanción directa sin apercibimiento previo.

En el artículo 83 del RGPD hallamos las condiciones generales para la imposición de *multas administrativas*. En su punto primero se aprecia como estas deben atender a cada caso individual para ser así efectivas, proporcionadas y disuasorias. Será la AEPD como autoridad de control la que deba garantizarlo.

Son varios los factores que voy a valorar a la hora de establecer una sanción para el responsable del tratamiento y el encargado, independientemente de la sanción que decida imponer la AEPD como autoridad competente al respecto.

En cuanto al nivel de graduación y atenuación de las sanciones contempla el artículo 83.2 RGPD, y lo modula atendiendo al llamado principio de responsabilidad proactiva, distinguiendo si se trata de una empresa o no. En el presente caso nos encontramos ante un Hospital, por ende, no se trata de un particular y debemos considerar que nos encontramos frente a una persona jurídica compuesta por muchos elementos que permite graduar la sanción. En el artículo 76 LOPDGDD se establecen criterios adicionales para la graduación de la sanción que se pueden tener en cuenta a la hora de su determinación[59].

Tomaré de referencia los distintos aspectos que establece el artículo 83.1 del RGPD, comenzando por la naturaleza, gravedad y duración de la infracción (artículo 83.2.a RGPD). La naturaleza ha quedado claramente establecida que se trata de datos de

[58] ALVÁREZ HERNÁNDEZ, J. *Practicum Protección...* cit, p. 896.
[59]ALVÁREZ HERNÁNDEZ, J. *Practicum Protección...* cit, p. 912 y 913

carácter personal con especial protección, al tratar asuntos relativos a la salud de los pacientes del Hospital Nuestra Señora de la Salud. Es por este motivo por el cual la violación de datos de carácter personal reviste una especial gravedad al afectar con su alcance a tantos afectados y ser datos tan vulnerables.

La duración de la infracción ya hemos apreciado como ha tenido una duración excesiva en el tiempo, incluso sin llegar a determinar todavía desde cuando obran los datos en poder de Revisatusalud.com, Consultatussíntomas.com, Descrubretupatología.com. Puede llegar a resultar oportuno preguntar al responsable de la página web que facilite información acerca de cuándo recibió esos datos, y recurrir a un perito informático de parte que ayude a resolver esta cuestión.

El siguiente aspecto es la intencionalidad o negligencia de la infracción (artículo 83.2.b RGPD). No considero que haya intencionalidad por parte del Hospital o Dataprotector que se originara la brecha de seguridad que derivó en la violación de datos de carácter personal. No obstante, ello no obsta a apreciar una grave negligencia por su parte al no prestar atención a las indicaciones de Antonio Marcuello como DPD, en cuanto a medidas de seguridad previas, o la notificación a interesados o AEPD cuando fueron conocedores de la violación.

En relación a las medidas adoptadas por el encargado o responsable del tratamiento para paliar los daños y perjuicios sufridos por los interesados (artículo 83.2.c RGPD), de sus actuaciones extraemos que resultan claramente insuficientes para mitigar los efectos de la brecha de seguridad.

El grado de responsabilidad del responsable o el encargado del tratamiento (artículo 83.2.d) es claramente alto, y más teniendo en consideración que para determinar esta se tiene en cuenta las medidas técnicas u organizativas que hayan adoptado, habiendo visto que no fueron suficientes.

El sexto aspecto a considerar es el grado de cooperación con la autoridad de control con el fin de poner remedio a la infracción y mitigar los posibles efectos adversos de la infracción (artículo 83.2.f). No ha habido ninguna cooperación voluntaria del Hospital Nuestra Señora de la Salud o Dataprotector con la AEPD con el fin de poner remedio a

la infracción. Un aspecto recurrente en el Dictamen, y que no podemos olvidar es que se trata de datos de carácter especial afectados por la infracción (artículo 83.2.g).

El último aspecto del RGPD que voy a tener en cuenta para estimar la posible sanción se trata de la forma en que la autoridad de control tuvo conocimiento de la infracción, en particular si el responsable o el encargado notificó la infracción y, en tal caso, en qué medida (artículo 83.2.h).

Dataprotector indicó que notificó la violación de datos tan pronto como fue conocedora de la brecha de seguridad mediante una comunicación a la AEPD y, simultáneamente, al responsable del tratamiento. La fecha de esta comunicación se remonta al año 2021, tres meses después de que los afectados observaran que sus datos de carácter personal se encontraban en las páginas web y hubieran avisado de ello a Nuestra Señora de la Salud.

Como el responsable y encargado del tratamiento incumplen de manera negligente varias de las disposiciones del RGPD, la cuantía total de la multa administrativa no será superior a la cuantía prevista para las infracciones más graves, artículo 83.3 RGPD.

El artículo 83.5 del RGPD nos ofrece un abanico para solicitar una multa administrativa al encargado y responsable del tratamiento de hasta 20.000.000€ al haber afectado a varios principios básicos para el tratamiento recogidos en los artículos 5,6,7 y 9, y además por afectar a los derechos de los interesados del artículo 12 a 22, como el derecho de oposición.

Pero no debemos olvidar la normativa española en materia de protección de datos porque el RGPD en su artículo 84,1 nos remite a los Estados miembros para que en sus normas establezcan otras sanciones aplicables a las infracciones del presente Reglamento.

De hecho, la LOPDGDD en su artículo 76.2 nos permite tener en cuenta otros factores no previstos por el RGPD como son:

- El carácter continuado de la infracción al haberse prolongado durante varios años en el tiempo.
- La existencia de una total vinculación del encargado y responsable con la realización de tratamientos de datos personales, al tener encomendado esta finalidad del tratamiento.
- La afectación a los derechos de los menores, siendo Francisco García Martínez de 13 años de edad, hijo de los interesados que plantean la consulta.

Por todo ello considero y recomiendo solicitar a Don Juan García Ferrer y María José Martínez Amor la imposición de 10.000.000€ al Hospital Nuestra Señora de la Salud como responsable del tratamiento al haber cometido las infracciones siguientes:

- vulneración del principio de confidencialidad del artículo 6.1 RGPD
- no notificar a los afectados los derechos que se le confieren en materia de protección de datos
- falta de formulación previa del contrato con el encargado, artículo 28.3 RGPD
- la falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento, en los términos exigidos por el artículo 32.1 del Reglamento.
- Falta de comunicación a la autoridad competente (AEPD) de la brecha de la violación de datos de carácter personal.
- Hacer caso omiso de las recomendaciones realizadas por el DPD para evitar que se origine una posible brecha de seguridad.

En cuanto a Dataprotector considero que la multa administrativa debe ser menor, primero por haber cometido un número inferior de infracciones respecto al responsable, y segundo por no tener conocimiento de cómo haber actuado en caso de una violación de datos de carácter personal al no haber suscrito un contrato con el mismo No por ello le exime de culpa, como ya hemos indicado con anterioridad ello no le impide conocer la normativa de protección de datos y cómo se debe actuar frente a tales situaciones.

Aun así, considero oportuno solicitar la imposición de una multa administrativa de 5.000.000€ a Dataprotector como encargado del tratamiento por haber cometido:

- la falta de notificación del encargado del responsable al responsable del tratamiento en el plazo de 72 horas desde que fue conocedor de la brecha de seguridad.
- Hacer caso omiso de las recomendaciones realizadas por el DPD para evitar que se origine una posible brecha de seguridad.

Ya se ha pronunciado en varias ocasiones en sus procedimientos AEPD en relación a la posibilidad de imponer una sanción con una cuantía de 20.000.000€, cabría resaltar los siguientes los cuales se centran en el ámbito sanitario:

Un procedimiento de la AEPD[60] que dimana sobre ello es el interpuesto por un interesado contra el INSTITUTO DEL DAÑO CEREBRAL Y PSÍQUICO, S.L por afectar también a uno de los principales básicos del tratamiento de datos, siendo en este caso la negativa del derecho de acceso del interesado a su historial clínico. Como se le niega este derecho se comete una infracción muy grave del artículo 83 RGPD y, por ende, la posibilidad de imponer esta sanción.

Con ello quiero resaltar la idea de que no resulta desorbitado solicitar una multa de tal magnitud al ver como la propia AEPD recoge en el Procedimiento anteriormente mencionado prevé esta multa, y la propia normativa determina este rango.

QUINTO. Responsabilidad civil

En el apartado de reparación del daño ya se ha descrito la necesidad de indemnización de daños y perjuicios reclamable por los afectados y se ha indicado que los sujetos que deben hacer frente a dicha responsabilidad son el responsable y el encargado al ser los causantes de la brecha de seguridad.

En primer lugar, el responsable del tratamiento sigue siendo el principal sujeto sobre el que recae la responsabilidad civil por daños y perjuicios cuando se comete una infracción normativa. El tratamiento de datos se concibe como una actividad que genera riesgos, y el ser el responsable la figura que adopta las decisiones básicas al respecto,

[60]Procedimiento AEPD Nº: PS/00281/2020

este es el responsable último de todos los daños que materialicen de los riesgos del tratamiento[61].

Una vez que quede acreditado las infracciones descritas en el apartado anterior, el responsable deberá compensar a los afectados sin que pueda probar que su comportamiento fue diligente o que fue culpa del encargado la infracción[62].

Es el propio RGPD el que define varios tipos de obligaciones que incumben al responsable del tratamiento de cuyo incumplimiento puede servir de título de imputación suficiente de responsabilidad por los daños que se derivaran. En la mayoría de los casos, para determinar la infracción se determinará de observar si el responsable adoptó o no el estándar de diligencia exigible[63].

Podemos apelar a comprobar el nivel de adopción de las medidas de seguimiento y control suficientes para comprobar si ha habido o no un cumplimiento de la normativa de protección de datos correcto, y si no lo ha habido, que el responsable del tratamiento responda por los daños que ha causado.

Toda vez que la responsabilidad objetiva por daños derivados de un tratamiento ilícito de datos personales se materializa en la respuesta de este frente al titular de los datos personales, tanto por los daños causados por una infracción propia como por la cometida por sus encargados.

En segundo lugar, debemos abordar la responsabilidad civil de Dataprotector como encargado del tratamiento. Del mismo modo que al Hospital como responsable, la responsabilidad de Dataprotector se basa en el incumplimiento de una obligación que le incumbe personalmente conforme al RGPD.

---

[61] Véase GELLERT, R.M, "Understanding data protection as risk regulation", Journal of Internet Law 3, num.18, 2015.
[62] ABERASTURI GORRIÑO, U, "El derecho a la indemnización en el artículo 19 de la Ley Orgánica de Protección de Datos de Carácter Personal", Revista Aragonesa de Administración Pública núm. 41-42, 2013, pp. 173-206; p. 190
[63] RUBÍ PUIG, A. "Daños por infracciones del derecho a la…" cit; p. 63

Se deberá valorar subjetivamente si Dataprotector ha adoptado unas medidas suficientes y adecuadas, ha llevado a cabo esfuerzos razonables, o, en definitiva, si ha cumplido con el deber de diligencia exigible en atención a los daños[64]. Si hubiera existido, como legalmente se exige, un contrato entre las partes ayudaría a dilucidar cuáles eran las concretas obligaciones a adoptar por el encargado para determinar su responsabilidad civil.

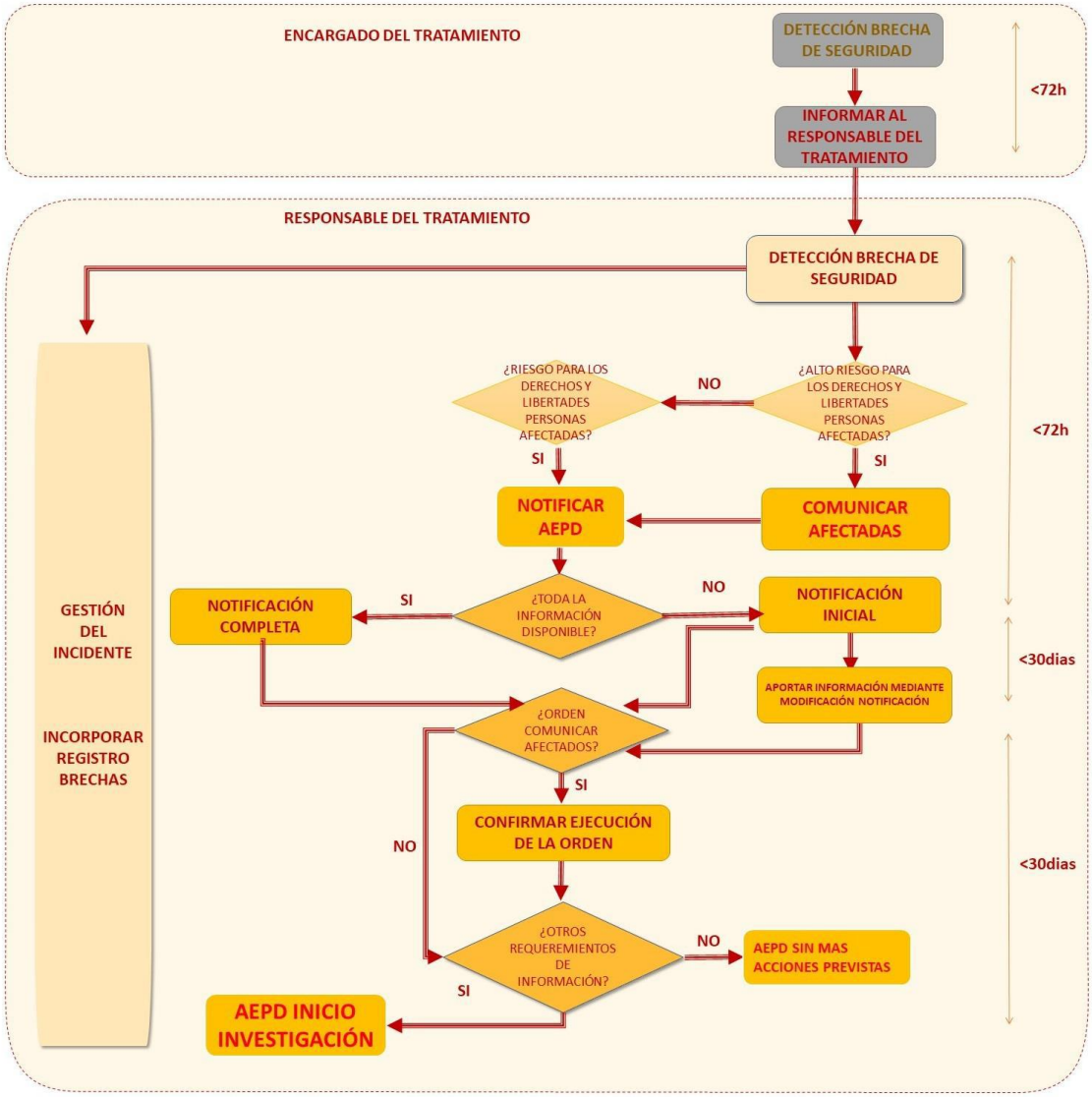
Por supuesto, si los daños derivan de una infracción que, únicamente incumbe al responsable, Dataprotector puede exonerarse del cumplimiento, se refleja en el Fundamento precedente que hay infracciones que solo afectan o bien al encargado, o bien al responsable, como se indica en el artículo 82.2 RGPD.

No obstante, si el incumplimiento se ha producido exclusivamente por el encargado, ambos sujetos responden solidariamente, así que los afectados podrán exigir dicha indemnización bien al Hospital, bien a Dataprotector. Al ser el responsable del tratamiento el que determina los fines y medios, y ser el garante último frente a los interesados del cumplimiento de todas las obligaciones derivadas del tratamiento se justifica esta responsabilidad[65]. Es más, la LOPDGDD, en su artículo 30.2 prevé esta regla de responsabilidad solidaria entre responsable y encargado del tratamiento.

En el artículo 82.5 del RGPD donde, si se desea, se puede ejercer una acción de repetición a favor del encargado o del responsable cuando se haya satisfecho la indemnización de daños al perjudicado. El régimen jurídico de la acción de repetición será el previsto en nuestro CC es el general del artículo 1145.

En la tabla adjuntada a continuación, a modo de resumen conceptual se aprecia de manera simplificada cómo deberían haber actuado el responsable del tratamiento y el encargado del tratamiento tan pronto como fueron conocedores de la brecha de seguridad, y lo que hubiera impedido que incurrieran en la responsabilidad civil aquí descrita.

[64] RUBÍ PUIG, A. "Daños por infracciones del derecho a la…" cit; p. 66
[65] RUBÍ PUIG, A. "Daños por infracciones del derecho a la..." cit; p. 68



66

FUNDAMENTO TERCERO. EJERCICIO DE LOS DERECHOS

PRIMERO. Denuncia ante la Agencia Española de Protección de Datos por parte de los afectados.

Juan García Ferrer y María José Martínez Amor, al igual que el resto de los afectados tienen varias vías a su disposición para conseguir que el Hospital y

66 AGENCIA ESPAÑOLA PROTECCIÓN DE DATOS. *Guía para la notificación de brechas…* cit., p. 14

Dataprotector cesen en su conducta infractora y tomen las medidas necesarias para que los daños ocasionados se dejen de producirse y sean indemnizados por ello.

Puede ocasionarse problemas de coordinación por unos mismos hechos infractores de la normativa sobre protección de datos, al confluir, el proceso administrativo sancionador de la AEPD y el afectado que decida acudir a la jurisdicción civil, derivando en pronunciamiento divergentes sobre unos mismos hechos[67].

La primera vía es mediante la interposición de una reclamación ante la autoridad de control en protección de datos, al haberse originado la brecha de seguridad en España y tener los afectados en este país su residencia habitual, el fuero aplicable es el del ámbito de la AEPD.

La AEPD se trata de una autoridad administrativa independiente de ámbito estatal, con personalidad jurídica, plena capacidad pública y privada y con plena independencia en su actuación, rigiéndose en su ámbito de actuación por lo dispuesto en el RGPD y en la LOPDGDD.

Previamente el encargado o el responsable del tratamiento, conforme al artículo 13.2.d RGPD, cuando Juan García Ferrer y María José Martínez Amor otorgaron su consentimiento para, tanto el tratamiento de sus datos, como los de su hijo, el responsable debería haberles indicado su derecho a presentar una reclamación ante la autoridad de control.

Dentro de las funciones de la AEPD se encuentra, conforme al artículo 47 LOPDGDD la de ejercer las potestades previstas en el artículo 57 del RGPD, es decir, atender las peticiones y reclamaciones formales formuladas por los afectados e interesados, informando a los interesados de sus derechos y del estado de la investigación de dicha reclamación[68].

[67] RUBÍ PUIG, A "Problemas de coordinación y compatibilidad entre la acción indemnizatoria..." cita p. 18
[68] ALVÁREZ HERNÁNDEZ, J. *Practicum Protección...* cit, p. 938

La LOPDGDD en su Título VIII explica de manera pormenorizada cuales son los procedimientos con los que cuentan los afectados en caso de vulneración de la normativa de protección de datos.

Al haberse producido varias vulneraciones de los artículos 15 a 22 del RGPD, en virtud del artículo 63 del LOPDGDD estamos dentro del régimen jurídico aplicable.

La denuncia interpuesta por los afectados se fundamenta en la violación de datos de carácter personal sufrida por los afectados derivado de la conducta negligente del Hospital Nuestra Señora de la Salud y Dataprotector.

No considero que esta solicitud no pase el filtro de la admisión a trámite de las reclamaciones del artículo 65 LOPDGDD al tratarse claramente de una cuestión que versa sobre un aspecto de protección de datos, y no ser abusiva, carecer de fundamento o no aportar indicios racionales de la existencia de una infracción, y por ello la AEPD deberá admitirla.

Posteriormente la Presidencia de la Agencia Española de Protección de Datos dictará acuerdo de iniciación del procedimiento para el ejercicio de la potestad sancionadora, artículo 63 LOPDGDD. En esta fase se concretarán los hechos, identificación de la persona o entidad contra la que se dirige el procedimiento (Hospital Nuestra Señora de la Salud), las infracciones cometidas y sus sanciones.

Considero oportuno que tanto Juan García Ferrer y María José Martínez Amor, como el resto de afectados soliciten, en virtud del artículo 69 LOPDGDD, una serie de medidas provisionales con el objeto de proteger sus datos de carácter personal. La AEPD adoptará dichas medidas en el caso que considere que se produzca un menoscabo grave del derecho a la protección de datos[69].

Con carácter preferente solicitaría el bloqueo o eliminación de todos aquellos datos de carácter personal que obren en poder de Revisatusalud.com,

[69] ALVÁREZ HERNÁNDEZ, J. *Practicum Protección...* cit, p. 997

Consultatussíntomas.com, Descrubretupatología.com, toda vez que se encuentra dentro de las competencias de la AEPD ordenar al responsable que bloquee los datos.

No es la primera vez que la AEPD aprueba esta medida, sirviendo como ejemplo el Procedimiento PS/00146/2011 donde se acordó la inmovilización de un fichero, obligando a la entidad responsable a cesar en la utilización de los datos cedidos de carácter personal, y que el acceso a dicha información quedase totalmente imposibilitado.

Por supuesto los afectados pueden solicitar una acción indemnizatoria, conforme al artículo 82 RGPD, frente al responsable o encargado de tratamiento, al haber infringido estos la normativa sobre protección de datos y haberles causado una serie de graves daños y perjuicios.

Esta idea se ve ratificada en el Considerando 146 del RGPD que indica que el concepto de daños y perjuicios debe interpretarse a la luz de la jurisprudencia del Tribunal de Justicia de la Unión Europea. Esta indemnización que reciban los afectados debe ser total y efectiva.

SEGUNDO. Reclamación por vía judicial.

La posibilidad de la reclamación ante la AEPD no implica que Juan García Ferrer y María José Martínez Amor deban ejercer con carácter exclusivo la acción prevista en el artículo 82 RGPD, y de ahí los problemas de coordinación. Es el artículo 146 RGPD es donde se determina cuál es el régimen que se prevé para determinar la compensación de daños y perjuicios.

Los afectados pueden, si lo desean, esperar a que la AEPD haya concluido el procedimiento sancionador contra el responsable o el encargado del tratamiento por infringir la normativa sobre protección de datos, y posteriormente interponer una demanda civil. De hecho, recomiendo esta opción dado que, en la demanda, como

documento probatorio podrá adjuntar la Resolución firme de la AEPD para probar la infracción normativa[70].

Todos los interesados también han visto afectado su derecho a la intimidad, por ello supone una ventaja acudir al remedio indemnizatorio del artículo 9.3 LO 1/1982, haciendo valer la presunción iuris et de iure de causación de daño moral luego de probarse la intromisión ilegítima en uno de los derechos que protege esta Ley[71]. Es común que los letrados acudan a esta posibilidad cuando se produzca una infracción de la normativa de protección de datos.

Puede que no sea tan atractivo para los afectados el acudir al procedimiento del artículo 82 RGPD, por un lado, por las incertezas sobre la coordinación entre este tipo de acciones y los procedimientos seguidos ante la AEPD. Otro aspecto que resta es la mayor facilidad del art.9.3 de la Ley 1/1982 para el ejercicio de la acción indemnizatoria y la tendencia de los Tribunales españoles a reconocerla con mayor preferencia que la acción del artículo 82 RGPD.

No obstante, con ello no pretendo determinar la acción indemnizatoria a la que decidan acudir los afectados, solo mostrar las distintas opciones procesales con la que cuentan entre las cuales pueden elegir libremente.

La reclamación en vía judicial se fundamenta en que, los afectados por la violación de datos de carácter personal, al tratarse de ficheros de datos privados del Hospital Nuestra Señora de la Salud, pueden ejercer la acción de responsabilidad civil ante los órganos del orden jurisdiccional civil o bien contencioso-administrativo agotada la vía previa, e incluso orden penal al verse afectado el derecho a la intimidad contemplado en los artículos 197 a 200 del CP. Por consiguiente, la demanda ejercitando la acción de responsabilidad civil ante el órgano jurisdiccional objetivo puede ejercitarse sin necesidad de reclamación previa ante la AEPD[72].

[70] RUBÍ PUIG, A. “Problemas de coordinación y compatibilidad entre la acción inemniatoria…” cit., p. 21
[71] ibidem cit., p. 27
[72] BUSTO LAGO, J.M “La Responsabilidad Civil de los..”. cit, p. 37 y 38

El cauce procesal a seguir será el juicio ordinario reflejado en el artículo 241.1.2 LEC, al pretender los interesados la tutela el derecho a la intimidad, honor y propia imagen que se ha visto afectado por la violación de datos, con intervención obligada del Ministerio Fiscal como parte y con carácter preferente para su resolución.

Una estimación subjetiva de la cantidad a reclamar por vía judicial de los afectados, incluyendo tanto daños y perjuicios, como daños morales, estimo que podría llegar a ascender a 100.000€. El baremo que he usado para cuantificar dicho daño se trata de:

- Cantidad de los afectados: como se ha descrito en los antecedentes de hecho, han sido publicados los datos de carácter personal de 500 afectados, siendo un número muy elevado.
- Categoría de datos: los datos de carácter personal afectados revisten de categoría especial, al tratarse de datos de la salud, de ahí que la indemnización exigible sea mayor.
- Falta de la diligencia debida del responsable y encargado del tratamiento, debido a que, a raíz de una serie de inobservancias de la normativa de protección de datos se ha originado la brecha de seguridad.
- Daños morales: aunque se trata del elemento más subjetivo y difícil de cuantificar, claramente se ha producido un perjuicio moral en el honor e intimidad de los pacientes, difícilmente reparable ya que ahora es conocido por varios internautas en la red cuáles son las patologías que estos sufren y padecen.

Como el caso que nos ocupa en la Sentencia del Juzgado de Primera Instancia núm. 7 de Santander[73], cuantificó la indemnización de daños y perjuicios en 22000€ en base a: una vulneración de la intimidad de la denunciante, tras publicar multitud de sus imágenes sin su consentimiento, y la cantidad de los de 8.000 € reclamada por cada uno de los padres por vulneración del derecho de imagen de sus hijos menores, que fueron publicadas sin su consentimiento, lo que hace un total de 22.000 €, estimando así íntegramente la demanda.

[73] SJPI, 12 de enero de 2018.

Atendiendo a las consideraciones vertidas en el presente dictamen, y sobre el extremo objeto de consulta, el Letrado que suscribe cree posible sentar las siguientes:

4. CONCLUSIONES

PRIMERA.

A la luz de las distintas circunstancias acaecidas en el caso que nos ocupa, y tras haber realizado un análisis detallado y exhaustivo del comportamiento de las figuras del responsable y del encargado del tratamiento, que poseen encomendados el tratamiento de datos de carácter personal considero oportunas las distintas pretensiones de los afectados y con el respaldo legal suficiente para que estas se estimen.

SEGUNDA.

Como se puede apreciar, los datos de carácter personal, y sus principios se encuentran totalmente incardinados con derechos reconocidos constitucionalmente como el derecho a la intimidad. Por ello su vulneración implica las consecuencias jurídicas tan remarcables que hemos podidos observar en el presente trabajo.

TERCERA.

A lo largo del Dictamen se ha podido apreciar todas las negligencias que han cometido el Hospital y Dataprotector, desde la tardía notificación a la AEPD de la violación de datos de carácter personal, hasta no notificar a los interesados los derechos que estos pueden ejercer, entre muchas otras.

Todas estas infracciones cometidas por el responsable del tratamiento y el encargado del tratamiento son sancionables conforme a la normativa vigente de protección de datos y, a consecuencia de ello, les corresponde cumplir las pertinentes sanciones.

CUARTA.

Los afectados se encuentran totalmente facultados a solicitar que se resarzan los daños y perjuicios ocasionados por estas graves negligencias cometidas por los responsables del tratamiento de datos.

Y, por supuesto, a que se supriman los datos de los afectados de Internet para que no puedan ser consultados por cualquier internauta a través de los motores de búsqueda.

Este es mi Dictamen, que someto a cualquier otro mejor fundado en Derecho.

En Zaragoza, a 16 de noviembre de 2021.

Fdo.: Javier Turón Hernández

5. BIBLIOGRAFÍA

ABERASTURI GORRIÑO, U, "El derecho a la indemnización en el artículo 19 de la Ley Orgánica de Protección de Datos de Carácter Personal", Revista Aragonesa de Administración Pública núm. 41-42, 2013, pp. 173-206

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Directrices para la elaboración de contratos entre responsables y encargados del tratamiento*.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Guía para la notificación de brechas de datos personales*, 2021

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Guía para pacientes y usuarios de la sanidad*, 2019

ALVÁREZ HERNÁNDEZ, J. *Practicum Protección de Datos 2021*, Thomson Routers, Pamplona (Navarra), 2021

BUSTO LAGO, JOSÉ MANUEL "La Responsabilidad Civil de los responsables de ficheros de datos personales y de los encargados de su tratamiento". Revista Doctrinal Aranzadi Civil-Mercantil num.5, 2006

FERNÁNDEZ LÓPEZ, J. M, «El derecho fundamental a la protección de los datos personal. Obligaciones que derivan para el personal sanitario», Dialnet, Extraordinario XI Congreso Derecho y Salud.

GELLERT, R.M, "Understanding data protection as risk regulation", Journal of Internet Law 3, num.18, 2015.

GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29. *Directrices sobre los delegados de protección de datos (DPD*), 2017

GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29, *Directrices sobre la notificación de las violaciones de la seguridad de los datos personales acuerdo con el Reglamento 2016/*679, 2018

LAÍN ENTRALGO, P., "La historia clínica, historia y teoría del relato patográfico», Madrid, 1998 (reimpresión del original de 1950)", pp. XVi

MERINO MARTÍN, J «Los datos personales relativos a la salud y la Historia Clínica», Revista Aranzadi Doctrinal Num.10, 2019

MESSIA DE LA CERDA BALLESTEROS, J. A. "Consideraciones y perspectivas del delegado de protección de datos". Revista Aranzadi de Derecho y Nuevas Tecnologías num.47, 2018

RUBÍ PUIG, A. "Daños por infracciones del derecho a la protección de datos personales El remedio indemnizatorio del artículo 82 RGPD." Revista de Derecho Civil, vol. V, núm. 4, octubre-diciembre de 2018

RUBÍ PUIG, A. "Problemas de coordinación y compatibilidad entre la acción indemnizatoria del artículo 82 RGPD y otras acciones en derecho español", Mimeo, Universitat Pompeu Fabra, 2018, pp. 1-34

TRONCOSO REIGADA, A. "Las categorías especiales de datos personales en el Reglamento General de Protección de Datos de Unión Europea", *El Derecho.com*, Lefebvre 2019.

RECURSOS ELECTRÓNICOS

- https://www.aepd.es/es/derechos-y-deberes/conoce-tus-derechos Consulta día 11/11/2021
- https://www.aepd.es/es/areas-de-actuacion/internet-y-redes-sociales/derecho-al-olvido Consulta día 11/11/2021
- https://www.google.com/webmasters/tools/legal-removal-request?complaint_type=rtbf&visit_id=637663615838423141-2500234284&hl=es&rd=1 Consulta día 12/11/2021

6. LISTADO DE ABREVIATURAS

- 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 (Reglamento general de protección de datos)→ RGPD
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. → LOPDGDD
- Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. → CP
- Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil. → LEC
- Código Civil → CC
- Constitución Española → CE
- STS → Sentencia del Tribunal Supremo
- AN → Audiencia Nacional
- TJUE → Tribunal de Justicia de la Unión Europea
- Agencia Española de Protección de Datos → AEPD