Identificación del expediente

Resolución de procedimiento sancionador núm. PS 20/2022, referente al Instituto Catalán de la Salud (Hospital de Viladecans)

Antecedentes

1. En fecha 11/06/2021, tuvo entrada en la Autoridad Catalana de Protección de Datos un escrito de una persona por el que formulaba denuncia contra el Hospital de Viladecans, dependiendo del Instituto Catalán de Salud (ICS), con motivo de un presunto incumplimiento de la normativa sobre protección de datos personales. La persona denunciante exponía lo siguiente:

1.1 Que el Hospital de Viladecans había hecho públicas varias URLs donde introduciendo sólo el DNI, sin otra comprobación, se podían obtener datos personales de los pacientes. Concretamente, su nombre, dirección, CIP, fecha de nacimiento, teléfono y correo electrónico.

1.2 Que para acreditar la anterior manifestación, aportaba las siguientes URLs en las que haciendo clic en la opción 'lupa', se obtenían los datos personales mencionados:

https://ciutadania.metrosud.cat/ciutadania/FRM/frm_cambio_identificativo.aspx
https://ciutadania.metrosud.cat/ciutadania/FRM/frm_cambi_data.aspx
https://ciutadania.metrosud.cat/ciutadania/

2. La Autoridad abrió una fase de información previa (núm. IP 252/2021), de acuerdo con lo que prevé el artículo 7 del Decreto 278/1993, de 9 de noviembre, sobre el procedimiento sancionador de aplicación a los ámbitos de competencia de la Generalidad, y el artículo 55.2 de la Ley 39/2015, de 1 de octubre, del procedimiento administrativo común de las administraciones públicas (en adelante, LPAC), para determinar si los hechos eran susceptibles motivar la incoación de un procedimiento sancionador.

3. En esta fase de información previa, en fecha 14/06/2021, el Área de Inspección de la Autoridad realizó una serie de comprobaciones a través de Internet sobre los hechos objeto de denuncia. Así, se constató que accediendo a la web del Hospital de Viladecans (http://www.viladecanshospital.cat/ca/default.aspx), apartado 'Unidad de atención a la ciudadanía > Hagámoslo fácil' en las opciones 'Reclamaciones quejas y sugerencias' y 'Cambio de Datos identificativos', introduciendo el DNI de la persona denunciante y haciendo clic en la opción 'lupa', se obtenían los siguientes datos personales:

Por lo que respecta a la primera opción: nombre, apellidos, número de CIP y teléfono.

Por lo que respecta a la segunda opción: nombre, apellidos, número de CIP, teléfono, dirección del domicilio, y fecha de nacimiento.

También se comprobó que en el mismo apartado 'Unidad de atención a la ciudadanía > Hagámoslo fácil', en las opciones 'Información visitas y pruebas pendientes / cambio de fecha' y 'Consulta lista de espera quirúrgica', siguiendo el mismo proceso de acceso, se podía obtener el número de CIP de la persona denunciante.

Seguidamente, se levantó diligencia de constancia por parte de la instructora y se conservó copia automatizada de los datos personales a los que se había tenido acceso mediante la introducción del DNI de la persona denunciante.

4. En la misma fecha, 14/06/2021, se requirió a la entidad denunciada para que confirmara que mediante introducción de DNI de cualquier paciente en las rutas especificadas en el punto anterior, se podían obtener, en función de la opción seleccionada ("Reclamaciones, quejas y sugerencias", "cambio de datos identificativos", "Solicitud de informes de consultas externas", "solicitud documentación clínica / otros informes de pruebas (no imágenes)", "solicitud copia de 'imagen', 'información visitas y pruebas pendientes / cambio de fecha', 'consulta lista de espera quirúrgica', 'cambio de datos identificativos', 'solicitud cambio de facultativo especialista', 'para cualquier otro tipo de consulta') los siguientes datos personales:

- Nombre, apellidos, número de CIP y teléfono;
- Nombre, apellidos, número de CIP, teléfono, dirección del domicilio, y fecha de nacimiento; o
- Número de CIP

También se requirió a la entidad que indicara en relación a qué pacientes se podían obtener estos datos y si se podían visualizar otros datos clínicos o de salud vinculados al paciente.

5. Con fecha 06/07/2021 y dentro del marco de esta fase de información previa, el Área de Inspección de la Autoridad volvió a acceder a Internet para efectuar nuevas comprobaciones sobre los hechos objeto de denuncia. Así, se constató que accediendo a la página web del Hospital de Viladecans, apartado 'Unidad de atención a la ciudadanía > Hagámoslo fácil' aparecía un mensaje que decía 'Aplicación temporalmente fuera de servicio. Disculpad las molestias' y, por tanto, los datos ya no eran accesibles.

6. En fecha 19/07/2021, el Instituto Catalán de la Salud (Hospital de Viladecans) dio cumplimiento al requerimiento de información a través de escrito en el que exponía lo siguiente:

- Que por error técnico, en la web del Hospital de Viladecans se publicó un entorno de pruebas donde mediante introducción del DNI del paciente, se recuperaba la 'información de filiación' que, según manifestaba, consistía en su nombre, número de CIP , dirección del domicilio, teléfono y dirección de correo electrónico; y que en ningún caso eran datos abiertos de los pacientes del hospital ni de cualquier paciente atendido en la organización, sino sólo de los pacientes 'activos' del Hospital de Viladecans.
- Que no se podía visualizar ningún dato relacionado con la información clínica y asistencial del paciente.
- Que en el momento de detección del error técnico se procedió a la despublicación de las páginas web de forma que no se pueda acceder desde el exterior, es decir, Internet.
- Asimismo, manifestó que en el momento de presentación de respuesta al requerimiento (19/07/2021), ya no se podía acceder a ninguna de las URL denunciadas.

7. En fecha 20/04/2022, la directora de la Autoridad Catalana de Protección de Datos acordó iniciar un procedimiento sancionador contra el ICS por una presunta infracción prevista en el artículo 83.4.a) en relación con el artículo 32; todos ellos del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril, relativo a la protección de las personas

físicas en lo que se refiere al tratamiento de datos personales ya la libre circulación de éstas (en adelante, RGPD). Asimismo, nombró a persona instructora del expediente a la señora (...), funcionario a de la Autoridad Catalana de Protección de Datos. Este acuerdo de iniciación se notificó a la entidad imputada en fecha 22/04/2022.

En el acuerdo de iniciación se concedía a la entidad imputada un plazo de 10 días hábiles para formular alegaciones y proponer la práctica de pruebas que considerase convenientes para defender sus intereses.

El plazo se ha superado con creces y no se han presentado alegaciones.

Hechos probados

La página web del Hospital de Viladecans (http://www.viladecanshospital.cat/ca/default.aspx) permitía acceder a los datos personales de los pacientes, siguiendo la ruta ' *Unidad de atención a la ciudadanía > Hagámoslo fácil',* seleccionando una de las cuatro opciones que se especificarán a continuación, y tan sólo introduciendo el DNI y haciendo clic en la opción ' *lupa'* , sin requerir de ningún otro dato adicional, ni contraseña, ni medida de autenticación adicional .

Opciones:
- O pción ' *Reclamaciones quejas y sugerencias'* : el nombre, apellidos, número de CIP y teléfono.
- Opción ' *Cambio de Datos identificativos'* : el nombre, apellidos, número de CIP, teléfono, dirección del domicilio, y fecha de nacimiento.
- O pción ' *Información visitas y pruebas pendientes / cambio de fecha'* y opción *'Consulta lista de espera quirúrgica'* : el número de CIP

Esta situación se mantuvo por un período de tiempo indeterminado que, como mínimo, comprende desde el día 14/06/2021, fecha en la que el Área de Inspección de la Autoridad efectuó comprobaciones a través de Internet y confirmó la accesibilidad a los datos personales de un paciente mediante introducción de su DNI como único requerimiento de acceso; y hasta una fecha indeterminada pero en todo caso anterior al día 6/07/2021, fecha en la que el Área de Inspección efectuó nuevas comprobaciones y constató que ya no se podía acceder a la ruta mencionada en el primer párrafo de este apartado.

Fundamentos de derecho

1. Son de aplicación a este procedimiento lo que prevén la LPAC , y el artículo 15 del Decreto 278/1993, según lo que prevé la DT 2a de la Ley 32/2010, de 1 de octubre, de Autoridad Catalana de Protección de Datos. De conformidad con los artículos 5 y 8 de la Ley 32/2010, la resolución del procedimiento sancionador corresponde a la directora de la Autoridad Catalana de Protección de Datos.

2. De acuerdo con el artículo 64.2.f) de la LPAC y de conformidad con lo que se indica en el acuerdo de iniciación de este procedimiento, procede dictar esta resolución sin una propuesta de resolución previa, dado que entidad imputada no ha formulado alegaciones al acuerdo de iniciación.

Este acuerdo contenía un pronunciamiento preciso sobre la responsabilidad imputada.

3. Por lo que se refiere al hecho descrito en el apartado de hechos probados, relativo a la seguridad de los datos, es necesario acudir al artículo 32 del RGPD, que dispone:

"1. Teniendo en cuenta el estado de la técnica , las costas de aplicación , y la naturaleza , el alcance , el contexto y las 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 las datos personales de forma rápida en caso de incidente físico o técnico;*
d) *un proceso de verificación, evaluación y valoración regular de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.*
2. *Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichas datos.*
3. *La adhesión a un código de conducta aprobado a tenor del artículo 40 oa un mecanismo de certificación aprobado a tenor del artículo 42 podrá servir de elemento para demostrar el cumplimiento de los requisitos establecidos en el apartado 1 del presente artículo.*
4. *El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales sólo pueda tratar dichas datos siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud del derecho de la Unión o de los Estados miembros".*

Asimismo, de acuerdo con lo dispuesto en la disposición adicional primera de la Ley orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales, cabe mencionar lo que establece el Real decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (ENS) en el ámbito de la Administración electrónica, en su artículo 16:

Artículo 16. ***Autorización y control de los accesos.***

El acceso al sistema de información deberá ser controlado y limitado a los usuarios, procesos, dispositivos y otros sistemas de información, debidamente autorizados, restringiendo el acceso a las funciones permitidas. "

El apartado 4.2.5 *" Mecanismo de autenticación "* del Anexo II ("Medidas de Seguridad") del ENS, determina lo siguiente:

"Los mecanismos de autenticación frente al sistema se adecuarán al nivel del sistema atendiendo a las consideraciones que sean, pudiendo usarse los siguientes factores de autenticación:

- "algo que se sabe": contraseña o claves concertadas.

- "algo que se tiene": componentes lógicos (tales como certificados software) o dispositivos físicos (en expresión inglesa, tokens)

- "algo que se se": elementos biométricos.

Los factores anteriores podrán utilizarse de forma aislada o combinarse para generar mecanismos de autenticación fuerte.

(…)

Nivel BAJO
a) Como principio general, se admitirá el uso de cualquier mecanismo de autenticación sustentado en un solo factor.
b) En el caso de utilizarse como factor " algo que se sabe ", se aplicarán reglas básicas de calidad de la misma .
c) Se atenderá a la seguridad de las credenciales de forma que:
1. Las credenciales se activarán una vez extendido bajo el control efectivo del usuario .
2. Las credenciales estarán bajo el control exclusivo del usuario .
3. El usuario reconocerá que las ha recibido y que conoce y acepta las obligaciones que implica su tenencia , en particular, el deber de custodia diligente , protección de su confidencialidad e información inmediata en caso de pérdida .
4. Las credenciales se cambiarán con una periodicidad marcada por la política de la organización , atendiendo a la categoría del sistema al que se accede .
5. Las credenciales se retirarán y serán deshabilitadas cuando la entidad (persona, equipo o proceso) que autentican termina su relación con el sistema.
(...)"

También el artículo 9.4 de la Ley 21/2000, de 29 de diciembre, sobre los derechos de información concerniente a la salud y autonomía del paciente, ya la documentación clínica, determina que *"los centros sanitarios deben tomar las medidas técnicas y organizativas adecuadas para proteger los datos personales recogidos y evitar su destrucción o pérdida accidental, así como el acceso, alteración, comunicación o cualquier otro procesamiento que no sean autorizado".*

Durante la tramitación de este procedimiento se ha acreditado debidamente el hecho descrito en el apartado de hechos probados, reconocido además por la propia entidad denunciada en sus alegaciones en fase de información previa (IP 252/ 2021), cuando admite haber cometido ' *un error técnico* ' al publicar ' *un entorno de pruebas donde introduciendo el DNI de un paciente se recuperaba información de filiación (nombres, CIP, dirección, teléfono y dirección de correo electrónico).'*

Este hecho es constitutivo de la infracción prevista en el artículo 83.4.a) el RGPD, que tipifica la vulneración de *"las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43"* entre los cuales existe la obligación descrita en el artículo 32 referida a la seguridad del tratamiento.

A su vez, esta conducta se ha recogido como infracción grave en el artículo 73.f) de la LOPDDDD, en la siguiente forma:

"f) La falta de adopción de las medidas técnicas y organizativas que sean apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento, en los términos que exige el artículo 32.1 del Reglamento (UE) 2016/679".

4. El artículo 77.2 LOPDGDD dispone que, en el caso de infracciones cometidas por los responsables o encargados enumerados en el art. 77.1 LOPDGDD, la autoridad de protección de datos competente:

> *"(...) debe dictar una resolución que las sancione con una amonestación. La resolución establecerá asimismo las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se haya cometido.*
> *La resolución se notificará al responsable o encargado del tratamiento, a cuyo órgano dependa jerárquicamente, en su caso, ya los afectados que tengan la condición de interesado, en su caso."*

En términos similares a la LOPDDDD, el artículo 21.2 de la Ley 32/2010 , determina lo siguiente:

> *"2. En el caso de infracciones cometidas con relación a ficheros de titularidad pública, el director o directora de la Autoridad Catalana de Protección de Datos debe dictar una resolución que declare la infracción y establezca las medidas a adoptar para corregir sus efectos . (...)".*

En el presente caso, no procede requerir al ICS la adopción de medidas correctoras para corregir los efectos de las infracciones, ya que se trata de un hecho ya consumado y, además, el ICS, en el momento de detección del error, procedió a la despublicación de las páginas Web. Asimismo , manifestó que en el momento de presentación de respuesta al requerimiento de esta Autoridad (19/07/2021), ya no se podía acceder a ninguna de las URL denunciadas.

Por todo esto, resuelvo:

1. Amonestar al Instituto Catalán de la Salud como responsable de una infracción prevista en el artículo 83.4.a) en relación con el artículo 32, ambos del RGPD.

No es necesario requerir medidas correctoras para corregir los efectos de la infracción, de conformidad con lo expuesto en el fundamento de derecho 4.

2. Notificar esta resolución en el Instituto Catalán de la Salud .

3. Comunicar la resolución al Síndic de Greuges, de conformidad con lo que prevé el artículo 77.5 del LOPDDDD.

4. Ordenar que se publique esta resolución en la web de la Autoridad (apdcat.gencat.cat) , de conformidad con el artículo 17 de la Ley 32/2010, de 1 de octubre.

Contra esta resolución, que pone fin a la vía administrativa de acuerdo con los artículos 26.2 de la Ley 32/2010, de 1 de octubre, de la Autoridad Catalana de Protección de Datos, y 14.3 del Decreto 48/2003 , de 20 de febrero, por el que se aprueba el Estatuto de la Agencia Catalana de Protección de Datos, la entidad imputada puede interponer, con carácter potestativo, un recurso de reposición ante la directora de la Autoridad Catalana de Protección de Datos Datos, en el plazo de un mes a contar desde el día siguiente de su notificación, de acuerdo con lo que prevén el artículo 123 y siguientes de la LPAC. También puede interponer directamente un recurso contencioso administrativo ante los Juzgados de lo Contencioso-Administrativo, en el plazo de dos meses a contar desde el día siguiente de su notificación, de acuerdo con los artículos 8, 14 y 46 de la Ley 29/1998, de 13 de julio, reguladora de la jurisdicción contencioso-administrativa.

Si la entidad imputada manifiesta a la Autoridad su intención de interponer recurso contencioso administrativo contra la resolución firme en vía administrativa, la resolución se suspenderá cautelarmente en los términos previstos en el artículo 90.3 de la LPAC.

Igualmente, la entidad imputada podrá interponer cualquier otro recurso que estime conveniente para defender sus intereses.

La directora,