

Identificación del expediente

Resolución de procedimiento sancionador núm. PS 47/2019, referente al Instituto Catalán de la Salud

Antecedentes

1. En fecha 19/02/2019, tuvo entrada en la Autoridad Catalana de Protección de Datos un escrito de una persona por el que formulaba denuncia contra el Instituto Catalán de la Salud (ICS), con motivo de un presunto incumplimiento de la normativa sobre protección de datos de carácter personal.

En concreto, la persona denunciante, que presta servicios como personal administrativo en un centro del ICS, exponía lo siguiente:

- a. Que en mayo de 2017 había formulado una queja ante el Síndic de Greuges exponiendo que el personal encargado de programar las visitas de los/las pacientes a través del software SAP-Argos -software que sería único y compartido para todos los centros de el ICS en Girona y del Instituto de Asistencia Sanitaria (IAS)- podía acceder al dato relativo al diagnóstico. La persona denunciante indicaba que las personas encargadas de programar las visitas son personas que, como ella, pueden no tener un perfil sanitario, es decir, que son personas con un perfil de administrativo e, incluso de celador/a, por lo que consideraba del todo desproporcionado que este personal accediera a este tipo de información.
- b. Que el Síndic de Greuges había iniciado expediente (...) en relación a su queja. Que en oficio de 11/10/2018, esta institución puso en su conocimiento que, a resultas de sus actuaciones, el Departament de Salut le había facilitado *"una copia del diseño funcional a aplicar para anonimizar dentro del sistema los diagnósticos de los de diferentes puntos, a nivel de episodio como el de la orden clínica, por lo que no se visualizarán en el descriptivo para los usuarios que no sean facultativos, ni personal de enfermería"*, por lo que confiaba en que con esta medida *"el campo diagnóstico no sea accesible para el personal no asistencial"*.
- c. Que en febrero de 2019, cuando se programaba una visita, todavía seguía siendo visible el campo diagnóstico por parte del personal no asistencial.

La persona denunciante, junto con su escrito, aportaba, entre otra, la siguiente documentación:

- Copia de queja formulada ante el Síndic de Greuges en el mes de mayo de 2017.
- Copia del oficio del Síndic de Greuges de 11/10/2018, dirigido a la persona aquí denunciante, al que se ha hecho mención en el apartado b) precedente.
- Copia de un correo electrónico de 05/11/2018 remitido por la Jefa de Admisiones del ICS a varias personas, en el que se informa que *"esta semana se dejarán de ver los diagnósticos a las órdenes clínicas"*.
- Varias impresiones de pantalla del software SAP-Argos -a las que había accedido la persona denunciante como personal con perfil administrativo del ICS- en la que se visualiza el campo diagnóstico de una persona a la que se le había programado una visita .

2. La Autoridad abrió una fase de información previa (núm. IP 53/2019), 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 de motivar la incoación de un procedimiento sancionador, la identificación de la persona o personas que pudieran ser responsables y las circunstancias relevantes que concurrían.

3. En esta fase de información, en fecha 27/03/2019 se requirió el ICS para que informara sobre las siguientes cuestiones:

- Confirmara si el software SAP-Argos utilizado por el ICS en Girona es compartido con el IAS, de forma que, tanto el personal con perfil administrativo o celador/a adscrito al ICS, como el adscrito al IAS, puede acceder al campo diagnóstico de los/las pacientes de cualquiera de las dos entidades.
- Indicara las razones por las que en la fecha del requerimiento no se ha implementado ninguna medida destinada a evitar que el personal no asistencial (administrativo o celador/a) tenga acceso, a través del software SAP-Argos, al diagnóstico de los/las las pacientes.

4. En fecha 11/04/2019, el ICS respondió el requerimiento mencionado a través de escrito en el que exponía lo siguiente:

- Que, efectivamente, el software SAP-Argos utilizado por el ICS en Girona es compartido con el IAS, de modo que, tanto el personal con perfil administrativo o celador/a adscrito al ICS, como el adscrito al IAS, puede acceder al campo diagnóstico de los/las pacientes de cualquiera de las dos entidades
- Que *“los administrativos no tengan acceso a la información de los diagnósticos está desarrollado a nivel de SAP-ARGOS y comporta un cambio estructural. El siguiente paso es su implantación, en la que debe valorarse el impacto asistencial que ello conlleva. En estos momentos, el ICS se encuentra recogiendo todos los roles de los profesionales que no verían y que sí verían la información. Una vez efectuado este cribado, se realizará la implantación del cambio estructural sobre estos profesionales. Que el calendario planificado por estas actuaciones está previsto entre abril y mayo de 2019”*.

5. En fecha 11/06/2019 se requirió nuevamente el ICS para que informara de lo siguiente:

- Indicara si en la fecha del requerimiento el personal con perfil administrativo o celador/a adscrito al ICS, y al IAS, puede acceder al campo diagnóstico de los/las pacientes de cualquiera de las dos entidades mediante el software SAP-ARGOS.
- En caso de responder negativamente a la anterior pregunta, lo acreditara documentalmente.

Dado que el ICS no atendió este requerimiento, se reiteró lo mismo en fecha 03/07/2019.

6. En fecha 11/07/2019 el ICS dio respuesta a este segundo requerimiento, e informaba de lo siguiente.

- Que *"el personal con perfil administrativo o celador/a adscrito al ICS puede acceder al campo diagnóstico de los pacientes de cualquiera de las dos entidades mediante el software SAP ARGOS"*.
- Que *"se está modificando el sistema informático para cumplir con lo que se les pide. En estos momentos, el evolutivo de SAP Argos que va a permitir ocultar la información de diagnósticos al personal no sanitario ya está hecho. Para implementarlo y ponerlo en marcha debe ir acompañado de la definición de un nuevo rol de administrativo. En SAP Argos están trabajando y tienen previsto que durante este mes se pueda poner en marcha, para que se cumpla lo que se pide en el ICS"*.

7. En fecha 19/07/2019, el ICS informó a esta Autoridad que habían *"definido y están en producción la creación de un nuevo rol de usuario y las modificaciones necesarias en el programa SAP Argos para que al personal no sanitario que, por su trabajo no debe ver diagnósticos, se le asigne (y ya han empezado a hacer) ese nuevo rol que impide la visualización del diagnóstico"*.

El ICS aportaba diversa documentación para acreditar este extremo.

8. En fecha 29/11/2019, 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 25.2; ambos del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27/4, relativo a la protección de las personas físicas en lo que se refiere al tratamiento de datos personales y a la libre circulación de éstas (en adelante, RGPD) .

Este acuerdo de iniciación se notificó a la entidad imputada en fecha 12/12/2019.

9. En el acuerdo de iniciación se concedía a la entidad imputada un plazo de 10 días hábiles, contados a partir del día siguiente de la notificación, para formular alegaciones y proponer la práctica de pruebas que considerase convenientes para defender sus intereses.

10. En fecha 07/01/2020 el ICS presentó un escrito ante la Autoridad mediante el cual no se formulaban alegaciones en el acuerdo de iniciación, sino que se limitaba a detallar las actuaciones que habían llevado a cabo a fin de evitar en el futuro hechos como los que propiciaron el inicio de este procedimiento sancionador. En concreto, el ICS informaba haber implementado las siguientes medidas (que acreditaba mediante la aportación de varias impresiones de pantalla del aplicativo SAP Argos):

- Que *"en fecha 2/10/2019 se creó un nuevo rol para el personal no sanitario, que dicho perfil no presenta el diagnóstico en las pantallas a las que tienen acceso"*
- Que *"con este evolutivo de SAP Argos se anonimizan los diagnósticos a los grupos de usuarios que no sean facultativos o personal de enfermería"*.

11. En fecha 09/03/2020, la instructora de este procedimiento formuló una propuesta de resolución, por la que proponía que la directora de la Autoridad Catalana de Protección de Datos amonestara al ICS como responsable de una infracción prevista en el artículo 83.4.a), en relación con el artículo 25.2; ambos del RGPD.

Esta propuesta de resolución se notificó en fecha 11/03/2020 y se concedía un plazo de 10 días para formular alegaciones.

12. Este plazo -a pesar de la suspensión de plazos administrativos prevista por el Real Decreto 463/2020, de 14 de marzo, por el que se declara el estado de alarma para la gestión de la situación de crisis sanitaria ocasionada por el COVID-19 ; suspensión que fue levantada en fecha 01/06/2020 de acuerdo con el artículo 9 del Real decreto 537/2020, de 22 de mayo -, se ha superado con alegaciones, se han presentado

Hechos probados

Del conjunto de las actuaciones practicadas en este procedimiento, se considerarán acreditados los hechos que se detallan a continuación.

El Instituto Catalán de la Salud no tenía implementada una medida de seguridad que impidiera que personal no sanitario (personal administrativo y celadores/as), a través del aplicativo SAP-Argos (de gestión de historias clínicas), pudiera acceder a el dato "diagnóstico" de los/las pacientes, cuando el acceso a dicho dato no sería necesario para ejercer las funciones que tienen encomendadas. Esta situación, admitida por el propio ICS, se mantuvo al menos hasta el 02/10/2019, fecha en la que, según ha informado dicha entidad, se creó un nuevo rol para el personal no sanitario por lo que no se muestra el campo "diagnóstico" en las pantallas a las que tienen acceso.

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 la 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. La entidad imputada no ha formulado alegaciones en la propuesta de resolución. Tampoco las formuló ante el acuerdo de iniciación, ya que, tal y como se recoge en el antecedente 10º, en su escrito de 07/01/2020 el ICS se limitaba a detallar las actuaciones que habían llevado a cabo por para evitar en el futuro hechos como los que habían propiciado el inicio de este procedimiento sancionador.

3. En relación con los hechos descritos en el apartado de hechos probados, se debe acudir al artículo 25.2 del RGPD, que prevé lo siguiente:

“El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación ya su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sino la intervención de la persona, a un número indeterminado de personas físicas”.

Tal y como indicaba la persona instructora, durante la tramitación de este procedimiento se ha acreditado debidamente el hecho descrito en el apartado de hechos probados, que se considera constitutivo de la infracción prevista en el artículo 83.4.a) del RGPD, que tipifica como tal la vulneración “de las obligaciones del responsable y del encargado a tenor de los artículos (...) 25 a 39 (...)” del RGPD.

La conducta que aquí se aborda se ha recogido como infracción grave en el artículo 73.e) de la Ley orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales (LOPDGDD), en la siguiente forma:

“La falta de adopción de las medidas técnicas y organizativas apropiadas para garantizar que, por defecto, sólo se tratan los datos personales necesarios para cada uno de los fines específicos del tratamiento, de conformidad con lo que exige el artículo 25.2 del Reglamento (UE) 2016/679”.

4. El artículo 77.2 de la LOPDDDD dispone que, en el caso de infracciones cometidas por los responsables o encargados enumerados en el apartado 1º de dicho precepto, 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 Autoritat Catalana de Protecció de Dades debe dictar una resolució que declare la infracció i establezca les mesures a adoptar per corregir els efectes (...)”.

En el caso que aquí nos ocupa, de acuerdo con lo expuesto por la instructora en la propuesta de resolución, esta Autoridad estima que no resulta necesario requerir al ICS la adopción de ninguna medida correctora ya que, tal y como se ha avanzado, esta entidad ha informado haber llevado a cabo diversas actuaciones para evitar que determinadas categorías de personal puedan acceder a datos de salud de las personas usuarias que no son necesarias para desarrollar las funciones que tienen atribuidas.

Resolución

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 25.2; 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 4º.

2. Notificar esta resolución al Instituto Catalán de la Salud.

3. Comunicar la resolución que se dicte en el 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, 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,

Traducción Automática