apdcat
Autoritat Catalana de Protecció de Dades

Calle Rosselló, 214, esc. A, 1r 1a
08008 Barcelona



Identificación del expediente

Resolución del procedimiento sancionador núm. PS 39/2021, referente al Servicio Catalán de la Salud.

Antecedentes

1. En fecha 14/07/2020, tuvo entrada en la Autoridad Catalana de Protección de Datos un escrito por el que un Delegado de Protección de Datos (DPD) de un hospital participante en un estudio promovido y financiado por el Servicio Catalán de la Salud (en adelante, CatSalut), ponía en conocimiento de esta Autoridad unos hechos que podrían contravenir la normativa de protección de Datos. En concreto, el DPD exponía que el hospital en el que ejercía sus funciones, inicialmente había aceptado participar en el estudio llamado *"Evaluación del estado inmunitario del personal sanitario en Cataluña ante el virus SARS-COV2: información para las estrategias y tomas de decisiones del sistema sanitario catalán";* y, exponía que en el marco de este estudio se había detectado una brecha de seguridad en la plataforma que el CatSalut utilizaba para este estudio, en concreto indicaba que *"se ha observado que en la plataforma si pones el NIF en el buscador al que se tiene acceso como usuario de la encuesta del estudio, se ve absolutamente todos los datos que tiene el RCA* [Registro Central de Personas Aseguradas] *(dirección, número afiliación, CAP, tipo de cobertura….). Si nos vamos inventando NIFs, podemos acceder a los datos de cualquier persona".*

Junto a este escrito se aportaba diversa documentación, entre otra, el documento titulado *"EVALUACIÓN DEL ESTADO INMUNITARIO DEL PERSONAL SANITARIO EN CATALUÑA FRENTE AL VIRUS SARS-CoV2 Comunicación de datos de profesionales",* de 29/06/2020 , que detallaba el diseño del estudio y los protocolos a seguir en la recogida de información. Entre otros, y en cuanto a la relación con las personas que podrían participar con el estudio, se indica lo siguiente:

*"(...) se enviará un correo electrónico a cada profesional, indicando la posibilidad de adherirse a este estudio. Dentro del texto de este correo, se informará de la dirección a la que los profesionales pueden acceder para poder cumplimentar una breve encuesta y dar su consentimiento explícito a la participación en este estudio (...)".*

2. Aunque el DPD había puesto en conocimiento de la Autoridad estos hechos utilizando el formulario de notificación de violación de seguridad, se consideró que, dada la naturaleza de los hechos descritos, esta notificación debía ser considerada como una denuncia, de lo que se informó en el DPD del hospital.

3. En consonancia con lo anterior, la Autoridad abrió una fase de información previa (núm. IP 216/2020), 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.

Calle Rosselló, 214, esc. A, 1r 1a
08008 Barcelona

4. En esta fase de información, en fecha 24/07/2020 se requirió el DPD denunciante para que informara en qué circunstancias concretas -mediante el aplicativo al que accedía el personal sanitario que había decidido participar en el citado estudio - se podían visualizar las
datos que constaban en la RCA de cualquier persona cuyo NIF se introdujera en el buscador del citado aplicativo.

5. En fecha 26/07/2020 el DPD del hospital dio respuesta a este requerimiento en los siguientes términos:

*"Podemos transcribir lo que detectaron nuestros servicios de información: "El problema de seguridad pues sí, es cierto. He puesto el NIF de mi mujer en el buscador al que se tiene acceso como usuario de esta encuesta y veo absolutamente todos los datos que tiene el RCA (dirección, número afiliación, CAP, tipos de cobertura...). Si nos vamos inventando NIFs, podemos acceder a los datos de cualquier persona».*
*Como otro trabajador del centro sanitario en primer momento:*
*«Se han cedido a terceros sin mi consentimiento explícito datos personales: como número y apellidos, NIF, CIP, sé que es así porque te identifica con el NIF y automáticamente carga el CIP, (…)*

*El programa tiene un bug de seguridad y he podido ver las variables del mismo, no he trasteado más, pero no está adecuadamente protegido, envío foto".*

6. En fecha 31/07/2020 se requirió el CatSalut -como responsable del tratamiento del RCA, y como promotor del estudio citado- para que informara sobre en qué circunstancias las personas trabajadoras de los centros hospitalarios que habían decidido participar en el estudio de investigación, podían acceder a datos de terceras personas contenidas en el RCA; y en concreto, si este acceso permitía visualizar: a) los datos de cualquier persona inscrita en ese registro; o, b) los datos de las personas trabajadoras de los centros que participaban en el estudio.

7. Mediante escrito de 03/08/2020 el CatSalut solicitó una ampliación del plazo para dar respuesta al requerimiento, que le fue concedida en fecha 05/08/2020.

8. Mediante escrito de 31/08/2020 el CatSalut solicitó una nueva ampliación del plazo para dar respuesta al requerimiento, que le fue denegada en fecha 16/09/2020. El mismo día se advirtió a la entidad que de no dar respuesta al requerimiento, se podía incurrir en una infracción de la normativa de protección de datos.

9. En fecha 23/09/2020 el CatSalut dio respuesta al requerimiento, exponiendo lo siguiente:

- *"El sistema está previsto de forma que para acceder a la encuesta se necesita un Link personalizado que envía la aplicación a través de un Token único, con este Link que sólo recibe la persona interesada* [la persona participante en el estudio ], *se accede a una página donde se*

Calle Rosselló, 214, esc. A, 1r 1a
08008 Barcelona

*pide el DNI y se comprueba que la relación TOKEN-DNI se cumpla sino no puede continuarse.*

*Durante los primeros días en la encuesta hubo un bug que te permitía cambiar el DNI y poner el de otra persona. En el momento que se conoció el problema se solucionó de inmediato y ya no se puede modificar nada de la persona participante en el estudio, esto concretamente se solucionó el 21/07/2020 que fue el día que se tuvo conocimiento de la incidencia".*

- *"No se puede concretar con exactitud si el acceso a los datos del RCA permitía visualizar los datos de cualquier registro, los datos de todas las personas que participaban en el estudio, dado que desde el mismo momento en que se tuvo conocimiento de la 'incidencia se solucionó y en estos momentos no es reproducible, lo que en estos momentos no se puede hacer la comprobación".*

10. En fecha 21/06/2021, la directora de la Autoridad Catalana de Protección de Datos acordó iniciar un procedimiento sancionador contra el CatSalut por una presunta infracción prevista en el artículo 83.4.a), en relación con el artículo 32; ambos del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril, relativo a la protección de las personas físicas en cuanto al tratamiento de datos personales ya la libre circulación de éstas (en adelante, RGPD ). Este acuerdo de iniciación se notificó a la entidad imputada en fecha 23/06/2021.

11. 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.

Este plazo se ha superado con creces y no se han formulado alegaciones.

Hechos probados

Las personas trabajadoras de determinados centros sanitarios recibieron un correo mediante el cual se ofrecía a dichos profesionales la posibilidad de adherirse al estudio de investigación llamado *"Evaluación del estado inmunitario del personal sanitario en Cataluña frente al virus SARS-COV2: información para las estrategias y tomas de decisiones del sistema sanitario catalán";* promovido por el CatSalut. En este correo se facilitaba a la persona trabajadora un link personalizado a través de un Token único -asociado al DNI- al que debían conectarse para llenar la encuesta y dar su consentimiento explícito a la participación en el estudio.

Desde, al menos el 14/07/2020, hasta el 21/07/2020, el sistema permitía a la persona usuaria de la encuesta cambiar el DNI en el buscador del aplicativo y poner el de otra persona, de forma que, en caso de hacerlo, se podían visualizar los datos de esta tercera persona contenidas en el Registro Central de personas Aseguradas (como, domicilio, nº CIP, etc), del que es responsable del tratamiento el CatSalut.

Calle Rosselló, 214, esc. A, 1r 1a
08008 Barcelona



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. 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 la entidad imputada no ha formulado alegaciones en el acuerdo de iniciación. Este acuerdo contenía un pronunciamiento preciso sobre la responsabilidad imputada.

3. En relación con los hechos descritos en el apartado de hechos probados, es necesario acudir al artículo 5.1.f) del RGPD), que regula el principio de integridad y confidencialidad, según el cual los datos personales serán *" tratados de tal modo que se garantice una adecuada seguridad de las datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas".*

Por su parte, el artículo 32 del RGPD, en lo referente a la seguridad de los datos, establece lo siguiente:

> *"1. Teniendo en cuenta el estado de la técnica, las costas de aplicación, 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 los datos personales de forma rápida en caso de incidente físico o técnico, y* d) *un proceso de verificación, evaluación y valoración regulares 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*

Calle Rosselló, 214, esc. A, 1r 1a
08008 Barcelona

*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".*

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 (en adelante, LOPDGDD), es necesario hacer referencia al 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, más concretamente, su artículo 16 relativo a la 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. *"Control de acceso"* del Anexo II ("Medidas de Seguridad") del ENS, determina lo siguiente:

*El control de acceso cubre el conjunto de actividades preparatorias y ejecutivas para que una determinada entidad, usuario o proceso, pueda, o no, acceder a un recurso del sistema para realizar una determinada acción.*
*(…)*
*En todo control de acceso se requerirá lo siguiente:*
*a) Que todo acceso esté prohibido, salvo concesión expresa.*
*b) Que la entidad quede identificada singularmente [op.acc.1].*
*c) Que la utilización de los recursos esté protegida [op.acc.2].*
*d) Que se definan para cada entidad los siguientes parámetros: a qué se necesita acceder, con qué derechos y bajo qué autorización [op.acc.4].*
*e) Serán diferentes las personas que autoricen, usen y controlen el uso [op.acc.3].*

*f) Que la identidad de la entidad quede suficientemente autenticada [op.acc.5].*
*g) Que se controle tanto el acceso local ([op.acc.6]) como el acceso remoto ([op.acc.7]).*

*Con el cumplimiento de todas las medidas indicadas se garantizará que nadie accederá a recursos sin autorización. Además, quedará registrado el uso del*

Calle Rosselló, 214, esc. A, 1r 1a
08008 Barcelona

*sistema ([op.exp.8]) para poder detectar y reaccionar a cualquier fallo accidental o deliberado.*

*Cuando se interconecten sistemas en los que la identificación, autenticación y autorización tengan lugar en diferentes dominios de seguridad, bajo distintas responsabilidades, en los casos en que sea necesario, las medidas de seguridad locales se acompañarán de los correspondiente acuerdos de colaboración que delimiten mecanismos y procedimientos para la atribución y ejercicio efectivos de las responsabilidades de cada sistema ([op.ext]).*

Y, concretamente, el epígrafe 4.2.2 *"Requisitos de acceso",* determina lo siguiente:

| *dimensiones ICAT* | | | |
|---|---|---|---|
| *nivel* | *bajo medio alto* | | |
| | *aplica =* | | = |

*Los requisitos de acceso se atenderán a lo que a continuación se indica:*
*a) Los recursos del sistema se protegerán con algún mecanismo que impida su utilización, salvo a las entidades que disfruten de derechos de acceso suficientes.*

*b) Los derechos de acceso de cada recurso, se establecerán según las decisiones de la persona responsable del recurso, atendiéndose a la política y normativa de seguridad del sistema.*
*c) Particularmente se controlará el acceso a los componentes del sistema ya sus archivos o registros de configuración."*

Durante la tramitación de este procedimiento se ha acreditado debidamente el hecho descrito en el apartado de hechos probados, relativo a la falta de implementación de un control de acceso adecuado, lo que es constitutivo de la infracción prevista en el artículo 83.4.a) del RGPD, del RGPD, que tipifica como tal la vulneración de *las obligaciones del responsable y del encargado (...),* en este caso aquellas vinculadas con la seguridad del tratamiento.

La conducta que aquí se aborda 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."*

Calle Rosselló, 214, esc. A, 1r 1a
08008 Barcelona

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 caso de que aquí se ocupe no procede requerir al CatSalut para que adopte ninguna medida correctora para corregir los efectos de la infracción, puesto que en el seno de la información previa que precedió a este procedimiento sancionador (antecedente 9º), la entidad informó a esta Autoridad que *"en el momento en que se conoció el problema se solucionó inmediatamente y ya no se puede modificar nada de la persona participante en el estudio, esto concretamente se solucionó el 21/07/2020 que fue el día en que se tuvo conocimiento de la incidencia".*

Por todo esto, resuelvo:

1. Amonestar al Servicio 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 4º.

2. Notificar esta resolución al Servicio 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

Calle Rosselló, 214, esc. A, 1r 1a
08008 Barcelona

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,