Machine Translated by Google

apdcat
Autoritat Catalana de Protecció de Dades

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

Identificación del expediente

Resolución de procedimiento sancionador núm. PS 54/2021, referente al Departamento de Salud de la Generalidad de Cataluña.

Antecedentes

1. En fecha 30/06/2021 tuvo entrada en la Autoridad Catalana de Protección de Datos un escrito de una persona por el que formulaba denuncia contra el Departamento de Salud, con motivo de un presunto incumplimiento de la normativa sobre protección de datos personales.

En concreto, la persona denunciante exponía que había detectado determinadas vulnerabilidades de seguridad en el sitio web que el Departamento de Salud ha puesto a disposición de la ciudadanía para pedir cita de vacunación (https://vacunacovid.catsalut.gencat.cat), ya que *"permite acceder de forma muy fácil por parte de terceros no autorizados a datos de vacunación, tarjeta sanitaria, móvil, correo, nombre completo, cita por vacunación, etc. Para ello sólo es necesario disponer del número de DNI (o tarjeta sanitaria) de la víctima. No es necesario otro paso extra para verificar la autenticidad, ni recibir ningún SMS de verificación (aparte del inicial)".*

La persona denunciante detallaba en su escrito la forma en que se podía acceder a información de terceras personas, y literalmente indicaba los siguientes pasos a seguir:

"1.(...)
2.(...)
3.(...)
4.(...).
5.(...)
6.(...)
7.(...)

En definitiva, la persona denunciante exponía que una vez el usuario se validaba en el sitio web https://vacunacovid.catsalut.gencat.cat, haciendo determinados llamamientos a la API (aplication programming interface) de la web a través de la consola del navegador, se podía acceder a datos de terceras personas.

Junto a su escrito, la persona denunciante aportaba impresiones de pantalla en las que documentaba cada uno de los pasos que había seguido para poder acceder a información de terceras personas. En la documentación aportada se habían anonimizado los datos de estas terceras personas.

A esta denuncia se le asignó el núm. IP 264/2021.

Traducción Automática

Machine Translated by Google

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

2. La Autoridad abrió una fase de información previa, 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.

3. En fecha 05/07/2021, se recibió a la Autoridad una notificación del Departamento de Salud de una violación de seguridad de datos personales, de acuerdo con lo que prevé el artículo 33 del RGPD, consistente en un posible ciberataque en la *"plataforma K2 de vacunaciones",* a raíz de haberse detectado un volumen inusual de consulta en dicha plataforma.

4. En la fase de información previa iniciada a raíz de la denuncia, en fecha 09/07/2021 se requirió el Departamento de Salud para que diera cumplimiento a lo siguiente:

- Informes sobre la vulnerabilidad detectada por la persona denunciante (antecedente 1º), las circunstancias que le habrían propiciado y si ya había sido enmendada.
- Indicara si, con carácter previo a la puesta en marcha de la plataforma https://vacunacovid.catsalut.gencat.cat, se había elaborado un análisis de riesgos en lo que se refiere al tratamiento de datos personales a través de este canal. En caso afirmativo, aportara una copia.

5. En fecha 22/07/2021 entró en la Autoridad un escrito del Departamento de Salud mediante el cual complementaba la notificación de la violación de seguridad que había realizado en fecha 05/07/2021.

En el citado escrito el Departamento de Salud describía la brecha de seguridad como *"el ataque consiste en realizar peticiones secuenciales de DNI, aprovechando una carencia en la validación de las peticiones, saltándose la cola de espera y peticionando directamente el nodo" .*

6. El mismo día 22/07/2021, el Departamento de Salud respondió el requerimiento de información de 09/07/2021 (antecedente 4º), a través de escrito en el que exponía lo siguiente:

- Que *"la vulnerabilidad descrita en el expediente se identificó el día 1 de julio a raíz del incidente de seguridad notificado en el expediente NVS 67/2021 producido contra la web (https://vacunacovid.catsalut.gencat .cat)",* la cual consiste en *"el retorno de información vinculada a una persona validante sólo el CIP o DNI. La información que devolvía en un primer momento es: DNI, CIP, nombre y apellidos, teléfono móvil, dirección electrónica, día y hora de la cita, lugar de vacunación, tipos de vacuna".*
- Que *"se han adoptado las siguientes medidas de contención, mitigación y mejoras:*
  • Ampliar el código de verificación de 6 cifras numéricas a 6 cifras alfa numéricas . • Mover la validación del código del Frontal en el nodo. • Aplicación de medidas de baneo de IP por número de peticiones por minuto (máximo de 500 peticiones desde España y 50 por minuto desde extranjero)

Traducción Automática

Machine Translated by Google

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

• Bloqueo por un indicador de compromiso identificado en el User Agent de la petición atacante.

• Bloqueo de las IP atacantes conocidas • Cifrado de la respuesta • Contacto con el servicio de abuso de los proveedores de las IP atacantes

• Restringir la información que devuelve la aplicación al realizar una petición, dejando sólo la información respecto a la cita (fecha, hora y lugar de la vacunación y tipo de vacuna)".

- Que *"los casos individuales eran de difícil detección pero las peticiones masivas activaban el sistema de control y seguimiento".*
- Que *"respecto al análisis de riesgos, debido por un lado a la urgencia de iniciar el proceso de vacunación y por otro lado, la necesidad de incorporar el máximo volumen de población al proceso de vacunación en el menor tiempo posible se realizaron pruebas de seguridad por no se hizo un análisis de riesgos con profundidad".*

7. En fecha 14/07/2021, tuvo entrada en la Autoridad Catalana de Protección de Datos otro escrito de denuncia contra el Departamento de Salud, con motivo de un presunto incumplimiento de la normativa sobre protección de datos personales.

En concreto, la entidad denunciante exponía que en un medio de comunicación digital (https://www.(...)) se había publicado una noticia en la que se indicaba que *"la página web de autocita para recibir la vacuna contra el coronavirus de la Generalidad de Cataluña, ha expuesto datos personales de los ciudadanos que han hecho uso de esta plataforma a terceros no autorizados".*

A esta denuncia se le asignó el núm. IP 283/2021

8. En fecha 22/09/2021 se requirió el Departamento de Salud para que diera cumplimiento a lo siguiente:

- Informara si el problema de seguridad del que se hacía eco la noticia indicada era el mismo al que se refería la vulnerabilidad de seguridad a la que el Departamento de Salud había hecho referencia en su oficio fecha 22/07/2021, de respuesta al requerimiento que esta Autoridad le había dirigido en el marco de la información previa iniciada a raíz de la denuncia núm. IP 264/2021. Y, de no ser así diera respuesta a lo siguiente:
- Informara detalladamente sobre el problema de seguridad al que se estaría refiriendo la noticia, las circunstancias que le hubieran propiciado y si ya ha sido subsanado.

9. En fecha 08/10/2021, el Departamento de Salud contestó este segundo requerimiento mediante escrito a través del cual manifestaba lo siguiente:

- Que el problema de seguridad del que se hacía eco la noticia indicada es el mismo al que se refería la vulnerabilidad de seguridad detectada en el marco de la información previa iniciada a raíz de la denuncia núm. IP 264/2021, en la medida en que coinciden las fechas de publicación y

Traducción Automática

Machine Translated by Google

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

que la misma noticia incluye el contenido literal del comunicado de prensa efectuado por el Departamento de Salud en el sentido de que se había comunicado a la Autoridad la brecha de seguridad a través de la correspondiente notificación de violación de seguridad que dio lugar a la expediente NVS 67/2021.

10. En fecha 27/10/2021, la directora de la Autoridad Catalana de Protección de Datos acordó iniciar un procedimiento sancionador contra el Departamento de Salud por dos presuntas infracciones: una infracción prevista en el artículo 83.5.a), en relación con el artículo 5.1.f); y otra infracción prevista en el artículo 83.4.a), en relación con el artículo 35; 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 Este acuerdo de iniciación se notificó a la entidad imputada en fecha 27/10/2021.

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. Este plazo se superó con creces sin que el Departamento de Salud formulara alegaciones.

11. En fecha 21/12/2021, la instructora de este procedimiento formuló una propuesta de resolución, en la que proponía la modificación de la calificación jurídica de los hechos imputados que se había efectuado en el acuerdo de iniciación y lo de conformidad con lo previsto en el artículo 89.3 de la LPAC. La instructora, una vez detenidamente valorada la documentación incorporada a las actuaciones, estimó que los dos hechos imputados constituían, cada uno de ellos, una vulneración de la seguridad de los datos. A la vista de lo anterior, en la propuesta de resolución la instructora proponía que la directora de la Autoridad Catalana de Protección de Datos amonestara al Departamento de Salud como responsable de la infracción prevista en el artículo 83.4.a) en relación con el artículo 32 del RGPD.

Esta propuesta de resolución se notificó en fecha 21/12/2021 y se concedía un plazo de 10 días para formular alegaciones.

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

Hechos probados

1. Desde una fecha indeterminada, pero en cualquier caso hasta el día 30/06/2021, los sistemas de información del Departamento de Salud permitían que, una vez el usuario se validaba en el sitio web https://vacunacovid. catsalut.gencat.cat (web que el Departamento había puesto a disposición de la ciudadanía para pedir cita de vacunación), haciendo llamadas a la API de la web, éste pudiera acceder a datos de otros usuarios del sistema de salud (como el DNI, el CIP, nombre y apellidos, teléfono móvil, dirección electrónica, día y hora de la cita, lugar de vacunación y tipos de vacuna).

Traducción Automática

Machine Translated by Google

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

2. En relación con el tratamiento de datos vinculado a la puesta en marcha del sitio web https://vacunacovid.catsalut.gencat.cat, el Departamento de Salud no realizó un análisis de riesgos para determinar las medidas técnicas y organizativas apropiadas para garantizar la seguridad de los datos.

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. En relación con los hechos descritos en los puntos 1º y 2º del apartado de hechos probados, relativos a la seguridad de los datos, se debe acudir al artículo 32 del RGPD, el cual dispone que:

> *"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 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 personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichas datos. (...)"

Como se ha dicho, respecto a las conductas descritas en los puntos 1 y 2 del apartado de hechos probados, se considera que en el seno de este procedimiento ha quedado probado que el Departamento de Salud ha vulnerado las medidas de seguridad que se detallan a continuación de forma separada, con cita de los preceptos que las regulan:

Traducción Automática

Machine Translated by Google

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

2.1.- En relación con el hecho probado 1º:

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), 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, y concretamente su apartado 4.2.2 *"Requisitos de acceso"* del Anexo II *("Medidas de Seguridad"):*

> *"Los requisitos de acceso se atendrán 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".*

2.2.- En relación con el hecho probado 2º:

En este punto hay que hacer expresa referencia a lo que prevé el apartado 2º del artículo 32 del RGPD ya transcrito, que obliga al responsable del tratamiento a llevar a cabo un análisis de riesgos de aquellos tratamientos que prevea realizar, fin y efecto de determinar las medidas de seguridad a implementar.

De conformidad con lo expuesto, los hechos recogidos en los puntos 1º y 2º del apartado de hechos probados constituyen 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 8, 11, 25 a 39, 42 y 43",* entre las que se encuentra la prevista en el artículo 32.

Estas conductas se han 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."*

3. 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."*

Traducción Automática

Machine Translated by Google

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

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 virtud de esta facultad, y en lo que se refiere al hecho probado 2º, procede requerir al Departamento de Salud para que lo antes posible y en todo caso en el plazo máximo de 1 mes a contar desde el día siguiente de la notificación de esta resolución, acredite a esta Autoridad haber realizado un análisis de riesgos de conformidad con el artículo 32 del RGPD, a fin de determinar las medidas técnicas y organizativas apropiadas para garantizar la seguridad de los datos tratados a través de la plataforma https://vacunacovid.catsalut.gencat.cat.

En cuanto al hecho probado 1º, no procede requerir la adopción de ninguna medida correctora, ya que el Departamento de Salud acreditó a esta Autoridad, en el marco de la NVS 67/2021, haber tomado las medidas adecuadas para solucionar la incidente de seguridad detectado en la plataforma https://vacunacovid.catsalut.gencat.cat.

Por todo esto, resuelvo:

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

2. Requerir al Departamento de Salud para que acredite ante esta Autoridad haber llevado a cabo la actuación señalada en el fundamento de derecho 3º, en el plazo indicado.

3. Notificar esta resolución al Departamento de Salud.

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

5. 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

Traducción Automática

Machine Translated by Google

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

el 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.

Traducción Automática