CNS 20/2015

Dictamen en relación con el Proyecto para dar valor a la información del sistema sanitario catalán en el marco de las políticas públicas, VISC+ (versión marzo de 2015)

Se remite a la Autoridad Catalana de Protección de Datos, en fecha 20 de marzo de 2015, documentación relativa al nuevo enfoque del Proyecto VISC+, en base a la cual se solicita, en relación con las previsiones de la Moción parlamentaria sobre VISC+, la elaboración de un dictamen en que se analicen los elementos que se han incorporado al proyecto después del Dictamen 34/2014, emitido por esta Autoridad el 23 de julio de 2014, sobre el Proyecto VISC+ del Departamento de Salud.

En concreto, se envía a la Autoridad los siguientes documentos, en la versión de marzo de 2015:

1. Cambios aplicados a los documentos en base a las recomendaciones de la APDCAT.
2. Información sobre el tipo de datos y el proceso de anonimización de VISC+.
3. Información de interés social del proyecto (Memoria social).
4. Análisis de riesgos (para CatSalut, la ciudadanía y la continuidad de VISC+).
5. Valoración de los modelos de gestión de VISC+ (AQuAS o colaboradores externos).
6. Estándares de recolección de datos.
7. Garantías éticas de uso de los datos (código ético).
8. Informe de evaluación de impacto sobre la privacidad de VISC+.
9. Encargo de gestión del Departamento de Salud, CatSalut y ICS a la Agencia.

Analizada la documentación aportada, relativa al nuevo enfoque del Proyecto VISC+, y la normativa aplicable, y visto el informe de la Asesoría Jurídica, se dictamina lo siguiente.

I

(…)

II

Antecedentes

El año 2014 una entidad de derecho público (en adelante, la entidad), formuló consulta a esta Autoridad en relación con el "proyecto VISC+", referido a la licitación de un contrato de colaboración público privada para la implantación y la operación de un modelo de gestión de servicios para dar valor a la información del sistema sanitario catalán en el marco de las políticas públicas (en adelante, proyecto VISC+). En relación con la consulta formulada, esta Autoridad emitió el Dictamen 34/2014.

Posteriormente a la elaboración del Dictamen 34/2014, la Autoridad mantuvo diversas reuniones con los responsables del Proyecto, con el fin de analizar el contenido del

mismo y los cambios incorporados a raíz de las recomendaciones y sugerencias formuladas por la Autoridad, desde la perspectiva de la protección de datos personales (Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (en adelante, LOPD), y el resto de normativa aplicable).

Hay que hacer mención de la Moción 150/X, del Parlamento de Cataluña, sobre el Proyecto VISC+ (BOPC, nº. 421, de 3 de noviembre de 2014), en el que el Parlamento insta al Gobierno, entre otros, a detener la licitación del proyecto VISC+ hasta que se haya acabado el proceso participativo y deliberativo a que hace referencia la moción. Según la Moción, este proceso participativo tiene que contar con la participación de representantes de los grupos parlamentarios, colegios profesionales de especialidades implicadas, profesionales y direcciones de los centros asistenciales y de investigación, expertos en investigación social y biomédica, así como con representantes de la Apdcat, entre otros.

La Moción del Parlamento insta a aportar, a todos los agentes invitados al proceso deliberativo mencionado y al Parlamento de Cataluña, diversa documentación, entre otros, *"el informe de la Apdcat sobre el Proyecto VISC+, y correcciones hechas al proyecto para ajustarse a las recomendaciones y advertencias que hace este informe, especialmente en cuanto a las garantías que sólo se utilizarán datos debidamente anonimizados."*

Con motivo de las previsiones de la Moción del Parlamento, en fecha 14 de enero de 2015 se hizo una Jornada de debate sobre la reutilización de datos y el proyecto VISC+ con representantes de los grupos parlamentarios, en los que también participó la Apdcat. En esta Jornada, la Apdcat recordó las consideraciones principales hechas tanto en el Dictamen 34/2014 como posteriormente, siempre desde la perspectiva de la protección de datos de carácter personal.

Finalmente, hay que recordar que antes de la emisión de este dictamen se ha publicado la Resolución SLT/570/2015, de 16 de marzo, por la cual se hace público un encargo de gestión que formalizan el Departamento de Salud, el Servicio Catalán de la Salud y el Instituto Catalán de la Salud con la Agencia de Calidad y Evaluación Sanitarias de Cataluña (DOGC, nº. 6843, d'1.4.2015).

III

Objeto del dictamen

Tal como se ha expuesto, esta Autoridad ya emitió el Dictamen 34/2014 sobre el proyecto VISC+. En aquel documento se analizaban las implicaciones generales de un proyecto de esta naturaleza y los aspectos concretos derivados de los documentos que formaban parte del proyecto sometidos a dictamen. Aquel dictamen se concluía con una serie de consideraciones sobre aspectos que había que mejorar en el proyecto.

El dictamen que se emite ahora, se centrará básicamente en el análisis de las modificaciones introducidas en el proyecto a raíz de aquel primer dictamen, como también sobre otras cuestiones nuevas que se plantean a la vista de la evolución que ha sufrido el proyecto.

La solicitud de dictamen que se formula se refiere específicamente al conjunto de documentos de respuesta a la Moción 150/X del Parlamento de Cataluña, sobre

VISC+, en su versión de marzo de 2015, que se aportan con la consulta. En concreto se trata de los documentos siguientes:

1. Cambios aplicados a los documentos en base a las recomendaciones de la APDCAT
2. Información sobre el tipo de datos y el proceso de anonimización de VISC+
3. Información de interés social del proyecto (Memoria social)
4. Análisis de riesgos (para CatSalut, la ciudadanía y la continuidad de VISC+)
5. Valoración de los modelos de gestión de VISC+ (entidad de derecho público o colaboradores externos)
6. Estándares de recolección de datos
7. Garantías éticas de uso de los datos (código ético)
8. Informe de evaluación de impacto sobre la privacidad de VISC+
9. Encargo de gestión del Departamento de Salud, CatSalut y ICS en la entidad

Para facilitar la lectura de este dictamen, se hará referencia, en adelante, al número de los nueve documentos mencionados (Documento nº. 1; Documento nº. 2, etc).

Hay que tener en cuenta que con el envío de la documentación que hay que analizar en este dictamen (versión de marzo de 2015), la entidad recuerda que, como resultado del debate con los grupos parlamentarios, se ha reenfocado el proyecto VISC+, de modo que algunos de los documentos que formaban parte de las versiones anteriores del Proyecto y que habían sido analizados por esta Autoridad en el Dictamen 34/2014, ya no son de aplicación.

En concreto se trataría, según la información aportada por la entidad de los siguientes documentos:

- Documento de solución final Técnico
- Documento de solución final Administrativo
- Procedimiento VISC+ de tratamiento y cesión de datos anonimizados

El hecho de que estos tres documentos ya no resulten de aplicación al Proyecto VISC+ y, por lo tanto, ya no deban ser tenidos en cuenta de cara a la elaboración del presente dictamen, no desvirtúa algunas de las consideraciones que, desde la perspectiva de la protección de datos personales, ha formulado esta Autoridad a través del Dictamen 34/2014, al cual nos remitimos.

En cualquier caso, el objeto de este dictamen es el análisis y la valoración del contenido de los documentos aportados en fecha 20 de marzo de 2015, especialmente con respecto a los cambios introducidos respecto de la versión analizada al Dictamen 34/2014.

IV

Sobre la información que se tratará en el proyecto VISC+

Desde la perspectiva de la protección de datos hay que partir de la base que la recogida y el posterior tratamiento de datos personales tiene que dar cumplimiento a lo que dispone la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, y el Real Decreto 1720/2007, de 21 de diciembre, de desarrollo de la Ley Orgánica (LOPD y RLOPD, respectivamente).

El artículo 4.1 de la LOPD recoge el principio de calidad de los datos, que en su vertiente de proporcionalidad, establece el siguiente:

"1. Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido."

El principio de proporcionalidad despliega sus efectos tanto en relación con los ficheros de datos que, según la documentación aportada, tienen que formar parte del proyecto, como, en definitiva, de la información que se podrá comunicar a los posibles cesionarios o receptores de la información.

El Documento nº. 2 explicita que la información que será objeto de tratamiento *"está contenida en los ficheros declarados responsabilidad del Departamento de Salud, del Servicio Catalán de la Salud y del Instituto Catalán de la Salud, que se encuentran regulados por la Orden SLT/25/2014, de 3 de* febrero: "En concreto*, el Documento nº. 2 hace referencia a:*

El Fichero estadístico de encuesta de salud; el Fichero de estadística sobre causas de la muerte; el Fichero de la historia clínica; el Fichero de patologías específicas; el Fichero de prestación farmacéutica; el Fichero de registro del conjunto mínimo básico de datos (CMBD); el Fichero de pacientes del Instituto Catalán de la Salud.

Respecto de ello, a efectos de claridad, se recomienda hacer referencia al título exacto de los ficheros regulados en la Orden SLT/25/2014, entre otros, en relación con el "Registro de prestación farmacéutica" o el "Fichero de pacientes de la División de Atención Primaria del Instituto Catalán de la Salud". Con respecto al "Fichero de la historia clínica", hay que decir que no se encuentra regulado en la citada Orden con esta denominación, y por lo tanto convendría referirse a la denominación exacta del fichero regulado en dicha Orden.

El fichero estadístico de encuesta de salud y el fichero de estadística sobre causas de la muerte, citados, no son ficheros regulados por la Orden SLT/25/2014, citada, ya que son dos ficheros de tipo estadístico, inscritos en el Instituto de Estadística de Cataluña (Idescat). En cualquier caso, el Documento nº. 2 incluye el enlace en el web del Idescat, de manera que queda claro que estos ficheros son ficheros estadísticos.

Todavía en relación con la información que será objeto de tratamiento en el proyecto VISC+, **se considera adecuada la inclusión de la descripción de los ficheros que contienen la información que tratará VISC+, así como de los principales sistemas de información que generan, almacenan y gestionan esta información** (páginas 5 a 16 Documento nº. 2). Estos cuadros explicativos identifican la finalidad de los ficheros y los sistemas de información y clarifican la información que se tratará en el contexto del proyecto.

No obstante, en la documentación enviada se hace referencia a la futura incorporación de nueva información *"cumpliendo con todas las medidas legales y de seguridad necesarias"* (pág. 4 Documento nº. 2). Obviamente la incorporación de nueva información requiere cumplir con la normativa y las medidas de seguridad exigibles, pero más allá de esto, si la información que se incorpora difiere sustancialmente de la que se ha previsto inicialmente (esto sucedería, por ejemplo, si se pretendiera incorporar al proyecto información de tipo genético) sería necesario llevar a cabo, de nuevo, una evaluación de los riesgos inherentes a esta incorporación y del impacto que esto puede tener en la privacidad de las personas afectadas.

En cualquier caso, esta previsión tendrá que ser interpretada de acuerdo con las exigencias del principio de calidad, en su vertiente de proporcionalidad y de minimización.

V

Encargo del tratamiento

El apartado 4 del Documento nº. 8, relativo a los *"flujos de información",* prevé lo siguiente:

"Actualmente los datos personales de salud residen en diferentes ubicaciones bajo la responsabilidad de los titulares de los diferentes ficheros.

Por lo tanto, AQuAS, como responsable de desarrollar el Proyecto VISC+, será la encargada del tratamiento de datos personales de salud para anonimizarlos y ponerlos a disposición de terceros interesados según se describe en el apartado anterior. En este sentido y para dar cumplimiento a los requerimientos del artículo 12 de la LOPD, los responsables de los ficheros encargan a AQuAS este tratamiento."

En relación con esta cuestión, el Documento nº. 9, aportado, consiste en un *"encargo de gestión que formalizan el Departamento de Salud, el Servicio Catalán de la Salud y el Instituto Català de la Salud con la Agencia de Calidad y Evaluación Sanitarias de Catalunya"*

Este encargo de gestión, firmado con fecha de 13 de noviembre de 2014, ha sido objeto de publicación a través de la Resolución SLT/570/2015, de 16 de marzo, por la cual se hace público un encargo de gestión que formalizan el Departamento de Salud, el Servicio Catalán de la Salud y el Instituto Català de la Salut con la Agencia de Calidad y Evaluación Sanitarias de Cataluña (DOGC, nº. 6843, d'1.4.2015).

Este encargo de gestión incluye como anexo 2 el modelo de encargo del tratamiento, de acuerdo con el art. 12 de la LOPD, que tendrá que firmar cada una de las entidades responsables de los ficheros con AQuAS

Hay que hacer notar que por lo que se desprende del apartado referido al "a*lcance y contenido de la actividad encargada"* del Documento nº. 9, el alcance de este encargo de gestión supera el ámbito propio del proyecto VISC+. Así, en el encargo de gestión se incluye:

"a) Anonimización de la información contenida en los ficheros que contienen datos de carácter personal del Departamento de Salud, del Servicio Catalán de la Salud y del Instituto Catalán de la Salud con datos de salud o centros asistenciales de interés para la investigación y la evaluación médicas, los cuales se relacionan en el Anexo 1 del presente encargo de gestión. Quedan fuera de este encargo los ficheros de gestión interna del Departamento de Salud, del Servicio Catalán de la Salud y del Instituto Catalán de la Salud.

b) Utilización de la información anonimizada para algunas de las finalidades señaladas en el Anexo 2.

c) Cesión a terceros de información anonimizada para algunas de las finalidades señaladas en el Anexo 2.

d) Cesión a terceros de información personal para algunas de las finalidades señaladas en el anexo 2, siempre que haya consentimiento previo de cada uno de los afectados para la realización de la cesión y que se compruebe que el cesionario dispone de una auditoría que demuestre el cumplimiento en todas las fases del tratamiento de la información de todas las medidas exigidas por la Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, así como por la normativa que la despliega.

La cesión de datos identificables conlleva que el cesionario se constituye en responsable de los ficheros con las obligaciones que la normativa establece a este respecto.

Las utilizaciones y cesiones de datos indicadas únicamente abarcarán los datos estrictamente necesarios para la finalidad concreta de cada actuación según las finalidades señaladas en el anexo 2 y que no resulten excesivos, y de conformidad con lo que establezca la normativa vigente. Las cesiones a terceros sólo se harán a entidades dedicadas a la finalidad que se justifique para la cesión de los datos y la cual esté incluida dentro de las señaladas en el anexo 2."

A su vez, el anexo 2, al cual se remite el apartado que acabamos de reproducir, dentro del apartado "Servicios encargados" incluye no sólo finalidades de investigación y evaluación (de hecho no hay una referencia expresa a la evaluación del sistema sanitario) sino también finalidades de tipo asistencial, administración y gestión de centros sanitarios, gestión sanitaria para la administración sanitaria, inspección para la administración sanitaria, estudios de epidemiología, docencia y actividad estadística dentro del Plan estadístico.

Por otra parte el documento analizado no explicita el nivel de medidas de seguridad alto que correspondería a los datos que son fuente de información del proyecto VISC+, sino que parece admitir también ficheros de nivel de seguridad inferior.

Igualmente, en la relación de ficheros incluidos en el Anexo 1 del Documento nº. 9, se sigue incluyendo la siguiente fórmula (que esta Autoridad ya consideró desaconsejable desde la perspectiva del principio de calidad (FJ XIV del Dictamen 34/2014):

"Y en el futuro cualquier otro fichero del (responsable) con datos de salud o centros asistenciales de interés siempre que se justifique para algunas de las finalidades señaladas en el anexo 2 (...)".

El Pacto segundo del encargo de gestión (Resolución SLT/570/2015, citada), prevé expresamente que *"El encargo de gestión previsto en el pacto primero se articula mediante un encargo de tratamiento que reúne los requisitos establecidos en el artículo 12 de la LOPD y del cual tiene constancia la Autoridad Catalana de Protección de Datos."*

Al respecto hay que señalar que el Dictamen 34/2014 se refiere sólo al proyecto VISC+ que, según se desprende del resto de la documentación adjuntada, incluye sólo la anonimización de datos de salud para su cesión con finalidades de investigación y de evaluación del sistema sanitario.

Por lo tanto, la referencia contenida en el Pacto segundo del encargo de gestión según el cual la Autoridad Catalana de Protección de Datos tiene constancia del encargo de gestión, es errónea, dado que esta autoridad sólo se ha pronunciado respecto del proyecto VISC+.

Respecto al Anexo 2 del Documento nº. 9, que incluye el modelo relativo al "*Encargo de tratamiento de anonimización de datos y de cesión de datos anonimizados y personales para finalidades señaladas en este anexo."*, vistos los cambios sustanciales operados por el nuevo enfoque del proyecto VISC+, que se analizan en este dictamen, el encargo del tratamiento de datos a través del cual los responsables de los ficheros encargarán a la entidad el tratamiento y la anonimización de datos, no se puede referir a la "cesión de datos anonimizados y personales", pues VISC+ sólo puede comportar, en su concepción actual, cesión de datos anonimizados.

Por lo tanto, las menciones a cesiones de datos personales y las remisiones a finalidades que van más allá de las de investigación y evaluación, no se ajustan a dicho nuevo enfoque de VISC+.

VI

Sobre el modelo de gestión del proyecto

El modelo inicial de VISC+, se articulaba a través de la constitución de un encargo del tratamiento entre el Departamento de Salud, el Servicio Catalán de la Salud (CATSALUT) y el Instituto Catalán de la Salud (ICS), como responsables de los ficheros de datos implicados en el proyecto, y la entidad, como prestador de servicios y encargado del tratamiento, que tenía que permitir a la entidad anonimizar la información a fin de que una vez anonimizada el Adjudicatario la facilitara a los clientes o usuarios finales.

En este esquema inicial, el Adjudicatario se tenía que encargar de definir, construir y poner en marcha un catálogo de servicios útil, eficiente, competitivo e innovador, y contrastar las necesidades del mercado y los clientes finales del proyecto, así como definir un plan de difusión y de comercialización, canalizando de manera adecuada la demanda del mercado nacional e internacional. El Adjudicatario también tenía que ejecutar otros proyectos o iniciativas relacionadas con VISC+, y crear un centro de competencia en analítica en datos de salud, las funciones y composición del cual se describían en documentación que en el momento actual ya no es vigente (Documento Técnico).

Este esquema se ha modificado sustancialmente en la versión del proyecto que es objeto de este dictamen (versión de marzo de 2015), aunque hay algunos aspectos que no resultan bastante claros:

En la Memoria del proyecto (Documento nº. 3), se explicita que *"VISC+ será gestionado y operado en su totalidad por la Agencia. También se contará con un colaborador externo que, mediante un contrato de servicios, desarrollará algunos elementos necesarios para que la Agencia pueda gestionar y operar VISC+ (por ejemplo: una plataforma que permita el análisis de los datos anonimizados, contenidos en el web o la creación de algoritmos de análisis estadístico)."*

En el mismo Documento nº. 3 (apartado 6.2), se prevé que:

"La gestión del proyecto VISC+ es propia de la Agencia, que aportó su pericia y conocimiento sobre el sistema de salud catalán y los datos que se generan. La Agencia también es quien tendrá toda la relación con los potenciales solicitantes de servicios VISC+ (los centros de investigación públicos de Cataluña).

No obstante, la Agencia contará con un colaborador externo que, mediante un contrato de servicios resultado de un proceso de diálogo competitivo, desarrollará algunos elementos necesarios para que la Agencia pueda gestionar y operar VISC+ (como por ejemplo: una plataforma que permita el análisis de los datos anonimizados, contenidos en el web o la creación de algoritmos de análisis estadístico)."

En el Documento de Análisis de riesgos (Documento nº. 4, pàgs. 6 y 7), se explicita que este análisis *"se ha realizado asumiendo la hipótesis que el modelo de gestión del proyecto VISC+ es el que implica una gestión realizada de forma íntegra por la Agencia, con los posibles colaboradores externos participando exclusivamente en la prestación de servicios a la Agencia."*

En este mismo apartado del Documento nº. 4, se concreta, como minimización del riesgo de dependencia de estos colaboradores, que la entidad ostentará el control, gobernanza y ejecución del proyecto, dejando las tareas más técnicas al posible colaborador externo (mediante una colaboración asimilada a un contrato de servicios). Se añade la previsión que este contrato de servicios regule unos acuerdos de nivel de servicio (ANS) de los cuales se hará un control exhaustivo.

En el apartado 3.2 del Documento nº. 8, se explicita que la gobernanza del proyecto es *"siempre y en exclusiva de la agencia, que será quien hará tanto la anonimización de los datos y su custodia, el análisis de las solicitudes que se reciban así como su aprobación (...)".)*

Sobre el modelo de gestión, el Documento nº. 4, citado, remite al Documento nº. 5, en el que se analizan los dos modelos alternativos:

- "VISC+ gestionado y operado integralmente por la Agencia"
- "VISC+ gestionado y operado conjuntamente entre la Agencia y colaboradores"

A los efectos que nos interesan, en el primer modelo se prevé que la entidad ejecute todos los aspectos técnicos y operativos, y se añade que la entidad es la responsable, entre otros, de *"construir todos los elementos tecnológicos del proyecto: plataformas o programas de explotación de los datos anonimizados, páginas web de comunicación, programas de control y auditoría, servidores e infraestructura de apoyo, etc".* En este primer modelo no se hace ninguna mención a la participación de ningún colaborador o agente externo, ni siquiera en relación con tareas puramente técnicas.

Con respecto al segundo modelo, sí admite la participación de colaboradores, los cuales serán responsables de (ver pág. 8 Documento nº. 5):

"- Crear los servicios VISC+, analizando las necesidades concretas de los solicitantes y construyéndolos (incluyendo los servicios de análisis y estadística de datos, servicios de informes maquetados en diversos formatos como PDFs, infografías o pósters, etc.). También se tendrá que asegurar que los servicios sean flexibles (estén adaptados a las necesidades constantes de los solicitantes) y se crean y se entregan lo más rápidamente posible (en un tiempo razonable para el peticionario) y con la calidad esperada.

- Construir todos los elementos tecnológicos del proyecto: plataformas o programas de explotación de los datos anonimizados, páginas web de comunicación, programas de control y auditoría, servidores e infraestructura de apoyo, etc.
- Hacer todas las inversiones requeridas, tanto para la adquisición de productos y servicios tecnológicos (por ejemplo: licencias o servicios de desarrollo), como la

formación continuada en materia de análisis estadístico de grandes volúmenes de datos."
Ahora bien, el citado Documento nº. 5 no explicita cuál de los dos modelos es el seleccionado, más allá de exponer los pros y contras de los dos modelos.

Analizados conjuntamente los documentos 3, 4, y 8 de la nueva versión de marzo de 2015, parece deducirse que el modelo escogido es el segundo de los dos modelos analizados en el Documento nº. 5, ya que el primero no prevé ningún tipo de colaboración externa, y en base a la información de los docs. 3 y 4 sí se admitiría la concurrencia de colaboradores externos.

Con respecto a las funciones de los colaboradores externos, aunque los docs. 3 y 4 hacen referencia a que el/los colaborador/es llevarían a cabo cuestiones meramente técnicas y de apoyo a la entidad, el Documento nº. 5 explicita, cómo se ha mencionado, que los colaboradores llevarían a cabo tareas que claramente van más allá de meras cuestiones técnicas (crear servicios, analizar solicitudes, construir todos los elementos tecnológicos...).

Por todo ello **sería muy recomendable que este Documento nº. 5 explicitara una conclusión y clarificara qué modelo se escoge**, con el fin de transmitir una información clara a los afectados. **También habría que aclarar el rol del/de los colaborador/es,** en el sentido de sí tienen que llevar a cabo cuestiones meramente técnicas como las que se ejemplarizan (una plataforma que permita el análisis de los datos anonimizados, contenidos para el web o la creación de algoritmos de análisis estadístico, tal como se desprende del Documento nº. 3 (apartado 6.2)), o si serán responsables de todo lo que se prevé en el Documento nº. 5 (pág. 8, mencionada).

VII

Sobre la finalidad del tratamiento, los destinatarios de la información y los servicios previstos

Tal como hemos visto, el artículo 4.1 del LOPD prevé que la información sólo puede tratarse "en r*elación con el ámbito y las finalidades determinadas, explícitas y legítimas para las cuales se han obtenido."*

El apartado 2 del mismo artículo 4 añade:

> *2. Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos.*
> *(...)".*

a) Finalidades del tratamiento

Por lo que respecta al principio de finalidad, la LOPD exige que las finalidades para las cuales se trate la información sean determinadas, explícitas y legítimas. Por eso, habrá que examinar las previsiones relativas a las finalidades que tiene que tener el proyecto VISC+, con el fin de verificar si se ajustan a las exigencias de dicho principio.

En la documentación aportada, referida al nuevo enfoque del proyecto VISC+, se define como un aspecto clave del mismo que la información anonimizada y

descontextualizada *"puede ser utilizada sólo con una finalidad de investigación médica o de evaluación del sistema de salud."* (pàg. 3 y 8 Documento nº. 3).

Esta limitación de finalidades (estudios de investigación médica o de evaluación del sistema de salud) también se prevé en el apartado 2.2 del Documento nº. 7, referido al *"principio de cumplimiento de finalidades legales".*

En versiones anteriores del proyecto, se preveía la posibilidad de tratar los datos en relación con cualquiera de las finalidades legalmente previstas, en el contexto de la normativa de autonomía del paciente (Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de los derechos y obligaciones en materia de información y documentación clínica, y Ley 21/2000, de 29 de diciembre, sobre los derechos de información concerniente la salud y la autonomía de los paciente y la documentación clínica). Teniendo en cuenta las consideraciones del Dictamen 34/2014 referidas al principio de finalidad, a las que nos remitimos, se valora positivamente que la nueva versión del proyecto recoja con mayor claridad el objetivo de VISC+, referido a las finalidades de investigación y de evaluación del sistema de salud.

Ahora bien en algún documento (primer párrafo del apartado 1 del Documento nº. 3) la redacción que se utiliza sigue siendo bastante ambigua dado que se refiere a "alguna de las finalidades que prevé la ley", en lugar de referirse expresamente a la investigación y la evaluación del sistema sanitario.

b) Destinatarios de la información

A diferencia de las previsiones iniciales del proyecto respecto de las múltiples tipologías de los potenciales "clientes finales" de la información, la documentación que ahora se analiza explicita que podrán solicitar servicios a VISC+ los centros de investigación acreditados por CERCA en el ámbito de las ciencias médicas y de la salud, y que VISC+ está orientado a los investigadores de los centros de investigación públicos de Cataluña que realicen estudios de investigación (pág. 3 y 4 Documento nº. 3). La documentación objeto de análisis también limita los potenciales solicitantes de VISC+ a los centros acreditados por CERCA en otros apartados (Documento nº. 5, Documento nº. 3, entre otros).

Según la información disponible en el web http://cerca.cat, y las previsiones de la Ley 7/2011, del 27 de julio, de medidas fiscales y financieras (arts. 64 y ss), la Institución CERCA (Centros de Investigación de Cataluña), es el medio propio y servicio técnico de la Administración de la Generalitat de Catalunya para el seguimiento, apoyo y facilitación de la actividad de los centros de investigación del sistema CERCA, los cuales se encuentran referenciados, en el mismo web. Según el artículo 64.1 de la Ley 7/2011, los centros CERCA tienen que ser creados o participados por la Administración de la Generalitat y, si procede, junto con unas o más universidades o con otras entidades públicas o privadas.

Visto esto, se recomienda que las menciones hechas en la documentación aportada (Docs. 3 y 5), a los "centros de investigación públicos", se haga a "centros de investigación acreditados por CERCA", a efectos de claridad, dado que, por la información disponible, no se descarta que algún centro integrado en CERCA pueda tener naturaleza jurídico privada.

Ahora bien, según el apartado 5.2 del Documento nº. 3, los servicios previstos de VISC+ van dirigidos a los siguientes grupos de colectivos:

- Centros de investigación acreditados por CERCA (...).
- Agentes del sistema sanitario integral de utilización pública de Cataluña (SISCAT), que planteen una necesidad de conocimiento en relación con la calidad, efectividad, eficiencia, etc, de los servicios sanitarios o de los tratamientos.

Esta previsión se confirma en el apartado 2.1 (Documento nº. 7), en el que también se explicita la exclusión de VISC+ de determinadas tipologías de peticionarios (farmacéuticas, consultoras, aseguradoras de salud, empresas de colocación o de contratación de personal, empresas publicitarias, de marketing o de prospección comercial, etc). Si bien se considera pertinente que estas entidades no formen parte del objetivo del proyecto, no parece clara la justificación que, en el caso de las empresas aseguradoras, la exclusión se limite a las aseguradoras en el ámbito de la salud. Piénsese que aunque el riesgo asegurado no sea propiamente la salud, la información sobre la salud puede ser relevante en otros tipos de seguros (p. ej. seguros de vehículos).

En estos términos, vistas las finalidades únicas de VISC+ (investigación y evaluación), claro está que no sólo los centros acreditados por CERCA son los destinatarios o "clientes" de VISC+, sino que también lo son los Agentes del sistema sanitario de utilización pública de Cataluña.

Por lo tanto, a los efectos de transmitir una información IO más clara y coherente posible entre todos los documentos objeto de consulta, convendría añadir la referencia a los Agentes del SISCAT como destinatarios de los servicios de VISC+, en aquellos documentos en que sólo se hace referencia a los centros acreditados de CERCA (entre otros, apartado 6.2 del Documento nº. 3).

En la versión sometida a dictamen se han suprimido las referencias anteriores al ámbito internacional del flujo informativo en el contexto del proyecto (Documento nº. 5, entre otros) y en algún punto se especifica que está orientado a los investigadores de los centros de investigación públicos de Cataluña (apartado 2 y apartado 6.2 del Documento nº. 3). No obstante, en algún otro documento sí que se da entrada a la posibilidad de que se trate de centros de investigación de otros países (página 5 del Documento nº. 4 o página 15 del Documento nº. 8). Convendría aclarar este aspecto.

En definitiva, la información aportada refleja que se ha limitado las tipologías de clientes finales, si bien sigue faltando algunas concreciones que se han apuntado en este apartado.

c) Tipología de servicios que son objeto de VISC+

La documentación aportada permite comprobar que se ha reducido el número de estos servicios. Si inicialmente VISC+ preveía el tratamiento de datos, anonimizados o no, en relación con servicios de datos abiertos; servicios de datos no abiertos; servicios de licenciamiento, para explotación y análisis de los datos incluidos en el objeto del contrato; servicios de informes estándar: comercialización de informes de análisis y evaluación, basados en los datos incluidos en el alcance del presente contrato; servicios de informes ad hoc, adaptados a necesidades específicas del solicitante; servicios de optimización de la gestión de servicios sanitarios o de práctica clínica, u otros servicios ad hoc que no se concretaban, la documentación aportada (apartado 5.1 Documento nº. 3) limita las tipologías de servicios a facilitar datos para la realización de estudios, realización de análisis estadísticos y preparación de informes.

La mención a que los conjuntos de datos se destinan a investigadores en biomedicina que dispongan de proyectos de investigación, se tendría que complementar con la mención que éstos tienen que estar integrados en centros CERCA, por coherencia con las previsiones del proyecto respecto de sus destinatarios.

En cualquier caso, vista la información aportada, relativa a las finalidades previstas, a los servicios ofrecidos y a los destinatarios de los datos anonimizados en el contexto del nuevo enfoque del proyecto VISC+, y sin perjuicio de las consideraciones que se acaban de hacer, se considera adecuado, desde la perspectiva de los principios de finalidad y de calidad, que se hayan clarificado y acotado, tanto **las finalidades** para las cuales se justifica el tratamiento de datos (investigación y evaluación), como **los grupos o tipologías de clientes finales o destinatarios** (centros acreditados de CERCA y Agentes del sistema sanitario integral de utilización pública de Cataluña), así como **la tipología de servicios ofrecidos** (datos para la realización de estudios, realización de análisis estadísticos y preparación de informes).

VIII

Anonimización de los datos personales en el contexto del proyecto VISC+

En origen, tal como se expone en el Dictamen 34/2014, el proyecto VISC+ preveía el tratamiento de datos personales y la anonimización de estos datos, a efectos de su comunicación posterior a terceros, sin descartar la cesión y el tratamiento por parte de terceros de datos de salud no anonimizados.

Visto el esquema planteado inicialmente, basado en un doble procedimiento de comunicación de datos anonimizados y de datos personales, esta Autoridad recomendó la priorización del procedimiento de cesión de datos previamente y debidamente anonimizadOs, teniendo en cuenta que la anonimización ofrece un tratamiento menos invasivo y de menor riesgo para los derechos de los afectados. En concreto, se recomendó la priorización de la cesión de datos anonimizados asociados a un código no identificable o, si es posible, no asociados a ningún código, por delante de los supuestos de cesión de datos personales de personas identificables que hayan prestado su consentimiento (FJ IX Dictamen 34/2014).

La evolución del proyecto VISC+ ha llevado, según la documentación que ahora se analiza, a circunscribir el alcance del proyecto, exclusivamente, al tratamiento y comunicación de datos anonimizados por la entidad. Se excluye del proyecto, pues, la posibilidad de comunicar datos de carácter personal, en los términos en que se planteaba inicialmente. Tal como se desprende de la documentación aportada, el proyecto comportará la anonimización de toda la información personal por parte de la entidad, antes de su comunicación a terceros, descartando de esta manera la comunicación de datos personales de salud no anonimizados, a los destinatarios finales.

Así se explicita en la documentación aportada, según la cual VISC+ utilizará datos anonimizados de salud (pág. 3 Documento nº. 2). A ello se añade, entre otros, que *"la anonimización de los datos de salud y la custodia de los datos ya anonimizados será realizada por la Agencia, de forma que ninguna otra organización ajena a la Agencia o ningún peticionario de datos tendrá nunca acceso a datos personales"* (pág. 17 Documento nº. 2, y pág. 3 Documento nº. 3).

En base a las consideraciones expuestas abastamente en el Dictamen 34/2014, así como en ocasiones posteriores, y vista la documentación aportada, **hay que valorar**

positivamente el nuevo posicionamiento del proyecto VISC+, ya que, más allá de priorizar, en el sentido apuntado por esta Autoridad, el tratamiento de datos anonimizados, **limita el alcance del proyecto a este flujo informativo en particular (comunicación de datos anonimizados),** descartando la comunicación de datos personales no anonimizados.

Sin perjuicio de ello, y como ya ha puesto de manifiesto la Autoridad anteriormente, convendría matizar alguna afirmación incluida en la documentación, con el fin de transmitir una información a los afectados lo más clara posible, respecto de las implicaciones de VISC+. En concreto, nos referimos a la previsión del apartado *"Riesgos para la ciudadanía"* (pág. 4 Documento nº. 4), en el cual se afirma que:

"(...) hace falta remarcar y hacer énfasis que durante el funcionamiento de VISC+ no se utilizarán datos personales, ya que el tratamiento y el análisis estadístico se hará sobre datos anonimizados".

Si bien es cierto que, vista la información aportada, se ha descartado la cesión de datos personales en el contexto de VISC+, teniendo en cuenta el concepto de "tratamiento de datos" (artículo 3.c) LOPD), se tendría que aclarar que VISC+ sí tratará datos personales en origen, ya que la anonimización por parte de la entidad es una fase más del "tratamiento" de los datos. Convendría, pues, matizar la afirmación que VISC+ no utilizará datos personales.

Por otra parte, en el Documento nº. 8 en el apartado 3.2.2.5 se indica que "*Los datos que contengan información personal o variables que permitan la identificación indirecta de las personas tendrán que cumplir las medidas de seguridad...*". Vista la evolución del proyecto hace falta entender que esta previsión se está refiriendo sólo a los datos que estén en poder de la entidad y que todavía no hayan sido sometidos al proceso de anonimización, pero en ningún caso se puede referir a los datos disponibles para los clientes finales dado que éstos tendrán que estar siempre anonimizados. Tal como ya dijimos, los datos anonimizados tendrían que cumplir también las medidas de seguridad, pero en este caso no se trataría de información personal.

La anonimización de la información tratada constituye pues el elemento clave del proyecto y por ello se tiene que llevar a cabo con las mayores garantías posibles. Por ello hay que tener presente que, vistas las potencialidades del tratamiento que ofrece el entorno del *big data,* a la hora de valorar la posibilidad de reidentificar a una determinada persona, se tiene que tener en cuenta la evolución de la tecnología disponible en cada momento y la información disponible. Y esto incluye no sólo la información anonimizada aislada que sobre aquella persona se pueda facilitar en el marco de un determinado proyecto, sino también la información que se puede facilitar en el marco de otros proyectos o la que esté a disposición del solicitante o, en general, de cualquier persona.

En el proceso de anonimización descrito en la documentación aportada (Documento nº. 2, y Documento nº. 8), se prevé eliminar la información identificativa de personas físicas (datos identificativos, así como información genética), eliminar o reducir al mínimo imprescindible el detalle de la información u otras variables que puedan dar lugar a identificaciones indirectas, así como aplicar técnicas de alteración de los datos. También se prevé atribuir un código anónimo de persona con el fin de permitir relacionar los diferentes conjuntos de datos y aplicar un segundo código diferente para cada proyecto. Estos códigos se tendrán que crear mediante algoritmos que no permitan que terceras personas puedan relacionarlo con una persona concreta.

Ahora bien, hace falta recordar que el apartado referido al proceso de anonimización contenido en el Documento nº. 8 (página 7), difiere del mismo apartado del Documento nº. 2 (página 17), que recogería la última versión del proyecto. Los dos apartados de los dos documentos citados, deberían tener el mismo contenido. Por lo tanto, convendría sustituir los puntos 3 y 4 del apartado 3.2.2.2 del Documento nº. 8, por los puntos 3, 4 y 5 del apartado 4.1 del Documento nº. 2.

Al margen de ello, estas previsiones se consideran adecuadas, y también la previsión de anonimizar otros datos, como los de los profesionales sanitarios que han atendido al paciente, en línea con las recomendaciones del Dictamen 34/2014 (aunque se tiene que señalar que hay una discordancia en el punto 4 del apartado 3.2.2.2 del Documento 8 que prevé anonimizar los datos de los profesionales sanitarios sólo en función de la finalidad que se quiera dar a ciertos datos. Esta previsión se tendría que corregir en el sentido previsto en el punto 5 del apartado 4.1 del Documento nº. 2).

Ahora bien, en relación con esta cuestión, esta Autoridad ya puso de manifiesto que no parece que la previsión de eliminación de información relativa a personas jurídicas sólo sea pertinente en caso de ficheros estadísticos (punto 4 del apartado 4.1 Documento nº. 2), porque si en el resto de ficheros se ha incluido información de este tipo (deducible por ejemplo a través de la identificación del responsable del fichero) también se tendría que eliminar. En principio, como medida de anonimización, esto se tendría que prever para cualquier supuesto.

Y también en la línea de lo que ya se puso de manifiesto en nuestro anterior Dictamen, la anonimización debería afectar también a los datos relativos al centro donde ha sido atendido el paciente o códigos geográficos, en línea con lo que ya prevé el apartado 2.9 del Documento nº. 7.

IX

Garantías éticas de uso de los datos

Entre los documentos nuevos aportados con la solicitud de este dictamen se ha incluido el documento "*Garantías éticas de uso de los datos*" (Documento nº. 7). En general este documento establece una serie de principios a tener en cuenta tanto en el momento del desarrollo del proyecto, como en la evaluación de la demanda y en el posterior seguimiento de la utilización de la información, que conviene tener en cuenta, y que resultan especialmente relevantes.

No obstante, a la vista de la documentación aportada convendría hacer alguna precisión en relación con diferentes aspectos:

a) Procedimiento de gestión de la demanda:

Aunque a lo largo de la diferente documentación del proyecto aparecen diferentes menciones a este aspecto, la configuración final resulta bastante confusa.

El apartado 5.1 del Documento nº. 3 indica que, en los casos que lo establezca la normativa vigente, hará falta que los proyectos hayan pasado por un CEIC. Según la información aportada (apartado 6.1 del mismo Documento nº. 3 y apartado 3.2.2 del Documento 7), se prevé que todas las peticiones tienen que ser sometidas al CEIC, *"excepto en los casos de peticiones de estadística descriptiva o de peticiones de*

análisis destinadas a un uso interno por parte del solicitante que no tengan que ser publicados."

Por otra parte, el apartado 2.6 del Documento 7 al prever que se hará público si las peticiones aprobadas "han contado con la aprobación del CEIC de referencia de la Agencia o no", está admitiendo que la intervención del CEIC no será vinculante.

Todavía respecto al rol del CEIC, hay que señalar que en el apartado 3.2.1 del Documento nº. 8 (pág. 6), se prevé que el CEIC *"Tendrá como principal función la de velar por la correcta aplicación de los criterios científico-èticos en la gestión de la demanda, especialmente en aquellas solicitudes donde haya que evaluar el impacto para la privacidad de los datos si se prevé que éstos son de riesgo elevado."*

A la vista de estas previsiones, no queda muy clara cuál será la función del CEIC en el proceso de gestión de la demanda. Por una parte el apartado 6.1 del Documento 3 y 3.2.2 del Documento 7 prevén que todas las peticiones tienen que contar con la aprobación de un CEIC (parece que no tendría que ser necesariamente el CEIC al cual se adscriba la entidad) "*excepto en los casos de peticiones de estadística descriptiva o de peticiones de análisis destinados a un uso interno por parte del solicitante que no tengan que ser publicadas*". Por otra parte, el apartado 5.1 se refiere sólo a los casos en que "*lo establezca la normativa vigente*", aunque en este caso parece que no se está refiriendo a la intervención del CEIC de la entidad, sino del CEIC que corresponda a la institución que realiza la investigación. Y el apartado 6.3 del Documento nº. 3 o el Documento 8 atribuyen al CEIC velar por la aplicación de los criterios científico-èticos, especialmente en los casos de riesgo elevado.

Vistas estas discordancias, que no contradicciones, **convendría clarificar el papel del CEIC o de los CEIC en el proceso de gestión de la demanda**, en el sentido de prever la necesidad de intervención del CEIC al cual se adscriba la entidad en el proceso de aprobación de la demanda en todos los casos, sin perjuicio de las funciones de seguimiento que se le puedan atribuir especialmente en aquellos casos de riesgo elevado.

b) Principio de protección de la privacidad

El apartado 2.9 de este documento, relativo al *"principio de protección de la privacidad"* incluye diferentes principios y obligaciones con el objeto de proteger la privacidad de las personas afectadas.

Aunque en términos generales el contenido de este apartado resulta adecuado desde la perspectiva de la protección de datos, hay que señalar que en este apartado se prevé que: *"El uso de datos anonimizados mediante servicios VISC+ garantiza que no hay riesgo para la privacidad de las personas".* Teniendo en cuenta las consideraciones del Dictamen 34/2014, convendría matizar esta afirmación, teniendo en cuenta que el riesgo cero respecto de la reidentificación de información previamente anonimizada no es alcanzable.

Al margen de ello, en este apartado se recoge también como principio "*la proporcionalidad de la petición, sólo accediendo a los datos anonimizados mínimos imprescindibles para dar cobertura a la petición*". Esta previsión también resulta pertinente, si bien sería conveniente añadir una referencia "en *especial con respecto a los datos de salud de los cuales se pueda derivar unas mayores consecuencias discriminatorias o estigmatizadores para las personas afectadas*".

c) Obligaciones que tiene que asumir el solicitante de la información:

Dentro de este mismo apartado 2.9 al cual nos acabamos de referir, se recoge también la necesidad de que la entidad y el solicitante firmen un convenio que establezca las obligaciones que asume el cliente en relación con el respeto a la privacidad.

Sería conveniente que en este convenio se incluyera también la previsión que la información utilizada se tiene que destruir una vez ya no sea necesaria para el proyecto, y que ello se tiene que acreditar ante la entidad. A estos efectos sería recomendable que en la solicitud se indicara el plazo en que la entidad se compromete a hacerlo.

Y todavía en relación con este apartado resulta pertinente que se incluyan las obligaciones que asume el solicitante de los datos (no hacer acciones para reidentificar, comunicar situaciones de riesgo de reidentificación, no destinar los otros datos a ninguna otra finalidad, someterse a auditorías de la Agencia, o la medida que se acaba de proponer para la destrucción de la información una vez ya no sea necesaria para el proyecto). Ahora bien, ni en este documento, ni en el resto de documentos sometidos a dictamen se hace ninguna referencia a las consecuencias derivadas del incumplimiento.

En la medida en que las acciones que lleve a cabo la entidad receptora de la información permitan reidentificar personas físicas, podría entrar en juego el régimen sancionador previsto en la normativa de protección de datos o, incluso, el derecho penal. Ahora bien, en caso de que el solicitante incumpla alguna de sus obligaciones sin que eso implique reidentificar personas (por ejemplo, utilizar los datos anónimos con fines publicitarios, o llevar a cabo acciones encaminadas a la reidentificación aunque no se alcance la misma) no sería de aplicación la normativa de protección de datos. Para estos casos sería conveniente que este documento previera que en el convenio también se tienen que incluir las medidas que se pueden utilizar en estos casos (publicidad del incumplimiento, pérdida del derecho a solicitar nuevos conjuntos de información, penalizaciones económicas etc.)

X

Ejercicio de derechos ARCO y posibilidad de "opt-out"

El apartado 2.4 del Documento nº. 7, relativo al *"principio de respeto de los derechos del paciente",* dispone lo siguiente:

"El proyecto VISC+ se construye a partir de datos anonimizados de salud. De esta manera, cuando se tratan datos personales, los derechos de acceso, rectificación, cancelación y oposición (ARCO) del paciente respecto de sus datos personales no son de aplicación.

No obstante, la Agencia apoya el hecho que los derechos ARCO del paciente puedan continuar ejerciéndose delante de los responsables de los ficheros y adicionalmente y, de forma complementaria a estos derechos, la entidad ofrece la posibilidad a los pacientes que lo pidan que sus datos no sean anonimizados e incluidos en VISC+ para hacer investigación."

Respecto de esta previsión, de entrada, convendría matizar que los derechos ARCO continúan siendo de aplicación respecto de los datos personales de origen (tratados en los diferentes ficheros y sistemas de información que son fuente de información de VISC+), hasta que se proceda a su anonimización por parte de la entidad. Por lo tanto, los derechos ARCO, y en especial el derecho de oposición (art. 6.4 LOPD), tienen que poder continuar ejerciéndose delante de los correspondientes responsables de los ficheros.

En cualquier caso, y más allá de la posibilidad de ejercicio del derecho de oposición, **hay que valorar muy positivamente que se explicite, en la documentación aportada, la posibilidad de que los afectados ejerciten el *opt-out*** con el fin de mantenerse al margen del proyecto VISC+, en el sentido que sus datos no sean anonimizados ni incorporados a VISC+. Es decir, se prevé que los ciudadanos podrán decidir libremente si quieren que sus datos se excluyan de este proyecto. Hay que tener en cuenta que el derecho de oposición previsto en la normativa de protección de datos y que se puede ejercer delante del responsable del tratamiento, requiere que la persona que lo ejercita alegue una causa justificada basada en su situación personal. En cambio, con la incorporación del mecanismo de *opt-out*, sería posible que aquellas personas que a pesar de las garantías que ofrezca el sistema, no deseen participar en el proyecto, puedan hacerlo sin tener que alegar una justificación específica.

Ahora bien, más allá de la mención que se hace en el documento examinado, con el objetivo de dar a los afectados la mejor información posible, convendría explicitar el alcance y el objetivo del *opt-out*, el mecanismo para ejercerlo, y las consecuencias que implicará su ejercicio. Aparte de esto, en su momento también habrá que prever los correspondientes formularios para ejercer el *opt-out*, así como la difusión informativa de la posibilidad de ejercerlo.

En definitiva, de la misma manera que el correcto cumplimiento del deber de información por parte de los responsables de los datos (ex. art. 5 LOPD) es clave a fin de que los ciudadanos puedan ejercer los derechos ARCO -cuestión que esta Autoridad ha puesto de manifiesto abastamente-, una información adecuada sobre el proyecto VISC+ (sobre la anonimización que se producirá de los datos, sobre los destinatarios de la información, sobre las finalidades del proyecto, etc), y también sobre la posibilidad de ejercer el *opt-out* permitiría a los afectados tomar una decisión libre e informada sobre la no participación en el proyecto.

En este sentido también resulta positivo que se haya reforzado la transparencia del proyecto mediante la previsión de publicar las solicitudes recibidas, el título de la investigación, el grupo de investigación que la promueve, si ha sido aprobada o no y, si procede, los resultados de la investigación (apartado 2.6 del Documento nº. 7 o apartados 1.7, 5.2 y 6.1 del Documento nº. 3).

XI

Análisis de riesgos

En el Dictamen 34/2014 se recordaba la conveniencia de tener en cuenta, en el contexto del Proyecto VISC+, las consideraciones del Dictamen 5/2014 del Grupo de Trabajo del Artículo 29, respecto de la necesidad de hacer un análisis de riesgos en función de las técnicas de anonimización utilizadas y las posibilidades de reidentificación inherentes a estas técnicas.

La incorporación al proyecto de un informe de evaluación de impacto sobre la privacidad de VISC+ (Documento nº. 8), así como de un informe de análisis de riesgos en relación con el proyecto (Documento nº. 4), es, sin ningún tipo de duda, una buena práctica con respecto a la protección de datos.

Sin perjuicio de algunas consideraciones que ya se han hecho anteriormente en relación con el contenido de estos documentos, y que no hace falta reiterar, hay que señalar todavía algunas cuestiones.

En relación con la reidentificación, el apartado 3.2.2.4 del Documento 8, prevé que cuando se identifiquen riesgos de reidentificación se comunicará a esta Autoridad, y la Agencia emprenderá un plan de acción para mitigarlo, y evitar que se materialice este riesgo o que vuelva a aparecer, previsiones que se consideran adecuadas.

Con respecto a otras previsiones del apartado 5.2 del Documento nº. 8 *"riesgos iniciales y medidas de mitigación propuestas"* (pág. 14 y ss), hay que señalar las cuestiones siguientes:

Con respecto al riesgo "*No cumplimiento de los requerimientos de notificación de los tratamientos en las Agencias de Protección de Datos correspondientes (Catalana y/o Española)*", hay que señalar que dado que la única entidad que tratará datos de carácter personal en este proyecto es la entidad que formula la consulta, las notificaciones se tendrán que hacer siempre a la Autoridad Catalana de Protección de Datos. La intervención de la Agencia Española de Protección de Datos sólo se tendría que producir, si procede, en el caso de transferencias internacionales de datos (art. 41 en relación con el 37.l) LOPD), pero ello se tendría que prever, si procede en el apartado dedicado a la descripción de los riesgos derivados de las transferencias internacionales.

Con respecto al riesgo *"No disponer de la habilitación legal que legitime a AQuAS a hacer el tratamiento y la cesión de datos de salud",* y vista la nueva orientación del proyecto, se tendría que eliminar la mención a la cesión de datos de salud.

Con respecto al riesgo "*Enriquecimiento de los datos personales de forma no prevista en las finalidades iniciales al realizar un cruce con otras bases de datos de terceros*" se indica que "en c*aso de que algún interesado quiera cruzar datos provenientes de VISC+ con otras fuentes de información, la petición será rechazada automáticamente*" pero no se indica de qué medios dispone la entidad para detectar los casos en que el interesado "quiera" hacerlo. Más que conocer la voluntad de llevar a cabo el cruce, habría que referirse a los casos en que haya indicios de que se puede llevar a cabo el cruce.

Con respecto al riesgo de ubicación de los datos fuera del territorio español, hay que decir que, de acuerdo con el artículo 5.1.s) del RLOPD, sólo se considera transferencia internacional el tratamiento de datos que supone una transmisión de estos datos fuera del territorio del Espacio Económico Europeo. De acuerdo con ello, parece que el riesgo se tendría que identificar con la ubicación de los datos fuera del Espacio Económico Europeo. En cualquier caso, convendría una clarificación de este apartado y también del apartado 3.2.2.5 del Documento nº. 8 dado que si los datos sólo se pueden almacenar en servidores dentro del espacio económico europeo, y los datos que se comunican a los clientes son siempre anonimizados, no tendría sentido la referencia a la autorización previa de la AEPD contenida en el apartado 3.2.2.5.

Con respecto al riesgo *"Uso de los datos para finalidades no especificadas o incompatibles con las declaradas por el solicitante (...)",* como estrategia de mitigación

se prevé *que "No se cederán ni tratarán datos personales ni anonimizados para finalidades no especificadas o no compatibles con el solicitante y lo qué prevé la Ley."* Vista la información aportada, y vista la nueva orientación del proyecto, según la cual la cesión de datos personales no se puede producir en ningún caso (ni siquiera en relación con las finalidades de investigación y evaluación propias de VISC+), convendría eliminar de esta frase la mención a la cesión de datos personales.

XII

Medidas de seguridad

Si bien el Proyecto VISC+ supone el tratamiento de información que habrá sido previamente anonimizada por la entidad, esta Autoridad ha puesto de manifiesto la conveniencia de plantear un modelo integral de seguridad de la información para el conjunto del proyecto VISC+, aplicable al tratamiento de datos, que vaya más allá de las previsiones de seguridad que prevé el título VIII del RLOPD.

Teniendo en cuenta las consideraciones hechas por esta Autoridad (FJ XII Dictamen 34/2014, y posteriormente), en relación con el modelo integral de seguridad, y vistas las modificaciones que se han ido incorporando al proyecto, hay que hacer las siguientes consideraciones.

En el Documento nº. 2 se hace constar que las medidas de seguridad y anonimización han sido sometidas a consideración de la Apdcat y que se han incorporado todas sus sugerencias y recomendaciones. En concreto, la documentación aportada (punto 4, Documento nº. 2, entre otros) explicita que VISC+ aplicará las medidas de seguridad y control de accesos que recomiendan las ISO 27000/27001, como mejor práctica en cuanto a estándares internacionales respecto de la gestión de seguridad de la información. Esto responde a una recomendación específica del Dictamen referido, por lo que resulta adecuado.

Respecto de las auditorías de seguridad, la información aportada hace referencia a las mismas en diversos documentos. En el apartado 4.2 del Documento nº. 2, se prevé que:

"La Agencia realizará auditorías para asegurar el correcto funcionamiento y cumplimiento de las medidas de seguridad que implemente VISC+. Más concretamente la agencia ejecutará las siguientes medidas:
- Una auditoría inicial de seguridad, una vez se hayan anonimizado los datos de salud por primera vez.
- Implementar un modelo de verificación continúa de la aplicación de los procedimientos y resultados de los procesos de seguridad, haciendo públicos informes periódicos.
- Una auditoría completa cada 2 años.
- Una auditoría por cada cambio relevante en el proyecto VISC+ que pueda tener un impacto sobre la privacidad."

Como se ponía de manifiesto en el Dictamen 34/2014, *"Con el fin de simplificar el modelo de auditoría, esta Autoridad propone un modelo más sencillo de implementar y potencialmente más eficaz, esto es, un modelo de auditoría continuada, en base a la verificación de la aplicación de los procedimientos y resultados de los procesos de seguridad, realizada internamente por el Adjudicatario, y con emisión de informes periódicos (quizás trimestrales, o incluso semestrales) para ser analizados por AQUAS, y una auditoría formal cada 2 años, realizada por una entidad externa e*

independiente, que finalice con un informe de auditoría con los contenidos mínimos exigidos por la normativa de protección de datos (artículo 96.2 RLOPD)."

En relación con las previsiones sobre auditorías, en el apartado 5.2 *"riesgos iniciales y medidas de mitigación propuestas"* (pág. 16 Documento nº. 8), se prevé que en *"fase de operación de VISC+ ya se contempla la necesidad de realizar nuevas auditorías de calidad de forma frecuente para detectar casos de riesgo".*

En el mismo apartado 5.2, citado, del Documento nº. 8, se prevé que *"(...) el solicitante se compromete a que, si AQUAS lo considera, tenga que pasar auditorías posteriores para comprobar el cumplimiento de estas medidas".*

En la descripción del *"principio de evaluación externa"* (apartado 2.8 Documento nº. 7), se explicita que la entidad implementará un mecanismo de auditoría continuada para la operación diaria del proyecto, previsión que se ajusta a las consideraciones del Dictamen 34/2014.

En definitiva, vistas las diferentes previsiones sobre auditorías en la documentación que se examina, y eliminada la participación de un Adjudicatario con el rol que éste tenía atribuido en versiones anteriores del proyecto VISC+, parece deducirse que será la propia Agencia y, si ésta lo considera oportuno, los solicitantes de datos anonimizados, es decir, los Centros de investigación acreditados por CERCA y los diferentes agentes del sistema sanitario integral de utilización pública de Cataluña (SISCAT), los que tendrán que pasar auditorías.

Si es así, **se podría explicitar y clarificar cuáles tienen que ser los afectados por las auditorías.**

En este sentido, vista la documentación aportada, no parece que se haya previsto ninguna medida de auditoría respecto de los "colaboradores externos", que realizarían algunas tareas técnicas (ver, al respecto, el apartado 4, Documento nº. 4, así como el Documento nº. 5). Teniendo en cuenta lo que se ha mencionado respecto al rol que tienen que tener estos colaboradores externos, y en función de cuál tenga que ser finalmente esta participación de colaboradores externos, se recomienda valorar la previsión que, si la entidad lo considera oportuno, estos colaboradores externos tengan que pasar un proceso de auditoría, en definitiva, incorporarse en el proceso de auditoría continuada recomendado en el Dictamen 34/2014.

Teniendo en cuenta los cambios que se han ido produciendo en el proyecto, este apartado referido a las auditorías ya no incluye, lógicamente, ninguna referencia al Adjudicatario.

Ahora bien, el contenido del apartado 3.2.2.3 del Documento nº. 8, referido igualmente a las auditorías de seguridad, no parece adaptado a los cambios sufridos por el proyecto. Sería pues necesario, revisar el contenido.

Hay que referirse también al contenido del apartado 3.2.2.6 del mismo Documento nº. 8, sobre *"Otros requerimientos de seguridad".* En este apartado se prevé *que "La Agencia tendrá que preservar el modelo de seguridad, disponibilidad y uso de datos que esté vigente en cada momento y no podrá utilizarlos para ninguna otra finalidad ni facilitarlos a terceros. Estas obligaciones se extienden también a los solicitantes de los servicios y tendrán que estar recogidas en el modelo de convenio que se elabore para ser firmado entre la Agencia y el solicitante."*

Este párrafo se refiere al modelo de seguridad, disponibilidad y uso de los datos, que configuraba el Anexo 1 del Documento Técnico de la versión del proyecto que fue objeto de análisis en el Dictamen 34/2014. Dado que, según la información de que se dispone, tanto el Documento Técnico como su anexo ya no son vigentes, convendría revisar esta previsión.

En el punto 3.2.2.3 del mismo Documento 8 (pág. 8) también se hace referencia al dicho "modelo de seguridad, disponibilidad y uso de los datos", cuestión que debería ser revisada en el mismo sentido apuntado.

Resulta pertinente la previsión de designar a un delegado de protección de datos para el proyecto, aunque en la documentación aportada (pág. 4, Documento nº. 4, entre otros) se hace constar que ésta sería una recomendación incluida en el Reglamento CE 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000. Ahora bien, hay que puntualizar que este Reglamento sólo es aplicable a instituciones y organismos de la UE, a los cuales este Reglamento no recomienda, sino que impone, la figura del delegado de protección de datos a las instituciones europeas en las cuales es de aplicación.

Más allá de esta consideración formal, en el Dictamen 34/2014 se recomendaba concretar, entre otros, algunos aspectos técnicos referidos a la transmisión de datos a través de redes públicas o redes sin hilo de comunicaciones electrónicas (artículo 104 RLOPD), en concreto, concretar la red de comunicaciones que se utilizará; los requisitos del software utilizado para la transmisión de los datos; las restricciones a nivel de red con respecto al filtrado de direcciones IP (origen y destinación); los requisitos mínimos de los algoritmos de cifrado a utilizar, etc. También se recomendaba prever cifrar el canal de transporte, así como cifrar en origen los datos objeto de transmisión.

Al respecto, en el Documento nº. 2 se explicita que todo el software, los protocolos y canales de comunicación que se utilicen contarán con los requisitos de seguridad más elevados, entre otros, la aplicación de algoritmos de cifrado robustos, la restricción a nivel de red filtrando direcciones IP, o el cifrado de las transmisiones.

El apartado 4.3 del Documento nº. 2 (págs. 18 y 19) recoge diversas medidas de seguridad en las que se hacía referencia en el Dictamen, como la aplicación de procesos de código de caso anónimo o la comunicación de incidencias a la Apdcat.

De acuerdo con las consideraciones hechas en estos fundamentos jurídicos en relación con la consulta planteada, se hacen las siguientes,

Conclusiones

Se valora positivamente el nuevo posicionamiento del proyecto VISC+, que limita el alcance del proyecto a la comunicación de datos anonimizados, excluyendo la posibilidad de ceder datos personales.

Vistos los ejes fundamentales del nuevo enfoque del proyecto VISC+ (la eliminación de la posibilidad de comunicar datos personales, la limitación de las finalidades del proyecto, así como la limitación de los destinatarios), se recuerda que las previsiones del documento de Encargo de gestión formalizado por el Departamento de Salud, el Servicio Catalán de la Salud y el Instituto Catalán de la Salud con la Agencia de

Calidad y Evaluación Sanitarias de Cataluña (Documento nº. 9), no se ajusta a dicho nuevo enfoque sino que abarca otros aspectos no incluidos en el proyecto VISC+.

Se recomienda explicitar el modelo de gestión seleccionado, con el fin de transmitir una información clara a los afectados, así como aclarar el rol de los colaboradores externos, en el sentido de si tienen que llevar a cabo tareas meramente técnicas, o de mayor alcance. También se recomienda explicitar y clarificar cuáles tienen que ser los sujetos afectados por las auditorías.

Desde la perspectiva de los principios de finalidad y de calidad, resulta adecuado que se hayan clarificado y acotado tanto las finalidades para las cuales se justifica el tratamiento de datos (investigación y evaluación), como las tipologías de clientes finales o destinatarios (centros acreditados de CERCA y Agentes del sistema sanitario integral de utilización pública de Cataluña), así como la tipología de servicios ofrecidos, sin perjuicio de las diversas consideraciones hechas en relación con la documentación analizada.

Convendría clarificar el proceso de gestión de la demanda, en especial con respecto a la intervención del CEIC al cual se adscriba la entidad.

Habría que incorporar las previsiones adecuadas tanto con respecto a la destrucción de la información una vez ya no sea necesaria para el proyecto de investigación, como también las medidas que se pueden aplicar en caso de que el solicitante incumpla las obligaciones que ha asumido.

Se valora positivamente la transparencia prevista con respecto a las solicitudes atendidas, como también la posibilidad de que los afectados ejerciten el *opt-out* para mantenerse al margen del proyecto VISC+. No obstante, con respecto a esta última cuestión convendría dar a este tema un protagonismo mayor en el proyecto, con el fin de transmitir una información adecuada a los afectados.

Barcelona, 16 de abril de 2015

M. Àngels Barbarà Fondevila
Directora