CNS 26/2021

**Dictamen en relación con la consulta formulada por una Universidad pública sobre el desarrollo de una aplicación para teléfonos móviles como herramienta para recabar información en el marco de proyectos de investigación**

**Se presenta ante la Autoridad Catalana de Protección de Datos un escrito del Delegado de Protección de Datos de una Universidad pública en el que se pide que la Autoridad emita un dictamen sobre el desarrollo de una aplicación para teléfonos móviles como herramienta a utilizar por los grupos de investigación para recabar información en el marco de proyectos de investigación**

**En concreto, se plantean las siguientes cuestiones:**

**a) Si el proceso de anonimización de la información que se proporciona a través de esta aplicación móvil puede considerarse adecuado.**

**b) Si, en caso de existir un tratamiento de datos, esto supondría un impedimento para la viabilidad del proyecto desde la perspectiva de la normativa de protección de datos.**

**c) Si, en caso de existir un tratamiento de datos, la Universidad sería la responsable.**

**La consulta se acompaña de los documentos "APP SITUA. Análisis funcional" e "Informe de viabilidad anonimización de datos personales Proyecto SITUA APP".**

**Analizada la petición, y visto el informe de la Asesoría Jurídica y el informe del Área de Tecnología y Seguridad de la Información de la Autoridad, se dictamina lo siguiente.**



**(...)**

**II**

**La Universidad expone en su consulta que, apoyada por un Ayuntamiento, se pretende llevar a cabo un proyecto consistente en el desarrollo de una aplicación para teléfonos móviles, llamada "SITUA APP".**

**Esta aplicación se quiere utilizar por parte de los grupos de investigación de la Universidad para recabar información personal en el marco de los proyectos de investigación que lleven a cabo. A modo de ejemplo, hace referencia al caso del grupo de investigadores de Geografía y Género de su Departamento de Geografía en el marco del Proyecto de I+D+i "Procesos de reruralización y refeminización en el medio rural. Análisis desde la geografía del género" (Ref. PID2019-105773RB-I00), el cual cuenta con la financiación del Ministerio de Ciencia e Innovación (MICINN).**

**De acuerdo con el documento "APP SITUA. Análisis funcional", adjuntado a la consulta, se trata, en concreto, de crear una aplicación móvil a medida que permita registrar las incidencias que una persona pueda reportar a causa de actos o situaciones discriminatorias, de violencia de género,**

de acoso sexual, de homofobia, etc. que haya podido sufrir, a efectos de realizar un posterior análisis estadístico, para acabar identificando las zonas de una ciudad (inicialmente, Barcelona) que presentan una tendencia o son más favorables a sufrir este tipo de situaciones.

También se propone, dentro del proyecto, desarrollar una plataforma web para poder recuperar los datos registrados por los usuarios de esta aplicación móvil y así generar y visualizar los paneles estadísticos.

La Universidad afirma que el objetivo del proyecto es trabajar con datos agregados irreversiblemente anónimos, dado que, para su viabilidad, no requiere de la identificación de personas físicas concretas.

Por este motivo, solicita a esta Autoridad su valoración sobre la adecuación del procedimiento de anonimización de los datos con los que se está trabajando para garantizar que el proyecto puede desarrollarse sin generar riesgos para la privacidad de las personas físicas.

Hacer notar que el examen de esta cuestión se efectúa, a continuación, a partir de la información que se facilita en la consulta tomando como referencia el estudio del grupo de investigadores del Departamento de Geografía al que se ha realizado mención. Para otros estudios, en atención a la información que fuese objeto de tratamiento, este examen podría ser diferente.

III

En la consulta se plantea si el proceso de anonimización diseñado en el desarrollo de SITUA APP garantiza que nos encontramos ante un tratamiento de datos anonimizados.

De entrada, cabe destacar que los principios y garantías de la protección de datos no se aplican a la información anónima, es decir, a aquella información que ha perdido toda vinculación directa o indirecta con la persona física -o que ya no lo ha tenido desde su obtención-, de modo que el afectado deja de ser identificable sin esfuerzos desproporcionados.

Así se desprende claramente del considerante 26 del Reglamento (UE) 2016/679, del Parlamento y del Consejo Europeo, de 27 de abril de 2016, General de Protección de Datos (en adelante, RGPD):

> "Los principios de la protección de datos deben aplicarse a toda la información relativa a una persona física identificada o identificable. Las datos personales seudonimizados, que cabría atribuir a una persona física mediante la utilización de información adicional, deben considerarse información sobre una persona física identificable. Para determinar si una persona física es identificable, deben tenerse en cuenta todos los medios, como la singularización, que razonablemente pueda utilizar el responsable del tratamiento o cualquier otra persona para identificar directa o indirectamente a la persona física. Para determinar si existe una probabilidad razonable de que se utilicen medios para identificar a una persona física, deben tenerse en cuenta todos los factores objetivos, como los costes y el tiempo necesarios para la identificación, teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos. Por tanto los principios de protección de datos no deben aplicarse a la información anónima, es decir información que no guarda relación con una persona física identificada o identificable, ni a las datos convertidos en anónimos de forma que el interesado no sea identificable, o deje de serlo. En consecuencia, el presente Reglamento no afecta al tratamiento de dicha información anónima, inclusive con fines estadísticos o de investigación."

**Conviene aclarar que cualquier proceso de anonimización, aplicado a datos personales, debe tener por finalidad destruir el vínculo o nexo entre el dato personal y la persona física afectada, a quien se refiere la información. El objetivo es que la persona afectada no resulte identificable por terceros sin esfuerzos desproporcionados.**

**Mientras este nexo entre el dato y la persona física a la que se refiere pueda ser reconstruido de forma relativamente sencilla –en este sentido, hay que considerar todos sus factores objetivos, como los costes y el tiempo necesarios para la identificación, teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos-, no puede considerarse que la información ha sido objeto de un procedimiento de anonimización adecuado y seguirá sujeta a los principios y obligaciones derivados de la normativa de protección de datos.**

**Recuerda que el Grupo de Trabajo del Artículo 29 (en adelante, GTA29) en su Dictamen 5/2014 sobre técnicas de anonimización, al que nos remitimos, pone de manifiesto que el riesgo de reidentificación es inherente a cualquier técnica de anonimización, por lo que la intimidad y el derecho a la protección de datos del titular podría verse comprometida, aun cuando los datos hayan sido anonimizados.**

**Por este motivo, es necesario llevar a cabo siempre un análisis inicial y periódico de posibles riesgos de reidentificación y, a la vista del resultado obtenido, articular las medidas necesarias para atenuar la probabilidad de que se materialicen, previendo incluso medidas reactivas por atenuar el posible daño que pudiera derivarse hacia una persona física si dicha reidentificación tuviera lugar. Estas medidas o garantías tendrán que ser superiores en aquellos casos en que se traten categorías especiales de datos (como sucede en el presente caso), dado que el riesgo es mayor en atención al mayor impacto que representaría esta reidentificación, de materializarse, sobre los derechos y libertades de las personas afectadas.**

**Esta identificación y análisis del riesgo de reidentificación debería entenderse en el presente caso como una actividad enmarcada dentro de la evaluación de impacto en la protección de datos (AIPD) a que se refiere el artículo 35 del RGPD.**

**El RGPD requiere realizar una evaluación de impacto sobre la privacidad "cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o finas, entrañe un alto riesgo para los derechos y libertades de las personas físicas" (artículo 35.1). Y menciona expresamente como un supuesto en el que habrá que realizar una evaluación de impacto, la evaluación sistemática y exhaustiva que permita la elaboración de perfiles (artículo 35.2.a)) o el tratamiento a gran escala de categorías especiales de datos (artículo 35.2 .b)).**

**En relación con esta evaluación de impacto, la LOPDDDD enumera, en su artículo 28.2, algunos supuestos en los que se entiende probable la existencia de un alto riesgo para los derechos y libertades de las personas, entre los cuales "cuando se produjese el tratamiento no meramente incidental o accesorio de las categorías especiales de datos a que se refieren los artículos 9 y 10 del Reglamento (UE) 2016/679 y 9 y 10 de esta ley orgánica (...)" (letra c) ; "cuando el tratamiento implicase una evaluación de aspectos personales de los afectados con el fin de crear o utilizar perfiles personales de los mismos, en particular mediante la análisis o la predicción de aspectos referidos a su rendimiento en el trabajo, su situación económica, su salud , sus preferencias o intereses personales, su fiabilidad o comportamiento, su solvencia financiera, su localización o sus movimientos" (letra d); o "cuando se lleve a cabo el tratamiento de datos de grupos de afectados en situación de especial vulnerabilidad y, en particular, de menores de edad y personas con discapacidad" (letra e)).**

**Además, para facilitar a los responsables de los tratamientos la identificación de aquellos tratamientos que requieren una AIPD, el RGPD dispone que las autoridades de control deben publicar una lista con los tratamientos que requieran de una AIPD. Esta Autoridad considera que es necesario realizar una AIPD en los tratamientos incluidos en la lista que se encuentra disponible en el**

https://apdcat.gencat.cat/web/.content/02-drets_i_obligacions/obligacions/documents/Lista_DPIA-CAT.pdf.

En el presente caso, a pesar de preverse un tratamiento de datos anonimizados, hay que tener en consideración que concurrirían las circunstancias a las que se ha mencionado:

- Tratamiento que implicaría el perfilado o valoración de las personas usuarias de la aplicación; - Tratamiento que implicaría el uso de categorías especiales de datos (artículo 9 RGPD); - Tratamiento que haría referencia a datos de sujetos vulnerables, o en riesgo de exclusión social, incluso a menores de 14 años, a mayores con algún grado de discapacidad, a personas víctimas de violencia de género o de cualquier otra situación discriminatoria ; - Tratamiento que implicaría un nuevo uso de tecnologías emergente

Aunque, como se ha dicho, la normativa de protección de datos no resulta de aplicación al tratamiento de datos anónimos y por tanto a priori la realización de una AIPD no resultaría en este caso exigible, dado que se trata de un procedimiento que busca identificar y controlar los riesgos para los derechos y libertades de las personas asociados a un tratamiento de datos y que, como se ha visto, el riesgo de reidentificación es inherente a cualquier técnica de anonimización, el hecho de que el proyecto examinado concurran las circunstancias mencionadas pone de manifiesto, como mínimo, la conveniencia de la realización en parte (no necesariamente debería efectuarse un proceso completo) de una AIPD que permita medir, evaluar y gestionar

Ahora bien, más allá de esto, como veremos, la concurrencia de ciertos elementos nos llevarán a considerar que el proceso de anonimización de los datos que se propone en el presente caso no resultaría eficaz, por lo que puede decirse que la realización de esta AIPD por parte del responsable del tratamiento resultaría exigible.

A estos efectos, puede resultar de interés consultar la "Guía sobre la evaluación de impacto relativa a la protección de datos en el RGPD", disponible en la web de la Autoridad.

Para dar respuesta a la presente consulta, se analiza a continuación el proceso de anonimización propuesto, a efectos de determinar si existe el riesgo de acabar identificando a las personas usuarias de la aplicación sin esfuerzos desproporcionados. Hay que tener en cuenta que este análisis sólo puede servir a título orientativo, dado que corresponde al responsable del tratamiento en cada caso concreto realizar este análisis, a la vista de los datos y las circunstancias concretas que concurran en cada caso.



IV

En el documento "APP SITUA. Análisis funcional", adjuntado a la consulta, se efectúan algunas manifestaciones que resultan de especial interés a efectos de valorar el proceso de anonimización de datos a que se refiere la presente consulta.

En concreto, en este documento se recuerda que:

- La aplicación no utiliza datos que puedan relacionarse de forma unívoca con una persona física (identificadores), tales como: nombre, apellidos, DNI, correo electrónico, dirección, etc. o datos del dispositivo (identificador interno único (UUID), sistema operativo, versión, etc.).

- La aplicación genera y guarda un identificador aleatorio (código alfanumérico) que en ningún momento se relacionaría con la persona usuaria a la que hace referencia ni con el dispositivo móvil.

**- El acceso a la aplicación por la persona usuaria no requiere validación (introducción de un usuario y contraseña).**

**- La primera vez que se accede, la persona usuaria puede vincularse con alguno de los proyectos de investigación que se llevan a cabo, seleccionando, a tal efecto, el código del proyecto que resulte de su interés entre los códigos que se muestran.**

**Se ofrece también la opción de no vincularse a ningún proyecto concreto. En este caso, se le identifica como usuario sin proyecto asignado y "los datos se podrán tratar según proyecto".**

**Hacer notar que, facilitar datos personales para una finalidad genérica de investigación o recopilarlos con el objetivo de que queden al alcance de cualquier grupo investigador sin asociarlos a un estudio concreto, como parecería desprenderse de esta manifestación, no resultaría una adecuada actuación desde el punto de vista de la protección de datos. La persona usuaria debe ser consciente en el momento en que facilita sus datos personales (y esto incluye tanto la información del perfil como la reportada) de los fines a los que se destinarán estos datos, los cuales deben ser siempre determinados y explícitos (artículos 5.1.b) y 13.1.c) RGPD).**

**Según se describe, cuando la persona usuaria se vincula a un nuevo proyecto, la aplicación le asigna un nuevo código identificador (como si se tratara de un nuevo usuario), por lo que los proyectos en los que haya participado una misma persona usuaria no pueden vincularse entre sí. Sin embargo, parece que este mecanismo no impide vincular las incidencias reportadas por un mismo usuario en un mismo proyecto.**

**- Es necesario obligatoriamente cumplimentar un cuestionario. Los datos recogidos con este cuestionario formarán parte del "perfil" de la persona usuaria en la aplicación.**

**El citado documento incluye unas capturas de pantalla que muestran el tipo de información que se recoge para elaborar este perfil. Hacer notar que, salvo en el primer campo, no se muestra el desplegable del resto de campos a llenar.**

**La información (atributos) del perfil, según estas capturas, es la siguiente:**

- **Identidad de género (a seleccionar: hombre, mujer, trans, no binario, otros, no definida, no quiero responder).**
- **Orientación sexual.**
- **Edad.**
- **Religión.**
- **Racialización.**
- **Situación administrativa.**
- **Clase social.**
- **Diversidad funcional.**
- **Nacionalidad.**

**- A partir de ahí, la persona usuaria puede reportar una incidencia. La información que se recoge en este sentido comprende:**

- **Tipo de ubicación.**

  **A seleccionar: espacio público, espacio doméstico, comercio o servicio, espacio laboral, espacio formativo, centro sanitario, lugar libre, transporte público, y oficina o servicio de la administración pública.**

No se permitirá que el usuario registre ubicaciones predefinidas, "como podría ser identificar como hogar la dirección de la casa particular, para evitar que queden registrados datos privados".

Hacer notar que esta redacción resulta confusa, dado que puede dar a entender que se recogerá la dirección del domicilio de la persona usuaria.

• Localización manual.

La persona usuaria indica en un mapa el lugar de la incidencia (coordenadas). No se utiliza GPS.

• Preguntas relacionadas con la incidencia.

La persona usuaria debe responder un cuestionario obligatoriamente para definir la incidencia reportada.

El documento citado también incluye unas capturas de pantalla que muestran las preguntas y el tipo de información que se recoge en este sentido:

o Cómo te sientes en este sitio (se ofrece un campo abierto para describir cómo se siente la persona usuaria). o Qué emociones sientes (a seleccionar: preocupación, angustia, miedo, humillación, rabia, discriminación, exclusión, soledad, aceptación, seguridad, tranquilidad, apoyo, inclusión, alivio, libertad y/o alegría). o Qué grado de malestar sientes (se ofrece una barra deslizante para indicar el grado de malestar).

o Has sufrido alguna discriminación (en caso de seleccionar SI, se ofrece un desplegable para indicar la causa; un campo abierto para describir los hechos; y un calendario para seleccionar fecha y hora).

- Reportada la incidencia, la información se transmite a la base de datos y no queda ninguna registro en el dispositivo móvil de la persona usuaria.

Si no se ha completado el proceso de reportar una incidencia, los datos facilitados quedan almacenados en el dispositivo de la persona usuaria (no en la base de datos) y la próxima vez que la persona usuaria entra en la aplicación se mostrará el punto del proceso en el que se quedó. Es decir, sólo se envían los datos registrados cuando se genera una incidencia, no antes.

En caso de cancelar la incidencia, se borran los datos introducidos en relación con los campos “Tipo de ubicación” y “Localización manual”, no así los del “Perfil”. Éste sólo se borra en caso de reiniciar la aplicación.

V

Teniendo en cuenta todos los aspectos que se han expuesto, se pueden extraer, a los efectos de su interés, las siguientes consideraciones:

El “Proyecto” prevé la utilización de un código identificativo aleatorio en sustitución de otros datos que puedan comportar la identificación de la persona usuaria (nombre, DNI, UUID del móvil o cualquier otro identificador que pudiera obtenerse del dispositivo: IMEI, dirección MAC de la WIFI o del Bluetooth, etc.).

**La relación entre este identificador y la persona física a la que hace referencia parece que no sería conocida por el responsable ni por ninguna de las personas que tengan acceso a la información reportada.**

**Ahora bien, esta actuación por sí sola (uso de un código identificador aleatorio y no recoger identificadores directos) no es suficiente para considerar que los datos han sido correctamente anonimizados. Es necesario adoptar las medidas adecuadas dirigidas a reducir al máximo posible las posibilidades de reidentificar a las personas usuarias de la aplicación (de asociar los datos recopilados a una persona física concreta).**

**La aplicación examinada recoge información muy detallada para elaborar el "perfil" de la persona usuaria. Al menos, se recoge la identidad de género, orientación sexual, edad, religión, racialización, situación administrativa, clase social, diversidad funcional y nacionalidad. La lista podría ser mayor, dado que ésta sólo es la información que puede apreciarse en las capturas de pantalla incorporadas a la documentación adjunta, sin que en la información aportada conste que sólo se recogerán, a tal efecto, los atributos mencionados .**

**A esto hay que añadir que la información que recoge la aplicación en el momento de reportar una incidencia también es muy detallada, con la particularidad de ofrecer campos abiertos que todavía permitirían recopilar identificadores directos.**

**En el documento "Informe de viabilidad anonimización de datos personales Proyecto SITUA APP" se afirma que se utilizará "un bloqueador automático si se detecta la entrada de nombres, direcciones, teléfonos u otros datos que puedan identificar a una persona" y que "se incluirá un aviso visible advirtiendo a los usuarios para que no dejen datos personales", aunque a la vez se reconoce que estos mecanismos podrían no ser suficientes.**

**Destacar especialmente que, en lo que se refiere a la información sobre el lugar en el que se ha producido la incidencia, no sólo se recoge información sobre el tipo de entorno (doméstico, laboral, formativo, etc.), sino también su localización.**

**Para definir la localización de la incidencia, se prevé que la aplicación muestre un mapa con la visión general del ámbito geográfico de que se trate, el cual la persona usuaria podrá expandir para indicar "el punto" de la incidencia, momento en el que las coordenadas relativas a este punto quedarán registradas. Aunque afirma que de este modo no se registra la dirección concreta de la incidencia, no se puede obviar que el uso de coordenadas, a pesar de haberse introducido manualmente, puede permitir conocer la localización exacta de la incidencia (y aún en mayor medida si se pone en relación con el "tipo de ubicación") y, por tanto, de la persona que la reporta.**

**El hecho de que los datos de localización se obtengan manualmente (y no accediendo al GPS), si bien implica que la aplicación sea menos intrusiva (desde el punto de vista que no realiza un seguimiento del movimiento de las personas), no tiene un impacto práctico sobre el anonimato de los datos recogidos. En este sentido, un sistema de localización que sólo permitiera localizar las incidencias en áreas de población suficientemente amplias para no poder identificar a personas concretas garantizaría en mejor medida el anonimato.**

**Aparte de esto, las comunicaciones sobre las incidencias reportadas por la persona usuaria dentro de un mismo estudio parecen relacionarse utilizando el código aleatorio generado por la aplicación.**

**Aunque en el documento "APP SITUA. Análisis funcional" se afirma que el código identificativo en ningún momento se relaciona con la persona usuaria ni con su dispositivo móvil, también se indica que "como usuario se guardará un identificador aleatorio" que permite relacionar las diferentes incidencias de un usuario dentro de un mismo proyecto (apartado 2.1.1).**

Toda esta información (o atributos) a la que se ha ido haciendo referencia entraría dentro del concepto de identificadores indirectos, esto es, atributos que, si bien no identifican a una persona, su cruce sí podría permitir esa identificación.

Para poder afirmar que los datos tratados son anónimos debería justificarse que la información mencionada (información del perfil, información sobre la localización de la incidencia e incidencias reportadas) no es suficiente para llegar a identificar a una persona física (el usuario). Ahora bien, esto resulta cuestionable, especialmente a raíz del sistema previsto para recopilar la información sobre la localización (coordenadas) y el hecho de que ésta se ponga en relación con el campo "Tipo de ubicación".

A modo de ejemplo, en una incidencia la información sobre el tipo de ubicación (p. ej. doméstico) se combina con la localización que se facilita manualmente (coordenadas) y con la información del "perfil" (uso combinado o cruce de datos) aumenta considerablemente las posibilidades de reidentificar a la persona usuaria. De hecho, esto podría ocurrir también en todos aquellos ámbitos que son fácilmente asociables a una persona física como el laboral o el formativo.

Por otra parte, la información sobre una incidencia reportada también puede acabar ofreciendo información sobre otras incidencias, de modo que si una persona tiene conocimiento de una incidencia, a través del código podría asociar fácilmente también datos vinculados a otra incidencia.

En cualquiera de los ejemplos expuestos, la asociación entre registros de una misma persona comporta que la identificación de uno de estos registros pueda revelar sobre otros registros.

La necesaria aplicación del principio de minimización recogido en el artículo 5.1.c) RGPD (tratar la información personal mínima imprescindible) es clave cuando se tratan datos personales, pero también si se realiza un proceso de anonimización. Una anonimización efectiva requeriría reducir la información o atributos procesados que pueden actuar como identificadores indirectos.

Especialmente habría que modificar el sistema definido para reportar la localización de las incidencias. Las posibilidades de reidentificación serían menores si la localización se realizara por áreas geográficas (municipio, comarca...) en especial si el área tomada como referencia se hace variar en función del riesgo de reidentificación detectado.

Y también debería evitarse la posibilidad de enlazar las diferentes incidencias reportadas por una misma persona usuaria en relación con un mismo estudio (sólo parece garantizada la no trazabilidad entre estudios).

Por otro lado, desde un punto de vista técnico, es necesario tener en consideración que la conexión necesaria entre el dispositivo móvil de la persona usuaria y el dispositivo que recolecta los datos es suficiente para obtener una dirección IP, que podría identificar de forma bastante precisa al usuario, por ejemplo, si la comunicación se llevara a cabo desde su domicilio.

En la información aportada se indica que no se ha previsto recoger la dirección IP (según la documentación aportada no estaría entre la lista de atributos que se recogen a través de la aplicación), si bien en función de la tecnología utilizada podría quedar rastro. Ahora bien, que no se haya previsto recoger este dato, no permite descartar que según la tecnología utilizada, éste haga un tratamiento (como mínimo para el establecimiento de la comunicación).

Está claro que los proveedores de servicios de internet pueden relacionar fácilmente la dirección IP con una persona física, pero, además, en la práctica no puede descartarse que esta relación también se pueda llevar a cabo por otras vías.

**Por todo ello, cabe concluir que existe el riesgo de reidentificar a las personas usuarias de la aplicación sin esfuerzos desproporcionados, por lo que el proceso de anonimización a que se refiere la consulta no ofrecería suficientes garantías para considerar que nos encontramos ante de datos anonimizados.**

**De lo contrario, es decir, si no se puede asegurar una anonimización que ofrezca plenas garantías, nos encontraremos ante un tratamiento de datos personales, en su mayor parte, merecedoras de especial protección (artículo 9 RGPD), por lo que los principios y obligaciones de la legislación de protección de datos resultarían de plena aplicación.**

**VI**

**En la consulta se plantea si, de existir un tratamiento de datos personales, esto supondría un impedimento para la viabilidad del proyecto desde la perspectiva de la normativa de protección de datos personales.**

**El RGPD establece que todo tratamiento de datos personales debe ser lícito, leal y transparente (artículo 5.1.a)).**

**El artículo 6.1 del RGPD regula las bases jurídicas en las que puede fundamentarse el tratamiento de datos personales, en los siguientes términos:**

> **"1. El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones: a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos; b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado se parte o para la aplicación a petición del mismo de medidas precontractuales; c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento; d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física; e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento; f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.**
>
> **Lo dispuesto en la letra f) del párrafo primero no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones."**

**Es necesario, por tanto, tener en consideración que el tratamiento de datos personales debe tener, para ser lícito, una base jurídica, la cual puede ser el consentimiento de las personas afectadas o bien cualquier otra de las bases jurídicas indicadas en este artículo 6.1 de el RGPD.**

**Así se desprende claramente del considerante 40 del RGPD al establecer que "para que el tratamiento sea lícito, las datos personales deben ser tratados con el consentimiento del interesado o sobre alguna otra base legítima establecida conforme a Derecho, ya sea en el presente Reglamento o en virtud de otro Derecho de la Unión o de los Estados miembros a que se refiera el presente Reglamento, incluida la necesidad de cumplir la obligación legal aplicable al responsable del tratamiento o la necesidad de ejecutar un contrato en el que sea parte el interesado o al objeto de tomar medidas a instancia del interesado con anterioridad a la conclusión de un contrato."**

**Recuerda que la elección de la base jurídica en la que fundamentar un determinado tratamiento de datos debe llevarse a cabo siempre antes de comenzar el tratamiento, teniendo en cuenta la finalidad a la que responderá. Así se desprende de la obligación de informar al afectado sobre, entre otros aspectos, la base jurídica empleada por el responsable del tratamiento en el momento de la recogida de los datos (artículo 13.1.c) RGPD).**

**En el documento "Informe de viabilidad anonimización de datos personales Proyecto SITUA APP" se señala que el proyecto se nutre de información facilitada voluntariamente por los usuarios interesados en participar.**

**Teniendo en cuenta esta participación voluntaria y que el proyecto (la aplicación y la plataforma web) está en plena fase de desarrollo (por tanto, todavía no se habría producido ningún tratamiento de datos), podría plantearse la opción de articular el tratamiento de datos pretendido sobre la base del consentimiento explícito de las personas afectadas.**

**Ahora bien, recuerda que el consentimiento sólo puede ser una base jurídica adecuada si reúne las características establecidas en el artículo 4.11) del RGPD, es decir, el consentimiento del afectado debe ser informado, libre, específico y debe ser otorgado mediante una manifestación que muestre la voluntad del afectado de consentir o bien mediante una clara acción afirmativ**

**Además, dado que en el presente caso el tratamiento afecta a categorías especiales de datos, el consentimiento deberá ser explícito (artículo 9.2.a) RGPD).**

**Señalar, particularmente, la necesidad de que el consentimiento responda a fines determinados y específicos, es decir, no resultaría admisible la prestación de un consentimiento general, en el sentido, en el caso examinado, de una aceptación incondicionada para utilizar los datos de el usuario de la aplicación con fines generales de investigación. Este consentimiento debería ir asociado siempre a estudios de investigación concretos. Adquiere aquí plena importancia la protección de datos por defecto (artículo 25 RGPD), es decir, que en caso de que el usuario no determine un proyecto concreto, no se puede entender que los autoriza a todos, sino que**

**También habría que tener en consideración que si el tratamiento de datos se refiriera a personas menores de edad (la documentación aportada no aclara este aspecto) únicamente podría fundamentarse en su consentimiento cuando estas personas sean mayores de 14 años. En caso contrario, el tratamiento de datos sobre la base de su consentimiento sólo sería lícito si constase también el consentimiento del titular de la potestad parental o tutela, con el alcance que éste determine (artículo 7 LOPDGDD).**

**Por tanto, de utilizar la base jurídica del consentimiento, habría que adoptar los mecanismos adecuados para garantizar que las personas usuarias de la aplicación SITUA APP den el consentimiento para el tratamiento de sus datos en los términos indicados. Y también para garantizar que estas personas cuentan con información adecuada en relación a este tratamiento.**

**VII**

**Más allá de contar con legitimación suficiente para llevar a cabo el tratamiento de datos, corresponde al responsable la tarea de garantizar y poder demostrar que este tratamiento se ajustará en todo momento al RGPD (artículo 5.2 RGPD relativo al principio de responsabilidad proactiva) .**

**Esto, en términos prácticos, requiere la adopción e implantación de medidas técnicas y organizativas apropiadas a fin de cumplir los requisitos del RGPD y de proteger los derechos de las personas interesadas (artículo 24 RGPD).**

**En este sentido, y aparte de cumplir con el resto de principios y obligaciones previstos en la normativa de protección de datos, es necesario hacer referencia, particularmente, a dos mecanismos: el principio de transparencia de la información (artículos 5.1.a) y 12 RGPD ), y la aplicación de las medidas a las que se ha hecho referencia para dificultar la reidentificación.**

**El requisito de transparencia constituye uno de los principios fundamentales en el tratamiento de datos, estrechamente relacionado con los principios de lealtad y licitud del tratamiento, tal y como se desprende del artículo 5.1.a) del RGPD. Entregar información a los afectados, antes de obtener su consentimiento, resulta esencial para éstos puedan comprender qué es lo que están consintiendo realmente.**

**El artículo 13 del RGPD determina la información que el responsable del tratamiento debe entregar al afectado cuando los datos se obtienen de éste, como sucede en el presente caso.**

**Para facilitar este cumplimiento, la LOPDDDD (artículo 11) ha previsto la posibilidad de entregar al afectado esta información por capas o niveles. Este método consiste en presentar una información "básica" (información resumida) en un primer nivel, de modo que se pueda tener un conocimiento general del tratamiento, donde se indique una dirección electrónica u otro medio al que se pueda acceder de forma sencilla y inmediata al resto de la información, y, en un segundo nivel, ofrecer el resto de la información adicional (información detallada).**

**Cuando se opta por esta vía, dicha información "básica" deberá comprender la identidad del responsable del tratamiento, la finalidad del tratamiento y la posibilidad de ejercer los derechos habeas fecha establecidos en los artículos 15 a 22 del RGPD, así como, en su caso, el hecho de que los datos se utilizarán para la elaboración de perfiles (artículo 11.2 LOPDGDD).**

**De acuerdo con el considerante 42 del RGPD, a fin de considerar que el consentimiento es informado, es necesario comunicar al afectado "como mínimo la identidad del responsable del tratamiento y los fines del tratamiento a los que están destinados las datos personales".**

**Esto no significa sin embargo que, en atención a las circunstancias y el contexto en el que se lleva a cabo un determinado tratamiento, no sea necesario entregar más información al afectado para que éste entienda realmente el tratamiento de datos que tendrá lugar y el consentimiento pueda considerarse válido. En este sentido, se pronuncia el Grupo de Trabajo del Artículo 29 en su documento "Directrices sobre el consentimiento en el sentido del Reglamento (UE) 2016/679" (apartado 3.3.1), criterio que comparte esa Autoridad.**

**En un caso como el examinado, por tanto, sería también conveniente informar a las personas usuarias de la aplicación que, a pesar de disponer de su consentimiento explícito, se han adoptado las medidas adecuadas para reducir el riesgo de reidentificarlas, aunque deben ser plenamente conscientes de las posibilidades de reidentificación que existen.**

**También sería conveniente informarlas de la forma en que se llevará a cabo la difusión de los resultados del estudio de investigación en los que hayan participado.**

**En el documento "APP SITUA. Análisis funcional" se recuerda que la plataforma web que se desarrolle debe permitir gestionar los datos registrados y visualizar paneles estadísticos como pueden ser listados y ciertas gráficas (apartado 1.1). Ahora bien, más allá de esta previsión, en este documento (tampoco en el documento "Informe de viabilidad anonimización de datos personales Proyecto SITUA APP") no se contempla ninguna referencia sobre qué publicación o difusión se hará de los resultados obtenidos.**

**Hacer notar que, en función de su difusión, puede aumentar de forma considerable el riesgo de reidentificación de las personas usuarias de la aplicación. Por tanto, antes de llevarla a cabo, es necesario examinar cuidadosamente la información que se facilitará en este sentido.**

**En cualquier caso, habría que tener presente que, si se previera tratar datos de menores de edad, toda la información debería facilitarse con un lenguaje claro y sencillo, de tal modo que éstos pudieran identificar fácilmente quién es el responsable, la finalidad pretendida y comprender qué es lo que están autorizando.**

**Advertir también que el responsable del tratamiento deberá ser capaz de demostrar que las personas usuarias han consentido el tratamiento de sus datos en los términos indicados en el fundamento jurídico anterior (artículo 7.1 RGPD), así como que les ha facilitado la información pertinente (artículo 5.2 RGPD). A tal efecto, podría exigirse la marcación de una o varias casillas por el usuario antes de proceder a la descarga de la aplicación.**

**Más allá de esto, y aunque los datos se recojan con el consentimiento de las personas afectadas, es necesario poner de relieve el esfuerzo llevado a cabo por la Universidad para proponer soluciones técnicas encaminadas a garantizar el anonimato de las personas usuarias de la aplicación SITUA APP. Si bien no se pueda concluir que las medidas propuestas permitan considerar que la información resultante es realmente anónima, sí pueden considerarse como medidas adecuadas para reducir los riesgos para las personas afectadas.**

**Todo ello sin perjuicio del cumplimiento del resto de principios y obligaciones establecidas en la legislación de protección de datos.**

**VIII**

**En la consulta también se plantea si, en caso de constatarse un tratamiento de datos, la Universidad sería la responsable, si bien el proyecto sea liderado por dos profesoras de la Universidad y cuente con el apoyo de un Ayuntamiento.**

**De acuerdo con el artículo 4.7) del RGPD se entiende por responsable del tratamiento "la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros."**

**Tal y como se desprende de esta definición, el elemento clave para ser considerado responsable del tratamiento en materia de protección de datos personales es la capacidad de decidir o determinar la finalidad, el contenido, el uso o los medios del tratamiento. decir, tomar decisiones sobre qué hacer y cómo tratar los datos personales desde el momento en que éstos se recogen hasta su destrucción.**

**En el ámbito universitario, por tanto, pueden tener esta consideración de responsable del tratamiento la universidad, el órgano, el área, el servicio, la unidad administrativa o, incluso, el miembro de la comunidad universitaria que tenga la capacidad tomar las decisiones sobre la finalidad y los medios de este tratamiento.**

**Conviene aclarar, en este punto, que la entidad o personas que llevan a cabo el diseño y desarrollo de la aplicación SITUA APP y de la plataforma web no tendrían consideración de responsables del tratamiento de datos, a la vista de la definición que ofrece el artículo 4.7 del RGPD.**

**Este rol recaería en aquella persona, jurídica o física, que utilice estos medios (la aplicación y la plataforma) para llevar a cabo el estudio de investigación de que se trate y que, por tanto, tiene la capacidad para decidir cómo y para qué fines se recogerá y tratará la información personal. Por tanto, podría ser la Universidad, un departamento de la universidad o bien cualquier investigador o grupo de investigadores de la Universidad quien ostente la condición de responsable del tratamiento.**

**También conviene aclarar que si la entidad o las personas que llevan a cabo el diseño y desarrollo de la aplicación SITUA APP y de la plataforma web no forman parte del responsable del tratamiento, en caso de que tengan que acceder a datos personales sería necesaria la formalización de un encargo del tratamiento en los términos del artículo 28.3 del RGPD, dada la existencia de un tratamiento de datos por cuenta del responsable (artículo 4.8) RGPD).**

**De acuerdo con las consideraciones hechas hasta ahora en relación con la consulta planteada, se hacen las siguientes,**

**Conclusiones**

**Por la información de que se dispone, el proceso de anonimización propuesto no permitiría garantizar un tratamiento de datos anónimos en el seno del Proyecto al que se refiere la consulta.**

**Sin embargo, podría plantearse la opción de articular el tratamiento de datos pretendido sobre la base del consentimiento explícito de las personas afectadas (artículos 6.1.a) y 9.2.a) RGPD), sin perjuicio de la adopción de las medidas adecuadas para garantizar que este tratamiento se adecua al RGPD, tales como, facilitar una información detallada y clara al respecto, y aplicar las medidas a las que se ha hecho referencia para dificultar la reidentificación.**

**La condición de responsable del tratamiento de datos vinculado a la realización de un proyecto recaerá en aquella entidad o persona que decida o determine la finalidad, contenido, uso o medios de dicho tratamiento.**

**Barcelona, 2 de junio de 2021**