CNS 26/2021

Dictamen en relació amb la consulta formulada per una Universitat pública sobre el desenvolupament d'una aplicació per a telèfons mòbils com a eina per recollir informació en el marc de projectes d'investigació

Es presenta davant l'Autoritat Catalana de Protecció de Dades un escrit del Delegat de Protecció de Dades d'una Universitat pública en el qual es demana que l'Autoritat emeti un dictamen sobre el desenvolupament d'una aplicació per a telèfons mòbils com a eina a emprar pels grups de recerca per a recollir informació en el marc de projectes d'investigació.

En concret, es plantegen les qüestions següents:

a) Si el procés d'anonimització de la informació que es proporciona a través d'aquesta aplicació mòbil pot considerar-se adequat.

b) Si, en cas d'existir un tractament de dades, això suposaria un impediment per a la viabilitat del projecte des de la perspectiva de la normativa de protecció de dades.

c) Si, en cas d'existir un tractament de dades, la Universitat en seria la responsable.

La consulta s'acompanya dels documents "APP SITUA. Anàlisi funcional" i "Informe de viabilitat anonimització de dades personals Projecte SITUA APP".

Analitzada la petició, i vist l'informe de l'Assessoria Jurídica i l'informe de l'Àrea de Tecnologia i Seguretat de la Informació de l'Autoritat, es dictamina el següent.

I

(...)

II

La Universitat exposa en la seva consulta que, amb el suport d'un Ajuntament, es pretén dur a terme un projecte consistent en el desenvolupament d'una aplicació per a telèfons mòbils, anomenada "SITUA APP".

Aquesta aplicació es vol utilitzar per part dels grups de recerca de la Universitat per recollir informació personal en el marc dels projectes d'investigació que duguin a terme. A tall d'exemple, fa referència al cas del grup d'investigadors de Geografia i Gènere del seu Departament de Geografia en el marc del Projecte d'I+D+i "*Procesos de re-ruralización y re-feminización en el medio rural. Análisis desde la geografía del género"* (Ref. PID2019-105773RB-I00), el qual compta amb el finançament del *Ministerio de Ciencia e Innovación* (MICINN).

D'acord amb el document "APP SITUA. Anàlisi funcional", adjuntat a la consulta, es tracta, en concret, de crear una aplicació mòbil a mida que permeti registrar les incidències que una persona pugui reportar a causa d'actes o situacions discriminatòries, de violència de gènere,

d'assetjament sexual, d'homofòbia, etc. que hagi pogut patir, als efectes de fer-ne una posterior anàlisi estadística, per tal d'acabar identificant les zones d'una ciutat (inicialment, Barcelona) que presenten una tendència o són més favorables a patir aquest tipus de situacions.

També es proposa, dins del projecte, desenvolupar una plataforma web per poder recuperar les dades registrades per les persones usuàries d'aquesta aplicació mòbil i així generar i visualitzar els panells estadístics.

La Universitat afirma que l'objectiu del projecte és treballar amb dades agregades irreversiblement anònimes, atès que, per a la seva viabilitat, no requereix de la identificació de persones físiques concretes.

Per aquest motiu, sol·licita a aquesta Autoritat la seva valoració sobre l'adequació del procediment d'anonimització de les dades amb què s'està treballant per tal de garantir que el projecte es pot desenvolupar sense generar riscos per a la privacitat de les persones físiques.

Fer notar que l'examen d'aquesta qüestió s'efectua, tot seguit, a partir de la informació que es facilita en la consulta prenent com a referència l'estudi del grup d'investigadors del Departament de Geografia a què s'ha fet esment. Per a d'altres estudis, en atenció a la informació que fos objecte de tractament, aquest examen podria ser diferent.

III

En la consulta es planteja si el procés d'anonimització que s'ha dissenyat en el desenvolupament de SITUA APP garanteix que ens trobem davant un tractament de dades anonimitzades.

D'entrada, cal fer notar que els principis i garanties de la protecció de dades no s'apliquen a la informació anònima, és a dir, a aquella informació que ha perdut tota vinculació directa o indirecta amb la persona física -o que ja no l'ha tingut des de la seva obtenció-, de manera que l'afectat deixa de ser identificable sense esforços desproporcionats.

Així es desprèn clarament del considerant 26 del Reglament (UE) 2016/679, del Parlament i del Consell Europeu, de 27 d'abril de 2016, General de Protecció de Dades (en endavant, RGPD):

> *"Los principios de la protección de datos deben aplicarse a toda la información relativa a una persona física identificada o identificable. Los 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 lo 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 los 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."*

Convé aclarir que qualsevol procés d'anonimització, aplicat a dades personals, ha de tenir per finalitat destruir el vincle o nexe entre la dada personal i la persona física afectada, a qui es refereix la informació. L'objectiu és que la persona afectada no resulti identificable per tercers sense esforços desproporcionats.

Mentre aquest nexe entre la dada i la persona física a la qual es refereix pugui ser reconstruït de forma relativament senzilla –en aquest sentit, cal considerar-ne tots els factors objectius, com els costos i el temps necessaris per a la identificació, tenint en compte tant la tecnologia disponible en el moment del tractament com els avenços tecnològics-, no es pot considerar que la informació ha estat objecte d'un procediment d'anonimització adequat i seguirà subjecta als principis i obligacions derivats de la normativa de protecció de dades.

Fer avinent que el Grup de Treball de l'Article 29 (en endavant, GTA29) en el seu Dictamen 5/2014 sobre tècniques d'anonimització, al qual ens remetem, posa de manifest que el risc de reidentificació és inherent a qualsevol tècnica d'anonimització, per la qual cosa la intimitat i el dret a la protecció de dades del titular podria veure's compromesa, tot i que les dades hagin estat anonimitzades.

Per aquest motiu, és necessari dur a terme sempre una anàlisi inicial i periòdica de possibles riscos de reidentificació i, a la vista del resultat obtingut, articular les mesures necessàries per atenuar la probabilitat de que es materialitzin, preveient, fins i tot, mesures reactives per atenuar el possible dany que pogués derivar-se vers una persona física si la dita reidentificació tingués lloc. Aquestes mesures o garanties hauran de ser superiors en aquells casos en què es tractin categories especials de dades (com succeeix en el present cas), atès que el risc és major en atenció al major impacte que representaria aquesta reidentificació, de materialitzar-se, sobre els drets i llibertats de les persones afectades.

Aquesta identificació i anàlisi del risc de reidentificació caldria entendre-la en el present cas com una activitat emmarcada dins l'avaluació d'impacte en la protecció de dades (AIPD) a què es refereix l'article 35 de l'RGPD.

L'RGPD requereix fer una avaluació d'impacte sobre la privacitat *"cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas"* (article 35.1). I esmenta expressament com un supòsit en què caldrà fer una avaluació d'impacte, l'avaluació sistemàtica i exhaustiva que permeti l'elaboració de perfils (article 35.2.a)) o el tractament a gran escala de categories especials de dades (article 35.2.b)).

En relació amb aquesta avaluació d'impacte, l'LOPDGDD enumera, en llur article 28.2, alguns supòsits en què s'entén probable l'existència d'un alt risc per als drets i llibertats de les persones, entre els quals *"cuando se produjese el tratamiento no meramente incidental o accesorio de las categorías especiales de datos a las que se refieren los artículos 9 y 10 del Reglamento (UE) 2016/679 y 9 y 10 de esta ley orgánica (...)"* (lletra 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 el 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"* (lletra 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*" (lletra e)).

A més, per facilitar als responsables dels tractaments la identificació d'aquells tractaments que requereixen una AIPD, l'RGPD disposa que les autoritats de control han de publicar una llista amb els tractaments que requereixin d'una AIPD. Aquesta Autoritat considera que cal fer una AIPD en els tractaments inclosos en la llista que es troba disponible al següent enllaç:

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

En el present cas, tot i preveure's un tractament de dades anonimitzades, cal tenir en consideració que concorrerien les circumstàncies a què s'ha fet esment:

- Tractament que implicaria el perfilat o valoració de les persones usuàries de l'aplicació;
- Tractament que implicaria l'ús de categories especials de dades (article 9 RGPD);
- Tractament que faria referència a dades de subjectes vulnerables, o en risc d'exclusió social, fins i tot, a menors de 14 anys, a majors amb algun grau de discapacitat, a persones víctimes de violència de gènere o de qualsevol altra situació discriminatòria;
- Tractament que implicaria un nou ús de tecnologies emergents.

Tot i que, com s'ha dit, la normativa de protecció de dades no resulta d'aplicació al tractament de dades anònimes i per tant a priori la realització d'una AIPD no resultaria en aquest cas exigible, atès que es tracta d'un procediment que busca identificar i controlar el riscos per als drets i les llibertats de les persones associats a un tractament de dades i que, com s'ha vist, el risc de reidentificació és inherent a qualsevol tècnica d'anonimització, el fet que en el projecte examinat concorrin les circumstàncies esmentades posa de manifest, com a mínim, la conveniència de la realització en part (no necessàriament hauria d'efectuar-se un procés complet) d'una AIPD que permeti mesurar, avaluar i gestionar el risc de reidentificació.

Ara bé, més enllà d'això, com veurem, la concurrència de certs elements ens portaran a considerar que el procés d'anonimització de les dades que es proposa en el present cas no resultaria eficaç, per la qual cosa pot dir-se que la realització d'aquesta AIPD per part del responsable del tractament resultaria exigible.

A aquests efectes, pot resultar d'interès consultar la "Guia sobre l'avaluació d'impacte relativa a la protecció de dades al RGPD", disponible al web de l'Autoritat.

Per tal de donar resposta a la present consulta, s'analitza tot seguit el procés d'anonimització proposat, als efectes de determinar si existeix el risc d'acabar identificant les persones usuàries de l'aplicació sense esforços desproporcionats. Cal tenir però en compte que aquesta anàlisi només pot servir a títol orientatiu, atès que correspon al responsable del tractament en cada cas concret fer aquesta anàlisi, a la vista de les dades i les circumstàncies concretes que concorrin en cada cas.

IV

En el document "APP SITUA. Anàlisi funcional", adjuntat a la consulta, s'efectuen algunes manifestacions que resulten d'especial interès als efectes de valorar el procés d'anonimització de dades a què es refereix la present consulta.

En concret, en aquest document es fa avinent que:

- L'aplicació no utilitza dades que puguin relacionar-se de forma unívoca amb una persona física (identificadors), tals com: nom, cognoms, DNI, correu electrònic, adreça, etc. o dades del dispositiu (identificador intern únic (UUID), sistema operatiu, versió, etc.).

- L'aplicació genera i guarda un identificador aleatori (codi alfanumèric) que en cap moment es relacionaria amb la persona usuària a qui fa referència ni amb el dispositiu mòbil.

- L'accés a l'aplicació per la persona usuària no requereix validació (introducció d'un usuari i contrasenya).

- La primera vegada que s'accedeix, la persona usuària pot vincular-se amb algun dels projectes d'investigació que es duen a terme, seleccionant, a tal efecte, el codi del projecte que resulti del seu interès d'entre els codis que es mostren.

  S'ofereix també l'opció de no vincular-se a cap projecte en concret. En aquest cas, se l'identifica com a usuari sense projecte assignat i *"les dades es podran tractar segons projecte"*.

  Fer notar que, facilitar dades personals per a una finalitat genèrica d'investigació o recopilar-les amb l'objectiu que restin a l'abast de qualsevol grup investigador sense associar-les a un estudi concret, com semblaria desprendre's d'aquesta manifestació, no resultaria una actuació adequada des del punt de vista de la protecció de dades. La persona usuària ha d'ésser conscient en el moment en què facilita les seves dades personals (i això inclou tant la informació del perfil com la reportada) dels fins a què es destinaran aquestes dades, els quals han d'ésser sempre determinats i explícits (articles 5.1.b) i 13.1.c) RGPD).

  Segons es descriu, quan la persona usuària es vincula a un nou projecte, l'aplicació li assigna un nou codi identificador (com si es tractés d'un nou usuari), de manera que els projectes en què hagi participat una mateixa persona usuària no es poden vincular entre si. No obstant això, sembla que aquest mecanisme no impedeix vincular les incidències reportades per un mateix usuari dins un mateix projecte.

- Cal obligatòriament omplir un qüestionari. Les dades recollides amb aquest qüestionari formaran part del "perfil" de la persona usuària a l'aplicació.

  El document citat inclou unes captures de pantalla que mostren el tipus d'informació que es recull per elaborar aquest perfil. Fer notar que, llevat del primer camp, no es mostra el desplegable de la resta de camps a omplir.

  La informació (atributs) del perfil, segons aquestes captures, és la següent:

  - Identitat de gènere (a seleccionar: home, dona, trans, no binari, altres, no definida, no vull respondre).
  - Orientació sexual.
  - Edat.
  - Religió.
  - Racialització.
  - Situació administrativa.
  - Classe social.
  - Diversitat funcional.
  - Nacionalitat.

- A partir d'aquí, la persona usuària pot reportar una incidència. La informació que es recull en aquest sentit comprèn:

  - Tipus d'ubicació.

    A seleccionar: espai públic, espai domèstic, comerç o servei, espai laboral, espai formatiu, centre sanitari, lloc de lleure, transport públic, i oficina o servei de l'administració pública.

No es permetrà que l'usuari registri ubicacions predefinides, *"com podria ser identificar com a llar l'adreça de la casa particular, per evitar que quedin registrades dades privades"*.

Fer notar que aquesta redacció resulta confusa, atès que pot donar a entendre que es recollirà l'adreça del domicili de la persona usuària.

- Localització manual.

  La persona usuària indica en un mapa el lloc de la incidència (coordenades). No s'utilitza GPS.

- Preguntes relacionades amb la incidència.

  La persona usuària ha de respondre un qüestionari obligatòriament per tal de definir la incidència reportada.

  El document citat també inclou unes captures de pantalla que mostren les preguntes i el tipus d'informació que es recull en aquest sentit:

  - Com t'hi sents en aquest lloc (s'ofereix un camp obert per descriure com se sent la persona usuària).
  - Quines emocions hi sents (a seleccionar: preocupació, angoixa, por, humiliació, ràbia, discriminació, exclusió, soledat, acceptació, seguretat, tranquil·litat, suport, inclusió, alleujament, llibertat i/o alegria).
  - Quin grau de malestar hi sents (s'ofereix una barra lliscant per indicar el grau de malestar).
  - Hi has patit alguna discriminació (en cas de seleccionar SI, s'ofereix un desplegable per indicar-ne la causa; un camp obert per descriure els fets; i un calendari per seleccionar data i hora).

- Reportada la incidència, la informació es transmet a la base de dades i no queda cap registre al dispositiu mòbil de la persona usuària.

  Si no s'ha completat el procés de reportar una incidència, les dades facilitades queden emmagatzemades al dispositiu de la persona usuària (no a la base de dades) i el pròxim cop que la persona usuària entra a l'aplicació es mostrarà el punt del procés on es va quedar. És a dir, només s'envien les dades registrades quan es genera una incidència, no abans.

  En cas de cancel·lar la incidència, s'esborren les dades introduïdes en relació amb els camps "Tipus d'ubicació" i "Localització manual", no així les del "Perfil". Aquest només s'esborra en cas de reiniciar l'aplicació.

V

Tenint en compte tots els aspectes que s'han exposat, es poden extreure, als efectes que interessen, les consideracions següents:

El "Projecte" preveu la utilització d'un codi identificatiu aleatori en substitució d'altres dades que puguin comportar la identificació de la persona usuària (nom, DNI, UUID del mòbil o qualsevol altre identificador que es pogués obtenir del dispositiu: IMEI, direcció MAC de la WIFI o del Bluetooth, etc.).

La relació entre aquest identificador i la persona física a qui fa referència sembla que no seria coneguda pel responsable ni per cap de les persones que tinguin accés a la informació reportada.

Ara bé, aquesta actuació per si sola (ús d'un codi identificador aleatori i no recollir identificadors directes) no és suficient per considerar que les dades han estat correctament anonimitzades. Cal adoptar les mesures escaients adreçades a reduir al màxim possible les possibilitats de reidentificar les persones usuàries de l'aplicació (d'associar les dades recopilades a una persona física concreta).

L'aplicació examinada recull informació molt detallada per elaborar el "perfil" de la persona que n'és usuària. Com a mínim, es recull la identitat de gènere, orientació sexual, edat, religió, racialització, situació administrativa, classe social, diversitat funcional i nacionalitat. La llista però podria ser més gran, atès que aquesta només és la informació que pot apreciar-se en les captures de pantalla incorporades a la documentació adjunta, sense que en la informació aportada consti que només es recolliran, a tal efecte, els atributs esmentats.

A això cal afegir que la informació que recull l'aplicació en el moment de reportar una incidència també és molt detallada, amb la particularitat d'oferir camps oberts que encara permetrien recopilar identificadors directes.

En el document "Informe de viabilitat anonimització de dades personals Projecte SITUA APP" s'afirma que s'utilitzarà *"un bloquejador automàtic si es detecta l'entrada de noms, adreces, telèfons o altres dades que puguin identificar a una persona"* i que *"s'inclourà un avís visible advertint als usuaris perquè no deixin dades personals"*, tot i que alhora es reconeix que aquests mecanismes podrien no ésser suficients.

Destacar especialment que, pel que fa a la informació sobre el lloc en què s'ha produït la incidència, no només es recull informació sobre el tipus d'entorn (domèstic, laboral, formatiu, etc.), sinó també la seva localització.

Per tal de definir la localització de la incidència, es preveu que l'aplicació mostri un mapa amb la visió general de l'àmbit geogràfic que es tracti, el qual la persona usuària podrà expandir per tal d'indicar-hi "el punt" de la incidència, moment en què les coordenades relatives a aquest punt quedaran registrades. Tot i afirmar que d'aquesta manera no s'enregistra l'adreça concreta de la incidència, no es pot obviar que l'ús de coordenades, malgrat haver-se introduït manualment, pot permetre conèixer la localització exacta de la incidència (i encara en major mesura si es posa en relació amb el "tipus d'ubicació") i, per tant, de la persona que la reporta.

El fet que les dades de localització s'obtinguin manualment (i no accedint al GPS), si bé implica que l'aplicació sigui menys intrusiva (des del punt de vista que no fa un seguiment del moviment de les persones), no té un impacte pràctic sobre l'anonimat de les dades recollides. En aquest sentit, un sistema de localització que només permetés localitzar les incidències en àrees de població suficientment àmplies per a no poder identificar persones concretes garantiria en millor mesura l'anonimat.

A part d'això, les comunicacions sobre les incidències reportades per la persona usuària dins un mateix estudi sembla que es poden relacionar utilitzant el codi aleatori generat per l'aplicació.

Tot i que en el document "APP SITUA. Anàlisi funcional" s'afirma que el codi identificatiu en cap moment es relaciona amb la persona usuària ni amb el seu dispositiu mòbil, també s'indica que *"com a usuari es guardarà un identificador aleatori"* que permet relacionar les diferents incidències d'un usuari dins d'un mateix projecte (apartat 2.1.1).

Tota aquesta informació (o atributs) a què s'ha anat fent referència entraria dins del concepte d'identificadors indirectes, això és, atributs que, si bé no identifiquen a una persona, el seu encreuament sí podria permetre aquesta identificació.

Per tal de poder afirmar que les dades tractades són anònimes caldria justificar que la informació esmentada (informació del perfil, informació sobre la localització de la incidència i incidències reportades) no és suficient per arribar a identificar una persona física (l'usuari). Ara bé, això resulta qüestionable, especialment arran el sistema previst per recopilar la informació sobre la localització (coordenades) i el fet que aquesta es posi en relació amb el camp "Tipus d'ubicació".

A tall d'exemple, en una incidència la informació sobre el tipus d'ubicació (p. ex. domèstic) es combina amb la localització que es facilita manualment (coordenades) i amb la informació del "perfil" (ús combinat o encreuament de dades) augmenta considerablement les possibilitats de reidentificar la persona usuària. De fet, això podria ocórrer també en tots aquells àmbits que són fàcilment associables a una persona física, com ara el laboral o el formatiu.

Per altra banda, la informació sobre una incidència reportada també pot acabar oferint informació sobre altres incidències, de tal manera que si una persona té coneixement d'una incidència, a través del codi podria associar fàcilment també dades vinculades a una altra incidència.

En qualsevol dels exemples exposats, l'associació entre registres d'una mateixa persona comporta que la identificació d'un aquests registres pugui revelar sobre altres registres.

La necessària aplicació del principi de minimització recollit a l'article 5.1.c) RGPD (tractar la informació personal mínima imprescindible) és clau quan es tracten dades personals, però també si es fa un procés d'anonimització. Una anonimització efectiva requeriria reduir la informació o els atributs processats que poden actuar com a identificadors indirectes.

Especialment caldria modificar el sistema definit per reportar la localització de les incidències. Les possibilitats de reidentificació serien menors si la localització es fes per àrees geogràfiques (municipi, comarca...) en especial si l'àrea agafada com a referència es fa variar en funció del risc de reidentificació detectat.

I també caldria evitar la possibilitat d'enllaçar les diferents incidències reportades per una mateixa persona usuària en relació amb un mateix estudi (només sembla garantida la no traçabilitat entre estudis).

Per altra banda, des d'un punt de vista tècnic, cal tenir en consideració que la connexió necessària entre el dispositiu mòbil de la persona usuària i el dispositiu que recol·lecta les dades és suficient per obtenir una adreça IP, la qual podria identificar de forma força precisa a l'usuari, per exemple, si la comunicació es dugués a terme des del seu domicili.

En la informació aportada s'indica que no s'ha previst recollir l'adreça IP (segons la documentació aportada no estaria entre la llista d'atributs que es recullen a través de l'aplicació), si bé en funció de la tecnologia emprada en podria quedar rastre. Ara bé, que no s'hagi previst recollir aquesta dada, no permet descartar que segons la tecnologia emprada, aquesta en faci un tractament (com a mínim per a l'establiment de la comunicació).

És clar que els proveïdors de serveis d'internet poden relacionar fàcilment l'adreça IP amb una persona física, però, a més, a la pràctica no es pot descartar que aquesta relació també es pugui dur a terme per altres vies.

Per tot plegat, cal concloure que existeix el risc de reidentificar les persones usuàries de l'aplicació sense esforços desproporcionats, per la qual cosa el procés d'anonimització a què es refereix la consulta no oferiria suficients garanties per tal de considerar que ens trobem davant de dades anonimitzades.

Altrament, és a dir, si no es pot assegurar una anonimització que ofereixi plenes garanties, ens trobarem davant un tractament de dades personals, en la seva major part, mereixedores d'especial protecció (article 9 RGPD), per la qual cosa els principis i obligacions de la legislació de protecció de dades resultarien de plena aplicació.

VI

En la consulta es planteja si, en cas d'existir un tractament de dades personals, això suposaria un impediment per a la viabilitat del projecte des de la perspectiva de la normativa de protecció de dades personals.

L'RGPD estableix que tot tractament de dades personals ha de ser lícit, lleial i transparent (article 5.1.a)).

L'article 6.1 de l'RGPD regula les bases jurídiques en les que pot fonamentar-se el tractament de dades personals, en els termes següents:

> *"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 es parte o para la aplicación a petición de este 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 los 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."*

Cal, per tant, tenir en consideració que el tractament de dades personals ha de tenir, per ser lícit, una base jurídica, la qual pot ser el consentiment de les persones afectades o bé qualsevol altra de les bases jurídiques indicades en aquest article 6.1 de l'RGPD.

Així es desprèn clarament del considerant 40 de l'RGPD en establir que *"para que el tratamiento sea lícito, los 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 con objeto de tomar medidas a instancia del interesado con anterioridad a la conclusión de un contrato."*

Fer avinent que l'elecció de la base jurídica en què fonamentar un determinat tractament de dades s'ha de dur a terme sempre abans de començar el tractament, tenint en compte la finalitat a què respondrà. Així es desprèn de l'obligació d'informar l'afectat sobre, entre d'altres aspectes, la base jurídica emprada pel responsable del tractament en el moment de la recollida de les dades (article 13.1.c) RGPD).

En el document "Informe de viabilitat anonimització de dades personals Projecte SITUA APP" s'assenyala que el projecte es nodreix d'informació facilitada voluntàriament pels usuaris interessats en participar-hi.

Tenint en compte aquesta participació voluntària i que el projecte (l'aplicació i la plataforma web) està en plena fase de desenvolupament (per tant, encara no s'hauria produït cap tractament de dades), podria plantejar-se l'opció d'articular el tractament de dades pretès sobre la base del consentiment explícit de les persones afectades.

Ara bé, fer avinent que el consentiment només pot ser una base jurídica adequada si reuneix les característiques establertes a l'article 4.11) de l'RGPD, és a dir, el consentiment de l'afectat ha d'ésser informat, lliure, específic i ha d'ésser atorgat mitjançant una manifestació que mostri la voluntat de l'afectat de consentir o bé mitjançant una clara acció afirmativa.

A més, atès que en el present cas el tractament afecta categories especials de dades, el consentiment haurà d'ésser explícit (article 9.2.a) RGPD).

Assenyalar, particularment, la necessitat que el consentiment respongui a fins determinats i específics, és a dir, no resultaria admissible la prestació d'un consentiment general, en el sentit, en el cas examinat, d'una acceptació incondicionada per utilitzar les dades de l'usuari de l'aplicació amb fins generals d'investigació. Aquest consentiment hauria d'anar associat sempre a estudis d'investigació concrets. Adquireix aquí plena importància la protecció de dades per defecte (article 25 RGPD), és a dir, que en cas que l'usuari no determini un projecte concret, no es pot entendre que els autoritza tots, sinó que s'hauria d'entendre que els rebutja tots.

També caldria tenir en consideració que si el tractament de dades es referís a persones menors d'edat (la documentació aportada no aclareix aquest aspecte) únicament podria fonamentar-se en el seu consentiment quan aquestes persones siguin majors de 14 anys. Altrament, el tractament de dades sobre la base del seu consentiment només seria lícit si constés també el consentiment del titular de la potestat parental o tutela, amb l'abast que aquest determini (article 7 LOPDGDD).

Per tant, d'emprar la base jurídica del consentiment, caldria adoptar els mecanismes escaients per garantir que les persones usuàries de l'aplicació SITUA APP donen el consentiment per al tractament de les seves dades en els termes indicats. I també per garantir que aquestes persones compten amb informació adequada en relació amb aquest tractament.

VII

Més enllà de comptar amb legitimació suficient per dur a terme el tractament de dades, correspon al responsable la tasca de garantir i poder demostrar que aquest tractament s'ajustarà en tot moment a l'RGPD (article 5.2 RGPD relatiu al principi de responsabilitat proactiva).

Això, en termes pràctics, requereix l'adopció i implantació de mesures tècniques i organitzatives apropiades a fi de complir els requisits de l'RGPD i de protegir els drets de les persones interessades (article 24 RGPD).

En aquest sentit, i a banda de complir amb la resta de principis i obligacions previstos a la normativa de protecció de dades, cal fer referència, particularment, a dos mecanismes: el principi de transparència de la informació (articles 5.1.a) i 12 RGPD), i l'aplicació de les mesures a què s'ha fet referència per dificultar la reidentificació.

El requisit de transparència constitueix un dels principis fonamentals en el tractament de dades, estretament relacionat amb els principis de lleialtat i licitud del tractament, tal com es desprèn de l'article 5.1.a) de l'RGPD. Lliurar informació als afectats, abans d'obtenir el seu consentiment, resulta essencial per a aquests puguin comprendre què és el que estan consentint realment.

L'article 13 de l'RGPD determina la informació que el responsable del tractament ha de lliurar a l'afectat quan les dades s'obtenen d'aquest, com succeeix en el present cas.

Per tal de facilitar aquest compliment, l'LOPDGDD (article 11) ha previst la possibilitat de lliurar a l'afectat aquesta informació per capes o nivells. Aquest mètode consisteix en presentar una informació "bàsica" (informació resumida) en un primer nivell, de manera que es pugui tenir un coneixement general del tractament, on s'indiqui una adreça electrònica o un altre mitjà on es pugui accedir de manera senzilla i immediata a la resta de la informació, i, en un segon nivell, oferir la resta de la informació addicional (informació detallada).

Quan s'opta per aquesta via, la dita informació "bàsica" haurà de comprendre la identitat del responsable del tractament, la finalitat del tractament i la possibilitat d'exercir els drets habeas data establerts als articles 15 a 22 de l'RGPD, així com, si escau, el fet que les dades s'empraran per a l'elaboració de perfils (article 11.2 LOPDGDD).

D'acord amb el considerant 42 de l'RGPD, per tal de considerar que el consentiment és informat, és necessari comunicar a l'afectat *"como mínimo la identidad del responsable del tratamiento y los fines del tratamiento a los cuales están destinados los datos personales".*

Això no significa però que, en atenció a les circumstàncies i el context en què es du a terme un determinat tractament, no sigui necessari lliurar més informació a l'afectat per tal que aquest entengui realment el tractament de dades que tindrà lloc i el consentiment pugui considerar-se vàlid. En aquest sentit, es pronuncia el Grup de Treball de l'Article 29 en el seu document *"Directrices sobre el consentimiento en el sentido del Reglamento (UE) 2016/679"* (apartat 3.3.1), criteri que comparteix aquesta Autoritat.

En un cas com l'examinat, per tant, seria també convenient informar les persones usuàries de l'aplicació que, tot i disposar del seu consentiment explícit, s'han adoptat les mesures escaients per tal de reduir el risc de reidentificar-les, tot i que han de poder ser plenament conscients de les possibilitats de reidentificació que existeixen.

També seria convenient informar-les de la manera en què es durà a terme la difusió dels resultats de l'estudi d'investigació en què hagin participat.

En el document "APP SITUA. Anàlisi funcional" es fa avinent que la plataforma web que es desenvolupi ha de permetre gestionar les dades enregistrades i visualitzar panells estadístics com poden ser llistats i certes gràfiques (apartat 1.1). Ara bé, més enllà d'aquesta previsió, en aquest document (tampoc en el document "Informe de viabilitat anonimització de dades personals Projecte SITUA APP") no es contempla cap referència sobre quina publicació o difusió es farà dels resultats obtinguts.

Fer notar que, en funció de la difusió que se'n faci, pot augmentar de manera considerable el risc de reidentificació de les persones usuàries de l'aplicació. Per tant, abans de dur-la a terme, cal examinar acuradament la informació que es facilitarà en aquest sentit.

En tot cas, caldria tenir present que, si es preveiés tractar dades de menors d'edat, tota la informació s'hauria de facilitar amb un llenguatge clar i senzill, de tal manera que aquests poguessin identificar fàcilment qui és el responsable, la finalitat pretesa i comprendre què és el que estan autoritzant.

Advertir també que el responsable del tractament haurà de ser capaç de demostrar que les persones usuàries han consentit el tractament de les seves dades en els termes indicats en el fonament jurídic anterior (article 7.1 RGPD), així com que els hi ha facilitat la informació pertinent (article 5.2 RGPD). A tal efecte, podria exigir-se la marcació d'una o vàries caselles per la persona usuària abans de procedir a la descàrrega de l'aplicació.

Més enllà d'això, i tot i que les dades es recullin amb el consentiment de les persones afectades, cal posar en relleu l'esforç dut a terme per la Universitat per proposar solucions tècniques encaminades a garantir l'anonimat de les persones usuàries de l'aplicació SITUA APP. Per bé que no es pugui concloure que les mesures proposades permetin considerar que la informació resultant és realment anònima, sí que es poden considerar com a mesures adequades per a reduir els riscos per a les persones afectades.

Tot això, sens perjudici del compliment de la resta de principis i obligacions establertes a la legislació de protecció de dades.

VIII

En la consulta també es planteja si, en cas de constatar-se un tractament de dades, la Universitat en seria la responsable, per bé que el projecte sigui liderat per dues professores de la Universitat i compti amb el suport d'un Ajuntament.

D'acord amb l'article 4.7) de l'RGPD s'entén per responsable del tractament *"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 com es desprèn d'aquesta definició, l'element clau per ésser considerat responsable del tractament en matèria de protecció de dades personals és la capacitat de decidir o determinar la finalitat, el contingut, l'ús o els mitjans del tractament, és a dir, de prendre decisions sobre què fer i com tractar les dades personals des del moment en què aquestes es recullen fins a la seva destrucció.

En l'àmbit universitari, per tant, poden tenir aquesta consideració de responsable del tractament la universitat, l'òrgan, l'àrea, el servei, la unitat administrativa o, fins i tot, el membre de la comunitat universitària que tingui la capacitat de prendre les decisions sobre la finalitat i els mitjans d'aquest tractament.

Convé aclarir, en aquest punt, que l'entitat o les persones que duen a terme el disseny i desenvolupament de l'aplicació SITUA APP i de la plataforma web no tindrien consideració de responsables del tractament de dades, a la vista de la definició que ofereix l'article 4.7 de l'RGPD.

Aquest rol recauria en aquella persona, jurídica o física, que empri aquests mitjans (l'aplicació i la plataforma) per dur a terme l'estudi d'investigació de què es tracti i que, per tant, té la capacitat per decidir com i per a quins fins es recollirà i tractarà la informació personal. Per tant, podria ser la Universitat, un departament de la universitat o bé qualsevol investigador o grup d'investigadors de la Universitat qui ostenti la condició de responsable del tractament.

També convé aclarir que si l'entitat o les persones que duen a terme el disseny i desenvolupament de l'aplicació SITUA APP i de la plataforma web no formen part del responsable del tractament, en el cas que hagin d'accedir a dades personals seria necessària la formalització d'un encàrrec del tractament en els termes de l'article 28.3 de l'RGPD, atesa l'existència d'un tractament de dades per compte del responsable (article 4.8) RGPD).

D'acord amb les consideracions fetes fins ara en relació amb la consulta plantejada, es fan les següents,

Conclusions

Per la informació de què es disposa, el procés d'anonimització proposat no permetria garantir un tractament de dades anònimes en el si del Projecte a què es refereix la consulta.

Tot i això, podria plantejar-se l'opció d'articular el tractament de dades pretès sobre la base del consentiment explícit de les persones afectades (articles 6.1.a) i 9.2.a) RGPD), sens perjudici de l'adopció de les mesures escaients per garantir que aquest tractament s'adequa a l'RGPD, com ara, facilitar una informació detallada i clara al respecte, i aplicar les mesures a què s'ha fet referència per dificultar la reidentificació.

La condició de responsable del tractament de dades vinculat a la realització d'un projecte recaurà en aquella entitat o persona que decideixi o determini la finalitat, el contingut, l'ús o els mitjans d'aquest tractament.

Barcelona, 2 de juny de 2021