(Traducció no oficial. En cas de discrepàncies primarà la seva versió original).

Comunicat de la Comissió:
Guia sobre les apps de suport a la lluita contra la pandèmia de la COVID-19 en relació amb la protecció de dades.

1. INTRODUCCIÓ

1.1 Context

La pandèmia de la COVID-19 ha suposat un repte sense precedents tant per la Unió Europea com pels Estats Membres, els seus sistemes de sanitat, la seva forma de vida, els seus valors i la seva estabilitat econòmica. Les tecnologies digitals i les dades personals tenen un rol crucial en la lluita contra aquesta crisi. Aplicatius de mòbil instal·lats, normalment, als smartphones dels particulars, poden ajudar a les autoritats de salut nacionals i supranacionals a monitoritzar i contenir la pandèmia i són particularment rellevants en la fase de desconfinament, ja que permeten donar guies d'actuació a la població al mateix temps que donen suport als esforços de localització d'afectats i de contactes. En diferents estats, tant de la UE com tercers, les autoritats nacionals o regionals i els desenvolupadors han anunciat el llançament d'aquestes apps amb diferents funcions dirigides a donar suport a la lluita contra el virus.

El 8 d'abril de 2020, la Comissió adoptà una Recomanació enfocada a l'establiment d'un marc d'eines comú a la UE per a l'ús de la tecnologia i les dades per a sortir de la crisi de la COVID19, particularment en allò que feia referència a les aplicacions mòbils i l'ús de dades de mobilitat anonimitzades (en endavant, "la Recomanació"). L'objectiu de la Recomanació és, entre d'altres, desenvolupar un marc comú d'actuacions o d'eines per a l'ús d'aquests aplicatius, de coordinació supranacional, per tal d'incentivar el distanciament social als particulars, per controlar i limitar la propagació de la malaltia i per advertir i prevenir als interessats. La Recomanació estableix els principis generals que haurien de regir el desenvolupament d'aquestes eines i estableix que la Comissió publicaria una guia que faria referència a més a més a la protecció de dades i a la implicació d'aquestes en la privacitat.

Tal com hem dit, les aplicacions de mòbils poden ser claus en la fase de desconfinament arran de les seves funcionalitats de rastreig. Depenent de les característiques de les apps i de l'extensió de població que les utilitzin, les apps poden tenir un impacte clar en el diagnòstic, tractament i gestió de la COVID-19 dins i fora de l'àmbit hospitalari. En el moment d'aixecar les

mesures de contenció, el risc d'infecció creix en haver-hi més gent en contacte entre si. Aquests aplicatius poden ajudar a interrompre aquest procés infecciós i poden reduir el risc de rebrot significativament.

Un requisit important per al desenvolupament i establiment d'aquestes apps és la confiança dels particulars en aquestes. La gent necessita la certesa que el respecte als seus drets fonamentals està garantit i que les apps descrites aquí només s'empraran amb la finalitat específica de lluitar contra la pandèmia i no suposaran una eina de vigilància massiva; els interessats volen mantenir el control sobre les seves dades. Aquest ha de ser el fonament en què es basi l'efectivitat i l'adequació d'aquestes apps així que resulta essencial identificar solucions que siguin el menys intrusives possible, que respectin la normativa de protecció de dades i els drets dels particulars i que siguin efectives i adequades per lluitar contra la pandèmia. A més a més, un cop es consideri que la pandèmia està controlada, les apps haurien de deshabilitar-se automàticament.

Aquesta guia s'ha fet tenint en compte les aportacions fetes per part del Comitè Europeu de Protecció de Dades (EDPB) que en els dies vinents publicarà una guia sobre geolocalització i eines de rastreig en el context de la crisi sanitària de la COVID19.

1.2 Àmbit d'aplicació de la guia

Per tal d'assegurar una aproximació coherent en tota la UE i proveir als estats membres i desenvolupadors d'apps d'una guia sòlida, aquest document estableix les característiques i els requisits que els aplicatius haurien de garantir per tal de respectar la normativa europea de privacitat i protecció de dades sense privar que els estats membres puguin ampliar aquest marge de protecció en la seva normativa nacional.

Aquesta guia no és legalment vinculant, ja que només el TJUE pot interpretar la normativa europea, però busca donar suport en la creació de les aplicacions per lluitar contra la pandèmia que incloguin alguna o totes aquestes característiques:

- Apps que donin informació, recomanacions o alertes als particulars sobre la pandèmia;
- Apps d'autodiagnòstic;
- Apps que informin al particular de la seva proximitat amb una persona infectada per tal de donar-li instruccions relatives a si ha de confinar-se, on fer-se una prova, etc (rastreig de contactes); i/o
- Apps que informin o creïn un canal de comunicació entre pacients i doctors en el context d'un aïllament o en casos que es necessiti diagnòstics ulteriors (telemedicina).

D'acord amb la Directiva d'ePrivacitat, la imposició d'utilitzar una app com les descrites només es vàlid si existeix una norma específica, apropiada i proporcionada per a la protecció i consecució d'objectius específics que en reguli la utilització (art. 5). En el present cas, l'elevat nivell d'intrusisme d'aquestes apps i els reptes que aquestes plantegen, la Comissió considera

que cal dur a terme una anàlisi curosa de les mateixes abans d'optar pel seu establiment. Així, la Comissió recomana que aquestes apps siguin voluntàries la present guia no farà referència a les apps destinades a fer complir amb les obligacions de quarantena.

2. CONTRIBUCIÓ DE LES APPS EN LA LLUITA CONTRA LA COVID-19.

La funció d'autodiagnòstic és una eina per a les autoritats públiques sanitàries per tal de guiar als particulars en la necessitat de fer-se una prova de COVID-19, de donar informació sobre l'aïllament, sobre com evitar transmetre a tercers i sobre quan i com buscar assistència sanitària. A més a més pot ajudar als epidemiòlegs a comptabilitzar quins nivells de propagació de la pandèmia existeixen en un territori.

La funció de rastreig de contactes suposa una eina per tal d'identificar a persones que hagin estat en contacte amb una persona infectada de COVID19 i informar-los sobre quines mesures ha de dur a terme a continuació, ja sigui l'aïllament, realitzar una prova o informar sobre què fer en cas que apareguin símptomes. Aquesta funció és útil tant per als particulars com per a les autoritats, ja que pot ajudar enormement en la gestió del desconfinament. En coordinació amb els tests a la població, aquesta mesura pot ser extremadament beneficiosa per tal de contenir la pandèmia.

Ambdues funcions suposen una font de dades molt rellevants per a les autoritats sanitàries i faciliten la cessió d'aquestes dades a les autoritats nacionals epidemiològiques i al Centre Europeu de Prevenció i Control de Malalties (ECDC). Així, s'ajuda a entendre els patrons de transmissió que segueix el virus, i si es combina amb els tests a la població, permet estimar positivament el valor de símptomes respiratoris en una comunitat determinada i proporciona informació sobre la circulació del virus. Això sí, el grau de credibilitat d'aquestes estimacions deriva inexorablement del nivell de qualitat i credibilitat de les dades recollides.

Així, combinant aquestes apps amb estratègies de testar la població, les dues funcionalitats descrites poden proporcionar com hem dit dades sobre la circulació del virus i ajuden a valorar l'impacte de mesures com l'aïllament social i el confinament. Tal com es va establir a la Recomanació, per tal de fomentar la col·laboració transfronterera i per assegurar la detecció de contactes (particularment important en els casos de moviments entre països dels particulars) aquestes apps haurien de funcionar i en diferents estats membres. Quan una persona infectada estigui en contacte amb un usuari d'una app d'un estat diferent, la comunicació internacional de les dades d'aquella persona ha de fer-se, sempre que se'n limiti al màxim la casuística i sigui estrictament necessari. Sobre aquesta qüestió, tal com estableix la Recomanació, caldrà adoptar les mesures tècniques i els requeriments legals necessaris per a permetre aquesta cooperació internacional.

3 ELEMENTS PER A UN ÚS RESPONSABLE I ADEQUAT D'AQUESTES APPS.

Les funcions incloses en les apps poden tenir un impacte clar i intrusiu en diferents drets reconeguts per la Carta de Drets Fonamentals de la UE, com són la dignitat, el respecte per la vida privada i familiar, la protecció de dades, la llibertat de moviments, la no discriminació, la llibertat de dur a terme activitats econòmiques o el dret d'associació i reunió. En el que respecta a la privacitat i la protecció de dades, podem veure que l'impacte és encara més evident en tractar-se de funcions basades en la cessió de dades sensibles.

Els elements que es presenten a continuació busquen proveir a les autoritats d'eines per tal de limitar aquesta intrusivitat de les apps per tal de complir amb la normativa europea de protecció de dades i privacitat.

3.1 El responsable de tractament ha de ser una autoritat sanitària nacional (o entitats que duguin a terme tasques en el camp de la salut pública en base a l'interès públic).

La identificació de qui prendrà decisions sobre les dades tractades és crucial a l'hora d'establir qui és responsable que es compleixi amb les normes de protecció de dades i, particularment, és rellevant per tal de definir qui serà el responsable de complir amb el deure d'informació sobre quines dades es tractaran, de quins drets disposa, qui és el responsable en cas de bretxes de dades, etc.

Arran de la naturalesa de sensible de les dades compartides i la finalitat perseguida amb el tractament d'aquestes, la Comissió considera que les apps haurien de dissenyar-se de forma que les autoritats sanitàries en siguin els responsables. El responsable de tractament és l'encarregat de garantir el respecte amb el RGPD i la seva actuació haurà de regir-se conforme als principis descrits més endavant.

El fet que les autoritats sanitàries siguin els únics responsables de tractament d'aquestes dades permet que la població tingui més confiança en aquests aplicatius i conseqüentment que es compleixi més fàcilment amb el propòsit de protegir la salut pública.

3.2 El particular ha de mantenir el control sobre les seves dades.

Un factor determinant per a la confiança dels particulars en aquests aplicatius és demostrar que ells segueixen tenint el control sobre les seves dades personals. Per tal d'assegurar això, la Comissió considera que haurien de donar-se les següents garanties:

- La instal·lació de l'aplicatiu ha de ser voluntària i no ha de comportar conseqüències negatives per al particular que decideixi no instal·lar o no utilitzar-la.
- Les diferents funcions de l'app (ex. Informació, diagnòstic, rastreig de contactes, etc) no han d'entendre's com un bloc sinó que el particular ha de poder consentir l'ús de part o de totes les funcions d'aquesta.
- Si es fan servir o es recullen dades de proximitat (com ara geolocalització o sistemes basats en Bluetooth) aquestes han d'emmagatzemar-se al dispositiu del mateix interessat. Si aquestes dades han de compartir-se amb les autoritats de salut, el particular ha de consentir aquesta compartició i si es confirma que la persona d'interès està infectada;
- Les autoritats de salut han de proporcionar tota la informació necessària i rellevant sobre el tractament de dades que es durà a terme (dret d'informació del RGPD).
- El particular ha de poder exercir els drets reconeguts pel RGPD (particularment els de rectificació i supressió). Qualsevol restricció de drets feta en base al RGPD o a la directiva d'ePrivacy ha de justificar-se en base a la necessitat, legitimitat i proporcionalitat.
- Les apps han de desactivar-se automàticament a tot tardar quan la pandèmia es declari controlada, independentment de la desinstal·lació feta per l'usuari.

3.3 Bases legal del tractament.

3.3.1 Instal·lació d'apps i emmagatzematge d'informació al dispositiu del particular.

L'emmagatzematge de dades al dispositiu del particular i el consentiment a què es pugui accedir a les mateixes només es podrà dur a terme

1. si el particular ha consentit expressament a tal accés;
2. l'emmagatzematge o accés és estrictament necessari per al funcionament de l'app.

L'emmagatzematge d'informació al dispositiu del particular i permetre'n l'accés acostuma a ser el necessari perquè l'app funcioni. Ara bé, en el cas de rastreig de contactes requereix que s'emmagatzemin altres dades o que el mateix interessat n'aporti addicionals que no són necessàries per al funcionament de l'aplicatiu. Així doncs, les apps descrites en aquesta guia no podrien basar-se en la base legal descrita en el punt 2; fet que obliga a que la legitimació del tractament de dades descrit en aquesta guia passi exclusivament pel consentiment de l'interessat. Aquest consentiment haurà de ser lluir, específc, explícit i informat (d'acord amb el RGPD) i haurà d'expressar-se a través d'una acció afirmativa (eliminant-se així la possibilitat de construir tàcitament).

3.3.2 Base legal per al tractament fet per autoritats nacionals sanitàries

Les autoritats sanitàries dels estats membres tracten dades personals conforme a un imperatiu legal disposat en una norma de la UE o una pròpia de l'estat membre que determina com ha de

dur-se a terme el tractament i quines condicions en justifiquen la recollida (una norma legal que així ho estipuli o un interès general). Qualsevol normativa haurà d'establir les salvaguardes necessàries per a protegir els drets fonamentals dels particulars.

Les lleis de la UE o dels estats membres que existeixin amb anterioritat a l'esclat de la crisi de la COVID19 i aquelles que els estats membres estiguin aprovant per a lluitar contra la propagació d'epidèmies podrien emprar-se com a bases legals per al tractament de dades si recullen mesures que permetin la monitorització d'epidèmies i es compleix amb allò que disposa l'art. 6.3 del RGPD.

Arran de la naturalesa sensible de les dades tractades en aquest tipus d'apps, a més a més de la situació actual de la pandèmia, la legitimació d'aquests tractaments en base a normes legals ajudaria a mantenir un alt grau de certesa, ja que:

- Descriuria amb detall el tractament de dades de salut i especificaria clarament la finalitat del tractament,
- Identificaria clarament qui és el responsable del tractament
- Exclouria la possibilitat que es tractin dades per a finalitats diferents de les descrites en la llei, i
- Proveiria de salvaguardes específiques als particulars.

Malgrat això, el legislador nacional ha de tenir sempre en compte que la forma més eficient per a que els particulars confiïn en aquestes apps és optar per aplicatius que garanteixin que el particular manté el control sobre les seves dades i que els mateixos mantinguin la llibertat d'instal·lar o no aquests aplicatius o de compartir les dades o no amb les autoritats sanitàries sense que això comporti conseqüències adverses per als particulars.

3.4 Minimització de dades

Les dades derivades són aquelles produïdes pel mateix dispositiu o per les dades ja emmagatzemades als dispositius. Es protegeixen de la següent forma:

- Com a dades personals i d'acord amb la definició del RGPD. Les dades derivades de salut seran dades sensibles.
- Dades de localització: dades tractades per una xarxa electrònica de comunicacions o per un servei de comunicacions que indica la posició geogràfica d'un dispositiu. Es protegirà segons la directiva d'ePrivacy.
- Qualsevol informació emmagatzemada i a la que es tingui accés, es protegirà segons la directiva d'ePrivacy (art. 5.3).
- Les dades que no siguin personals, com per exemple aquelles que siguin anonimitzades i no es pugui desfer tal anonimització, no es protegiran pel RGPD.

La Comissió remarca que el principi de minimització de dades requereix que només es recullin i tractin aquelles dades que siguin adequades, rellevants i limitades a allò necessari per dur a terme la finalitat buscada. Així, es podran dur a terme informes per avaluar la necessarietat de recollir certes dades d'acord amb la finalitat perseguida.

La Comissió també vol remarcar que, per exemple, la funció de telemedicina o d'autodiagnòstic, no requereixen que l'app es vinculi als contactes del particular usuari de l'aplicatiu per a funcionar correctament.

Generar i tractar un volum inferior de dades personals suposa una clara limitació dels riscos inherents a la seguretat d'aquestes. Així, el compliment amb el principi de minimització de dades suposa una sèrie salvaguardes de seguretat.

Minimització de dades segons la funció:

- Apps informatives: les apps que tinguin una funció merament informativa no necessitaran tractar dades personals de salut dels particulars. Simplement, informarà els interessats sobre novetats. Per tal de complir amb les seves funcions no caldrà accedir a informació emmagatzemada al terminal de l'usuari i no es podran tractar més dades que les necessàries per informar.

- Apps d'autodiagnòstic i telemedicina: si l'app inclou una o aquestes dues funcions, es tractaran dades personals. Així, caldrà especificar un llistat de dades tractables en la norma legal que empari aquest tractament de dades per part de les autoritats sanitàries.
    - A més a més, les autoritats sanitàries podran requerir el número de telèfon de les persones que hagin emprat l'eina d'autodiagnòstic i hagin penjat els resultats. La informació emmagatzemada al dispositiu podrà processar-se només si és necessària per al funcionament de l'app.

- Apps de rastreig de contactes: la majoria d'infeccions per COVID19 es produeixen per partícules que viatgen a una distància limitada. Identificar tan ràpidament com es pugui a persones que hagin estat en proximitat amb infectats és un factor clau per interrompre la propagació de la cadena d'infecció. Determinar la proximitat és una funció necessària per determinar el temps i la distància dels contactes i hauria d'emprar-se amb una finalitat epidemiològica per tal d'evitar rebrots en fases de desconfinament. Les dades de proximitat doncs són necessàries per a aquesta funció. Tecnologies com el Bluetooth Low Energy (BLE) són precises i adients per a aquesta funció (més que tecnologies de geolocalització) perquè evita la possibilitat de rastrejar a l'usuari. La Comissió recomana doncs l'ús de BLE per a determinar la proximitat entre contactes.

Independentment de les mesures tècniques emprades per determinar la proximitat, el que no sembla necessari és emmagatzemar el moment exacte en què s'ha dut a terme el contacte. Ara bé, si que seria interessant emmagatzemar el dia en què es va produir el contacte per tal d'estimar si la persona ha desenvolupat símptomes o no i per enviar-li o no un missatge recomanant l'aïllament o no. Aquestes dades però només han de tractar-se en cas que hi hagi risc real: per la proximitat de contacte i la durada d'aquest. Per tal de determinar quan informar els possibles contactes hi ha dues aproximacions: o bé quan una persona comuniqui ha donat positiu, el sistema alerti a les persones que puguin ser contactes o bé quan es doni la situació de proximitat amb una persona infectada una base de dades gestionada per l'autoritat responsable emetrà una alerta i s'informarà els usuaris de l'app. En qualsevol cas l'alerta haurà de ser anonimitzada i no es podrà identificar o fer identificable a la persona infectada.

- Geolocalització: Les dades de geolocalització no són necessàries per a la funció de rastreig de contactes, ja que la seva finalitat no és la de monitoritzar els moviments dels particulars. A més a més, el tractament de dades de localització en aquest context seria difícilment justificable a la llum del principi de minimització de dades i suposaria una ingerència massa elevada a la privacitat de particulars. No es recomana doncs el seu ús per a aquesta funció.

3.5 Limitació de la revelació o l'accés a les dades:

3.5.1 Apps de funció informativa:

No s'emmagatzemarà informació ni es podrà accedir al terminal on estigui instal·lada l'aplicació. No es podrà compartir les dades amb les autoritats sanitàries més enllà d'aquella informació necessària per al funcionament de l'app. Com que aquesta funció es fa en base a la voluntat de comunicar, les autoritats sanitàries no han de tenir accés a altres dades.

3.5.2 Apps d'autodiagnòstic o de telemedicina:

Aquestes apps són útils per als estats membres per determinar qui hauria de sotmetre's a proves, proveir d'informació sobre confinament i com organitzar l'accés a la sanitat per part de grups de risc. Aquesta funció també pot ajudar a entendre el nivell d'extensió de la pandèmia entre la població. Així, es pot determinar que les autoritats sanitàries i epidemiològiques puguin tenir accés a la informació proporcionada pels pacients. L'ECDC podrà rebre dades agregades de les autoritats dels estats membres per a l'estudi de l'epidèmia.

Si s'opta per permetre una via de contacte alternativa a l'app amb les autoritats sanitàries, es podrà recollir també altres dades com pot ser el número de telèfon.

3.5.3 Apps de rastreig de contactes:

- Dades de les persones infectades: Les apps generen de forma aleatòria identificadors temporals de telèfons que estiguin en contacte amb l'usuari de l'app. Una opció pot ser que l'emmagatzematge d'aquests identificadors es faci al dispositiu de l'usuari o que es faci a través de bases de dades gestionades per les autoritats sanitàries. La primera opció casa millor amb el principi de minimització de dades, ja que les autoritats sanitàries només haurien de tenir accés a les dades de proximitat per tal de contactar amb persones amb risc d'infecció. Aquestes dades a més a més, només seran accessibles a les autoritats quan la persona infectada decideixi compartir-les amb elles. La persona infectada no pot ser informada de la identitat de les persones a qui potencialment hagi pogut contagiar o que hagin rebut una alerta.

- Dades dels contactes: la identitat de les persones infectades no es podrà revelar en cap cas als contactes, ja que és suficient comunicar l'existència o no del contacte amb una persona infectada en els últims 16 dies. Les dades dels contactes no han d'emmagatzemar-se i per tant, no poden cedir-se. Per tal de rastrejar aquests contactes d'una persona usuària de l'app que hagi comunicat el seu estat de positiu, les autoritats sanitàries seran informades d'aquest estatuts i de l'identificador de la persona per tal de comunicar-ho a les persones que hagin pogut estar en contacte amb la persona infectada des de 48h abans de la notificació fins a 14 dies abans.

L'ECDC podrà rebre dades agregades de les autoritats dels estats membres per a l'estudi de l'epidèmia.

3.6 Finalitat específica

La base legal d'una llei europea o nacional ha de delimitar la finalitat del tractament i aquest ha de ser indubtable, específic i limitat a aquelles dades necessàries per a complir amb l'objectiu desitjat. La finalitat específica dependrà de les funcionalitats de l'app i no seran exclusives: una mateixa app podrà complir amb diferents finalitats sempre que totes elles s'especifiquin a la normativa. Per tal de donar als particulars un control ple i efectiu de les seves dades, la Comissió recomana no barrejar finalitats molt diferents en un sol aplicatiu i en cas de fer-ho, que l'interessat tingui la capacitat de consentir la recollida de dades per cadascuna o cap de les finalitats establertes per l'aplicatiu.

La comissió vol desincentivar clarament l'ús de les dades recollides per aquestes finalitats per objectius diferents de la lluita contra la COVID19. Si es volen emprar aquestes dades per a la recerca científica o estadística, aquests objectius hauran d'incloure's en el llistat proporcionat per la normativa que empari aquests tractaments de dades.

- Apps informatives: la finalitat és informar de fets rellevants per part de les autoritats sanitàries en el context de la crisi.
- Apps de telemedicina i autodiagnòstic: la finalitat pot ser la recollida de dades relatives al número potencial de persones infectades o de risc i la comunicació entre aquests i els professionals mèdics. Aquestes dues finalitats haurien d'especificar-se i desenvolupar-se en la normativa que regeixi aquesta app.
- Apps de rastreig de contactes: la mera indicació de *"prevenir més infeccions de COVID-19*" no serà un criteri suficientment específic per determinar la finalitat. En aquest cas la comissió recomana especificar totes les finalitats futuribles o previsibles que es pugui donar a aquestes dades (per exemple "*retenció dels contactes de persones que utilitzin l'app i que poden haver estat en contacte amb la infecció del COVID19 per tal d'advertir a aquestes persones que podrien haver estat potencialment infectades*").

3.7 Limitar l'emmagatzematge de dades

El principi de limitar l'emmagatzematge de les dades en el temps implica que les dades no hauran de conservar-se més enllà del temps necessari. Aquest temps haurà de limitar-se per criteris de rellevància mèdica i de capacitat de dur a terme actuacions administratives.

- Apps informatives: Si es recullen dades perquè l'app funcioni, aquestes han de ser eliminades immediatament ja que no hi ha justificació a la seva conservació.
- Apps de telemedicina i autodiagnòstic: les autoritats sanitàries hauran d'eliminar les dades en el termini màxim d'un mes o quan la persona doni negatiu en un test. Si s'anonimitzen aquestes dades, les autoritats sanitàries podran conservar-les més temps per finalitats de recerca.
- Apps de rastreig de contactes: les dades de proximitat hauran d'eliminar-se immediatament quan ja no serveixin per a la finalitat d'informar els particulars (un mes màxim d'un mes (incubació + marge) o després que la persona hagi donat negatiu en un test). Les autoritats sanitàries podran conservar dades de proximitat per a finalitats de recerca si s'anonimitzen.

Les dades haurien d'emmagatzemar-se als dispositius dels usuaris i només aquelles dades que es comuniquin per part dels interessats i que siguin necessàries per complir amb la finalitat perseguida es podran emmagatzemar en un servidor disponible a les autoritats sanitàries.

3.8 Seguretat de les dades:

La Comissió recomana que les dades es guardin al terminal dels usuaris en una forma encriptada. En el cas que les dades es guardin en un servidor central, l'accés, inclòs l'accés

administratiu, haurà de registrar-se i identificar-se.

Les dades de proximitat només haurien de generar-se i guardar-se al terminar del particular en format encriptat i pseudoanònim; i per tal d'assegurar que tercers no puguin accedir-hi, l'activació del BLE ha de ser possible sense haver d'activar serveis de localització. Durant la recollida de dades mitjançant BLE és preferible que es generi una ID de l'usuari que sigui temporal i que es generi aleatòriament que no pas la ID del dispositiu. Aquesta mesura permet una capa addicional de protecció davant possibles filtracions de dades.

La Comissió recomana que el codi font de l'app sigui accessible al públic i revisable. Mesures addicionals per protegir les dades com ara l'eliminació automàtica o l'anonimització de les dades després d'un temps determinat són també recomanables. En general, el nivell de seguretat hauria d'adaptar-se a la naturalesa sensible de les dades recollides.

Qualsevol comunicació de dades haurà de ser encriptada. Quan la legislació nacional prevegi que les dades podran emprar-se per a una finalitat de recerca científica, haurà de pseudoanonimitzar-se.

3.9 Garantir la certesa o exactitud de les dades

Assegurar l'exactitud de les dades personals tractades no és només un prerequisit de l'eficiència de l'app però també un requisit de la normativa de protecció de dades. En aquest context, assegurar la certesa de la informació sobre si un contacte ha estat a prop d'una persona infectada o no és essencial per tal de minimitzar el risc de falsos positius. Això hauria de tenir-se particularment en compte quan es tractin d'escenaris en què dos usuaris de l'app entrin en contacte al carrer o als transports públics. Sembla improbable que l'ús de dades de localització basades en les xarxes mòbils siguin suficientment exactes. Per això es recomana confiar més en tecnologies que permetin una concreció més clara com les BLE.

3.10 Involucrar les autoritats de protecció de dades

Les autoritats de protecció de dades han d'estar plenament involucrades i han de ser consultades en el context del desenvolupament d'aplicatius i aquest desenvolupament i el posterior funcionament han de ser revisats per aquestes. Arran del tractament a gran escala de dades sensibles com les de salut, la Comissió vol fer menció a l'art. 35 del RGPD sobre avaluacions d'impacte.