

DIPUTACIÓ DE  
VALÈNCIA



*Protecció de Dades i Seguretat de la Informació*



# Butlletí protecció de dades

Butlletí del Departament de protecció de dades i Seguretat  
de la Informació de la Diputació Provincial de València

Butlletí N.º 14 | Agost 2021

**UTILITZACIÓ D'APPS I PRINCIPALS RISCOS PER ALS CIUTADANS**



## Í N D E X



|                                                | Pàg.     |
|------------------------------------------------|----------|
| <b>Introducció.....</b>                        | <b>1</b> |
| • Geolocalització                              | 2        |
| • Apps d'informació voluntària de contagiats   | 3        |
| • Apps de seguiment de contactes per bluetooth | 4        |
| • Passaports d'immunitat                       | 5        |
| • Recomanacions a tindre en compte             | 6        |
| <b>Material complementari .....</b>            | <b>7</b> |
| <b>Notícies d'actualitat .....</b>             | <b>7</b> |



Us convidem a traslladar-nos aquelles temàtiques que resulten del vostre interès per als pròxims butlletins informatius. Aquestes peticions hauran de dirigir-se a:

Diputació de València

Dpt. de Protecció de Dades i  
Seguretat de la Informació

Pl. de Manises, 4 46003 Valencia

email: [dpdsi@dival.es](mailto:dpdsi@dival.es)

### SUSCRIPCIONS

Si desitges subscriure's al nostre  
Butlletí informatiu accedeix al  
següent [enllaç](#)



## INTRODUCCIÓ

La tecnologia està canviant la manera de treballar de les Administracions Públiques (d'ara en avant, AA.PP.) i la seua relació amb els ciutadans buscant millorar temps, facilitant l'accessibilitat i simplificant tràmits, no obstant això, existeix un risc específic associat al tractament de dades personals per les AA.PP. en fer ús de tecnologies emergents. En aquest sentit, i responent a la realitat actual cal tindre en compte algunes de les tecnologies en la lluita contra la COVID-19, dels beneficis que prometen enfront de la pandèmia i dels costos en la privacitat dels individus.

Cal tindre en compte que abans d'implementar solucions tecnològiques per a enfrontar-nos a la COVID-19 és imprescindible que aquestes es troben integrades en el marc de mesures jurídiques i organitzatives realistes, eficaces, basades en criteris científics, legítimes i proporcionals. El benefici haurà de mesurar-se en funció d'una menor propagació de la infecció en termes globals, amb la possibilitat de recuperar la llibertat d'acció, i una protecció de la salut dels individus. Les dades de salut tenen un alt valor, per la qual cosa cal previndre que, aprofitant la incertesa que provoca una situació d'emergència, es produïsquen abusos per part de tercers que conduïsquen a situacions de pèrdua de llibertats.

En aquest butlletí es realitzarà una breu anàlisi, amb propòsit didàctic d'algunes de les tecnologies en la lluita contra la COVID-19, dels beneficis que prometen aportar enfront de la pandèmia i dels costos en la privacitat que ens poden implicar, en particular:

- Geolocalització mitjançant la informació recollida pels operadors de telecomunicacions.
- Apps de recollida d'informació de contagiats
- Apps de seguiment de contactes
- Passaports digitals d'immunitat





## GEOLOCALITZACIÓ

Aquesta tècnica consisteix en el fet que els operadors de telefonia mòbil proporcionen informació anonimitzada de la ubicació dels usuaris en les cel·les de telefonia que defineixen les seues antenes. Les operadores recullen habitualment dades de posició dels seus abonats.

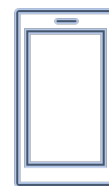
Amb aquesta informació, que és necessària per a prestar el servei, una operadora és capaç d'estimar quins números de telèfon hi ha en cada cel·la en un determinat moment, i fins i tot donar una ubicació aproximada de qualsevol telèfon mòbil actiu en una cel·la.



Aquesta informació, sense anonimitzar, pot ser demandada per les Forces i Cossos de Seguretat sempre mitjançant una ordre judicial. D'altra banda, la seua utilització anonimitzada va ser utilitzada per l'Institut Nacional d'Estadística per a estudis de mobilitat. Durant la gestió de la crisi de la COVID-19, el Govern i la Comissió Europea han demanat que les operadores proporcionen aquest tipus d'informació anonimitzada per a veure els moviments de població.

**"...DURANT LA GESTIÓ DE LA CRISI DE LA COVID-19, EL GOVERN I LA COMISSIÓ EUROPEA HAN DEMANAT QUE LES OPERADORES PROPORCIONEN AQUEST TIPUS D'INFORMACIÓ ANONIMITZADA PER A VEURE ELS MOVIMENTS DE POBLACIÓ".**

### REPRESENTEN AQUESTES DADES EN LA CRISI DE LA PANDÈMIA UNA AMENÇA A LA PRIVACITAT?



Amb una gestió acurada, l'accés apropiadament anonimitzat a aquesta informació no hauria de representar una amenaça major que la que ja representaven abans. És a dir, sempre hi ha la possibilitat d'una anonimització incompleta, una subcontractació poc rigorosa o un ciberatac que posara en mans d'un tercer la localització dels mòbils dels usuaris, encara que aquest risc ja existia abans de la pandèmia.

### REPRESENTEN AQUESTES DADES EN LA CRISI DE LA PANDÈMIA UN BENEFICI IMPORTANT?

Conèixer els patrons de mobilitat de la població, veure on es desplacen les persones quan treballen o els caps de setmana, pot ser beneficiós per a una administració en qualsevol temps.

Ara bé, cal avaluar de manera contínua la seua utilitat enfront dels escenaris canviants d'una situació de confinament global o parcial. Una derivada que s'ha apuntat és la possibilitat que s'usaren dades anonimitzades de geolocalització per a observar moviments globals, però amb la possibilitat que la policia demanara la reidentificació en determinats casos conforme als criteris establits per les autoritats sanitàries per a garantir el control de l'epidèmia.



## APPS D'INFORMACIÓ VOLUNTÀRIA DE CONTAGIS

En aquesta categoria estarien algunes aplicacions mòbils que van sorgir de forma quasi instantània, en alguns casos d'iniciatives ciutadanes, i que pretenien fer els seus propis



mapes i estadístiques de propagació de la COVID-19 a partir de dades proporcionades voluntàriament per nosaltres com a usuaris. En un entorn molt obert i transparent s'apel·la a la col·laboració desinteressada per a

descarregar-se aquestes aplicacions i pujar dades de localització i dades de la seua possible infecció, contribuint així a fer mapes i quadres de comandament amb una informació que teòricament no està filtrada per les autoritats

### REPRESENTEN AQUESTES APLICACIONS EN LA CRISI DE LA PANDÈMIA UNA AMENÇA A LA PRIVACITAT?

Aquestes Apps podrien ser-ho si els fins que declaren no són tan altruistes com els que promouen o les preses condueixen a desenvolupaments sense garanties per a la privacitat. No oblidem que el que s'està cedint als servidors en Internet són dades de salut i localitzacions precises.

Si la quantitat i qualitat d'aquestes dades fora la suficient, gràcies a un nombre significatiu d'usuaris, es disposarien de conclusions com a barris amb alt nivell d'infecció, amb l'estigma social que això pot implicar. És a dir, és necessari disposar d'una mostra significativa i que ningú, de manera maliciosa, estiga proporcionant informació falsa o manipulada per a beneficiar o perjudicar el conjunt.

**“...AQUESTES APPS PODRIEN SER-HO SI ELS FINS QUE DECLAREN NO SÓN TAN ALTRUISTES COM ELS QUE PROMOUEN O LES PRESSES CONDUEIXEN A DESENVOLUPAMENTS SENSE GARANTIES PER A LA PRIVACITAT. NO OBLIDEM QUE EL QUE S'ESTÀ CEDINT ALS SERVIDORS EN INTERNET SÓN DADES DE SALUT I LOCALITZACIONS PRECISES”.**



### REPRESENTEN AQUESTES DADES EN LA CRISI DE LA PANDÈMIA UN BENEFICI IMPORTANT?

Des del principi de l'ús voluntari i descontrolat no és possible saber mai la fiabilitat de la informació que contenen, per la qual cosa poden contribuir a divulgar notícies errònies i resultar un perjudici.



## APPS DE SEGUIMENT DE CONTACTES PER BLUETOOTH

Aquest tipus d'aplicacions usa la tecnologia bluetooth dels telèfons mòbils que permet la connexió amb aparells pròxims com a auriculars, altaveus o rellotges.

En aquest cas, les apps utilitzen el bluetooth per a enviar la “targeta” corresponent a l'usuari amb els mòbils que es va trobant en el seu camí, i alhora recol·lecta les “targetes” d'aqueixos mateixos mòbils. Cada targeta no té una identificació real de l'usuari, sinó un sobrenom de la seua identitat. D'aquesta manera cada mòbil té una col·lecció anònima de “targetes” de la gent amb la qual ha estat en el seu treball, en el transport o en el seu oci. Si un determinat usuari esbrina que està infectat, té a la seua mà la possibilitat de “declarar-ho” a través de l'app a un servidor central. En aqueix moment, se suposa que aquelles persones que amb les quals va estar en contacte en els últims dies, rebran un avís perquè valoren quines accions prendre, com podria ser confinar-se, contactar amb els seus serveis sanitaris o realitzar-se una prova.

Han sorgit diverses estratègies per a implementar aquesta tecnologia, existeixen opcions en les quals aqueix control descansa en el propi usuari (descentralitzades), i altres en un control centralitzat, suposadament per una autoritat.



### REPRESENTEN AQUESTES APLICACIONS EN LA CRISI DE LA PANDÈMIA UNA AMENÇA A LA PRIVACITAT?

Les principals amenaces a la privacitat d'aquesta mena de solucions venen de la realització de mapes de relacions entre persones, reidentificació per localització implícita, de la fragilitat dels protocols a l'hora construir “targetes” quasi anònimes, i de dispersar els senyals dels contagis de manera

que no s'identifique en cap cas la identitat dels contagiats. Ha de tindre's en compte que el tractament de la informació no sols afecta a l'usuari de l'aplicació sinó també la de tots els tercers amb els quals ha estat en contacte, per la qual cosa aquest tractament ha de complir els principis de protecció de dades. La possibilitat que, a causa de l'acumulació de les dades de forma centralitzada, es produïra un abús en una empresa poc ètica, s'ampliaren els propòsits del tractament o s'anara víctima d'un ciberatac constitueix una altra de les majors amenaces d'aquesta mena de solucions.

### REPRESENTEN AQUESTES DADES EN LA CRISI DE LA PANDÈMIA UN BENEFICI IMPORTANT?

Cal posar de manifest que les solucions tècniques no es poden considerar de forma aïllada. En primer lloc, és necessària la implicació d'un elevat nombre d'usuaris, alguns estudis parlen d'almenys el 60% d'una població. D'altra banda, depén del fet que es realitze una declaració responsable de la situació personal d'infecció, preferiblement supervisada per un professional per a evitar estratègies de desinformació. Finalment, és necessari disposar d'accés a test, no sols per a tots els usuaris, sinó per a poder actualitzar la informació periòdicament i perquè aquells que siguen notificats d'haver estat en contacte amb un infectat puguin realitzar la prova amb promptitud.

En la situació actual d'Espanya i d'altres països europeus, no sembla que aquestes aplicacions vagin a tindre èxit a curt termini com una estratègia global de lluita contra la pandèmia, més encara si tenim en compte el creixement de persones vacunades. Si pensem en un escenari futur, quan la malaltia estiga molt més controlada, sí que podria tindre el seu èxit en col·lectius concrets com a estudiants d'un centre, professionals d'una companyia o grups d'amics que decideixen voluntàriament usar l'aplicació.



## PASSAPORTS D'IMMUNITAT

Han començat a considerar-se l'ús d'Apps equivalents al que seria un passaport o salconduit en paper, mostrant un codi de colors o un codi QR, perquè un vigilant o un sistema de control d'accés puga deixar passar o no al portador, com podrien ser les targetes d'embarcament dels vols.

### REPRESENTEN AQUESTES APLICACIONS EN LA CRISI DE LA PANDÈMIA UNA AMENAÇA A LA PRIVACITAT?

Aquestes aplicacions estan valent-se d'un document d'identitat en el mòbil, amb el risc afegit d'incloure i mostrar una dada de salut, i incloent els riscos d'aquests sistemes: accés a les mans de ciberdelinqüents, encreuament amb altres dades com la localització, incorporació de metadades, o simplement no estar a l'abast de moltes persones que no poden usar telèfons intel·ligents. A diferència d'una targeta d'embarcament, les proves per a determinar si una persona està patint o ha superat la malaltia haurien de ser presencials, i el personal podria proporcionar a l'usuari un certificat o qualsevol suport de baixa tecnologia perquè el mostrara quan li fora requerit. Un sistema d'identitat mòbil només pot tindre avantatges quan l'alta es pot fer a distància o si la informació que gestiona canvia ràpidament.

### REPRESENTEN AQUESTES APLICACIONS EN LA CRISI DE LA PANDÈMIA UN BENEFICI IMPORTANT?

El passaport d'immunitat incorpora una dada sensible, com és qualsevol dada de salut, però al qual també se li ha donat la missió de servir com a salconduit d'accés. Un ús ben gestionat d'Apps per a certificacions o registres de salut, que els mantingueren actualitzats, assegurances i interoperables tindrà una certa utilitat en àmbits concrets sempre que l'accés a aquesta informació siga realitzat per personal vinculat al compliment de les finalitats relacionades amb polítiques públiques per al control de la pandèmia. No obstant això, com en totes les aplicacions que requereixen l'ús de telèfons intel·ligents i l'evidència d'una prova fiable d'infecció o d'anticossos, s'està lluny d'aconseguir a una totalitat de la població. Cal no oblidar, que no sols s'està recorrent a l'ús d'aquestes Apps, sinó també a l'ús del paper, on siga més accessible i menys invasiu per a la privacitat que l'ús de les tecnologies.

**"...UN ÚS BEN GESTIONAT D'APPS PER A CERTIFICACIONS O REGISTRES DE SALUT, QUE ELS MANTINGUERA ACTUALITZATS, ASSEGURANCES I INTEROPERABLES TINDRÀ UNA CERTA UTILITAT EN ÀMBITS CONCRETS SEMPRE QUE L'ACCÉS A AQUESTA INFORMACIÓ SIGA REALITZAT PER PERSONAL VINCULAT AL COMPLIMENT DE LES FINALITATS RELACIONADES AMB POLÍTIQUES PÚBLIQUES PER AL CONTROL DE LA PANDÈMIA. NO OBTANT AIXÒ, COM EN TOTES LES APLICACIONS QUE REQUEREIXEN L'ÚS DE TELÈFONS INTEL·LIGENTS I L'EVIDÈNCIA D'UNA PROVA FIABLE D'INFECCIÓ O D'ANTICOSSOS, S'ESTÀ LLUNY D'ACONSEGUIR A UNA TOTALITAT DE LA POBLACIÓ."**





## RECOMANACIONS A TINDRE EN COMPTE

En cas que es decidisca optar pel seu ús, s'haurien d'evitar els riscos anteriorment assenyalats, i és important per a això tindre en compte les següents recomanacions;

### QUÈ PODEN FER ELS USUARIS PER A EVITAR ELS RISCOS?



La finalitat ha d'estar clarament definida i ha de limitar-se a la gestió de mesures de distància social, control de vacunats o de contagis, com ara el control d'aforament o el control de distància.



Els tractaments que es proposen han de ser realment efectius en relació amb la finalitat i no poden generar falses expectatives de seguretat d'acord amb el principi de lleialtat del tractament. Han de quedar clares les finalitats concretes que es persegueixen, no mesclant funcionalitats com a fidelització, publicitat o xarxes socials.



La implementació de tractaments basats en Apps haurà de fonamentar-se en una anàlisi de necessitat i proporcionalitat que determine tant la utilització de l'App com el conjunt de dades mínim necessari per a aconseguir els fins que es persegueixen. En particular, la identitat de l'usuari o el seu seguiment, inclòs l'ús d'identificadors únics de qualsevol tipus o aquells procedents del bluetooth, només podrà tractar-se si són estrictament necessaris per a la finalitat de l'App, tal com s'ha abordat anteriorment en el butlletí.



No s'hauran de tractar categories especials de dades, en particular dades de salut, tenint en compte la finalitat perseguida i la anonimització d'aquests, i, en el seu cas, els estrictament necessaris per a gestionar els espais reservats a persones amb discapacitat.



L'ús d'una App ha de ser de caràcter voluntari, basat en el consentiment per al tractament de les dades personals necessàries per a cadascuna de les funcionalitats que es persegueixen. El tractament haurà d'estar basat en un consentiment lliure, informat i específic.



El tractament de dades personals de menors de 14 anys per aquesta mena d'Apps ha de ser consentit pels seus pares o tutors.





## MATERIAL COMPLEMENTARI

- L'AEPD publica unes directrius orientades a aplicacions mòbils educatives i d'activitat física, benestar i salut. Consulta [aquest enllaç](#).
- L'AEPD publica un informe sobre els tractaments de dades en relació amb el COVID-19. Consulta el document en [aquest enllaç](#).
- L'AEPD elabora unes recomanacions per al desplegament d'aplicacions mòbils en l'accés a espais públics. Consulta les recomanacions en [aquest enllaç](#).
- L'AEPD elabora una guia de privacitat i seguretat en Internet. Consulta [aquest enllaç](#) per a veure la guia.
- L'AEPD va elaborar una Nota Tècnica sobre el deure d'informar i altres mesures de responsabilitat proactiva en Apps per a dispositius mòbils. Consulta les recomanacions en [aquest enllaç](#).

## NOTÍCIES

- **La companyia de distribució Mercadona abonarà 2,5 milions d'euros de sanció proposada per l'Agència Espanyola de Protecció de Dades (AEPD) com a penalització per un projecte pilot que la companyia va testar en algunes botigues i que permetia detectar persones amb ordre d'allunyament dels seus establiments.** Així Mercadona anuncia en un comunicat, que "ha decidit donar per finalitzat el procediment obert per l'AEPD en relació amb el projecte pilot que va ser testat durant diversos mesos en 48 de les 1.640 botigues de les quals disposa la companyia", vistes la "indefinició i dubtes legals sobre el sistema de detecció anticipada que la companyia va implantar a manera de prova pilot". Consulta l'article en [aquest enllaç](#).
- **L'AEPD publica una nova guia per a gestionar el risc dels tractaments de dades personals i realitzar avaluacions d'impacte.** L'Agència Espanyola de Protecció de Dades (AEPD) ha presentat hui la guia '[Gestió del risc i avaluació d'impacte en tractaments de dades personals](#)', un document que incorpora l'experiència acumulada en l'aplicació de la gestió del risc en l'àmbit de la protecció de dades des de l'aplicació del Reglament General de Protecció de Dades (RGPD) i afig les interpretacions de l'AEPD, el Comité Europeu de Protecció de Dades i el Supervisor Europeu de Protecció de Dades. El document, **dirigit a persones responsables, encarregades de tractaments i persones delegades de protecció de dades (DPD)**, ofereix una visió unificada de la gestió de riscos i de les avaluacions d'impacte en protecció de dades, i facilita la integració de la gestió de riscos en els processos de gestió i governança de les entitats. Consulta l'article en [aquest enllaç](#).