EL USO DE LAS TECNOLOGÍAS EN LA LUCHA CONTRA EL COVID19. UN ANÁLISIS DE COSTES Y BENEFICIOS

Mayo de 2020

C/ Jorge Juan 6
28001 - Madrid

http://www.aepd.es
https://sedeagpd.gob.es

I. CONTENIDO

II. INTRODUCCIÓN

Antes de implementar soluciones tecnológicas para enfrentarnos a la COVID-19 es imprescindible que éstas se encuentren integradas en el marco de una estrategia de medidas jurídicas y organizativas realistas, eficaces, basadas en criterios científicos, legítimas y proporcionales.

La proporcionalidad se establece mediante un análisis del coste y el beneficio para la sociedad y los derechos y libertades del individuo. El beneficio tendrá que medirse en función de una menor propagación de la infección en términos globales, con la posibilidad de recuperar la libertad de acción, y una protección de la salud de los individuos.

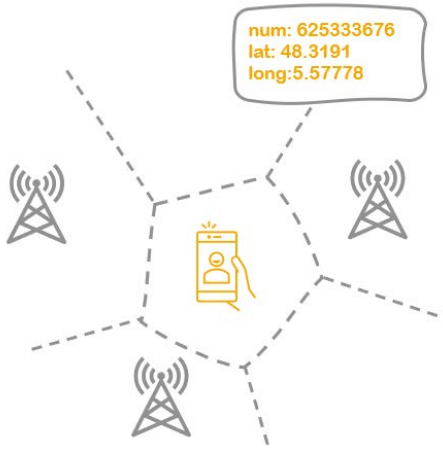
Los datos de salud tienen un alto valor, por lo que hay que prevenir que, aprovechando la incertidumbre que provoca una situación de emergencia, se produzcan abusos por parte de terceros que conduzcan a situaciones de pérdida de libertades, discriminación u otros daños en la situación personal de los ciudadanos.

En este documento se va a realizar un breve análisis, con propósito didáctico y sin pretender ser exhaustivos en su desarrollo, de algunas de las tecnologías en la lucha contra la COVID-19, de los beneficios que prometen aportar en la lucha frente a la pandemia y de los costes en la privacidad de los individuos que pueden acarrear, en particular:

- Geolocalización mediante la información recogida por los operadores de telecomunicaciones
- Geolocalización en redes sociales
- Apps, webs y chatbots para auto-test o cita previa
- Apps de recogida de información de contagiados
- Apss de seguimiento de contactos
- Pasaportes digitales de inmunidad
- Cámaras infrarrojas

III. GEOLOCALIZACIÓN DE LOS MÓVILES POR LOS OPERADORES DE TELECOMUNICACIONES

Esta técnica consiste en que los operadores de telefonía móvil proporcionen información anonimizada de la ubicación de sus usuarios en las celdas de telefonía que definen sus antenas. Las operadoras recogen habitualmente datos de posición de sus abonados, que calculan en función de la fuerza con que les llegan las señales de cada móvil a las distintas antenas de una zona. Con esta información, que es necesaria para prestar el servicio, una operadora es capaz de estimar qué números de teléfono hay en cada celda en un determinado momento, e incluso dar una ubicación aproximada de cualquier teléfono móvil activo en una celda. Esta información, sin anonimizar, puede ser demandada por las Fuerzas y Cuerpos de Seguridad siempre mediando una orden judicial. Por otro lado, su utilización anonimizada fue utilizada por el Instituto Nacional de Estadística[1] para estudios de movilidad. Durante la gestión de la crisis de la COVID-19, el Gobierno[2] y la Comisión Europea[3] han pedido que las operadoras proporcionen este tipo de información anonimizada para ver los movimientos de población.



¿REPRESENTAN ESTOS DATOS EN LA CRISIS DE LA PANDEMIA UNA AMENAZA A LA PRIVACIDAD?

Con una gestión cuidadosa, el acceso apropiadamente anonimizado a dicha información no debería de representar una amenaza mayor que la que ya representaban antes. Es decir, siempre cabe la posibilidad de una anonimización incompleta, una subcontratación poco rigurosa o un ciberataque que pusiera en manos de un tercero la localización de los móviles de los usuarios, aunque este riesgo ya existía antes de la pandemia. Por hacer un uso mayor de estos datos anonimizados, puede haber un riesgo mayor, pero no exponencialmente mayor.

---

1 https://www.ine.es/ss/Satellite?L=es_ES&c=INEmasNoticia_C&cid=1259952394212&idp=1254736092060&pagename=masINE%2FmasLayout El INE realiza un estudio piloto sobre movilidad a partir de datos agregados de telefonía móvil

2 https://www.boe.es/boe/dias/2020/03/28/pdfs/BOE-A-2020-4162.pdf . Orden SND/297/2020, de 27 de marzo

3 https://www.politico.com/news/2020/03/24/europe-mobile-data-coronavirus-146074 European Commission tells carriers to hand over mobile data in coronavirus fight

¿REPRESENTAN ESTOS DATOS EN LA CRISIS DE LA PANDEMIA UN BENEFICIO IMPORTANTE?

Conocer los patrones de movilidad de la población, ver dónde se desplazan las personas cuando trabajan o los fines de semana, puede ser beneficioso para una administración en cualquier tiempo. Pensemos que las infraestructuras, la sanidad o la policía son elementos que se podrían dimensionar dinámicamente con un buen modelo de movilidad. Pensemos, por ejemplo, en cómo se redimensionan estos factores cuando se produce un evento como un partido de fútbol o una manifestación. Ahora bien, hay que evaluar de forma continua su utilidad frente a los escenarios cambiantes de confinamiento global o parcial.

Una derivada que se ha apuntado es la posibilidad de que se usaran datos anonimizados de geolocalización para observar movimientos globales, pero con la posibilidad de que la policía pidiera la reidentificación en determinados casos conforme a los criterios establecidos por las autoridades sanitarias para garantizar el control de la epidemia.

IV. GEOLOCALIZACIÓN DE LOS MÓVILES A PARTIR DE REDES SOCIALES

La geolocalización de móviles a partir de los datos de redes sociales no es una novedad. Las direcciones IP desde las que accedemos a Internet pueden ser conocidas por los administradores de las páginas web, y se usan habitualmente con fines de publicidad. Algunos grandes proveedores como Facebook[4] o Google[5] han publicado recientemente los datos agregados en forma de grandes cuadros de mando.

¿REPRESENTAN ESTOS DATOS EN LA CRISIS DE LA PANDEMIA UNA AMENAZA A LA PRIVACIDAD?

En la medida de que el tratamiento realiza la localización de los interesados, esta práctica puede ser una amenaza a la privacidad, pero no exclusiva de este momento ni de esta situación. Esta amenaza puede ser más crítica si esta información es enriquecida con información personal derivada de la actividad en los perfiles de usuario o se toman acciones sobre sus perfiles. Las condiciones de uso y las políticas de privacidad de estos servicios no son una base jurídica adecuada para realizar estos tratamientos.

[4] https://covid-survey.dataforgood.fb.com/ Facebook & Carnegie Mellon University COVID-19 Symptom Map
[5] https://google.com/covid19-map/?hl=es Mapa de la enfermedad por coronavirus (COVID-19)

¿REPRESENTAN ESTOS DATOS EN LA CRISIS DE LA PANDEMIA UN BENEFICIO IMPORTANTE?

Estos datos podrían ser una ayuda para las autoridades siempre que la información recogida esté de acuerdo con un propósito y un fin previamente definido por las autoridades sanitarias y sean estas las que puedan definir desde la granularidad al formato necesario para aplicarlos a sus estrategias de prevención y control. En cualquier caso, habría que justificar en qué medida supone una mejora con respecto a otras fuentes de información que ya pudieran tener a su disposición dichas autoridades.

V. APPS, WEBS Y CHATBOTS PARA AUTO-TEST O CITA PREVIA

Dentro de este amplio grupo de soluciones estarían las aplicaciones o apps[6], webs y chatbots que implementan test de preguntas y respuestas, consultas de información, o incluso registro de citas previas en los servicios sanitarios. En este documento están agrupados todos en una misma categoría por ser tal vez las soluciones menos novedosas desde el punto de vista tecnológico, aunque, por otro lado, pueden estar entre las más utilizadas.

¿REPRESENTAN ESTAS APLICACIONES EN LA CRISIS DE LA PANDEMIA UNA AMENAZA A LA PRIVACIDAD?

Dependiendo de cómo estén realizadas y de cuáles sean sus objetivos pueden surgir amenazas a la privacidad. Estas pueden aparecer por la urgencia en ofrecer soluciones en funcionamiento que relajen los controles y requisitos para proteger los datos de los ciudadanos. En algunas de estas las aplicaciones[7] se han encontrado con posibles amenazas a la privacidad en la implementación de la misma. Por otra parte, no hay que olvidar que una app o una web es solamente un interfaz para mostrar y llevar datos a un servidor, y es ahí donde se hace el trabajo callado de atender las peticiones.

¿REPRESENTAN ESTOS DATOS EN LA CRISIS DE LA PANDEMIA UN BENEFICIO IMPORTANTE?

En general, cuando están bien construidas sí representan un gran beneficio puesto que acercan información y servicios de salud a las personas que hacen uso de sus servicios. Como efecto secundario, se consigue liberar de tráfico otros canales como el telefónico,

[6] Algunos ejemplos en España son https://www.coronamadrid.com/, https://canalsalut.gencat.cat/ca/salut-a-z/c/coronavirus-2019-ncov/stop-covid19-cat/, o https://www.euskadi.eus/koronabirusa-app-covid-eus/web01-a2korona/eu/

[7] https://blog.appcensus.io/2020/04/19/spanish-covid-19-apps/ Análisis de las apps españolas de AppCensus.

para que lo puedan usar personas que por su edad o sus circunstancias no pueden acceder a Internet. El riesgo, además de los enumerados anteriormente, sería invisibilizar a estas personas que no saben o no poseen un ordenador o un teléfono móvil, y dejarles sin servicios.

VI. APPS DE INFORMACIÓN VOLUNTARIA DE CONTAGIOS (COVAPPS)

En esta categoría estarían algunas aplicaciones móviles que han surgido de forma casi instantánea, en algunos casos de iniciativas ciudadanas[8], y que pretenden hacer sus propios mapas y estadísticas de propagación de la COVID-19 a partir de datos proporcionados voluntariamente por los usuarios. En un entorno muy abierto y transparente se apela a la colaboración desinteresada para descargarse estas aplicaciones y subir datos de localización y datos de su posible infección, contribuyendo así a hacer mapas y cuadros de mando con una información que teóricamente no está filtrada por las autoridades[9].

¿REPRESENTAN ESTAS APLICACIONES EN LA CRISIS DE LA PANDEMIA UNA AMENAZA A LA PRIVACIDAD?

Estas apps podrían serlo si los fines que declaran no son tan altruistas como los que promueven o las prisas conducen a desarrollos sin garantías para la privacidad. No olvidemos que lo que se está cediendo a los servidores en Internet son datos de salud y localizaciones precisas. Si la cantidad y calidad de estos datos fuera la suficiente, gracias a un número significativo de usuarios, se dispondrían de conclusiones como barrios con alto nivel de infección o zonas tóxicas, con el estigma social que eso puede acarrear para sus habitantes o sus negocios[10]. Es decir, es necesario disponer de una muestra significativa y que nadie, de forma maliciosa, esté proporcionando información falsa o manipulada para beneficiar o perjudicar al conjunto.

[8] https://github.blog/2020-03-23-open-collaboration-on-covid-19/ Open collaboration on COVID-19.
[9] https://covidtracking.com/about-project The COVID Tracking Project
[10] https://twitter.com/rcalo/status/1240028937008209920 Ryan Calo: Apps that purport to track people infected with COVID-19 are a terrible idea imo for several reasons.

¿REPRESENTAN ESTOS DATOS EN LA CRISIS DE LA PANDEMIA UN BENEFICIO IMPORTANTE?

Algunas iniciativas privadas justifican su actuación en la hipotética inacción o falta de confianza en las autoridades. Sin embargo, desde el principio del uso voluntario y descontrolado no es posible saber nunca la fiabilidad de la información que contienen, por lo que pueden contribuir a divulgar noticias erróneas y resultar un perjuicio.

VII. APPS DE SEGUIMIENTO DE CONTACTOS POR BLUETOOTH (CONTACT TRACE APPS)

Este tipo de aplicaciones usa la tecnología bluetooth de los teléfonos móviles que permite la conexión con aparatos cercanos como auriculares, altavoces o relojes.

En este caso, las apps utilizan el bluetooth para enviar la "tarjeta" correspondiente al usuario con los móviles que se va encontrando en su camino, y a la vez recolecta las "tarjetas" de esos mismos móviles. Cada tarjeta no tiene una identificación real del usuario, sino un apodo de su identidad. De esta manera cada móvil tiene una colección anónima de "tarjetas" de la gente con la que ha estado en su trabajo, en el transporte o en su ocio. Si un determinado usuario averigua que está infectado, tiene en su mano la posibilidad de "declararlo" a través de la app a un servidor central. En ese momento, se supone que aquellas personas que con las que estuvo en contacto en los últimos días, recibirán un aviso para que valoren qué acciones tomar, como podría ser confinarse, contactar con sus servicios sanitarios o realizarse una prueba.

Han surgido varias estrategias[11] para implementar esta tecnología, que básicamente varían en quién tiene el control sobre las identidades y la red de contactados por cada usuario. Existen opciones en las que ese control descansa en el propio usuario (descentralizadas), y otras en un control centralizado, supuestamente por una autoridad.

En el debate técnico sobre qué tipo de solución se aplicará en Europa, ha entrado hace algunos días un nuevo factor, y es que los gigantes Google y Apple se han aliado para ofrecer una solución de seguimiento[12] *o contact trace* usando sus sistemas iOS y Android. Entre otros factores, esto se debe a que el sistema iOS limita bastante las soluciones de

[11] https://github.com/DP-3T/documents y https://github.com/ROBERT-proximity-tracing DPT3T y Robert son buenos ejemplos de implementación de Contact Trace.

[12] https://www.apple.com/covid19/contacttracing/ Privacy-Preserving Contact Tracing

terceros que usan bluetooth en segundo plano[13] y, si no se realiza algún tipo de adaptación, los de usuarios de IPhone no podrían utilizar apropiadamente aplicaciones que no fueran de Apple.

¿REPRESENTAN ESTAS APLICACIONES EN LA CRISIS DE LA PANDEMIA UNA AMENAZA A LA PRIVACIDAD?

Las principales amenazas[14] a la privacidad de este tipo de soluciones vienen de la realización de mapas de relaciones entre personas, reidentificación por localización implícita, de la fragilidad de los protocolos a la hora construir "tarjetas" casi anónimas, y de dispersar las señales de los contagios de forma que no se identifique en ningún caso la identidad de los contagiados. Debe tenerse en cuenta que el tratamiento de la información no solo afecta al usuario de la aplicación sino también la de todos los terceros con los que ha estado en contacto, por lo que este tratamiento ha de cumplir los principios de protección de datos.

Hay estudios[15] sobre la robustez de los protocolos de criptografía y anonimización, y siempre existe una posibilidad de que aplicando suficiente tiempo y capacidad de cómputo puedan romperse y asociar los apodos anónimos con números de teléfono y personas. Desde el punto de vista de la privacidad, cuanto más cálculo se haga en la parte de servidor, menos control tienen los usuarios, por lo que las soluciones centralizadas siempre parecen menos respetuosas con la privacidad que las distribuidas[16] [17]. La posibilidad de que, debido a la acumulación de los datos de forma centralizada, se produjese un abuso en una empresa poco ética, se ampliarán los propósitos del tratamiento o se fuera víctima de un ciberataque constituye otra de las mayores amenazas de este tipo de soluciones.

¿REPRESENTAN ESTOS DATOS EN LA CRISIS DE LA PANDEMIA UN BENEFICIO IMPORTANTE?

Una vez más, es preciso poner de manifiesto que las soluciones técnicas no se pueden considerar de forma aislada. El éxito de este tipo de soluciones se basa en muchos factores que no dependen de la tecnología. En primer lugar, es necesaria la implicación de un elevado número de usuarios, algunos estudios[18] hablan de al menos el 60% de una población que, teniendo en cuenta a los niños y los ancianos, suponen casi todos los usuarios de móvil. Por otro lado, depende de que se realice una declaración responsable de la situación personal de infección, preferiblemente supervisada por un profesional para evitar estrategias de desinformación. Finalmente, es necesario disponer de acceso a test, no solo para todos los usuarios, sino para poder actualizar la información periódicamente y para que aquellos que sean notificados de haber estado en contacto con un infectado puedan realizar la prueba con prontitud.

---

[13] https://www.reuters.com/article/us-health-coronavirus-apps/bluetooth-phone-apps-for-tracking-covid-19-show-modest-early-results-idUSKCN2232A0 Bluetooth phone apps for tracking COVID-19 show modest early results

[14] https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf Mobile applications to support contact tracing in the EU's fight against COVID-19. eHealth Network

[15] https://github.com/DP-3T/documents/blob/master/Security%20analysis/Privacy%20and%20Security%20Attacks%20on%20Digital%20Proximity%20Tracing%20Systems.pdf Privacy and Security Risk Evaluation of Digital Proximity Tracing Systems. The DP-3T Project

[16] Carta del Comité Europeo de Protección de Datos https://edpb.europa.eu/sites/edpb/files/files/file1/edpbletterecadvisecodiv-appguidance_final.pdf

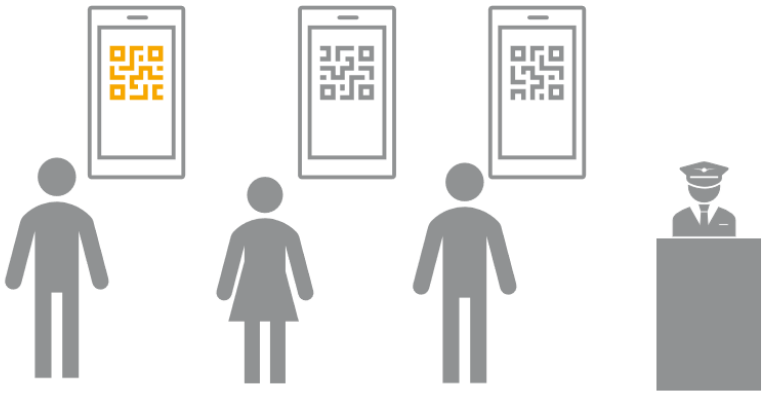
[17] Comunicación de la Comisión: Orientaciones sobre las aplicaciones móviles de apoyo a la lucha contra la pandemia de covid-19 en lo referente a la protección de datos https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020XC0417(08)&from=ES

[18] https://science.sciencemag.org/content/early/2020/04/09/science.abb6936.full Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing. Otra cita clarificadora es https://www.straitstimes.com/tech/google-launches-new-tool-to-help-public-health-officials-plan-social-distancing-measures

En la situación actual de España y de otros países europeos, no parece que estas aplicaciones vayan a tener éxito a corto plazo como una estrategia global de lucha contra la pandemia. Si pensamos en un escenario futuro, cuando la enfermedad esté mucho más controlada, sí podría tener su éxito en colectivos concretos como estudiantes de un centro, profesionales de una compañía o grupos de amigos que deciden voluntariamente usar la aplicación. Podemos pensar en el símil de los grupos de WhatsApp que comparten habitualmente las madres y padres de los niños de los colegios, y por el que se avisan, por ejemplo, si hay algún niño cercano con alguna infección o parásitos, con los problemas que conllevan.

VIII. PASAPORTES DE INMUNIDAD

En algunos países ha empezado considerarse el uso de apps[19] equivalentes a lo que sería un pasaporte o un salvoconducto en papel, mostrando en pantalla un código de colores o un código QR, para que un vigilante o un sistema de control de acceso pueda dejar pasar o no al portador. Este procedimiento es similar al que se usa con las tarjetas de embarque de los aeropuertos, solo que en lugar de decir que un usuario tiene un billete de avión válido o está en una lista, lo que revela es si el portador está contagiado, o presuntamente[20] inmunizado por haber pasado la enfermedad.



¿REPRESENTAN ESTAS APLICACIONES EN LA CRISIS DE LA PANDEMIA UNA AMENAZA A LA PRIVACIDAD?

Estas aplicaciones móviles están anticipando lo que puede ser un futuro documento de identidad en el móvil, con el riesgo añadido de incluir y mostrar un dato de salud, e incluyendo todos los riesgos que se derivan de las vulnerabilidades de dichos sistemas: acceso a manos de ciberdelincuentes, cruce con otros datos como la localización, incorporación de metadatos, lectura remota o simplemente no estar al alcance de muchas personas que no pueden usar teléfonos inteligentes.

A diferencia de una tarjeta de embarque, las pruebas para determinar si una persona está sufriendo o ha superado la enfermedad deberían ser presenciales, y el personal sanitario que lo realiza podría proporcionar al usuario un certificado en papel o cualquier

[19] https://www.bbc.com/mundo/noticias-52215521, https://nypost.com/2020/04/13/will-immunity-passports-be-the-ticket-out-of-coronavirus-lockdowns/ y https://www.infobae.com/america/ciencia-america/2020/04/01/que-son-los-pasaportes-de-inmunidad-del-coronavirus-covid-19-que-se-estudian-en-alemania-para-regresar-a-la-normalidad/ noticias sobre posible adopción de pasaportes en China, Alemania, Italia, Gran Bretaña, USA o Chile.

[20] https://www.who.int/news-room/commentaries/detail/immunity-passports-in-the-context-of-covid-19 La OMS dice que no hay suficientes evidencias de la inmunidad por anticuerpos.

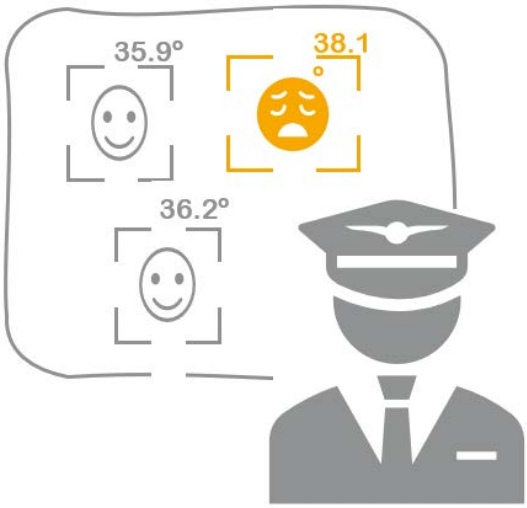
soporte de baja tecnología para que lo mostrara cuando le fuera requerido, junto con su documento de identidad. Un sistema de identidad móvil solo puede tener ventajas cuando el alta se puede hacer a distancia o si la información que gestiona cambia rápidamente, como en el caso de un monedero digital, lo que no es el caso.

¿REPRESENTAN ESTAS APLICACIONES EN LA CRISIS DE LA PANDEMIA UN BENEFICIO IMPORTANTE?

El pasaporte de inmunidad incorpora un dato sensible, como es cualquier dato de salud, pero al que también se le ha dado la misión de servir como salvoconducto de acceso. Hay informes[21] que apuestan por un avance de las aplicaciones de salud móvil (mHealth) permitiendo que, por ejemplo, un paciente lleve su historia clínica para enseñársela a un médico y recibir un tratamiento. Igualmente, el ejercicio de algunas actividades como trabajos o actividades físicas intensas pueden requerir que el candidato muestre un certificado médico antes de acceder. Un uso bien gestionado de apps para certificaciones o registros de salud, que los mantuviera actualizados, seguros e interoperables tendrá cierta utilidad en ámbitos concretos siempre que el acceso a dicha información sea realizado por personal vinculado al cumplimiento de las finalidades relacionadas con políticas públicas para el control de la pandemia. Sin embargo, como en todas las aplicaciones que requieren el uso de smartphones y la evidencia de una prueba fiable de infección o de anticuerpos, estamos lejos de alcanzar a una totalidad de la población, por lo que solo podemos preguntarnos por los beneficios que podrían tener en ámbitos muy concretos.

IX. CÁMARAS DE INFRARROJOS PARA LECTURAS MASIVAS DE TEMPERATURA

En las últimas semanas, el debate sobre las cámaras de videovigilancia con reconocimiento facial se ha visto desplazado por el debate alrededor de otro tipo de cámaras[22] que añaden la capacidad de tomar la temperatura a los individuos que cruzan un área, sin requerir en muchos casos ninguna acción por su parte. Dichas cámaras identifican mediante algoritmos de inteligencia artificial los rostros humanos, los discriminan del resto de elementos que aparecen en la imagen y revelan la temperatura corporal aproximada de cada individuo.



[21] https://www.who.int/goe/publications/goe_mhealth_web.pdf. New horizons for health through mobile technologies. WHO 2011.

[22] https://iberia.dahuasecurity.com/thermal/ Solución de monitoreo de temperatura corporal. Un ejemplo.

¿REPRESENTAN ESTOS SISTEMAS EN LA CRISIS DE LA PANDEMIA UNA AMENAZA A LA PRIVACIDAD?

La AEPD ya ha manifestado[23] su preocupación sobre el uso de estos dispositivos y la necesidad de contar con el criterio previo de las autoridades sanitarias antes de proceder a su instalación. El uso de cámaras u otros dispositivos para registrar la temperatura de los individuos supone un tratamiento de categorías especiales de datos que debe respetar los principios de legalidad, limitación de finalidad y exactitud.

La cámara térmica y la recogida del dato solo puede entenderse como parte de un tratamiento mayor, y no se puede tomar un dato de salud de una persona y tratarlo espontáneamente por cualquier gestor de un lugar público simplemente porque crea que es lo mejor para sus clientes o usuarios. En estos casos, tendremos un riesgo de discriminación, estigmatización y tal vez difusión pública de datos de salud. Todo ello se puede agravar con el riesgo de fugas de información sensible y el conflicto con aquellas personas entienden la medida como una agresión a sus derechos.

En algunos entornos, como el de la normativa de prevención de riesgos laborales, la toma de la temperatura podría ser de utilidad dentro del marco de un tratamiento más extenso del que formen parte otras comprobaciones y garantías adicionales que, en todo caso, respeten los derechos y libertades establecidos en el RGPD.

¿REPRESENTAN ESTOS SISTEMAS EN LA CRISIS DE LA PANDEMIA UN BENEFICIO IMPORTANTE?

La fiebre es una de las evidencias clínicas más probables asociadas a un infectado sintomático de Coronavirus[24], pero también hay que considerar que el porcentaje de infectados asintomáticos es elevado[25] y que la temperatura alta puede estar asociada a otras patologías[26]. Aplicar estas medidas sin un criterio establecido por las autoridades sanitarias con relación a qué valor de fiebre es significativo, sobre que otros síntomas han de ser comprobados, con una manipulación que puede carecer de la precisión suficiente en manos de personal no cualificado, la utilización de estos sistemas podría crear una falsa sensación de seguridad que facilite el contacto con personas realmente infectadas.

X. CONCLUSIÓN

En el presente documento se ha realizado un breve repaso de las principales tecnologías planteadas en la lucha contra la pandemia, sin pretender ser un análisis profundo de las mismas, y con el propósito de compilar aquellas opciones que se están manejando para controlar su expansión.

Nuestra sociedad se encuentra en un punto de inflexión crítico, no solo debido a la situación de pandemia, sino en relación con el planteamiento del modelo de derechos y libertades. Por lo tanto, hay que ser especialmente cuidadoso a la hora de tomar medidas que pueden tener consecuencias irreversibles y pueden estar guiadas únicamente por la urgencia, el miedo o, lo que es peor, otros intereses.

---

[23] https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/comunicado-aepd-temperatura-establecimientos Comunicado de la AEPD en relación con la toma de temperatura por parte de comercios, centros de trabajo y otros establecimientos

[24] https://www.thelancet.com/journals/laninf/article/PIIS1473-3099(20)30198-5/fulltext Clinical and epidemiological features of 36 children with coronavirus disease 2019 (COVID-19) in Zhejiang, China: an observational cohort study

[25] https://www.medrxiv.org/content/10.1101/2020.02.03.20020248v2 Estimation of the asymptomatic ratio of novel coronavirus infections (COVID-19)

[26] Además de ser fácilmente escamoteable mediante el uso de antitérmicos https://www.noticel.com/ahora/20200406/tomaron-medicamentos-para-ocultar-fiebre-y-ahora-estan-hospitalizados-por-covid-19/

En este punto, hay que recordar que las tecnologías de la información no pueden ser entendidas de forma aislada, sino siempre en el marco de un tratamiento con un objetivo definido. Este tratamiento ha de implementar una estrategia global basada en evidencias científicas, evaluando su proporcionalidad en relación con su eficacia, eficiencia y teniendo en cuenta de forma objetiva los recursos organizativos y materiales necesarios. Además, teniendo siempre presente que se han de cumplir los principios establecidos en el Reglamento General de Protección de Datos.