I. ACTUALIDAD

LA PROTECCIÓN DE DATOS PERSONALES EN LA PANDEMIA DE COVID-19

Fecha de recepción: 29 junio 2020.
Fecha de aceptación y versión final: 6 julio 2020.

Jesús Rubí Navarrete
Adjunto Dirección
Agencia Española Protección Datos

Resumen

Las medidas para hacer frente a la pandemia de COVID-19 han implicado nuevos retos para la privacidad en el ámbito jurídico, asistencial, de investigación, tecnológico, laboral y de control transfronterizo. La Agencia Española de Protección de Datos ha colaborado con las administraciones competentes para que los tratamientos de datos garantizaran la privacidad de los ciudadanos. Asimismo, ha elaborado y difundido diversos documentos prácticos, creando un microsite específico en su página web para dar orientaciones a responsables y encargados del tratamiento y a los ciudadanos sobre las garantías a adoptar en el marco de la pandemia. En algunos casos, ha iniciado actuaciones de investigación solicitando información para evaluar la conformidad de los tratamientos con la normativa de protección de datos. Y ha atendido las reclamaciones presentadas por los ciudadanos en relación con la pandemia. Ha participado activamente en el Comité Europeo de Protección de Datos para la elaboración de directrices comunes.

Palabras Clave

Autoevaluación, rastreo, aplicación, temperatura, investigación.

Abstract

The measures to face the COVID-19 pandemic have implied new challenges for privacy in the legal, healthcare, research, technological, labor and border control fields. The Spanish Data Protection Agency has co-operated with the competent administrations so that data processing operations guarantee citizens' privacy. It has also drafted and disseminated various practical documents, setting up a specific microsite on its website to provide guidance to data controllers, data processors and citizens on the guarantees

to be adopted in the context of the pandemic. In some cases, it has initiated investigative actions requesting information to assess the compliance of processing operations with data protection law. And it has handled the complaints lodged by citizens in relation to the pandemic. It has actively participated in the European Data Protection Board Committee in the drafting of common guidelines.

Keywords

Self-assessment, tracing, app, temperature, research.

1. INTRODUCCIÓN

La epidemia del COVID-19 ha incidido ampliamente en la aplicación de la normativa de datos personales como consecuencia, especialmente, de abordarse en un marco jurídico excepcional, como es el de la declaración del estado de alarma; implicar el tratamiento de categorías especiales de datos, como son los datos de salud para garantizar la asistencia sanitaria y el control de la pandemia; redefinir la posición jurídica de los agentes públicos y privados intervinientes y plantear iniciativas novedosas para la utilización de la tecnología en esta situación.

Situación que ha supuesto una profunda implicación de la Agencia de Protección de Datos para dar respuesta, con carácter urgente, a los retos que se han suscitado para garantizar la privacidad.

En este artículo quiero abordar los principales aspectos relacionados con la actividad de la Agencia en relación con la epidemia COVID-19 haciendo referencia a los informes en los que se abordan las bases jurídicas para el tratamiento de los datos, la delimitación de responsables y encargados del tratamiento y el tratamiento de datos en webs y apps para geolocalización o autoevaluación sanitaria, así como para el rastreo de contactos. También se analizarán temas que han suscitado una amplia polémica como, en particular, la toma de temperatura para el control de la epidemia y el reconocimiento facial en los exámenes a distancia.

Asimismo, incluiré una referencia a cuestiones vinculadas con la investigación sanitaria, como son los relativos a la conservación de la información generada en este periodo, a su incorporación a la historia clínica y a las opciones de reutilización posterior. Y, en relación con la investigación científica, a las recomendaciones del Comité Europeo de Protección de Datos (CEPD) en esta materia y al criterio de la Agencia en colaboración con la Agencia Española de Medicamentos y Productos Sanitarios (AEMPS) para permitir la monitorización remota de ensayos clínicos con medicamentos.

Incluiré una referencia a la tramitación de las reclamaciones presentadas en la Agencia en relación con la epidemia.

Seguidamente, destacaré las acciones de difusión desarrolladas por la Agencia y, en particular, las relativas a la toma de temperatura, al tratamiento de datos biométricos, especialmente, en exámenes a distancia, al pasaporte inmunitario, a la utilización de apps para el acceso a espacios públicos y al tratamiento de información sobre anticuerpos de COVID-19 para la oferta y búsqueda de empleo.

Complementariamente, comentaré algunas de las preguntas más frecuentes planteadas que se refieren fundamentalmente a la prevención de riesgos laborales en el entorno empresarial.

Y concluiré citando las actuaciones de la Agencia en el Comité Europeo de Protección de Datos con una referencia más detallada a la Directrices 03/2020 y 04/2020 sobre el tratamiento de datos relativos a la salud con fines de científica en el contexto del brote de COVID 19 y sobre el uso de datos de localización y herramientas de rastreo de contactos en el contexto de la pandemia.

2. LAS BASES JURÍDICAS PARA EL TRATAMIENTO DE DATOS PERSONALES Y LA POSICIÓN DE LOS AGENTES INTERVINIENTES

El análisis de las implicaciones del tratamiento de datos personales en la pandemia de COVID-19 tiene como punto de partida la afirmación de que en este entorno el derecho a la protección de datos no está suspendido, pero no puede ser ni es un obstáculo para dar respuesta a la misma, ya que el Reglamento (UE) 2016/679, General de Protección de Datos (RGPD) permite compatibilizar ambos aspectos.

La Agencia ha emitido numerosos informes respecto de diversas iniciativas de las autoridades sanitarias y, especialmente, del Ministerio de Sanidad, relacionadas con la garantía de la asistencia sanitaria y el control de la pandemia.

La epidemia de COVID-19 ha exigido el tratamiento masivo de datos de salud que, conforme al artículo 9 del RGPD. Son categorías especiales de datos con un régimen reforzado de protección. Garantías que se traducen en una regla general de prohibición de su tratamiento que sólo puede exceptuarse conforme a las previsiones del artículo 9.2 y que, una vez levantadas, hace necesario identificar una base jurídica para su tratamiento en el propio artículo 9 o en el artículo 6 de dicha norma.

A este respecto los informes señalan que la prohibición para el tratamiento de dichos datos se exceptúa por lo previsto en el artículo 9.2.g) e i) que se refieren a la concurrencia de un interés público esencial y, al interés público en el ámbito de la salud pública para la protección frente a amenazas transfronterizas graves de la salud, respectivamente.

Y que las bases jurídicas del tratamiento de datos son la consecución de un interés público esencial y la garantía del interés vital de los afectados y de terceros (art. 6.1.e) y e).

En algunos casos, pueden concurrir otras excepciones a la prohibición y otras bases jurídicas como el cumplimiento de obligaciones legales en el entorno laboral en el marco de la legislación de prevención de riesgos laborales (arts. 9.2.b) y 9.1.c)).

Según el Decreto por el que se declara el estado de alarma las autoridades competentes delegadas son el Ministro de Sanidad, el Ministro del Interior y el Ministro de Transportes, Movilidad y Agenda Urbana. Si bien, tiene un carácter prevalente el Ministro de Sanidad, al determinar los criterios conforme a los cuales deberá hacerse frente a la pandemia.

Ellos son los responsables de los tratamientos de datos personales que se lleven a cabo, por lo que tienen la competencia para decidir sobre los datos a tratar, las finalidades de los tratamientos y los medios para llevarlos a cabo.

Asimismo, las administraciones sanitarias de las Comunidades Autónomas serán responsables del tratamiento, ya que conservan las competencias que tenían atribuidas antes de la pandemia, si bien conforme a los criterios que establezca el Ministerio de Sanidad.

Por tanto, la intervención de otras entidades públicas o privadas, en las distintas iniciativas promovidas por dichas autoridades competentes, especialmente en el desarrollo de aplicaciones (Apps), sólo se podrán llevar a cabo, con carácter general, en la condición de encargados o subencargados del tratamiento de datos, conforme a las instrucciones que obligatoriamente se les hayan dado, para las finalidades que se hayan predeterminado y con las garantías que deben exigirse, conforme al artículo 28 del RGPD, mediante encomienda, convenio, contrato u otro acto jurídico.

En relación con las ofertas de colaboración consistentes en la aportación de tecnologías, se ha suscitado la cuestión de si la realización de la evaluación de impacto en la protección de datos debería realizarla el Ministerio de Sanidad o aportarla la entidad colaboradora. El Informe, partiendo de los principios de protección de datos desde el diseño y por defecto y de la obligación del encargado de colaborar para el cumplimiento de las obligaciones de los artículos de 32 a 36 RGPD, entre los que se encuentra la EIPD (artículo 28.3.f), concluye que deberá aportarse por la entidad privada que ha desarrollado la aplicación.

En relación con otras iniciativas privadas, que ofrecían apps para finalidades diversas, la Agencia emitió un comunicado advirtiendo sobre los riesgos de facilitar datos sensibles a webs privadas que, en ocasiones, no aportaban ni siquiera información sobre sus responsables ni sobre las finalidades del tratamiento.

3. LA APLICACIÓN ASISTENCIACOVID19

Se trata de una aplicación desarrollada para que los usuarios realicen una autoevaluación sobre el posible contagio de la enfermedad, a fin de evitar la congestión de los sistemas de información 112.

La utilización de la aplicación ASISTENCIACOVID19 y el suministro de información es voluntaria, pero el tratamiento ulterior de los datos se realizará conforme a las bases jurídicas señaladas (interés público e intereses vitales), sin consentimiento de los afectados.

La edad mínima para los usuarios para permitir el uso autónomo de la aplicación es de 16 años, como exige la Ley 41/2002, de 14 de noviembre, reguladora de los derechos de autonomía del paciente.

El tratamiento de los datos por motivos de interés público estará justificado mientras permanezca la situación de emergencia sanitaria, por lo que no podrán utilizarse una vez transcurrida la misma.

No obstante, los datos que se recojan deberán incorporarse a la historia clínica conforme a la ley antes citada, por lo que tienen que conservarse y tratarse una vez concluida la pandemia en los términos previstos en dicha norma y en la normativa autonómica que regula esta materia. Exigencia esta que posibilitará su uso posterior, no sólo en el ámbito de la asistencia sanitaria, sino también, en otros como la investigación, conforme a la normativa sectorial sanitaria. Los datos de geolocalización vía GPS del teléfono móvil sólo se utilizarán a los efectos de verificar que el usuario se encuentra en la Comunidad Autónoma en la que declara estar para recibir asistencia sanitaria por parte de ésta, así como evitar y controlar la propagación de la pandemia. La geolocalización es siempre voluntaria, sólo pueden utilizarse datos identificativos necesarios para la finalidad del tratamiento y datos anonimizados para la elaboración de mapas sobre la enfermedad.

4. LAS RECLAMACIONES PLANTEADAS ANTE LA AEPD

La Agencia ha recibido diversas reclamaciones que se refieren fundamentalmente al tratamiento de datos en el ámbito laboral, al control de la temperatura y a la difusión de redes sociales de información sobre personas contagiadas y sobre incumplimientos de las medidas de confinamiento. Asimismo, se ha presentado una reclamación respecto al servicio de videoconferencia ZOOM por enviar a Facebook datos personales de sus usuarios con dispositivos iOS (Apple), incluso de aquellos que no tenían cuenta en Facebook. Según la noticia publicada el 26 de marzo, los datos que se enviaban cuando el usuario abría la app incluían el modelo del dispositivo, el proveedor de la

red, la zona horaria, la ciudad de conexión y un identificador de dispositivo único para que los anunciantes pudieran enviar publicidad. Al día siguiente, Zoom publicó una información señalando que había eliminado estas opciones y actualizó su política de publicidad. La Agencia ha iniciado la tramitación de esta reclamación a través del mecanismo de cooperación respecto del tratamiento de datos por Facebook, siendo la agencia irlandesa la autoridad principal. Y, respecto de ZOOM, por tener un establecimiento en los Países Bajos. En este momento, la Subdirección General de Inspección de Datos está trabajando en la investigación e instrucción de las denuncias en los casos relacionados con la epidemia de COVID-19, así como en las reclamaciones a través del Canal Prioritario dado su carácter urgente. En los demás casos, se están analizando, si bien no se realizan notificaciones a los interesados al estar suspendidos los plazos.

Otras dos investigaciones están relacionadas con la actividad de empresas privadas que estaban realizando la toma de temperatura como medida de control de la epidemia.

Finalmente, la Agencia ha iniciado de oficio solicitudes de información respecto de diversas iniciativas de Administraciones Públicas relacionadas con diversos aspectos en el marco de la pandemia para analizar su adecuación a la normativa de protección de datos.

5. ACTIVIDADES DE DIFUSIÓN

La Agencia ha promovido la difusión de informaciones y documentos en relación con el COVID-19, dirigidos tanto a ciudadanos como a los responsables del tratamiento de los datos. Y ha creado una sección específica en la web de la Agencia en la que se incluyen estas informaciones, pudiendo destacarse las siguientes:

- Las alertas sobre ataques de phishing.
- El comunicado sobre webs y apps de autoevaluación, antes citado.
- La difusión de un post aclarando en este momento deben seguir cumpliéndose las notificaciones de las brechas de seguridad.
- Un documento sencillo con cinco medidas de seguridad que permitan cumplir las medidas de responsabilidad proactiva.
- Una nota técnica con recomendaciones para proteger los datos personales en situaciones de movilidad y teletrabajo.
- Recomendaciones para evitar el acceso de menores a contenidos inapropiados en internet.
- Un comunicado sobre la toma de temperatura por parte de comercios, centros de trabajo y otros establecimientos.

A continuación, se describirán más detalladamente otras iniciativas difundidas por la Agencia.

6. NOTA SOBRE EL USO DE TECNOLOGÍAS EN LA LUCHA CONTRA EL COVID-19

Esta nota realiza un análisis preliminar de algunas tecnologías aplicadas o que están valorándose en la lucha contra el Coronavirus examinando la relación entre los posibles beneficios para el control de la pandemia y los riesgos para la privacidad. En ella, la Agencia recuerda que la utilización de la tecnología no puede ser considerada de forma aislada, si no que ha de estar enmarcada en una estrategia coherente para la lucha contra el COVID-19 basada en evidencias científicas, evaluando su proporcionalidad en relación con su eficacia y todo ello en el marco de los criterios establecidos por el Ministerio de Sanidad. La mayor parte de las implicaciones de estas tecnologías ya las he comentado con anterioridad, por lo que en este momento quiero destacar, en particular, las relacionadas con el pasaporte de inmunidad.

7. EL PASAPORTE DE INMUNIDAD

Los aspectos más destacados de la nota son los siguientes:

- El pasaporte sería un equivalente a un salvoconducto en papel, mostrando en la pantalla un código de colores o un código QR que revela si el portador está contagiado o presuntamente inmunizado por haber pasado la enfermedad.
- Estas aplicaciones móviles presentan riesgos para la privacidad al incluir y mostrar un dato de salud. A lo que se añaden las vulneraciones propias de estos sistemas, como el posible acceso por ciberdelincuentes, el cruce con otros datos como la localización, la incorporación de metadatos o simplemente el no estar al alcance de quienes no tienen teléfonos inteligentes.
- No obstante, un uso bien gestionado de estas aplicaciones que mantuviera actualizados los registros de salud y fueran seguros e interoperables podrían tener cierta utilidad en ámbitos concretos, siempre que el acceso a la información se realice por personal vinculado a finalidades relacionadas con las políticas públicas para el control de la pandemia.

8. COMUNICADO SOBRE TOMA DE TEMPERATURA POR PARTE DE COMERCIOS, CENTROS DE TRABAJO Y OTROS ESTABLECIMIENTOS

Dadas las numerosas iniciativas sobre la toma de temperatura como instrumento de control de la epidemia, la Agencia emitió un comunicado específico sobre esta cuestión.

El comunicado parte de la premisa de que la toma de temperatura no puede analizarse como un hecho aislado, sino en el marco de un proceso que tiene como finalidad evitar contagios para controlar la epidemia.

Por ello, señala que el conjunto de tratamientos relacionados con la toma de temperatura implica, con carácter general, un tratamiento de datos personales y una injerencia particularmente intensa en los derechos de los afectados al referirse a datos de salud, presumir si padece o no una infección y sufrir posibles estigmatizaciones sociales (así podría suceder en el entorno educativo, laboral o comercial, por denegaciones de acceso).

El documento indica que, según las informaciones proporcionadas por las autoridades sanitarias, hay un porcentaje de personas contagiadas asintomáticas que no presentan fiebre, que la fiebre no es siempre uno de los síntomas presentes en pacientes sintomáticos y que puede haber personas que presenten temperaturas elevadas por causas ajenas al COVID-19. Por tanto, la toma de temperatura como mecanismo único indicativo del contagio puede generar una falsa sensación de seguridad para quienes accedan a un establecimiento.

Por ello, la toma de temperatura debe complementarse con actuaciones adicionales que permitan comprobar con rigor el posible contagio de la enfermedad.

Dichas medidas solo deben aplicarse atendiendo criterios definidos por el Ministerio de Sanidad, valorándose las opciones para adoptar medidas menos intrusivas con mayor eficacia.

El consentimiento no puede ser una base jurídica para estos tratamientos, que pueden suponer la denegación de servicios o el acceso a establecimientos, por lo que no podría considerarse prestado libremente.

El interés legítimo como base jurídica del tratamiento debería, en todo caso, excluirse por dos motivos: por una parte, porque esta previsión debería estar recogida expresamente en el derecho europeo o nacional con garantías adecuadas, circunstancia que no concurre. Y, por otra, porque el impacto sobre los derechos, libertades e intereses de los afectados haría que no resultara prevalente.

En el entorno laboral este tratamiento podría tener como base jurídica la obligación que tienen los empleadores de garantizar la seguridad y la salud de los trabajadores, siempre que se establezcan garantías adecuadas. A este respecto, son particularmente relevantes las directrices sobre el "procedimiento de actuación para los servicios de prevención de riesgos laborales frente a la exposición SARS-CoV-2" publicadas por los Ministerios de Sanidad y de Trabajo y Economía Social el 22 de mayo de 2020.

Las directrices incluyen previsiones específicas para los establecimientos con acceso público que se focalizan fundamentalmente en medidas organizativas, tales como el control de aforo, de la entrada de clientes, de mantener la distancia social y aislar mediante mamparas mostradores y cajeros.

En el ámbito de la prevención de riesgos laborales están también disponible en la web de la AEPD criterios sobre el tratamiento de datos en el apartado de preguntas más frecuentes. De estos criterios cabe destacar los siguientes:

- Que los empleadores, conforme a la normativa de prevención de riesgos laborales y con las garantías que se establecen, pueden conocer si los trabajadores están infectados para garantizar su salud, evitar contagios y adoptar medidas previstas por las autoridades competentes.
- Que pueden comunicar esta información al resto del personal de la empresa sin identificar a la persona afectada, salvo que fuera necesario para proteger la salud de los trabajadores.
- Que el trabajador infectado o sometido a aislamiento preventivo tiene la obligación de informar a su empleador, o en su caso, a los delegados de prevención de riesgos de esta circunstancia.

El comunicado sobre toma de temperatura finaliza concluyendo que sus consideraciones son particularmente aplicables a la utilización de dispositivos como cámaras térmicas, que implican una mayor intrusión en los derechos de las personas al ofrecer la posibilidad de grabar y conservar datos o tratar información adicional como la biométrica.

9. EL RECONOCIMIENTO FACIAL PARA LA REALIZACIÓN DE EXÁMENES A DISTANCIA EN LAS UNIVERSIDADES

En respuesta a una consulta de la Conferencia de Rectores de Universidades de España, la Agencia emitió un informe en el que se analiza la propuesta para la utilización del reconocimiento facial, es decir, de datos biométricos, como garantía para la realización de exámenes no presenciales.

El RGPD define los datos biométricos como "datos personales obtenidos a partir de un tratamiento técnico específico relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos." Y el artículo 9.1 considera que pueden estar incluidos entre las categorías especiales de datos con garantías reforzadas.

El informe aborda una primera cuestión de interés sobre el tratamiento de datos biométricos admitiendo que en función de los tratamientos que se realicen cabe diferenciar entre datos biométricos, que son categorías especiales de datos y otros que no lo son.

Para ello, tiene en cuenta el contenido del Considerando 51 del RGPD, que no considera categorías especiales a las fotografías; el Protocolo que enmienda el Convenio 108 del Consejo de Europa, que hace referencia a datos biométricos para identificación unívoca y no para autenticación; el Dictamen 3/2012

del Grupo de Trabajo del artículo 29 (GT29) sobre evolución de tecnologías biométricas que distinguen entre tratamientos con fines de identificación o con fines de verificación y autenticación, así como el Libro Blanco sobre inteligencia artificial de la Comisión Europea.

Al objeto de aclarar las dudas interpretativas que surgen respecto a la consideración de los datos biométricos como categorías especiales de datos puede acudirse a la distinción entre identificación biométrica y verificación/autenticación biométrica que establecía el Grupo del artículo 29 en su Dictamen 3/2012 sobre la evolución de las tecnologías biométricas:

- Identificación biométrica: la identificación de un individuo por un sistema biométrico es normalmente el proceso de comparar sus datos biométricos (adquiridos en el momento de la identificación) con una serie de plantillas biométricas almacenadas en una base de datos (es decir, un proceso de búsqueda de correspondencias uno-a-varios).
- Verificación/autenticación biométrica: la verificación de un individuo por un sistema biométrico es normalmente el proceso de comparación entre sus datos biométricos (adquiridos en el momento de la verificación) con una única plantilla biométrica almacenada en un dispositivo (es decir, un proceso de búsqueda de correspondencias uno-a-uno).

Atendiendo a la citada distinción, puede interpretarse que, de acuerdo con el artículo 4 del RGPD, el concepto de dato biométrico incluiría ambos supuestos, tanto la identificación como la verificación/autenticación. Sin embargo, y con carácter general, los datos biométricos únicamente tendrán la consideración de categoría especial de datos en los supuestos en que se sometan a tratamiento técnico dirigido a la identificación biométrica (uno-a-varios) y no en el caso de verificación/autenticación biométrica (uno-a-uno).

Y concluye que el reconocimiento facial en exámenes a distancia y el posible tratamiento de datos de terceros que puedan suplantar al examinando, tienen como finalidad una identificación unívoca y, por tanto, debe aplicarse el régimen de garantías reforzado para las categorías especiales de datos.

En cuanto a las bases jurídicas del tratamiento, el informe concluye que el consentimiento por parte del alumno para los exámenes a distancia sólo puede considerarse libre y, por tanto, válido, cuando se haya ofrecido una alternativa equivalente en cuanto a duración y dificultad, estableciendo procedimientos de evaluación que acrediten la igualdad entre los alumnos que consientan el tratamiento de datos biométricos y los que no lo hagan.

Y, respecto de la opción de considerar como base jurídica el interés público, considera que se requeriría una norma con rango de ley que lo habilitase y lo estableciera incluyendo garantías específicas para dichos tratamientos.

10. COMUNICADO SOBRE EL TRATAMIENTO DE LA INFORMACIÓN ACERCA DE TENER ANTICUERPOS PARA LA OFERTA Y BÚSQUEDA DE EMPLEO

La crisis sanitaria ha generado ciertas prácticas en el ámbito de la contratación laboral para solicitar a los candidatos a un puesto de trabajo información sobre la COVID-19 y el desarrollo de anticuerpos. Esta circunstancia ha determinado que la Agencia emitiera un comunicado sobre estas prácticas, cuyas principales conclusiones son las siguientes:

- Los datos que se solicitan se consideran categorías especiales de datos al ser datos de salud, cuyo tratamiento está prohibido, como regla general, si bien existen excepciones a esta prohibición como son el consentimiento o el ser necesario su tratamiento para la ejecución de un contrato de medidas precontractuales solicitadas. Conforme a las directrices sobre consentimiento del CEPD (wp259), en las circunstancias expuestas el consentimiento no podría considerarse prestado libremente. Y tampoco podría aplicarse la excepción basada en la ejecución del contrato por tanto que la solicitud de ese dato no sería necesaria para su formalización, siendo el tratamiento excesivo y contrario al principio de minimización de datos. En este sentido, solicitar información sobre el estado de inmunidad iría más allá de las obligaciones y derechos específicos que impone a la empresa la legislación laboral, y en particular, la normativa de prevención de riesgos laborales.

  En este sentido, se argumenta que la persona aún no es empleada y que la información sobre una posible inmunidad no contribuye significativamente a la protección del resto del personal, ya que los protocolos de prevención de riesgos deben aplicarse por igual a todo el personal en relación con la presencia de casos sospechosos; sin prever excepciones para las personas que hayan padecido la enfermedad.

  Adicionalmente, el tratamiento no responde a una finalidad legítima, puesto que daría lugar a una diferencia de trato que no obedece a una justificación objetiva y razonable.
- La inclusión del dato sobre inmunidad en el currículum debe evitarse, ya que el empleador destinatario del mismo no puede tratar la información por las razones expuestas para no infringir la normativa de protección de datos, debiendo proceder a suprimirla, lo que podría llegar a implicar la destrucción del currículum.

11. RECOMENDACIONES PARA EL DESPLIEGUE DE APPS MÓVILES EN EL ACCESO A ESPACIOS PÚBLICOS

Entre las iniciativas adoptadas en relación con la epidemia de COVID-19, se encuentra el desarrollo de apps no sanitarias para la reserva o control de aforo en lugares públicos.

La Agencia Española de Protección de Datos ha emitido una Recomendación sobre estas aplicaciones partiendo del principio de que deben fundarse en un análisis de necesidad y proporcionalidad para evaluar que los tratamientos sean realmente efectivos para la finalidad prevista, que no puede ser otra que la gestión de medidas de distancia social, como el control de aforo o el de distancia, y que se trata el conjunto mínimo de datos necesario. En este sentido, el uso de la identidad del usuario o de identificadores únicos sólo podrá realizarse si son estrictamente necesarios para dicha finalidad.

El uso de la app debe ser voluntario, basándose en un consentimiento libre, informado y específico. Para garantizar que el consentimiento es libre, el uso de la app no debe condicionar el acceso a espacios públicos debiendo ofrecerse alternativas con el mismo grado de facilidad de uso. En el caso de menores de 14 años, el consentimiento debe prestarse por sus padres o tutores.

En el caso de espacios públicos los responsables del tratamiento serán las administraciones competentes. La utilización de recursos de terceros privados deberá ofrecer garantías suficientes para evitar que el uso de la app permita desarrollar otras finalidades como la elaboración de perfiles, la publicidad o el seguimiento de las personas.

Finalmente, la Agencia recomienda la adopción de soluciones comunes en un mismo entorno de espacios públicos para evitar los potenciales riesgos de múltiples apps.

12. ACTUACIONES DE LA AGENCIA EN EL MARCO DEL COMITÉ EUROPEO DE PROTECCIÓN DE DATOS (CEPD)

La epidemia de COVID-19 ha afectado en mayor o menor medida al conjunto de Estados miembros de la Unión Europea, lo que ha dado a lugar a iniciativas tanto de la Comisión Europea como del Comité Europeo de Protección de Datos en relación con el uso de información personal.

La Agencia ha participado activamente en los trabajos del Comité Europeo de Protección de Datos desde el primer momento remitiendo los informes jurídicos a los que anteriormente se ha hecho referencia, que sirvieron de base a la primera Declaración sobre protección de datos y Coronavirus adoptada por el Comité el 19 de marzo.

Asimismo, ha participado en la elaboración de la carta en la que se respondía a la solicitud de informe de la Comisión Europea en relación con una guía sobre el uso de apps en la contención del COVID-19.

Posteriormente, el CEPD ha hechos públicos dos importantes documentos sobre el tratamiento de datos como son las Directrices 03/2020 sobre el tratamiento de datos relativos a la salud con fines de investigación científica en el contexto del brote de COVID-19 y las Directrices 04/2020 sobre el uso de datos de localización y apps de seguimiento de contactos en el contexto de la pandemia. Ambas se comentarán posteriormente. Y, en relación con el proceso de desescalada ha emitido una declaración sobre el tratamiento de datos en la apertura de fronteras.

13. LAS DIRECTRICES 03/2020 SOBRE EL TRATAMIENTO DE DATOS RELATIVOS A LA SALUD CON FINES DE INVESTIGACIÓN CIENTÍFICA EN EL CONTEXTO DEL BROTE DEL COVID-19

Sus principales conclusiones son las siguientes:

- Se aplican las excepciones a la prohibición de tratar datos de salud con fines de investigación con base en el interés público en el ámbito de la salud pública y los fines de investigación (artículo 9.2.i) y j) RGPD).
- Las bases jurídicas del tratamiento serán con carácter general el interés público sin consentimiento de los interesados, salvo en determinados casos que señala.
- Las transferencias internacionales de datos para fines de investigación contra COVID-19 tienen como base jurídica el ser necesarias para fines importantes de interés público por razones excepcionales (tan pronto sea posible, cláusulas contractuales estándar).

14. LAS DIRECTRICES 04/2020 SOBRE EL USO DE DATOS DE LOCALIZACIÓN Y APPS DE SEGUIMIENTO DE CONTACTOS EN EL CONTEXTO DE LA PANDEMIA

Las Directrices parten del criterio de que las apps de *contact tracing* deben integrarse en una estrategia global de salud pública y tener confirmación por una persona o institución cualificada en los supuestos de contagio. Es decir, no ser objeto de decisiones automatizadas, como puede ser las basadas exclusivamente en las tomas de temperatura.

Afirma que los datos de localización recogidos por las operadores de telecomunicaciones y similares sólo pueden ser cedidos si han sido anonimizados por el proveedor o, si indican la posición geográfica, con el consentimiento del interesado.

El almacenamiento de información en el dispositivo del usuario o el acceso a la información ya almacenada sólo debe permitirse si el usuario ha dado su consentimiento o si es estrictamente necesario para el servicio solicitado.

No obstante, las autoridades podrían obtener datos de geolocalización sin consentimiento sobre la base de un interés público.

Las apps de rastreo sólo podrán tratar información de proximidad y no movimientos (geolocalización), siendo preferible que los datos se anonimicen y que los indicadores únicos generados por las apps se renueven cada cierto tiempo para evitar el riesgo de identificación y seguimiento.

Entre las opciones de tratamiento de datos centralizado en una única base de datos a disposición de las autoridades o un tratamiento descentralizado, sin intervención de las autoridades, desde los terminales de los usuarios que hayan descargado la aplicación, las recomendaciones consideran preferible que los datos se almacenen y se traten de forma descentralizada por encajar mejor con el principio de minimización.

En cuanto a las personas que se comunicará la información de los contagiados, señalan que sólo deben ser informadas aquellas con las que el usuario contagiado ha estado en estrecho contacto, habiéndose verificado la infección a través de un profesional sanitario para alertar a estos contactos. Los criterios para la delimitación de qué se considera "estrecho contacto" deben ser fijados por las autoridades sanitarias (distancia, tiempo de contacto,…).

15. DECLARACIÓN SOBRE EL TRATAMIENTO DE DATOS EN LA APERTURA DE FRONTERAS

La apertura de fronteras puede implicar diversos tratamientos de datos (pruebas para COVID-19, certificados de profesionales sanitarios, apps de rastreo de contactos), por lo que el Comité insta a los Estados miembros a adoptar un enfoque europeo común basado en pruebas científicas.

Los aspectos que requieren una atención especial por parte de los Estados miembros son los siguientes:

- La legalidad, equidad y transparencia basándose en la base jurídica adecuada; la limitación de la finalidad, limitándose a la de combatir la pandemia, evitando su propagación; la minimización de datos; la conservación durante un breve periodo de tiempo para cumplir dicha finalidad y la seguridad de los datos.
- La decisión de permitir la entrada en un país no sólo debe basarse en la tecnología disponible (decisiones automatizadas). En cualquier caso, dicha decisión debe estar sujeta a salvaguardias adecuadas, que deben incluir información específica al interesado y el derecho a obtener la

intervención humana, a expresar su punto de vista, a obtener una explicación de la decisión alcanzada después de dicha evaluación y a impugnar la decisión.

Estas medidas no deben afectar a los menores.

- Cuando proceda, los Estados miembros deben definir claramente las responsabilidades entre la autoridad pública que actúa como responsable del tratamiento de datos y el encargado del tratamiento de datos en dicho acuerdo.
- La cesión de datos a otros responsables solo debe tener lugar si existe una base legal adecuada (autoridades sanitarias).

16. LA MONITORIZACIÓN REMOTA DE ENSAYOS CLÍNICOS DURANTE LA PANDEMIA DE COVID-19

En respuesta a una consulta de Farmaindustria, la Agencia elaboró un informe admitiendo la posibilidad remota de ensayos clínicos con medicamentos durante la epidemia de COVID-19. Monitorización que responde a la necesidad de garantizar el desarrollo de determinados ensayos clínicos y, en todo caso, la salud de los sujetos participantes. El resultado final de la consulta se fundamenta en una novación del contrato inicial entre el promotor y el centro del ensayo y dos anexos: un compromiso de confidencialidad entre el promotor y el monitor y un protocolo de seguridad de conexión remota.

El informe se ha elaborado partiendo de una comunicación fluida con Farmaindustria y en coordinación con la Agencia Española de Medicamentos y Productos Sanitarios (AEMPS). En particular, la intervención de la AEMPS se ha centrado en la valoración de los principios de necesidad y proporcionalidad sobre la monitorización remota que deben valorarse con criterios sanitarios. En consecuencia, el informe limita la posibilidad de monitorización remota a la duración de la situación sanitaria derivada de la pandemia del COVID-19; criterio que se reconoce jurídicamente en la parte expositiva de la novación del contrato. El análisis detallado de esta alternativa excedería de los límites del presente artículo. Los documentos pueden consultarse en el *microsite* de la AEPD sobre el COVID-19.