RESUMEN SESIÓN ONLINE APEP - AGENCIA ESPAÑOLA DE PROTECCION DE DATOS SOBRE CRITERIOS EN PROTECCIÓN DE DATOS RELACIONADOS CON COVID-19

Organizador	ASOCIACION PROFESIONAL ESPAÑOLA DE PRIVACIDAD
Fecha	21/05/2020 de 10:30 a 11:30 horas
Plataforma	Microsoft Teams
Ponentes	Mar España, Directora AEPD Jesús Rubí, Coordinador Unidad Apoyo y Relaciones Institucionales AEPD Luis de Salvador, Coordinador Unidad de Estudios Técnicos AEPD Marcos Judel, Presidente APEP

1. Inicio de la sesión

La sesión comienza a las 10:30 horas tras problemas técnicos iniciales con la conexión de los ponentes. Marcos Judel, Presidente de APEP realiza la presentación de los ponentes y realiza una breve explicación de las cuestiones a tratar y el funcionamiento del sistema de preguntas y respuestas en directo.

2. Desarrollo de la sesión: actividad de la Agencia

En primer lugar, toma la palabra Mar España, Directora de la AEPD, quien realiza una síntesis de la actividad de la Agencia desde el comienzo de la crisis del COVID-19, resaltando que han estado trabajando, fundamentalmente, a través de dos vías:

a. **La continuación de la gestión ordinaria de la Agencia.** Se destaca que la entrada de reclamaciones se ha reducido cuantitativamente desde el comienzo de la crisis. Se han recibido no más de un centenar de reclamaciones sobre cuestiones relacionadas con el COVID-19. Las principales:
    - Control de temperatura por parte de empresarios.
    - Legitimación de los vigilantes de seguridad para realizar la toma de temperatura.

- Difusión de datos de personas contagiadas o de incumplimiento de las medidas de confinamiento.
- Sobre el servicio de videoconferencia Zoom respecto al envío de datos personales a Facebook desde dispositivos Apple, para lo que se ha mantenido contacto con la autoridad de protección de datos holandesa e irlandesa, respectivamente. Tras la reclamación, Zoom ha procedido a modificar dicho aspecto en su Política de Privacidad.

Igualmente, destaca el valor de que cualquier consulta o reclamación a la Agencia esté precedida de un pronunciamiento previo del Delegado de Protección de Datos y de la importancia de los profesionales de la privacidad en este sentido.

b. Una intensa actividad extraordinaria en relación con el COVID-19. Desde el primer momento, la Agencia se ha puesto a plena disposición de las autoridades sanitarias competentes.

En relación, precisamente, con esta actividad extraordinaria, se procede a hacer mención a toda la desplegada por la Agencia y una breve síntesis de los puntos principales de los documentos adoptados:

i. **Informe núm. 17/2020.** Declara la plena vigencia y aplicación del derecho a la protección de datos de carácter personal y la normativa de protección de datos. No obstante, sin perjuicio de la plena aplicación de sus criterios y principios, ello no debe constituir un obstáculo para el tratamiento de datos en el marco de la pandemia. Asimismo, se centra fundamentalmente en analizar las bases de legitimación para el tratamiento de datos personales en relación con el COVID-19:
   - Por un lado, el interés público esencial y, por otro, la protección de un interés vital (propio o de terceras personas). El Informe concluye que, en el ámbito público, el responsable del tratamiento es el Ministerio de Sanidad y el resto de entidades públicas o incluso privadas (v.g. Telefónica, que ha contribuido al desarrollo de la aplicación COVID) se constituirían como encargados del tratamiento o subencargados.

- En el caso de las empresas pueden, además, concurrir otras bases jurídicas: cumplimiento de la Ley de Prevención de Riesgos Laborales (protección de la salud de sus trabajadores).

ii. **Preguntas frecuentes (FAQs) sobre el COVID-19 dirigidas a ciudadanos, empresas y otros sujetos obligados al cumplimiento de la normativa de protección de datos.** Se ha publicado ya una actualización del documento. Se procede a resumir algunas conclusiones:

- Los empleadores pueden conocer si las personas trabajadoras están infectadas para garantizar su salud a efectos de evitar contagios.
- Es obligatorio que los trabajadores se presten a la realización de test (v.g. PCR) si los facilita la empresa.
- La persona trabajadora infectada o sometida a aislamiento preventivo tiene la obligación de informar de esta circunstancia al empleador.

iii. **Comunicado en relación con la toma de temperatura por parte de comercios, centros de trabajo y otros establecimientos.** La Agencia muestra su preocupación y entiende que el marco para la toma de la temperatura debe ser definido por las autoridades sanitarias competentes, quienes deben indicar si existe evidencia científica de que la toma de temperatura es un tratamiento necesario para controlar la pandemia y, por ende, si constituye o no una medida efectiva. La contestación del Ministerio de Sanidad es que, por el momento, no existe evidencia científica de que la toma de temperatura en sí misma, como hecho aislado, sea algo efectivo para la lucha contra el contagio del COVID-19. También se sitúa dicha posición en la línea de un estudio publicado por la Comisión Europea en el que se analiza la toma de temperatura en situaciones anteriores (SARS, Ébola) y en el que se constata la existencia de un 20-25% de falsos positivos y negativos.

En el Comunicado, la Agencia sostiene que la toma de temperatura constituye un tratamiento de datos personales con una injerencia particularmente acentuada en los derechos de las personas, pues es susceptible de generar situaciones de estigmatización.

Desde el punto de vista de la legitimación para realizar la medición, en el ámbito empresarial podría justificarse en las obligaciones de prevención de riesgos laborales del empleador. No obstante, las bases de legitimación son dudosas en los supuestos de toma y/o registro de temperatura en tiendas o establecimientos abiertos al público.

El consentimiento no sería válido porque no se prestaría de una forma libre (por ejemplo, si la consecuencia fuese la denegación del acceso al establecimiento en cuestión). Asimismo, el interés legítimo quedaría excluido por dos motivos: porque debería regularse en una norma nacional o europea y porque el impacto en los derechos y libertades fundamentales de los interesados era tan acentuado que terminaría decayendo el interés legítimo en una ponderación entre ambos.

IV. Informe sobre la app "COVID". Se realizaron recomendaciones en cuanto a la Política de Privacidad y otros aspectos. Además, se destacó que los datos recogidos por medio de la app deben incorporarse a la historia clínica de conformidad con lo dispuesto por la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica. Finalmente, se recomendó también minimizar los datos de geolocalización, que solo podrán utilizarse para verificar que el usuario se encuentra en la Comunidad Autónoma en la que declara estar para recibir asistencia sanitaria de manera efectiva. Asimismo, la geolocalización debe ser siempre voluntaria y únicamente se podrán utilizar los datos necesarios para la finalidad del tratamiento.

V. Comunicado en relación con las webs y apps de iniciativa privada que ofrecen autoevaluaciones o consejos sobre el coronavirus. La Agencia procedió a investigar algunas apps que iban surgiendo (v.g. Stop Coronavirus). Se advirtió sobre los riesgos de que, cualquier ciudadano, con su buena voluntad, fuera aportando datos personales sensibles y su sintomatología a un responsable o una entidad que no se sabe exactamente para qué finalidad los va a destinar.

VI. Informe sobre los convenios de colaboración entre la Secretaría de Estado para el Avance Digital y Telefónica como encargado del tratamiento.

VII. Actuaciones relativas a la protección de los menores en Internet y en el uso de nuevas tecnologías.

VIII. Nota sobre el uso de las tecnologías en la lucha contra el COVID-19. La utilización de la tecnología no debe realizarse de una manera aislada, sino que deberá enmarcarse en una estrategia coherente y dirigida e impulsada por las autoridades sanitarias en base a la evidencia científica.

IX. Nota técnica con recomendaciones para proteger los datos personales en situaciones de movilidad y teletrabajo. Se incluye información sobre cómo hacer frente a amenazas como el *phising* o la suplantación de identidad. Se destaca la oportunidad existente tanto para el sector público como el privado de plantear nuevos métodos y modalidades de trabajo.

X. Posts y publicaciones relativas a las brechas de seguridad y a la obligatoriedad de su notificación. Se constata una bajada en el número de notificaciones de brechas de seguridad.

XI. Informe sobre el uso del reconocimiento facial para la realización de exámenes en las universidades y centros docentes. El Informe se emite tras una consulta realizada por la CRUE y se presentan la siguientes conclusiones:

- La diferenciación entre datos biométricos, como categorías especiales de datos, de otros datos que no lo son. Ello con base al Considerando núm. 51 del RGPD, el Convenio 108 del Consejo de Europa, el dictamen del GT29 y el Libro Blanco sobre Inteligencia Artificial en Europa.
- La finalidad del tratamiento es la identificación unívoca de una persona con arreglo a una plantilla biométrica y, por tanto, son categorías especiales de datos.
- El consentimiento únicamente se entenderá prestado de manera libre cuando la universidad hubiera ofrecido una alternativa equivalente en cuanto a duración y dificultad. En estos casos las normas de los exámenes deben estar publicadas. Asimismo,

los procedimientos de evaluación tienen que garantizar la igualdad entre el alumnado que consiente y el que no.

- Para basar el tratamiento en el interés público es necesaria una norma con rango de ley que lo habilite, que por ahora se desconoce.

XII. Actuaciones de la Agencia en el Comité Europeo de Protección de Datos:

- El Comité emite una primera declaración basándose, en gran medida, en el Informe 17/2020 de la Agencia.
- Respuesta a la solicitud de la Comisión Europea en relación con la "Guía sobre el uso de las apps para la contención del COVID-19".
- Publicación de dos recomendaciones: una relativa a la investigación científica y otra sobre el uso de datos de localización y apps de seguimiento de contactos. En relación con esta última, las apps deben formar parte de una estrategia de salud pública y que no pueden dar lugar a decisiones automatizadas solo por la información recabada a través de las mismas. Los datos de localización facilitados por los operadores de telecomunicaciones solo pueden ser cedidos si han sido anonimizados o si la persona interesada ha prestado su consentimiento. Finalmente, se da preferencia a los datos de proximidad frente a geolocalización y al almacenamiento descentralizado.

XIII. Pasaporte de inmunidad. Se trataría de un Código QR que, a modo de salvoconducto, permitiera mostrar en una pantalla si se ha pasado la enfermedad y si se está inmunizado frente a aquella. Es otra cuestión que queda en manos de las autoridades sanitarias. Por ahora, la gran mayoría de los países europeos han rehusado implantarlo. Se destaca el riesgo que estos pasaportes entrañan para la protección de datos debido a la existencia de datos de salud y posible cruce con otros datos como la geolocalización. No obstante, puede llegar a constituirse como un instrumento útil siempre que se encuentre unido a la interoperabilidad de las aplicaciones.

3. Preguntas y respuestas de las personas asistentes

Tras la exposición de la actividad de la Agencia, Marcos Judel retoma la palabra y se da apertura al turno de preguntas y respuestas. Debido a la existencia de preguntas similares se deciden agrupar en los siguientes bloques:

I. **Toma y registro de temperatura por empresas y entidades privadas en los accesos a sus instalaciones:**

   - ¿Existe legitimación?. Sí, con arreglo a la Ley de Prevención de Riesgos Laborales que se aplica tanto al sector público como al privado.
   - ¿Es proporcional?. Deberán aplicarse los principios de protección de datos (v.g. minimización, proporcionalidad). Podría ser suficiente con el control de temperatura realizado en el momento sin necesidad de registrarlo, porque el objeto no debe ser medir la temperatura o llevar un registro diario de la misma sino prevenir la transmisión y contagio del COVID-19. Asimismo, la medición de temperatura, de manera aislada, no está científicamente probada como un tratamiento efectivo para la prevención de contagios y puede generar una falsa seguridad jurídica y sanitaria. De ahí la importancia de la lealtad y la necesidad del tratamiento.
   - ¿Se puede medir solo a las personas trabajadoras o también a clientes o proveedores que quieran acceder a las instalaciones? Podría haber legitimación siempre y cuando esos clientes y proveedores, al estar en contacto con el personal de la plantilla, lo pudieran contagiar. En estos casos el empresario podría estar legitimado para tratar esos datos de clientes y proveedores si hay un riesgo de que esto se traduzca en el contagio del resto de la plantilla.

II. **Sobre la realización de Evaluaciones de Impacto.** Se tendrá que analizar caso por caso pero no hay duda de que pueden existir tratamientos de alto riesgo. No es lo mismo implantar un sistema de toma de temperatura en una gran factoría con multitud de trabajadores que en un pequeño establecimiento abierto al público.

En caso de tener que hacerse debe realizarse sobre el conjunto del tratamiento y sus operaciones, no solo sobre la toma de temperatura.

Es importante, en todo caso, contar con protocolos para su realización y que éstos sean conocidos por el personal de la empresa. Por ello, podría ser muy útil que el Ministerio de Sanidad definiese unos elementos generales y criterios fundamentales para la elaboración de estos protocolos.

III. **El uso de cámaras térmicas.** También es importante analizar cada caso y qué tipo de datos va a recoger, el funcionamiento y características concretas del sistema, etc. Si estamos hablando de un sistema de videovigilancia que, además, captura datos sobre temperatura corporal y utiliza algoritmos o inteligencia artificial para discernir qué es una persona y qué es una taza de café y con base a todo ello toma decisiones automatizadas, constituye, sin duda, un tratamiento bastante intrusivo.

IV. **Uso de dispositivos de contact tracing (pulseras, aplicaciones) en el ámbito laboral que permitan comprobar el cumplimiento del distanciamiento social obligatorio.** Se tendrían que aplicar los mismos criterios que para el registro de temperatura.

V. **Sobre la realización de test PCR a las personas trabajadoras antes de incorporarse a su puesto de trabajo presencial.** Si la empresa tiene dicha posibilidad y su disponibilidad, está legitimada para realizar los test PCR y, además, los trabajadores estarían obligados a someterse al mismo.

VI. **Sobre el reconocimiento facial en la realización de exámenes.** Es posible si va encaminado a la identificación del alumnado y que no haya una suplantación de identidad, siempre que se hayan adoptado medidas o criterios con anterioridad para valorar la proporcionalidad de dichas medidas y la injerencia que pueden tener sobre los derechos y libertades. De nuevo, importante valorarlo caso por caso y examinar lealtad, necesidad, proporcionalidad, etc

Necesidad de distinción entre el tratamiento de datos biométricos como categorías especiales de datos con fines de identificación (como es el caso de los exámenes) y aquellos

realizados con fines de verificación o autenticación, que no gozarían de las garantías de las categorías especiales.

VII. Sobre la historia clínica y el resto de información clínica. Se trata de una información enormemente valiosa y relevante. Tanto es así que, desde el punto de vista epidemiológico, el Ministerio de Sanidad en su Orden 404/2020, de 11 de mayo, prevé unas obligaciones de suministro de la información de todas las pruebas practicadas por las unidades de salud pública estatales y autonómicas, tanto del sistema público como privado y los servicios de prevención de riesgos laborales. Su finalidad es la de llevar a cabo una respuesta territorialmente más precisa y ajustada en caso de nuevos rebrotes.

Por ello, existirá una cesión de datos al Ministerio de Sanidad y las autoridades epidemiológicas. En estos casos, como los datos son obtenidos por el Ministerio de Sanidad pero no directamente de los propios interesados, se deberán cumplir con las cláusulas informativas e informar de esas cesiones con fines epidemiológicos y de control de prestación de la asistencia sanitaria.

Finalizada la pandemia, la información tratada con fines epidemiológicos deberá eliminarse o anonimizarse, pues solo podrá utilizarse de manera agregada o estadística.

Sin embargo, esta información tiene que incorporarse necesariamente a la historia clínica del paciente en cuestión, de conformidad con la Ley 41/2002 y deberá actualizarse con las nuevas pruebas o novedades. En lo que se refiere a esta información, a diferencia de la tratada con meros fines epidemiológicos, se va a poder tratar de la forma prevista por la Ley de Autonomía del Paciente y deberá conservarse por los plazos previstos en aquella, incluso sin ser información agregada.

4. Finalización de la sesión

La sesión finaliza sobre las 11:30 horas con agradecimiento del Presidente a las personas ponentes y asistentes y, de nuevo, destacando el papel fundamental de los profesionales de la privacidad y los delegados de protección de datos, reclamando la ayuda de la Agencia para seguir poniendo en valor su figura y ayudar a difundir y concienciar en las administraciones públicas y

en el sector privado que se debe contar con estos perfiles con el fin de ayudar al desarrollo de iniciativas desde la legalidad.