TRATAMIENTO DE DATOS DURANTE LA CRISIS DEL COVID-19: ANÁLISIS COMPARATIVO DE LAS POSTURAS ADOPTADAS POR LAS AUTORIDADES COMPETENTES EN MATERIA DE PROTECCIÓN DE DATOS DE LOS PAÍSES EUROPEOS MÁS AFECTADOS

20 de marzo de 2020

El pasado 11 de marzo de 2020, la Organización Mundial de la Salud (OMS) declaró a través de su director general, Tedros Adhanom Ghebreyesus la propagación del Coronavirus Covid-19 como una pandemia debido a la alta cantidad de personas infectadas y muertes que, hasta la fecha, ha causado el virus SARS-CoV-2.

De conformidad con datos de la OMS, se estiman que a fecha 19 de marzo de 2020 Italia, con 41.035 infectados; España, con 18.077 infectados; Alemania, con 15.320 infectados y Francia, con aproximadamente 11.000 infectados son los países europeos más afectados por la irrupción del Covid-19.

En este sentido, los gobiernos de los anteriores países, en vista del incremento considerable de contagiados a finales de febrero y en especial, durante las primeras semanas de marzo, implementaron las medidas oportunas con el fin de frenar el número de contagios diario y evitar de esta manera el colapso de sus respectivos sistemas sanitarios. En particular, en fecha 31 de enero de 2020, Italia declaró el estado de emergencia, seguido de España, quien en fecha 13 de marzo, es decir, con aproximadamente un mes y medio de retraso con respecto a los italianos, declaró el estado de alarma. Por otro lado, en fecha 16 de marzo, el estado de Baviera oficialmente declaró la presente crisis sanitaria como un caso de emergencia, siendo el primer estado germano en hacerlo. Por último, en fecha 17 de marzo de 2020 se declaró el estado de emergencia, entrando el mismo en vigor durante los próximos 12 días, si bien el mismo deberá ser declarado por decreto en el Parlamento, que desde ayer y durante el transcurso del día de hoy aprobará la misma.

Por otro lado, Reino Unido, cuya política de confrontación a la pandemia del Covid-19 ha sido radicalmente distinta a la de los anteriores países, sin perjuicio de que durante esta semana desde Downing Street se han dado indicios que apuntan

al abandono inminente de las mismas, (en estos últimos días se han cerrado múltiples estaciones de metro y en fecha del presente artículo entra en vigor la decisión que obliga a todos los colegios a cerrar), el número de infectados a fecha 19 de marzo ascendía a 3.269.

En vista de lo anterior, y ante la irrupción de medidas en particular de carácter laboral, como el teletrabajo, así como la implantación de tomas de temperatura diaria de los empleados y/o visitantes con carácter previo a su entrada a las instalaciones de la empresa, deviene necesario dibujar una comparativa entre las distintas posturas de las agencias de protección de datos (o autoridades de control) de los países más afectados. En primer lugar, porque muchas de las prácticas implementadas pueden conllevar el acceso a datos de carácter especial o sensibles, como son entre otros los datos de salud. En segundo lugar, porque estas prácticas a su vez pueden suponer una disminución en lo que respecta a las medidas de seguridad técnicas y organizativas que deben adoptarse para garantizar la protección de los mismos. Y por último, porque el Considerando 123 y el artículo 61 del Reglamento (UE) 2016/679 (en adelante, "RGPD") reflejan el deber de cooperación de las autoridades de control, quienes no solo lo harán entre ellas, sino también con la Comisión Europea con el fin de supervisar la aplicación de las disposiciones adoptadas de conformidad con el RGPD y contribuir a su aplicación coherente en toda la Unión.

Por tanto, resulta razonable afirmar que, en virtud del principio de asistencia mutua del RGPD, la realización de un análisis comparativo de las posturas de las Autoridades de Control de los países más afectados pueda predecir el desenlace o las pautas que adoptarán aquellas autoridades de control que se encuentren en países europeos menos afectados por el virus.

En este sentido, y habiendo analizado las posturas de la Agencia Española de Protección de Datos (en adelante, "AEPD"); la Comission National de l'Informatique et des Libertés francesa (en adelante, "CNIL"); el Garante per le Protezione dei Dati Personali italiano (en adelante, el "Garante de Privacy"); la Datenschutzkonferenz alemana (en adelante, "DSK") y la Information Commissioners Office británica (en adelante, "ICO"), se pueden derivar las siguientes conclusiones en lo que respecta al marco de la protección de datos personales:

1. Italia: la implementación de recientes medidas gubernamentales habilitan al tratamiento de datos personales de salud sin consentimiento, pero deberán en cualquier caso realizarse con atención a las pautas del Garante de Privacy

Como país europeo más afectado, la irrupción del Covid-19 en el país transalpino supuso que el Garante de Privacy fuese la primera autoridad de control de las analizadas en el presente artículo a tomar conciencia de la situación y emitir sus recomendaciones.

De esta forma, en fecha 2 de marzo de 2020, el Garante de Privacy emitió un comunicado a través de su página web oficial en la que destacaba la necesidad de que tanto entidades públicas como privadas siguiesen en todo momento las instrucciones del Ministerio de Sanidad y demás autoridades competentes. El Garante de Privacy buscaba evitar la propagación de la realización de actividades del tratamiento que no reunían las garantías de la normativa de privacidad.

En dicho comunicado, el Garante de Privacy se mostraba particularmente contrario a la recogida de los datos de salud de empleados de forma sistemática y generalizada por parte de empresarios, inclusive mediante la puesta a disposición de mecanismos tales como la realización de investigaciones específicas dirigidas a ciertos empleados, inclusive la recogida de información sobre la patología relativa a los mismos y/o a sus contactos más cercanos. En particular, la autoridad de control italiana recordaba la obligación de los empleados de informar a sus empresarios de cualquier riesgo que pudiese comprometer su salud y/o seguridad pudiendo en este sentido el empresario facilitar la forma de comunicación o pudiendo el empresario solicitar a aquellos empleados que pudiesen estar más expuestos a la realización de una visita médica extraordinaria.

Por tanto, y a fecha 2 de marzo de 2020, el Garante de Privacy se mostraba firme en defender que la investigación y recopilación de información sobre la sintomatología del Covid-19, así como sobre los desplazamientos recientes de cada persona física, es responsabilidad de los

profesionales del servicio médico. A tal efecto, el Garante en su comunicado hacía una llamada a todos los Responsables del tratamiento con el fin de evitar la toma de decisiones propias que pudiesen implicar un tratamiento de datos personales, inclusive de salud, sobre usuarios y empleados, cuando tales decisiones o iniciativas no habían sido previamente reguladas mediante normativa u ordenadas a través de las autoridades competentes.

Pues bien, en fecha 9 y 14 de marzo, ante el avance desenfrenado del Covid-19, tuvieron lugar las principales regulaciones y medidas en el sentido que indicaba el Garante de Privacy. En primer lugar, en fecha 9 de marzo entró en vigor el Decreto, cuyo artículo 14.1 reflejaba la primera de las desviaciones con respecto al comunicado del Garante de Privacy: la posibilidad de que individuos ajenos al esquema de sanidad y administración pública pudiesen a su vez llevar tratamientos de datos necesarios en el desempeño de las funciones que se les atribuye dentro de la emergencia del Covid-19. Conviene no obstante recordar que la disposición únicamente implica a aquellos sujetos encargados de la vigilancia y de la aplicación de las medidas contenidas en el artículo 3 del Decreto-Ley de 23 de febrero de 2020 nº 6.

Por último, en fecha 14 de marzo, los sindicatos y los empresarios de Italia suscribieron un protocolo en acuerdo con el gobierno italiano con el fin de prevenir nuevos contagios en los puestos de trabajo que incluye 13 medidas, entre las que se destacan la obligación de quedarse en casa por parte de todo empleado cuya temperatura corporal supere los 37,5 grados; la realización de controles de temperatura corporal por parte de los empresarios a los empleados antes de la entrada en el centro de trabajo; o el procedimiento a seguir en caso de presentar síntomas dentro del centro de trabajo.

Por tanto, y en aplicación del comunicado del Garante de Privacy del 2 de marzo de 2020, la entrada en vigor de, por un lado, el decreto ley 14/2020, y por otro, la suscripción de un acuerdo entre sindicatos y empresarios que cuenta con la aprobación del gobierno, podrán hacer posible la legitimación del tratamiento de datos personales en bases de legitimación tales como el interés público (artículo 6.1.e RGPD), y/o el cumplimiento de obligaciones legales (artículo 6.1.c RGPD) en el caso de todas aquellas entidades sujetas a lo dispuesto en el artículo 14 del Decreto Ley anterior.

Por tanto, los tratamientos efectuados por los Responsables del Tratamiento dentro del ámbito comentado en el párrafo anterior cumplirían con la postura del Garante de Privacy, puesto que se trata de iniciativas reguladas u ordenadas a través de las autoridades competentes, si bien se deberá garantizar en cualquier caso el cumplimiento de las garantías que ofrece el RGPD sobre los tratamientos efectuados durante el periodo de emergencia sanitaria.

2. Francia: Legitimación del tratamiento de datos de salud en la prevención de riesgos laborales pero respetando los principios del artículo 5 RGPD y de proporcionalidad.

Sin perjuicio de que la implementación de las principales medidas en atención a la emergencia sanitaria y la efectiva declaración del estado de emergencia en Francia no han tenido lugar hasta esta semana, en fecha 6 de marzo de 2020, y en vista de la extensión del virus por Europa, la CNIL emitió un comunicado que de forma práctica recuerda a los responsables del tratamiento cuales son las principales pautas a tener en cuenta en lo que respecta a los tratamientos de datos personales que se deriven de la situación del Covid-19, así como qué tratamientos hacer y cuáles no hacer.

Entre la lista de tratamientos que no se deberán llevar a cabo, la CNIL indica, entre otros: (i) restricciones de viaje y reuniones; (ii) el cumplimiento de medidas de higiene; o (iii) la recopilación de datos de salud que vayan más allá de la gestión de la presunta exposición al virus, recordando en este sentido la autoridad de control francesa que los datos de salud son objeto de protección tanto por el RGPD (artículo 9) como por las disposiciones del Código de Salud Pública ("Code de la santé publique"). La finalidad de la autoridad de control francesa en la indicación de las anteriores pautas como medidas a evitar parece ser la protección de la intimidad de las personas físicas, tanto afectadas como no.

Sin perjuicio de lo anterior, y con respecto al punto (iii), la CNIL pone diversos ejemplos sobre lo que podría ser considerado un tratamiento que "va más allá" de la gestión de la exposición al

virus. En particular, la CNIL señala iniciativas como la recopilación sistemática y generalizada, mediante consultas generales o solicitudes individuales, que busquen detectar posibles sintomatologías presentes en un empleado o usuario. En este sentido, la CNIL especialmente identifica prácticas como la toma diaria y obligatoria de temperatura corporal de cada empleado y usuario, así como su posterior envío a su superior jerárquico, como una práctica a evitar por las razones anteriores (posible vulneración de la intimidad del empleado sujeto al examen de temperatura; carácter generalizado y sistemático de la medida, e incluso, vulneración de los principios de protección de datos del artículo 5 del RGPD, en tanto el acceso por parte del superior inmediatamente jerárquico a datos de salud no es indispensable para llevar a cabo la finalidad de las medidas).

Sin embargo, la CNIL, por otro lado, avala la posibilidad de que el empresario pueda sensibilizar a sus empleados para que estos comuniquen a las autoridades sanitarias cualquier información en relación a un posible contagio; así como poner en marcha métodos de prevención tales como el trabajo a distancia, entre otros. En particular, la CNIL se refiere al artículo L.4121-1 del Código de Trabajo ("Code du Travail") francés para señalar que el empresario es responsable de la salud y seguridad de sus empleados, debiendo por tanto ser este quien, en materia de prevención de riesgos laborales, ponga en marcha las anteriores medidas, así como establezca una organización (por ejemplo, a través de un plan de continuidad de la actividad) y medios adecuados con el fin de prevenir contagios y reducir el impacto en la actividad económica.

De igual manera, la CNIL también se refiere a las obligaciones que deben cumplir los datos en virtud del Código del Trabajo, y en particular, la referida en el artículo L.4122-1 que obliga al trabajador a poner en práctica los medios disponibles por el empresario con el fin de preservar la seguridad y la salud, tanto propia como de terceros. En este sentido, la CNIL recuerda que los empleados deberán informar a su organización en caso de sospecha de contacto con el virus, quien, en caso de emergencia, podrá registrar: (i) la fecha y la identidad de la persona sospechosa de haber sido contagiada y (ii) las medidas adoptadas por parte de la organización en materia de prevención (contención, teletrabajo, etc.)

La anterior información recogida por el empleador podrá a su vez comunicarse a las autoridades sanitarias en cuestión, siendo estas las únicas capacitadas para adoptar las medidas adecuadas a la situación concreta. Por tanto, la CNIL coincide con la postura del Garante de Privacy reflejada en el apartado anterior cuando se refiere a que han de ser las autoridades sanitarias quienes indiquen las medidas y directrices adecuadas a la situación a seguir por los distintos responsables del tratamiento.

3. Reino Unido: Adopción de una postura flexible sin perjuicio de la aplicación de los principios del artículo 5 RGPD y de proporcionalidad, además de suficientes garantías en materia de seguridad. Legitimación del tratamiento de datos de salud en la prevención de riesgos laborales.

En fecha 12 de marzo de 2020, la ICO emitió un comunicado y una guía para empresas en la que manifestaba su postura con respecto a las implicaciones en materia de protección de datos que podría tener la irrupción del Covid-19.

Pues bien, y al margen de la inicial indiferencia y despreocupación que mostró el gobierno británico con respecto al Covid-19, la ICO en sus directrices si se plantea las consecuencias económicas que el virus podría tener en las islas británicas.

En este sentido, la ICO se muestra significativamente más flexible que en anteriores ocasiones, abandonando por primera vez la postura de autoridad de control estricta que impuso las sanciones más altas a nivel europeo hasta la fecha a British Airways y Marriot, que ya analizamos en su día, para expresamente anunciar que entiende que las empresas desvíen sus recursos de 'compliance' a aquellas áreas más afectadas por el impacto económico, e indicando que no penalizarán a aquellas organizaciones que entiendan que deben priorizar otras áreas durante la actual situación. Asimismo, la ICO también comunica que durante la pandemia pueden existir retrasos razonables en la atención a los requerimientos y/o solicitudes de información que se realicen.

La ICO, a su vez, también indica que la normativa de protección de datos no debe prevenir la rápida comunicación de datos por parte de las organizaciones, si bien las mismas habrán de realizarse en atención al principio de proporcionalidad.

Asimismo, se recuerda en el comunicado que tanto el gobierno como el servicio nacional de salud británico ("NHS") disponen de la potestad para enviar mensajes relacionados con la salud pública, al entender la ICO que los mismos no tienen fines de mercadotecnia directa que si protege la normativa en materia de servicios de sociedad de la información británica. Por tanto, el envío de dichos mensajes por parte de tales entidades será legítimo y no necesitará del consentimiento expreso del interesado, al ampararse en el interés público, en este caso, relacionado con la salud pública.

Asimismo, y en lo que respecta al ámbito de las relaciones laborales, la ICO si muestra una postura más estricta, recordando a los responsables del tratamiento que, si bien la normativa no es una barrera contra el teletrabajo en sí, se deben aplicar las mismas medidas de seguridad técnicas y organizativas que en el transcurso normal de la jornada laboral. Por tanto, la ICO, consciente de la situación extraordinaria que ha ocasionado el Covid-19, no avala la posibilidad de que decaiga el nivel de la seguridad que mantienen las organizaciones sobre los datos personales, entendiendo, a tal efecto, que la situación de emergencia sanitaria no debe tener como consecuencia el aumento en las posibilidades de que la información se pudiese ver comprometida a accesos ilícitos por parte de terceros.

Por último, y en lo que respecta al tratamiento de datos personales relativos a la salud de empleados y visitantes, la ICO adopta una posición similar a la del CNIL, indicando a las empresas que, en aplicación del Health and Safety at Work Act 1974, los empresarios tienen la obligación de garantizar la salud y seguridad de sus empleados.

Sin embargo, la ICO recuerda que la recopilación de cualquier dato personal debe estar sujeta al cumplimiento, en todo caso, de los principios de minimización del artículo 5 RGPD, así como del principio de proporcionalidad. A tal efecto, la ICO recuerda que, si bien el empresario tiene el deber de informar a sus empleados sobre los casos que puedan ocurrir dentro de su organización, no debe proporcionarse más información de la estrictamente necesaria para lograr el fin de prevención que busca la organización dicha comunicación. En este sentido, la ICO hace un llamamiento a las empresas a que, en aplicación del principio de minimización, no identifiquen a la persona infectada siempre y cuando no sea necesario.

En lo que respecta a la posible recopilación de datos de salud a empleados y visitantes en el momento de acceder a las instalaciones, la ICO entiende como razonable que se pueda recopilar información sobre los destinos recientes a los que se haya desplazado el interesado en cuestión y/o sobre si experimenta síntomas del Covid-19. En caso de que se deban recopilar datos de salud específicos, la ICO únicamente indica que los mismos habrán de recopilarse conforme a las garantías que ofrece la normativa, no ofreciendo, por tanto, suficientes garantías sobre las bases de legitimación en las que los mismos se podrían amparar, entre otras. Asimismo, y con el fin de minimizar el número de interesados sobre los que se recopila información, la ICO avala la posibilidad de que se recomiende al visitante considerar las directrices que pueda publicar el gobierno antes de desplazarse a la oficina.

4. España:

Como ya pusimos de manifiesto en nuestro anterior Boletín relativo a las implicaciones en materia de protección de datos que ha tenido la declaración, en fecha 13 de marzo, del estado de alarma declarado por el gobierno español ante la crisis sanitaria del Covid-19, en fecha 12 de marzo de 2020, es decir, un día antes de la declaración del estado de alarma, el gabinete jurídico de la AEPD, en vista de la calificación del Covid-19 como pandemia, emitió un informe jurídico en el que valoró la aplicabilidad de la normativa de protección de datos ante la inminente crisis sanitaria.

En particular, la AEPD indicó que, con independencia de la declaración del estado de alarma, la normativa de protección de datos seguiría resultando de aplicación, en tanto el objetivo de la misma es salvaguardar el derecho fundamental a la intimidad recogido en el artículo

18.4 de la Constitución y no existían razones ni se han adoptado hasta la fecha medidas que puedan permitir determinar la suspensión de derechos fundamentales en este sentido.

Asimismo, en su informe, la AEPD, al igual que la DSK alemana, también reconoce que existen múltiples bases de legitimación alternativas al consentimiento en las que justificar el tratamiento de los datos. En particular, la AEPD se refiere a la posibilidad de amparar el tratamiento de los datos personales en las bases del artículo 6.1.c) RGPD (Cumplimiento de una obligación legal) en especial a aquellos tratamientos de datos que realiza el empresario sobre sus empleados en virtud de la normativa de prevención de riesgos laborales y, en particular, del deber que impone dicha normativa al empresario de garantizar la seguridad y salud de los empleados. Asimismo, la AEPD también reconoce como bases de legitimación habilitantes para el tratamiento de datos personales de terceros aquellas contenidas en los artículos 6.1.d) RGPD (protección de los intereses vitales del interesado u otras personas físicas) y 6.1.e) RGPD (misión realizada en interés público). Recuerda, no obstante, la AEPD que, en el caso de las bases de legitimación señaladas en el 6.1.c) y 6.1.e) RGPD, estas habrán de ser establecidas por el Derecho de la Unión o el Derecho de los Estados miembros, como, por ejemplo, por medio de la normativa de prevención de riesgos laborales. Esta última habilitaría, en este caso, al empleador a tratar datos personales debido a la disposición que obliga a la salvaguarda de la seguridad y salud del empleado. Sin embargo, en lo que se refiere a la base de legitimación del 6.1.d) RGPD, la AEPD recuerda que la misma no requiere de dicha obligación, pudiendo emplearse para proteger, además de los intereses vitales del interesado, los de terceros afectados.

Asimismo, y en lo que se refiere al tratamiento de datos personales que puedan incluir categorías especiales de datos, como pueden ser los datos de salud, la AEPD indica que los responsables del tratamiento deberán contar con una base de legitimación adicional a la del artículo 6 RGPD, debido a que el artículo 9.1 RGPD contempla la prohibición del tratamiento de cualquier dato de categoría especial, salvo que medie alguna de las excepciones que se indican en el apartado 9.2 RGPD. En este sentido, la AEPD identifica hasta 5 posibles escenarios aplicables a la situación actual: (i) la necesidad de tratar los datos para el cumplimiento de obligaciones en el ámbito del derecho laboral (artículo 9.2.b RGPD) y que resulta de especial aplicación a los empleadores. Estos, como sujetos obligados por la normativa, deberán establecer las medidas necesarias para cumplir con su deber general de garantizar la salud y seguridad de sus empleados; (ii) cuando el tratamiento de los datos es necesario para proteger los intereses vitales del interesado cuando este no esté capacitado para dar su consentimiento (artículo 9.2.c RGPD); (iii) Cuando el tratamiento es necesario por razones de un interés público esencial (artículo 9.2.g RGPD); (iv) Cuando el tratamiento devenga necesario con fines de medicina preventiva o laboral o diagnóstico médico (artículo 9.2.h RGPD); y (v) cuando el tratamiento sea necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria.

No obstante, la AEPD, al igual que indica la CNIL, y en particular, el Garante de Privacy, recuerda, a su vez, que la existencia de las bases de legitimación anteriores no implica que la totalidad de empresas puedan, a modo de iniciativa propia, hacer uso de las anteriores excepciones para legitimar cualquier tratamiento de datos personales, inclusive datos de salud. En este sentido, la AEPD recuerda por medio de la normativa general de salud pública, compuesta principalmente por la Ley Orgánica 3/1986, de Medidas Especiales en materia de Salud Pública, y la Ley 33/2011, General de Salud Pública, que será en todo caso la autoridad sanitaria quien, ante casos de epidemia, adoptará las medidas convenientes, correspondiendo a tal autoridad la protección de los intereses de las personas físicas y debiendo ser los responsables del tratamiento quienes sigan las instrucciones que les otorguen las autoridades competentes. En particular, la AEPD enfatiza, en aplicación del considerando 54 del RGPD, la importancia de que los datos personales que se tratan en el contexto actual por motivos de salud pública no sean facilitados a terceros, como otros empresarios, para que los puedan tratar con otros fines.

Por último, conviene recordar que, por medio de la Disposición Adicional 3ª del Real Decreto 463/2020, de 14 de marzo, por el que se declara

el estado de alarma para la gestión de la situación de crisis sanitaria ocasionada por el Covid-19, los procedimientos ante la AEPD quedan suspendidos hasta la efectiva pérdida de vigencia del Real Decreto, sin perjuicio de lo dispuesto en el apartado 3 de dicha Disposición Adicional 3ª, que otorga la facultad al órgano competente de acordar, mediante resolución motivada, las medidas de ordenación e instrucción estrictamente necesarias para evitar perjuicios graves en los derechos e intereses del interesado. En este sentido, y durante el transcurso del estado de alarma, la AEPD adoptaría una postura de inactividad similar a la declarada por la ICO en su comunicado. Si bien dicha inactividad, en el caso de la primera, se declara en aplicación de una norma jurídica, y, en el caso de la segunda, de forma voluntaria en atención a las amenazas de carácter sanitaria que, desafortunadamente, existen en Europa actualmente.

5. Alemania: Tratamiento lícito de datos sin perjuicio de atender al principio de proporcionalidad y disponiendo de legitimación. Deber de supresión de los datos tras el fin de la situación extraordinaria.

Por último, en fecha 13 de marzo de 2020, es decir, 3 días antes de la declaración por parte del estado de Baviera del caso de emergencia, la DSK, formada por las autoridades de control en materia de protección de datos que existen a nivel regional en Alemania, publicó sus directrices ante la emergencia del Covid-19.

En particular, el DSK indica a las empresas que los tratamientos de datos personales efectuados con la finalidad de prevenir el contagio del Covid-19 en el centro de trabajo están debidamente justificados, si bien las mismas deberán aplicar el principio de proporcionalidad en los tratamientos. En particular, la DSK indica que las organizaciones disponen de justificación adicional para llevar a cabo dichos tratamientos en los casos en que el empleado se haya desplazado a un área clasificada como "área de riesgo" y/o en los casos en los que se detecte un contagio. La DSK define como "área de riesgo" todas aquellas áreas expresamente indicadas por el Instituto Robert Koch, que es la institución federal en materia de investigación científica y salud pública especializada en la prevención de enfermedades y epidemias.

Pues bien, para llevar a cabo los tratamientos anteriores, la DSK indica que el tratamiento de datos de los empleados del sector público podría encontrar amparo en el artículo 6.1.e) RGPD (misión realizada en el interés público) y, en lo que respecta a los trabajadores ajenos a dichos sector, la base de legitimación se encontraría en el artículo 6.1.f) RGPD (interés legítimo en conjunto con las leyes laborales y sociales). Asimismo, en caso de que exista además, tratamiento de datos de salud, la base de legitimación adicional que ampararía a los empleadores a tratar dichos datos personales se encuentra en el artículo 9.2.b) RGPD (tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos en el ámbito del derecho laboral), como dictaminaba a su vez la AEPD en su informe jurídico. En este sentido, la DSK va más allá de la definición proporcionada por el artículo 9.2.b) RGPD anterior, indicando que la definición de "Derecho laboral" ha de incluir el derecho civil alemán.

En vista de lo anterior, la DSK parece adoptar las posturas reflejadas por las autoridades de control francesa, británica y española, indicando que es el deber del empleador en mantener la seguridad y salud de sus empleados la que permite el tratamiento de datos de sus propios empleados para los fines anteriormente indicados.

Adicionalmente, la DSK también reconoce como tratamiento legítimo las recopilaciones de datos personales en el sentido del párrafo anterior para los usuarios y/o visitas de terceros a las instalaciones de la misma. De esta manera, y de conformidad con la DSK, se autorizará el tratamiento de datos de salud, por parte de los responsables del tratamiento, con el fin de determinar si los usuarios y/o visitas han estado en un área de riesgo definida por el Instituto Robert Koch, o para verificar si el mismo está infectado con el Covid-19, inclusive aquellos casos en los que el visitante o usuario haya estado en contacto con una persona que ha dado positivo en Covid-19.

En el caso de que se traten datos personales relativos a visitantes/usuarios, la DSK entiende que el tratamiento de los mismos se podría basar, en el caso de las visitas a organismos públicos, en los artículos 6.1.c) RGPD (cumplimiento de una obligación legal) y 6.1.e) RGPD (misión en interés

público). En este sentido, y en relación con los datos de visitas a organismos no públicos, la DSK vuelve a indicar que será suficiente para amparar el tratamiento de los datos tomar como base de legitimación el interés legítimo (artículo 6.1.f) RGPD). Asimismo, y en caso de que se pudiesen tratar a su vez datos personales de salud, la base de legitimación que amparará el tratamiento de dicha categoría de dato especial será la base de legitimación del 9.2.i) RGPD (tratamiento necesario por razones de interés público en el ámbito de la salud pública como la protección frente a amenazas transfronterizas o para garantizar altos niveles de calidad y de seguridad de la asistencia sanitaria).

Por último, la DSK, al contrario que las anteriores autoridades de control, se refiere de forma expresa al ciclo íntegro del dato, al indicar que el cumplimiento del principio de proporcionalidad a su vez implica que, tras superar la situación extraordinaria actual causada por el Covid-19, los responsables del tratamiento deberán garantizar la supresión de los datos personales recabados para las finalidades de prevención anteriores. En este sentido, solo la AEPD, al referirse en su Informe al considerando 54 del RGPD que indica que los datos recogidos por motivos de salud pública no debe dar lugar a que terceros como empresarios los traten con otros fines, puede dejar entrever una intención en que los mismos sean suprimidos al finalizar la situación actual de emergencia y, por tanto, la finalidad principal por la que los mismos se recogieron y fueron tratados.

6. Conclusiones: Puntos en común y divergencias en las posturas de las autoridades de control y comunicado del 16 de marzo del Comité Europeo de Protección de Datos

En aplicación del principio de Asistencia mutua del artículo 61 RGPD que refleja el deber de cooperación que tienen las autoridades de control con el fin de aplicar de forma coherente el RGPD, y habiendo expuesto las posturas de las distintas autoridades de control en materia de protección de datos de los países con mayor número de afectados en fecha del presente artículo, junto con el Reino Unido, como país que inicialmente apostó por un modelo de estrategia radicalmente distinto al del resto de países, todo ello sin perjuicio del posible cambio de estrategia que pudiese tomar Downing Street los próximos días en atención a las últimas medidas tomadas, los Responsables del Tratamiento que traten datos personales para finalidades relacionadas con la prevención de contagios del Covid-19 deberán tener en cuenta los siguientes puntos:

i. En lo que respecta a la aplicabilidad de la normativa de protección de datos, las autoridades de control de los países analizados en el presente artículo dan por supuesto la aplicación de la normativa a la situación de emergencia sanitaria en la que vivimos actualmente. En particular, la AEPD cuestiona la aplicabilidad en su Informe Jurídico 0017/2020 avalando al aplicabilidad de las garantías del RGPD. En este sentido, la situación generada por el Covid-19 parece distar de ser una situación en la que se pudiese decretar como inaplicable la normativa de protección de datos;

ii. En lo que respecta a las distintas posiciones generales adoptadas por las autoridades de control, se han identificado hasta dos tipos de postura; por un lado, la reflejada por la ICO en su informe o por la AEPD a raíz de la entrada en vigor del Real Decreto 463/2020 de 14 de marzo, más flexible, en la que adquieren importancia otros factores en la lucha contra la situación de emergencia. La ICO, en particular, ha señalado que no penalizará a aquellas entidades que deban priorizar otras áreas en vista de la situación, asumiendo retrasos razonables en la atención a los requerimientos. La actividad de la AEPD, por otro lado, permanecerá inactiva en virtud de la Disposición Adicional 3ª, reduciéndose su actividad a aquellos casos que pueden presentar un perjuicio para los derechos del interesado, como también determina dicha Disposición Adicional. Por otro lado, una segunda postura, aplicable al CNIL y la DSK, sobre la que no existen indicios en sus comunicados de inactividad ante esta situación, si bien en los próximos días, la declaración de sus respectivos estados de emergencia podría cambiar el devenir de estas posturas;

iii. Asimismo, todas las autoridades de control coinciden en subrayar la importancia de que cualquier tratamiento de datos personales que se realice durante el estado actual de crisis sanitaria se efectúe con las

garantías ofrecidas por el RGPD y en atención al principio de proporcionalidad;

iv. En lo que respecta a las posibles bases de legitimación que pudiesen amparar el tratamiento de datos personales, la AEPD y la DSK indican la posibilidad de que el tratamiento de datos personales pueda efectuarse en las bases de legitimación reconocidas en los apartados c), d), e) y f) del artículo 6.1 RGPD. En este sentido, la DSK ofrece más garantías sobre la AEPD, indicando los casos específicos en los que aplica el uso de cada base de legitimación. Por su parte, la CNIL y la ICO se refieren a la normativa laboral y, en particular, al deber del empleador en garantizar la seguridad y salud de los empleados para, de forma implícita, subrayar que la base de legitimación recogida en el artículo 6.1.c) RGPD será igualmente válida para los tratamientos que se efectúen en tal sentido. Por su parte, la entrada en vigor con fecha 14 de marzo del protocolo suscrito entre empresarios y sindicatos italianos, que cuenta, además, con el apoyo del gobierno, contempla disposiciones que podrían dejar entrever la existencia de un interés vital (artículo 6.1.d RGPD) o de un interés público (artículo 6.1.e RGPD) que justifiquen el tratamiento de los datos sin necesidad de recabar el consentimiento;

v. En lo que respecta al tratamiento de datos de empleados con fines de prevención de riesgos por parte de los empleadores, la ICO, AEPD, DSK y CNIL se amparan en sus respectivas normativas de prevención de riesgos laborales como base para legitimar los tratamientos efectuados en este sentido. Por su parte, el Garante de Privacy no hace alusión a dicha normativa, si bien la entrada en vigor del protocolo suscrito entre sindicatos y empresarios, que cuenta con el apoyo del Gobierno italiano, deja entrever que se podrán efectuar tratamiento de datos personales a los empleados para, entre otras, garantizar la toma de temperatura como medida de prevención;

vi. En lo que respecta al tratamiento de datos personales de salud de los empleados, la AEPD y el DSK dejan entrever hasta 5 posibles excepciones contenidas en el artículo 9.2 RGPD que permitirían levantar la prohibición de tratar datos personales de categoría especial, como los de salud, que indica el artículo 9.1 RGPD. En lo que respecta a la CNIL, ICO y el Garante Privacy, sus respectivos comunicados e informes no hacen mención a ninguna excepción al artículo 9.1 RGPD concreta, si bien se desprende de su lectura que el tratamiento de datos personales de salud de empleados podrá encontrar cabida en las excepciones de los apartados b), g) o i) del artículo 9.2 RGPD;

vii. En lo que respecta a las comunicaciones de datos personales efectuadas a terceros, todas las agencias recuerdan la importancia de que los mismos puedan ponerse a disposición de las autoridades competentes, si bien la AEPD hace especial hincapié, mediante el análisis del considerando 54 del RGPD, en que los datos personales no se deberán divulgar a otros terceros, como empresarios, para que los puedan tratar con finalidades distintas;

viii. En lo que respecta precisamente a la autoridad competente, la AEPD y la CNIL señalan a las autoridades sanitarias como las autoridades competentes que se encargan de la gestión de directrices y de la emisión de instrucciones a seguir por los distintos responsables del tratamiento. De igual forma, el Garante Privacy también señala a las autoridades sanitarias como las competentes, si bien, el término de autoridad competente ha podido verse incrementado por medio del artículo 14 del Decreto Ley 14/2020 que permite a individuos ajenos al esquema de sanidad llevar a cabo tratamientos de datos en el desempeño de las funciones que se les atribuye dentro del estado de emergencia del Covid-19. Por su parte, la ICO de forma implícita también parece reconocer a las autoridades sanitarias como las competentes en la gestión de tratamientos efectuados en base al Covid-19, si bien la autoridad de control británica da mayor control a los responsables para que dentro de lo razonable, y en aplicación de las garantías y del principio de proporcionalidad, determinen sus tratamientos. Sin embargo, la ICO reconoce el envío de mensajes por parte de las autoridades sanitarias relacionados con la salud pública como práctica excluida del ámbito de aplicación de la normativa de

servicios de la sociedad de la información, al no poder ser considerados los mismos como prácticas de marketing; Por último, el DSK no hace referencia en su comunicado a las autoridades de control, limitándose en tal sentido a indicar qué tratamientos son legítimos, en qué escenarios y cuáles son las bases de legitimación que amparan dichos tratamientos;

ix. En el caso del tratamiento de datos personales de visitantes, la AEPD y la ICO autorizan al tratamiento de datos a los visitantes, siempre y cuando se respeten los principios del artículo 5 RGPD y de proporcionalidad. La AEPD, en particular, hace alusión a las obligaciones que asume el empresario por virtud de la normativa de prevención de riesgos laborales para, adicionalmente, justificar un posible tratamiento a visitantes. Por su parte, el Garante Privacy, en su comunicado, parecía restringir la toma de decisiones por parte de responsables del tratamiento a modo de iniciativa propia. En este sentido, el Garante Privacy indicaba que la facultad para tratar los datos corresponde a las autoridades sanitarias. Sin embargo, la entrada en vigor en fecha 14 de marzo del protocolo anteriormente analizado puede suponer un cambio en este sentido, pudiéndose de esta manera tratar datos de visitas con el fin de cumplir con la totalidad de las disposiciones que adquieren los empresarios por medio del protocolo. La DSK, por otra parte, justifica el tratamiento de datos de visitantes siempre y cuando se encuentre amparado en el supuesto anteriormente analizado, con fines de verificación y prevención. En lo que respecta al CNIL, sin embargo, la práctica de tratamientos generalizados o sistemáticos, y aquellos que resulten invasivos para la intimidad, podrían tener un riesgo, debiendo, en tal sentido, adoptar el responsable del tratamiento una postura más informativa. Sin perjuicio de lo anterior, y siempre y cuando se lleven a cabo las medidas oportunas y las garantías adecuadas para que el tratamiento no pueda considerarse sistemático o generalizado, el tratamiento de datos personales de visitantes podría encontrar justificación. En cualquier caso, resulta interesante decir que, sin perjuicio de las opiniones anteriores, los responsables del tratamiento deberán en cualquier caso informar de los tratamientos a efectuar en la forma que indica el artículo 13 RGPD.

x. En lo que respecta a la aplicación de medidas de seguridad, la ICO indica de forma expresa en su comunicado que la adopción de medidas como el teletrabajo no implica una reducción justificada en la adopción de medidas de seguridad técnicas y organizativas para la adecuada protección de los datos personales;

xi. En lo que se refiere al final del ciclo del dato, todas las autoridades de control hacen referencia, de forma implícita, a que el tratamiento de los datos durante la presente situación, y con fines relacionados al Covid-19, deberá realizarse conforme al principio de proporcionalidad para que se entienda como lícito. Por otro lado, dos son las autoridades de control que se refieren en más detalle a la posible supresión de los datos. Por un lado, la AEPD que indica que los datos personales no deben mantenerse por más tiempo del estrictamente necesario. Y por otro, la DSK alemana que si indica la necesidad, por parte de los responsables, de garantizar que los datos han sido debidamente suprimidos.

Por último, en fecha 16 de marzo, el Comité Europeo de Protección de datos publicó, asimismo, su opinión en lo que respecta al tratamiento de datos personales en el contexto del Covid-19.

El comunicado centraliza la mayor parte de las opiniones de las autoridades de control aquí analizadas y contrastadas. En particular, el Comité indica que el RGPD establece las bases legales para permitir que tanto empleadores como autoridades competentes de salud pública traten datos personales en el contexto de epidemias, como la ocasionada por el Covid-19, sin la necesidad de recabar el consentimiento por parte del interesado. En particular, el Comité, como ya lo hicieran la DSK o la AEPD, se refiere a la posibilidad de legitimar los tratamientos efectuados en los artículos 6.1.d) y e) RGPD, así como la posibilidad emplear el artículo 6.1.c) RGPD en caso de que el tratamiento sea necesario para cumplir con una obligación legal.

Sin perjuicio de lo anterior, el Comité también recuerda que la posibilidad de amparar el tratamiento en bases de legitimación adicionales no puede impedir, por un lado, la aplicación de las medidas de seguridad acordes a la evaluación del riesgo concreto que tiene cada actividad del tratamiento y, por otro lado, el cumplimiento del deber de información que mantienen los responsables del tratamiento con sus interesados.

En este sentido, puede resultar conveniente, especialmente si se tratan datos personales de salud, que, con carácter previo a la realización de un tratamiento de datos personales con finalidades de prevención, se realice una evaluación de impacto sobre el tratamiento con el fin de determinar y mitigar el posible impacto del tratamiento en los derechos y libertades de los interesados.

Departamento: Propiedad Intelectual y Nuevas Tecnologías
Contactos:
Joaquín Muñoz – Jmunoz@ontier.net
Álvaro Vidal – Avidal@ontier.net