FACULTAD DE CIENCIAS SOCIALES Y JURÍDICAS

GRADÓ EN DERECHO

Universidad de Jaén

Facultad de Ciencias Sociales
y Jurídicas

LA PROBLEMÁTICA DE LA PROTECCIÓN DE DATOS ANTE LA PANDEMIA.

Alumna: María Belén Romero Cámara

Índice

Índice de abreviaturas

- Ley de protección de datos de carácter personal (LOPD)
- Real Decreto 1720/2007 (RLOPD)
- Tribunal constitucional (TC)
- Ley orgánica 5/1992, de 29 de octubre de regulación del tratamiento automatizado. . . (LORTAD)
- La agencia española de protección de datos (AEPD)
- Ley de Prevención de Riesgos Laborales (LPRL)
- Centros de Atención Primaria (CAPs)
- reglamento general de protección de datos (RGPD)
- la ley organiza de protección de datos y garantía de los derechos digitales (LOPDGDD)

- **RESUMEN ESPAÑOL**

La pandemia COVID-19 ha generado impactos sociales y políticos adicionales a los estrictamente sanitarios, llevando a que los países en el contexto principal decretaran los estados de emergencia, la limitación de manera temporal algunos derechos y libertades civiles, para preservar la vida y salud de los ciudadanos; y de otra parte, han acelerado la transformación digital con el desarrollo y uso de herramientas tecnológicas para complementar las medidas de salud pública. Diversos organismos internacionales han expresado su preocupación respecto a la vulneración del derecho a la protección de datos personales en este nuevo escenario, e incluso han propuesto lineamientos éticos a tener en cuenta. En mi trabajo de fin de grado, analizare el ámbito de la ley de protección de datos y analizaremos diferentes puntos y preguntas de la pandemia respecto a los derechos fundamentales.

- **RESUMEN INGLES**

The COVID-19 pandemic has generated social and political impacts in addition to those strictly health, leading cuntries in the main context to decree states of emergency, temporarily limitin some rights and civil liberties, to preserve the life and health of the citicens; and on the other hand, they have acceleratesthe digitak transformation with the development and use of technological tolos to complement public health measures. Various international organizations have expressed their concern regarding the violation of the right to protection of personal data in this new scenario, and have even proposed ethical guidelines to be taken into account. In my final degree Project, i will analyze the field of data protection law and we will analyze diferrent points and questions of the pandemic regarding fundamental rights.

INTRODUCCIÓN

La protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental protegido por el artículo 18.4 de la Constitución española, que ya en el año 1978 previó que el uso la informática podría entrar en conflicto con la intimidad de las personas cuando dispuso que «la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos».

A nivel legislativo, la concreción y desarrollo de este derecho fundamental tuvo lugar en sus orígenes mediante la aprobación de la Ley Orgánica 5/1992, de 29 de octubre, reguladora del tratamiento automatizado de datos personales (LORTAD). Esta fue reemplazada por la Ley Orgánica 15/1999, de 5 de diciembre, de protección de datos personales (LOPD).

A nivel europeo, en los últimos años de la pasada década se intensificaron los impulsos tendentes a lograr una regulación más uniforme y garantista del derecho fundamental a la protección de datos en el marco de una sociedad cada vez más globalizada. Dichos impulsos desembocaron en la publicación del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos (RGPD), que entró en vigor en mayo de 2018. Aunque no era necesario un mayor desarrollo legislativo, pues los reglamentos europeos producen efecto directo en los ordenamientos jurídicos de los países miembro desde su publicación en el Diario Oficial de la Unión Europea, en España se quisieron precisar algunos aspectos del RGPD a través de la Ley Orgánica 3/2018, que el 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).

La pandemia del COVID-19 ha traído aparejada la adopción de nueva normativa estatal en distintas materias que nos obliga a tomar una serie de medidas extraordinarias de prevención y protección en el desarrollo de nuestra actividad, medidas que nos plantean ciertas dudas respecto a la protección de datos.

1. EL ÁMBITO OBJETIVO Y SUBJETIVO DE LA LEY ORGANIZADA 15/1999 DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL.

2.1 Objeto de ley

En primer lugar, este derecho a la protección de datos de carácter personal se encuentra regulado en primer lugar por la constitución. Exactamente en su artículo 18.1 hace especial referencia al honor e intimidad, conceptos de los cuales los encontramos directamente relacionados con la protección de datos.

En segundo lugar, el derecho a la protección de datos también los encontramos regulado por la ley organiza 15/1999, de 13 de diciembre, de protección de datos de carácter personal, y también en el Real Decreto 170/ 2007, de 21 de diciembre, por el que se aprueba el reglamento de desarrollo de la ley orgánica de protección de datos.

Respecto a la constitución Española, en su artículo 18.1, como hemos dicho anteriormente hace referencia al derecho al honor y a la intimidad, los cuales se encuentran relacionados con la aplicación de la LOPD, puesto que en su artículo 1 se establece la protección del tratamiento de los datos que afecten a estos dos derechos. En este artículo se dice: "*se garantiza el derecho al honor, a la intimidad personal y familiar y a la su propia imagen."*

Pardo Falcón[1] realizo un estudio analizando cada uno de estos derechos de una forma individual. En primer lugar, sobre el derecho al honor, dice que el tribunal constitucional, realiza una especial diferenciación entre los sujetos activos al derecho, que estos son los titulares del derecho, y los sujetos pasivos, que estos son aquellos capaces a incumplirlo.

Sobre los sujetos activos este TC indica que "*el derecho al honor, tiene en nuestra constitución un significado personalista, en el sentido de que el honor es un valor referido a personas individualmente consideradas"* (STC 107/88, de 8 de junio, FJ 2º).

Pardo Falcón tiene una especial consideración a esta expresión ya que considera que se afirma que los sujetos son las personas físicas, puesto que cuando se habla de personas jurídicas-publicas, el tribunal constitucional establece que es más correcto utilizar los términos de dignidad, prestigio y autoridad moral que de derecho al honor.

Por otra lado, el autor afirma que en lo que respecta al derecho a la intimidad, expresado como un derecho como tal, ha sido añadido a los diferentes textos constitucionales o jurídicos de distintos países de forma muy marginal, según ha afirmado el TC ello se debe a que " *el avance de la tecnología actual y el desarrollo de los medios de comunicación de masas ha obligado a extender esa protección más allá del aseguramiento del domicilio y del respeto de la vida privada".*

Por ello, dice afirmando que este derecho al igual que el derecho al honor, están ligados a la personalidad de la persona, por lo que solo afecta a la personas físicas. Según expresa Arenas Ramiro[2], el artículo 18 de la CE del que estábamos hablando antes, eleva a derechos fundamentales los derechos de la personalidad reconocidos y protegidos hasta entonces por el derecho civil.

[1] PARDO FALCON, J. (1992). "Los derechos del artículo 18 de la Constitución española en la jurisprudencia del Tribunal Constitucional". Revista Española de Derecho Constitucional, n.34, pp. 146 y 158.

[2] ARENAS RAMIRO, M. (2006). El derecho fundamental a la protección de datos en Europa, Valencia: Tirant lo Blanch, pp. 439-441.

De los dos derechos que se regulan en el artículo 18, el derecho a la intimidad es el que tiene una estrecha conexión con el derecho a la protección de datos personales. Ambos tienen como objeto la garantía de una esfera en la que el individuo puede desarrollarse libremente. Su evolución de este derecho siempre ha ido relacionada con el concepto de lo "publico", se ha entendido siempre como el derecho del individuo a estar solo.

Finalmente, Alzaga Villaamil[3] afirma bajo su opinión que los derechos al honor, a la intimidad personal y a la familiar, son derechos fundamentales que forman parte de los bienes de la personalidad, es decir, están vinculados a la vida privada, por lo que, por su carácter, no es de los que eventualmente puedan ser titulares las personas jurídicas.

Por otra parte, nos vamos a centrar ahora en la regulación de la protección de datos en la propia ley. La ley 15/1999, de 1 de diciembre, de protección de datos de carácter personal (LOPD). Según Martínez Martínez[4], se trata de una ley organiza, que solo era un proyecto para reformar la ley orgánica 5/1992, de 29 de octubre de regulación del tratamiento automatizado de datos de carácter personal, aunque finalmente se derogo.

La ley LOPD sustituye a la LORTAD después de que fuera derogada para así traspasar al ordenamiento interno los cambios introducidos en materia de protección de datos, por la directiva 95/46 CE sobre la protección de datos personales y garantizar y proteger las libertades públicas y sus derechos fundamentales de las personas físicas según Arenas Ramiro.

Fijándonos en la LOPD, el objeto de la ley viene contenido en su artículo 1, donde establece lo siguiente:" la presente ley orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas y especialmente de su honor e intimidad personal y familiar".

Según el preámbulo de la ley y del RLOPD, a raíz de esta definición se puede afirmar que la LOPD comprende, el tratamiento automatizado y el no automatizado de los datos de carácter personal.

Sobre el objeto de la ley que nos hemos referido anteriormente, se afirma que la LOPD nació con el objetivo de garantizar la protección de la intimidad de las personas frente a los abusos que puedan surgir en el tratamiento de los datos personales que estén en el algún fichero. Por otro lado, el autor Aparicio Salom[5] indica en su estudio que el objeto de la ley es la protección de la privacidad, la cual define como aquel ámbito d la vida privada que se ve afectado por la posibilidad de que las actuaciones cotidianas del ciudadano se observen y la información procedente de ellas se acumule y se conserve.

Esta protección de la privacidad que se garantiza supone una posibilidad real de que el interesado tenga el control de los usos y finalidades a que se destina dicha información relativa a su perfil a propósitos que el rechaza.

Finalizando, el desarrollo legislativo de la materia sorbe protección de datos que se recoge en el Real Decreto 1720/ 2007, de 21 de diciembre, por el que se aprueba el Reglamento de

[3] ALZAGA VILLAAMIL, O. (2017). Comentario sistemático a la Constitución española de 1978, Madrid: Marcial Pons, pp. 141-142.

[4] MARTÍNEZ MARTINEZ, R. (2008). "El Real Decreto 1720/2007, de 21 De diciembre, por el que se aprueba el reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. Aspectos clave." Revista Jurídica de Castilla y León, n. 16, pp. 257-293.

[5] APARICIO SALOM, J. (2002). Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal, Navarra: Aranzadi, p. 27.

desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

2.2 Ámbito subjetivo de aplicación

Podemos encontrar diferentes sujetos en la ley a los que se hace referencia o afecta de algún modo en algún momento. En primer lugar, encontramos a las personas físicas cuyos datos pueden ser objeto de tratamiento. En segundo lugar, encontramos al responsable del tratamiento y el encargado del tratamiento. Y por último, encontramos a la agencia española de Protección de Datos la cual se encarga del cumplimiento de la ley y de controlar su correcta aplicación.

2.2.1 Las personas físicas y jurídicas

En vista del artículo 1 de la LOPD, podemos ver que la ley sola e exclusivamente regula el tratamiento de datos personales de las personas físicas, dejando excluidas a las personas jurídicas. Este precepto de ley dispone lo siguiente: *"la ley tiene por objeto garantizar y proteger el tratamiento de datos personales, las libertades públicas y derechos fundamentales de las personas físicas".*

Por ello, entendemos como persona física los seres humanos que son capaces de adquirir y contraer obligaciones, y tienen unos atributos concretos, que son; personas jurídicas, capacidad, nombre, domicilio, estado civil, patrimonio y nacionalidad.

Respecto a las personas jurídicas se trata de unas entidades donde, sin tener existencia individual física, gozan de personalidad jurídica y están sujetas a derechos y obligaciones. Sobre estas personas jurídicas, el autor anteriormente mencionado Aparicio Salom[6] afirma que al estar excluidas, las personas jurídicas que aparecen en el artículo 35 del código civil[7], no tendrán las garantías establecidas en la ley.

Por otra parte, en la LOPD no se tiene en cuenta que las entidades jurídicas son solo instrumentos de los que se sirven las personas físicas para alcanzar determinadas finalidades, y es difícil que haya una separación del tratamiento informático de datos sobre la actividad empresarial, del tratamiento de otros datos de la esfera privada de los particulares. En definitiva, la ley hubiese podido profundizar un poco más en esta cuestión y reconocer a las personas jurídicas su titularidad del derecho al honor y a la intimidad informática en el tratamiento de unos datos que siempre acaban afectando al entorno personal.

La LOPD no define que debe entenderse por persona física identificable, ya que cuando se habla de persona física, se alude a personas físicas identificables o identificadas. En cambio, la directiva 95/46/ CE, en su artículo 2.a) establece que "*se considera personas físicas identificables a toda aquella persona cuya identidad pueda determinarse mediante un número de identificación o uno o varios elementos específicos, característicos de sus identidades físicas, fisiológica, psíquica, económica, cultural o social".*

Para que el tratamiento de los datos pueda ser realizado, siempre se va a requerir el consentimiento del interesado o afectado, como dice el artículo 3 de la LOPD, se entenderá por

[6] APARICIO SALOM, J. (2002). Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal, Navarra: Aranzadi, p. 39.

[7] Art. 35 CC: Son personas jurídicas, las corporaciones, asociaciones y fundaciones de interés público reconocidas por la ley. Y las asociaciones de interés particular, sean civiles, mercantiles o industriales, a las que la ley conceda personalidad propia.

interesado a aquella persona física titular de los datos que sean objeto del tratamiento, y por consentimiento toda aquella manifestación de voluntad, libre, inequívoca, especifica e informada, mediante la que el interesado consienta el tratamiento de los datos personas que le conciernen.

Una vez identificados dichos términos sobre el interesado, afectado y sus consentimientos, vamos a hacer referencia al tratamiento de datos referidos a los menores de edad. Estos menores de edad los encontramos regulados de una manera distinta, puesto que en la ley no existe un artículo específico que regule expresamente el tratamiento de los datos de los menores de edad. Por ello, hasta la aprobación del RLOPD de la LOPD, a estos menores se les aplicaba las normas generales previstas en la legislación. Después de su aprobación del RLOPD, ya aparece una regulación específica para la obtención y el tratamiento de estos datos. Exactamente es en su artículo 13 del RLOPD donde se encuentran establecidas las condiciones cobre el consentimiento de los menores para el tratamiento de sus datos personales.

También para la obtención de sus datos personales, hay una distinción entre los menores de hasta 13 años de edad y de los menores mayores de 14 años de edad. En el artículo 13.1 del RLOPD, se establece lo siguiente:" *podrá procederse al tratamiento de los datos de los mayores de catorce años con su consentimiento, salvo en aquellos casos en los que la ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela. En el caso de los menores de catorce años se requerirá el consentimiento de los padres o tutores".*

El autor Andreu Martínez[8], dice que se establece con ello una suposición de madurez a partir de los 14 años para el tratamiento de sus datos personales. Así establecer esta edad mínima para que el menor pueda consentir el tratamiento de sus datos personales, permite ofrecer una mayor seguridad jurídica.

También teneos que añadir que se fija una edad mínima de 14 años porque se considera que, como hemos señalado antes, se tiene una cierta madurez para obtener la capacidad de obrar en algunos actos. Además esta diferenciación de edad no solo se realiza en esta ley sino en otras.

Una vez sabiendo la diferenciación de grupos de los menores, vemos que en primer lugar, respecto a los menores de edad con menos de 14, Andreu afirma que el consentimiento del tratamiento de los datos personales deberán prestarlo los tutores legales o los titulares de la patria potestad. En cuanto los padres presten dicho consentimiento en las situaciones donde haya una normalidad familiar, se realizara de forma conjunta o por uno de ellos con el consentimiento expreso del otro, excepto en los actos cotidianos o de urgencia necesidad, que bastara con el consentimiento de uno de ellos. En los casos donde la situación familiar se encuentre en crisis matrimonial, en los actos cotidianos, uno de los progenitores el que suele vivir con el menor, podrá actuar e solitario, aunque se requerirá el consentimientos de ambos para las cuestiones que de considere más grave. En segundo lugar indica que cuando nos referimos al grupo de menores de edad mayores de 14 años, se considera que estos tienen capacidad para consentir el tratamiento de sus datos personales, incluidos los de carácter sensible, ya que el en el artículo 13 del LROPD, no hace falta la distinción entre qué tipo de datos pueden consentir ellos mismos, aunque de acuerdo con el artículo 13.2 del RLOPD, este consentimiento solo servirá para el tratamiento de los datos que le afectan.

[8] ANDREU MARTÍNEZ, M .B. (2013), La protección de datos personales de los menores de edad, Navarra: Aranzadi, pp. 67-92.

Un dato interesante respecto al consentimiento del menor, es que en términos generales, el RLOPD, deja claro que no se podrá utilizar a este menor para obtener información de su núcleo familiar exceptuando datos de identidad y dirección del representante legal.

Para que se pueda comprobar la veracidad del consentimiento de los representantes legales y la del menor, Andreu, afirma la existencia de mecanismos de prueba. Exactamente en el artículo 13.4 del RLOPD, es el responsable del fichero o del tratamiento quien debe llevar a cabo los procedimientos que garanticen la edad del menor y el consentimiento de los representados. Estos mecanismos de verificación deben otorgar una cierta fiabilidad, pero habrá que diferenciar entre diferentes mecanismos según el contexto en que se soliciten los datos.

Por último, el artículo 5 de la LOPD establece el deber de información al interesado. Por lo cual este deber se toma como más importante en el caso de los menores de edad, ya que si no se informa de manera correcta no se puede garantizar que el menor preste su consentimiento siendo consciente de para que lo presta.

Dicha información deberá realizarse, según la LOPD, de forma inteligible, con lenguaje sencillo, claro y adaptado al interesado, sobre todo si se trata de niños, es decir, utilizando palabras que puedan ser comprendidas por el menor.

2.2.2 El responsable del tratamiento y el encargo del tratamiento.

Otro aspecto a tener en cuenta en el ámbito subjetivo de aplicación de esta ley (LOPD), es el que afecta directamente al responsable del fichero o al tratamiento de los datos.

Primero, vamos a definir lo que entendemos por "responsable del tratamiento", que según el artículo 3.d) de la LOPD "es aquella persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento de datos".

Este responsable es diferenciado del encargado del tratamiento, según el autor Lesmes Serrano[9], en el que es el responsable quien decide sobre la creación del fichero de su finalidad y de su contenido, por lo tanto, es quien decide la realización de operaciones o procedimientos sobre los datos personales de un fichero del que no es titular. También afirma que en la LOPD no hay establecidas ningunas condiciones ni característica ni ninguna condiciones que el responsable de dicho tratamiento debería reunir, aunque se debe tratar de un perfil que tenga conocimiento tanto técnico como jurídico ya que existen varios casos que no define la ley y hay que interpretarlos.

Por último, en la definición de responsable del tratamiento, se establece que pueden ser responsable de este las personas físicas, los órganos administrativos y las personas jurídicas. Esta condición debe darse en cada sujeto para poder ser responsable del tratamiento. Por ello a la hora de asumir la responsabilidad, en las personas físicas no presentan problemas, puesto que pueden ser identificadas, aunque en las personas jurídicas, privadas o públicas o los órganos administrativos deben cumplir con unas obligaciones y responsabilidades, y así deberá nombrarse a una persona física que pueda ser identificadas y así hacerse cargo de las responsabilidades de las personas jurídicas.

[9] LESMES SERRANO, C. (2008). La Ley de Protección de Datos: Análisis y comentario de su jurisprudencia. Valladolid: Lex Nova, p 115.

Por segundo cuando hablamos del "encargado del tratamiento", entendemos según el artículo 3.g) de la LOPD, que es la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trata datos personales por cuenta del responsable del tratamiento.

Por lo tanto, nos encontramos ante una tercera persona, que por encargo del responsable del tratamiento, realiza operaciones o procedimientos técnicos, o carácter automatizado o no, del tratamiento de datos. Esto tenemos que completarlo con el artículo 5.i) del RLOPD, donde define al encargado del tratamiento como las personas físicas o jurídicas, públicas o privada, u órgano administrativo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento o del responsable del fichero. Esta figura la encontramos detallada en el RLOPD, en los artículos 20, 21 y 22.

Por otra parte, tenemos que fijarnos también en el artículo 12 de la LOPD, en el que establece que el cargo deberá estar formalizado por un contrato por escrito o de algún modo en que se acredite su celebración y contenido, y el encargado solamente podrá realizar el tratamiento de datos siguiendo las instrucciones ofrecidas por el responsable del tratamiento.

En estas dos figuras se deberá adoptar medidas de seguridad para el tratamiento de los datos, entendiendo por seguridad de los datos personales, aquellas medidas de carácter técnico, como establece el artículo 9 de la LOPD[10] a través de la adopción de mecanismos o dispositivos que eviten su alteración, perdida, tratamiento o acceso no autorizado. Se demuestra que nos referimos a una función técnica, por lo que se aplica la necesidad del responsable de tener conocimientos técnicos.

[10] Artículo 9 LOPD: "1. l responsable del fichero, y, en su caso, el encargado del tratamiento deberá adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural. 2. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones (…)"

2.2.3 La agencia española de protección de datos

La agencia Española de protección de datos es "la autoridad estatal de control independiente encargada de velar por el cumplimiento de la normativa sobre protección de datos. Garantiza y tutela el derecho fundamental a la protección de datos de carácter personal de los ciudadanos". Esta autoridad fue creada para velar por el respeto al derecho del honor, a la intimidad y a la propia imagen. Este ejerce de sus propias funciones para hacer cumplir el derecho y la normativa relacionada con la protección de datos, convirtiéndose así en una autoridad independiente y autónoma.

La AEPD es definida como un ente de derecho público que tiene una personalidad jurídica y una plena capacidad privada y pública, con la que actúa con total independencia de las administraciones públicas en el ejercicio de sus funciones.

Se relaciona este ente con el gobierno a través del ministerio de justicia y en él se cuenta con un presupuesto propio e independiente de los presupuestos generales del estado. Esto se regula por su propia normativa y por su propio marco normativo que está formado por las siguientes disposiciones:

- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (Título VI con rango de ley ordinaria).
- Real Decreto 1720/2007, por el que se aprueba el Reglamento de Desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
- Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

Las funciones principales que encontramos en la AEPD, son realizar las de registrar y resolver reclamaciones y denuncias, el registro y consulta de ficheros con su posterior autorización de transferencia, como también resolver cualquier consulta que planten los ciudadanos en su página.[11]

Además, la AEPD, realiza otra serie de funciones:

En relación con los afectados:

- Promover campañas de difusión a través de los medios.
- Atender a sus peticiones y reclamaciones.
- Velar por la publicidad de los ficheros de datos de carácter personal.
- Informar de los derechos reconocidos en la ley.

[11] Fuente: Agencia Española de Protección de Datos.

En relación con las normas:

- Informar preceptivamente los proyectos de normas de desarrollo de la ley orgánica de Protección de datos.
- Informar los proyectos de normas que indican en materia de protección de datos.
- Dictar las instrucciones y recomendaciones precisas para adecuar los tratamientos automatizados a los principios de la ley orgánica de protección de datos.
- Dictar recomendaciones de aplicación de las disposiciones legales y reglamentarias en materia de seguridad de los datos y control de acceso a los ficheros.

En relación con quienes tratan datos:

- Emitir las autorizaciones previstas en la ley.
- Requerir medidas de corrección.
- Ejercer la potestad sancionadora en los términos previstos en el Titulo VII de la ley orgánica de Protección de Datos.
- Ordenar, en caso de ilegalidad, el cese en el tratamiento y la cancelación de los datos.
- Recabar de los responsables de los ficharos la ayuda e información que precise para el ejercicio de sus funciones.
- Autorizar las transferencias internacionales de datos.

En materia de telecomunicaciones:

- Recibir las notificaciones de las eventuales quiebras de seguridad que se produzcan en los sistemas de los proveedores de servicios de comunicaciones electrónicas y que puedan afectar a datos personales.
- Tutelar los derechos y garantías de los abonados y usuarios en el ámbito de las comunicaciones electrónicas, incluyendo el envió de comunicaciones comerciales no solicitadas realizadas a través de correo electrónico o medios de comunicaciones electrónicas equivalente.

Otras funciones:

- Elaboración de una Memoria Anual, que es presentada por el director de la Agencia ante las Cortes.
- Representación de España en los foros internacionales en la materia.
- Cooperación con diversos organismos internacionales y con los órganos de la Unión Europea en materia de protección de datos.
- Control y observancia de lo dispuesto en la ley reguladora de la Función Estadística Publica.

2.3 Ámbito objetivo de aplicación

El autor Freixas Gutiérrez[12] sostiene que la LOPD queda en el ámbito de aplicación de los datos de carácter personal que estén informatizados y los datos que estén en un soporte físico que puedan ser susceptibles de tratamiento. Tal y como establece en su artículo 3 a) de la LOPD, establece que se entiende por dato personal "los datos concernientes a personas físicas, identificadas o identificables". Con estos datos se refiere por ejemplo al nombre, al apellido, al número de cuenta, a números de teléfono, a las direcciones, a informes médicos etc.

Se entenderá por dato personal cualquier información que aporte datos sobre una persona por los que se puede llegar a determinar su identidad y elaborar su perfil.

La LOPD no es la encargada de regular todos los ficheros de los datos personales, es decir, hay algunos casos de los ficheros que tienen características que la ley no tiene reguladas o algunos ficheros de los cuales son regulados por algunas leyes específicas que a continuación nombraremos algunas.

Fijándonos en el artículo 2 de la LOPD, establece que de su regulación quedan excluidos los siguientes; primero aquellos ficheros de particular, ficheros que son mantenidos por personas físicas con fines personales o domésticos. En segundo lugar, queda excluido el registro de materias clasificadas. No se concreta en la ley cuales son las materias que están incluidas como clasificadas, por lo cual es la ley 48/78 de 7 de octubre la que establece que las materias clasificadas son actos, documentos, informaciones datos u objetos donde el conocimiento por personas no autorizadas pueda dañar o poner en peligro la seguridad y defensa del estado. Por lo tanto, este tipo de materias se ven clasificadas en la categoría de secreto y reservado en atención al grado de protección que requieran. En los datos sobre la defensa y la seguridad del estado, es normal que estos datos estén regulados específicamente por otras leyes. Por tercer lugar, excluimos los ficheros de investigación del terrorismo y de la delincuencia organizada, por lo que entran los ficheros policiales que se crean para investigación y que únicamente deben informar a la agencia española de protección de datos de sus características, existencia y finalidades.

Otros de los ficheros que encontramos excluidos por tener normativas específicas son los ficheros de régimen electoral, los ficheros estadísticos y los militares. También encontramos excluidos los ficheros de imágenes y sonidos obtenidos mediante la utilización de videocámaras.

[12] La protección de datos de carácter personal en el derecho español. Pág. 120

3. REGLAMENTO UNIÓN EUROPEA.

El Reglamento UE 2016/679, de 27 de abril de 2016 será aplicable a partir del 25 de mayo de 2018 afectando al conjunto de derechos a través de los cuales la actual Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal garantiza a las personas el poder de control sobre sus datos personales.

El vigente Reglamento 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, junto con la Directiva 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo, configurarán desde el 25 de mayo de 2018 el nuevo marco europeo de protección de datos.

El nuevo Reglamento nace con un triple objeto:

- establecer las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y las normas relativas a la libre circulación de tales datos.

- proteger los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales.

- pretende que la libre circulación de los datos personales en la Unión no pueda ser restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales.

En relación con su ámbito de aplicación, se establecen dos distinciones:

En el ámbito de aplicación material el Reglamento se aplicará al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero. Por el contrario, no se aplica al tratamiento de datos personales:

a) en el ejercicio de una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión

b) por parte de los Estados miembros cuando lleven a cabo actividades comprendidas en el ámbito de aplicación del capítulo 2 del título V del TUE;

c) efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas;

d) por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención.

Por otro lado, en el ámbito territorial como matiza el art. 3 del Reglamento se aplica "al tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no." Adquiriendo especial relevancia el punto 3 del citado artículo al matizar la aplicación: "al tratamiento de datos personales por parte de un responsable que no esté establecido en la Unión sino en un lugar en que el Derecho de los Estados miembros sea de aplicación en virtud del Derecho internacional público." Es decir, el Reglamento UE 2016/679, de 27 de abril de 2016 será aplicable al tratamiento de datos fuera de la Unión.

Debemos destacar también los siguientes principios que son desarrollados en su capitulo II:

- Principios relativos al tratamiento. El responsable del tratamiento de los datos será responsable del cumplimiento y capaz de demostrarlo.
- Licitud del tratamiento. El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones especificadas en el apdo. 1, del art. 6.
- Condiciones para el consentimiento. Cuando el tratamiento se base en el consentimiento se regulan las condiciones y características del mismo. En este apartado aparecen las «Condiciones aplicables al consentimiento del niño en relación con los servicios de la sociedad de la información»
- Tratamiento de categorías especiales de datos personales. Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física. Esto no será de aplicación cuando concurra una de las circunstancias del apartado 2, art. 9.
- Tratamiento de datos personales relativos a condenas e infracciones penales. El tratamiento de datos personales relativos a condenas e infracciones penales o medidas de seguridad sólo podrá llevarse a cabo bajo la supervisión de las autoridades públicas o cuando lo autorice el Derecho de la Unión o de los Estados miembros que establezca garantías adecuadas para los derechos y libertades de los interesados. Solo podrá llevarse un registro completo de condenas penales bajo el control de las autoridades públicas.
- Tratamiento que no requiere identificación. Si los fines para los cuales un responsable trata datos personales no requieren o ya no requieren la identificación de un interesado por el responsable, este no estará obligado a mantener, obtener o tratar información adicional con vistas a identificar al interesado con la única finalidad de cumplir el Reglamento.

En este reglamento, las novedades que vemos es la extensa regulación del Reglamento presentará novedades en aspectos como:

- Los ya citados principios aplicables al tratamiento de datos y Condiciones para el consentimiento.

- La regulación del denominado «derecho al olvido» o derecho de supresión de los datos personales. El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando concurra alguna de las circunstancias citada en el Art. 17.

- Derecho a la portabilidad de los datos. El interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado, cuando se den las circunstancias citadas en el Art. 20.

- Responsabilidad del responsable del tratamiento. Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el

tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario.

- Registro de las actividades de tratamiento. Cada responsable o encargado del tratamiento de datos (o su representante) realizarán un registro que deberá contener toda la información indicada en el art. 30

- Notificación de una violación de la seguridad de los datos personales a la autoridad de control. En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente de conformidad con el artículo 55 sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación.

- Evaluación de impacto relativa a la protección de datos. El responsable del tratamiento de los datos realizará (en particular si utiliza nuevas tecnologías), antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares.

- Consulta previa a la autoridad de control en caso de identificarse riesgos en el tratamiento. El responsable consultará a la autoridad de control antes de proceder al tratamiento cuando una evaluación de impacto relativa a la protección de los datos en virtud del artículo 35 muestre que el tratamiento entrañaría un alto riesgo si el responsable no toma medidas para para mitigarlo.

- Regulación de las transferencias internacionales de datos. Solo se realizarán transferencias de datos personales que sean objeto de tratamiento o vayan a serlo tras su transferencia a un tercer país u organización internacional si, a reserva de las demás disposiciones del presente Reglamento, el responsable y el encargado del tratamiento cumplen las condiciones establecidas en el presente capítulo, incluidas las relativas a las transferencias ulteriores de datos personales desde el tercer país u organización internacional a otro tercer país u otra organización internacional. Todas las disposiciones del presente capítulo se aplicarán a fin de asegurar que el nivel de protección de las personas físicas garantizado por el presente Reglamento no se vea menoscabado (arts. 45-47).

- Cooperación entre la autoridad de control principal y las demás autoridades de control interesadas (arts. 60 a 67).

Otra nueva figura destacable es el Delegado de protección de datos

Los arts. 37-39, crean una nueva figura, el Delegado de protección de datos, de esta forma a partir de 2018, El responsable y el encargado del tratamiento designarán un delegado de protección de datos siempre que:

a) el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial;

b) las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala, o

c) las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales con arreglo al artículo 9 y de datos relativos a condenas e infracciones penales a que se refiere el artículo 10.

Este delegado tendrá como mínimo las siguientes funciones:

a) informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del presente Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros;

b) supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes;

c) ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35;

d) cooperar con la autoridad de control;

e) actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36, y realizar consultas, en su caso, sobre cualquier otro asunto.[13]

[13] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

3. ANÁLISIS DE LA PROTECCIÓN DE DATOS EN LA PANDEMIA

3.1. Introducción

La pandemia COVID-19 ha generado impactos sociales y políticos adicionales a los estrictamente sanitarios, llevando de un aparte a que los países, en el contexto de los estados de emergencia decretados, limiten de manera temporal algunos derechos y libertades civiles, para preservar la vida y salud de los ciudadanos; y de otra parte, han acelerado la transformación digital con el desarrollo y uso de herramientas tecnológicas para complementar las medidas de salud pública. Diversos organismos internacionales han expresado su preocupación respecto a la vulneración del derecho a la protección de datos personales en este nuevo escenario, e incluso han propuesto lineamientos éticos a tener en cuenta.

La pandemia de COVID-19 se ha convertido en una situación de emergencia mundial, con consecuencias devastadoras en cuanto a pérdida de vidas y contracción económica, que impide de manera significativa avanzar hacia el logro de los Objetivos de Desarrollo Sostenible de las Naciones Unidas. Las comunidades pobres y vulnerables se encuentran en una situación particularmente peligrosa ante esta enfermedad mortal y sus consecuencias económicas.

Cada vez hay más pruebas de que la recopilación, uso, difusión y procesamiento de datos pueden ayudar a limitar la propagación del virus y a acelerar la recuperación, especialmente mediante la localización digital de contactos. Los datos de movilidad obtenidos a partir del uso que hacen las personas de teléfonos móviles, correos electrónicos, cuentas bancarias, redes sociales, servicios postales, por ejemplo, pueden ayudar a controlar la propagación del virus y a realizar las actividades contempladas en los mandatos de las Organizaciones del Sistema de las Naciones Unidas.

Entre los datos así recopilados y procesados, incluidos aquellos utilizados para la localización digital de contactos o la vigilancia general de la salud, pueden figurar grandes cantidades de datos confidenciales personales y no personales. Esto podría tener consecuencias importantes más allá de la fase inicial de respuesta a la crisis. Por ejemplo, si esas medidas se aplicasen para fines no directa o específicamente relacionados con la respuesta a la COVID-19, podrían conducir a violaciones de libertades y derechos humanos fundamentales. Ese problema es especialmente acuciante si algunas de las medidas de emergencia introducidas para hacer frente a la pandemia, como la localización digital de contactos, se convierten en una práctica habitual.

El Secretario General de las Naciones Unidas subrayó en su informe de políticas sobre derechos humanos y COVID-19 que «los derechos humanos son clave para configurar la respuesta a la pandemia, tanto para la emergencia de salud pública como para el impacto más amplio en la vida y los medios de sustento de las personas. Los derechos humanos ponen a las personas en el centro del escenario. Las respuestas que son moldeadas por los derechos humanos, y que los respetan, producirán mejores resultados para vencer la pandemia, garantizar la atención médica para todos y preservar la dignidad humana».

Cualquier recopilación, uso y procesamiento de datos que realicen las Organizaciones del Sistema de las Naciones Unidas en relación con la pandemia de COVID-19 debería fundamentarse en los derechos humanos y aplicarse respetando debidamente la legislación internacional aplicable y los principios de protección de datos y privacidad, incluidos los principios de protección de datos personales y privacidad de las Naciones Unidas. Cualquier medida para hacer frente a la pandemia de COVID-19 debería tomarse respetando también los mandatos de las respectivas Organizaciones del Sistema de las Naciones Unidas y teniendo en cuenta el equilibrio entre los derechos pertinentes, incluido el derecho a la salud y la vida y el derecho a un desarrollo económico y social.

Teniendo en cuenta los principios de protección de datos personales y privacidad de las Naciones Unidas, el informe de políticas del Secretario General de las Naciones Unidas sobre derechos humanos y COVID-19 y las pertinentes normas sobre salud y humanidad, en lo relativo a la recopilación, uso y procesamiento de datos por las Organizaciones del Sistema de las Naciones Unidas en sus operaciones se deberá, al menos:

- Velar por que esas operaciones sean legítimas, limitadas en su ámbito y tiempo y necesarias y proporcionales a los propósitos especificados y válidos en la respuesta a la pandemia de COVID-19;
- Velar por que los datos se mantengan confidenciales y en seguridad durante un tiempo limitado y se destruyan o borren debidamente de conformidad con los propósitos mencionados;
- Velar por que todo intercambio de datos se realice de conformidad con la legislación internacional aplicable y los principios de protección de datos y privacidad y por qué este intercambio se evalúe a partir de una diligencia debida y valoraciones de riesgo adecuadas.
- Vincular las medidas tomadas relativas a datos a mecanismos y procedimientos aplicables para asegurarse de que cumplen los principios y propósitos mencionados, están justificadas sobre esa base y se interrumpen en cuanto dejan de ser necesarias, y
- Ofrecer transparencia para generar confianza en la aplicación de iniciativas actuales y futuras.

A fin de contener la pandemia y reducir al mínimo sus efectos negativos en el mundo es necesaria una respuesta mundial, coordinada, integradora y basada en la solidaridad de todo el Sistema de las Naciones Unidas. Aunque la presente declaración tiene por objeto hacer frente a los desafíos que supone la actual pandemia de COVID-19, puede servir de precedente para el uso de datos en cualquier respuesta rápida a una crisis futura de escala similar respetando la protección de datos y la privacidad.

3.2. Diferentes problemas creados a raíz de la protección de datos se considera vulnerada

Fijándonos en la declaración del estado de alarma la cual no permite limitar derechos y libertades más allá de lo que dispone el artículo 11 de la ley orgánica 4/1981. Lo que este decreto permite, no es suspender derechos sino solo adoptar medidas que puedan condicionar su ejercicio pero no su prohibición.

Así es como debemos interpretar el artículo 55.1 de la constitución el cual solo permite suspender derechos cuando se declare el estado de excepción o de sitio, pero no con el estado de alarma.

Aun así no todos los derechos pueden ser suspendidos, sino solo los reconocidos en los artículos 17, 18, apartados 2 y 3, artículos 19, 20, apartados 1, a) y d), y 5, artículos 21, 28, apartado 2, y artículo 37, apartado 2 de la Constitución.

El derecho a la protección de datos deriva del artículo 18.4 de la Constitución, como declaró ya hace tiempo el Tribunal Constitucional en su Sentencia 292/2000 de modo que ni siquiera en los estados de excepción y sitio puede ser suspendido; mucho menos, pues, en el estado de alarma.

Ya con carácter general la presidencia del Comité Europeo de Protección de Datos hizo pública el 16 de marzo una declaración sobre el tratamiento de datos personales en el contexto de la crisis del Covid-19 , en la que resalta que la normativa sobre protección de datos y en particular el Reglamento (UE) 2016/679, no impiden tomar medidas en la lucha contra la pandemia del coronavirus, pero advierte que incluso en estas excepcionales circunstancias quienes traten datos personales deben asegurar su protección.

Sin perjuicio de que el propio Reglamento y la Directiva 2002/58/CE sobre la privacidad y las comunicaciones electrónicas prevén reglas que pueden aplicarse al tratamiento de datos que se lleve a cabo en un contexto como el actual, que permitiría incluso obviar en ciertos casos el consentimiento de los afectados.

Las Autoridades de Protección de Datos de varios países han hecho públicos también informes u opiniones sobre el tema, que para algunos suponen una “inoportuna doctrina de las autoridades europeas de protección de datos frente al Covid-19”. Incluso se ha llegado a afirmar que podemos llegar “a la muerte por protección de datos”.

Por su parte la Agencia Española de Protección de Datos ha hecho público el pasado 12 de marzo (antes pues del Real Decreto 463/2020, publicado en el BOE del 14 de marzo) el importante Informe 0017/2020 de su Gabinete Jurídico, sobre tratamientos de datos resultantes de la actual situación derivada de la extensión del virus Covid-19 y unas “Preguntas Frecuentes” sobre el Coronavirus, centradas en el tratamiento de datos en el ámbito laboral. Asimismo la Autoridad Catalana de Protección de Datos ha publicado una “Nota en relación con los tratamientos de datos personales relacionados con las medidas para hacer frente al COVID-19”.

De entre estos documentos me parece especialmente relevante el Informe de la AEPD, sin perjuicio de la notable utilidad que tiene tanto la respuesta a esas preguntas frecuentes como la Nota de la Autoridad Catalana. El citado Informe 0017/2020 parte de la base de que “la normativa de protección de datos personales, en tanto que dirigida a salvaguardar un derecho fundamental, se aplica en su integridad a la situación actual,

dado que no existe razón alguna que determine la suspensión de derechos fundamentales, ni dicha medida ha sido adoptada". En efecto, tras el Real Decreto 463/2020 no se ha suspendido el derecho a la protección de datos y su ejercicio, por el mero hecho de declarar el estado de alarma, no queda limitado.

Ahora bien, como también advierte el Informe, "la propia normativa de protección de datos personales contiene las salvaguardas y reglas necesarias para permitir legítimamente los tratamientos de datos personales en situaciones, como la presente, en que existe una emergencia sanitaria de alcance general". La advertencia de la Agencia es totalmente acertada, como también lo es la que recoge a continuación: "Por ello, al aplicarse dichos preceptos previstos para estos casos en el RGPD, en consonancia con la normativa sectorial aplicable en el ámbito de la salud pública, las consideraciones relacionadas con la protección de datos , dentro de los límites previstos por las leyes, no deberían utilizarse para obstaculizar o limitar la efectividad de las medidas que adopten las autoridades, especialmente las sanitarias, en la lucha contra la epidemia, por cuanto ya la normativa de protección de datos personales contiene una regulación para dichos casos que compatibiliza y pondera los intereses y derechos en liza para el bien común".

Especialmente relevante me parece la afirmación de que la protección de datos no debe utilizarse para obstaculizar o limitar las medidas que deban tomarse para luchar contra la epidemia. No puedo estar más de acuerdo con tal afirmación. En numerosas ocasiones, constantemente mejor dicho, vengo afirmando que la protección de datos no es un derecho impertinente que "prohíba" sin más "hacer cosas"; más bien marca el camino que indica "cómo deben hacerse las cosas". Ni en situaciones de pandemia global como la que estamos sufriendo, aún conscientes de que como parece ser lo peor está por llegar, podemos poner en entredicho un derecho fundamental como es el de la protección de datos. Muchas fueron las voces que reclamaban poco menos que acabar con la protección de datos tras los atentados del 11S. La seguridad, se decía, estaba por encima de la privacidad. Hubo que luchar, y no poco, para hacer ver que la seguridad y la privacidad no son contradictorias sino complementarias. Es decir, y volviendo a la crisis del coronavirus: la protección de datos en ningún caso va a ser un obstáculo para luchar con todas las armas que en nuestras manos estén contra el coronavirus. Y estoy seguro de que esta es la posición de las autoridades de protección de datos.

3.3.Informe 0017/2020

En dicho informe hablado anteriormente, vemos que el reglamento general de protección de datos (RGPD), contiene unas reglas necesarias para permitir legítimamente que los tratamientos de los datos personales en situaciones en las que existe una emergencia sanitaria de alcance general. Como consecuencia de ello, según este informe, la protección de datos no debería utilizarse para obstaculizarse o limitar la efectividad de las medidas que adopten las autoridades.

Este informe recoge que el RGPD, reconoce exactamente que en su considerado artículo 46 como baje jurídica para el tratamiento licito de los datos personales en diversos casos excepcionales, como el control de pandemias y su propagación, la misión realizada en interés público (art 6.1e) o los intereses vitales del interesado u otras personas físicas (art6.1 d), sin que se pueda perjudicar a otras bases. Estas bases permiten el tratamiento de datos sin consentimiento de los afectados.

Estos datos de salud están catalogados en el reglamento como categorías de datos, prohibiéndose su tratamiento salvo que pueda ampararse en alguna de las excepciones recogidas en la normativa. Este informe precisa las excepciones que se recogen en el artículo 9.2 RGPD:

- El cumplimiento de obligaciones en el ámbito de derecho laboral y de la seguridad y protección social, en el cual en el informe recuerda la obligación de empleadores y de su personal en materias de prevención de riesgos laborales y que corresponde a cada trabajador velar por su propia seguridad y salud en el trabajo y por la de aquellas personas a las que pueda afectar su actividad profesional a causa de sus actos y omisiones en el trabajo. Ello supone que el personal deberá informar a su empleado en caso de sospecha de contacto con el virus a fin de salvaguardar, además de por su propia salud, por la de los demás trabajadores del centro de trabajo para que se puedan adoptar las medidas oportunas.
- Por otro lado el interés público en el ámbito de la salud pública (art 9.2 i) que en este caso se configura como interés público esencial (art 9.2 g).
- Cuando sea necesario para la realización de un diagnostico medico (art 9.2 h)
- Cuando el tratamiento es necesario para proteger intereses vitales del interesado o de otras personas, cuando el interesado no esté capacitado para prestar su consentimiento (art 9.2c)

Por otra parte, también hace referencia este informe a la ley orgánica 3/1986 de medidas especiales en materia de salud pública o la ley 33/2011 general de salud pública. La primera de esta norma señala que con el fin de controlar las enfermedades transmisibles, la autoridad sanitaria, además de realizas las acciones preventivas generales, podrán adoptar las medidas oportunas para el control de los enfermos de las personas que estén o hayan estado en contacto con los mismos y del medio ambiente inmediato, así como las que se consideren necesarias en caso de riesgo de carácter transmisible.

Respecto a la materia de riesgo de transmisión de enfermedades, epidemia, crisis sanitaria etc., esta normativa aplicable ha otorgado a las autoridades sanitarias de las distintas AAPP las competencias para adoptar las medidas necesarias previstas por la ley cuando así lo exijan razones sanitarias de urgencia o necesidad. Desde el punto de vista de los datos personales, la protección de los intereses vitales de las personas físicas corresponde en el ámbito de la salud a las distintas autoridades sanitarias de las diferentes administraciones públicas, quienes podrán adoptar las medidas necesarias para salvaguardar a las personas en situaciones de emergencia sanitaria.

Así pues serán las autoridades sanitarias de las distintas AAPP quienes deberán adoptar las decisiones necesarias y los distintos responsables de los tratamientos de datos personales que deberán seguir dichas instrucciones, incluso cuando ello suponga un tratamiento de datos personales de salud.

Por lo tanto se expresa del mismo modo y también en aplicación a lo establecido que en la normativa de trabajo y de prevención de riesgos laborales, los empleados podrán tratar, de acuerdo con dicha normativa y con las garantías que dichas normas establecen, los datos necesarios para garantizar la salud de todo su personal y evitar contagios en el seno de la empresa y/o centros de trabajo.

Por último, este informe destaca que los tratamientos de los datos personales, aun e estas situaciones de emergencia sanitaria, deben seguir siendo tratados de conformidad con la

normativa de protección de datos personales , puesto que estas normas han previsto esta eventualidad, por lo que le son de aplicación sus principios y entre ellos el de tratar los datos personales con licitud , lealtad y transparencia, limitación de la finalidad, principio de exactitud y el principio de minimización de datos.

Por último, sobre el último aspecto hace una referencia expresa a que los datos tratados habrán de ser exclusivamente los limitados a los necesarios para la finalidad pretendida, sin que se pueda extender dicho tratamiento a otros datos personales no estrictamente necesarios para dicha finalidad.[14]

[14] Agencia española de protección de datos. N/ ref 0017/2020

4. ¿QUE OCURRE CON LOS DERECHOS FUNDAMENTALES EN LA PANDEMIA?

Durante estos meses hemos visto restringidos nuestros derechos y libertades constitucionales hasta niveles que jamás nos hubiéramos imaginado. Durante los primeros meses de la pandemia tuvimos la prohibición de no poder salir de nuestras casas, salvo por razones que fueran justificadas por el Real Decreto publicado por el gobierno. Esta prohibición de la libertad está bastante justificada por la situación en la que nos encontrábamos en ese momento (actualmente continua la pandemia aunque no esa restricción).

En ese contexto el pasado año se declaró el estado de alarma en virtud del artículo 116 de la constitución. [15]En la que dio paso a varias lagunas legales, en la que tuvieron que poner medidas diferentes organismos como la Agencia Española de Protección de Datos que hicieron públicas para que poder recomendar a los ciudadanos.

Uno de los principales problemas que surgieron fue la existencia de la globalización y la digitalización de los contenidos, donde la mayoría de las personas que tiene acceso a internet tienen a su disposición inmensas cantidades de información. El acceso a todos esos datos provoca la necesidad de que todos los consumidores de contenido hagan un trabajo incesante de verificación con el fin de contrastar lo que es real y lo que no, para lograr así construir una realidad lo más objetiva posible y evitar la propagación de bulos, que es otra de las grandes preocupaciones en los tiempos que corren. Con esto tuvieron que tener demasiado control puesto que se difundieron bastantes noticias que eran bulos y en la actualidad continua pasando, noticias que no fueron contractadas y de las cuales tuvieron que limitar. Por esta razón, WhatsApp limito las cadenas de reenvíos, prohibiendo que sus usuarios reenvíen a más de un contacto mensajes que han sido previamente reenviados en multitud de ocasiones, Facebook comunico también que alertará a los usuarios que compartan o interactúen con noticias falsas que estén relacionadas con el coronavirus y diversas medidas que se tomaron. Algunos ejemplos de las noticias falsas que se produjeron fueron que el COVID se trataba de un arma biológica, sobre cómo se podía curar, como se contagiaba… etc.

Todas estas medidas, cuyo principal objetivo parece ser lícito o, al menos, estar justificado para garantizar el derecho a recibir y comunicar información veraz, colisionan de forma patente con

---

[15] Artículo 116 constitución española: Una ley orgánica regulará los estados de alarma, de excepción y de sitio, y las competencias y limitaciones correspondientes. El estado de alarma será declarado por el Gobierno mediante decreto acordado en Consejo de Ministros por un plazo máximo de quince días, dando cuenta al Congreso de los Diputados, reunido inmediatamente al efecto y sin cuya autorización no podrá ser prorrogado dicho plazo. El decreto determinará el ámbito territorial a que se extienden los efectos de la declaración. El estado de excepción será declarado por el Gobierno mediante decreto acordado en Consejo de Ministros, previa autorización del Congreso de los Diputados. La autorización y proclamación del estado de excepción deberá determinar expresamente los efectos del mismo, el ámbito territorial a que se extiende y su duración, que no podrá exceder de treinta días, prorrogables por otro plazo igual, con los mismos requisitos. El estado de sitio será declarado por la mayoría absoluta del Congreso de los Diputados, a propuesta exclusiva del Gobierno. El Congreso determinará su ámbito territorial, duración y condiciones. No podrá procederse a la disolución del Congreso mientras estén declarados algunos de los estados comprendidos en el presente artículo, quedando automáticamente convocadas las Cámaras si no estuvieren en período de sesiones. Su funcionamiento, así como el de los demás poderes constitucionales del Estado, no podrán interrumpirse durante la vigencia de estos estados.
Disuelto el Congreso o expirado su mandato, si se produjere alguna de las situaciones que dan lugar a cualquiera de dichos estados, las competencias del Congreso serán asumidas por su Diputación Permanente. La declaración de los estados de alarma, de excepción y de sitio no modificarán el principio de responsabilidad del Gobierno y de sus agentes reconocidos en la Constitución y en las leyes."

el derecho a la libertad de expresión de los usuarios de redes sociales. Estos dos derechos están consagrados en el artículo 20 CE, es decir, se ubican en la Sección 1ª del Capítulo 2º de la CE, en la que se recogen los derechos fundamentales y libertades públicas, que tienen una especial protección constitucional basada en el artículo 53.2 CE. Sin embargo, hoy en día, tanto la doctrina, como la jurisprudencia del Tribunal Constitucional han señalado que *"ningún derecho, ni aún los de naturaleza o carácter constitucional, pueden considerarse como ilimitados"* (STC 11/1981, de 8 de abril, FJ 7º). En este mismo sentido se pronuncia el TC en otras sentencias, como la STC 58/2018, de 4 de junio, FJ 6º. Además, la lógica doctrinal indica que los límites a los derechos fundamentales nacen precisamente por su colisión con otros intereses jurídicos igualmente fundamentales.

Por esta razón, aunque el derecho a la libertad de expresión tenga limites como derecho fundamental, las medidas que han sido adoptadas pueden resultar desproporcionadas con el fin que siguen. Cada persona debería ser libre de compartir en sus redes sociales lo que considere, siempre que no cometa ningún ilícito penal o no atente contra derechos fundamentales de otras personas. Por tanto, con el fin de garantizar la libertad de expresión de los usuarios de redes sociales, y para evitar la creación de bulos, lo ideal, más que controlar y limitar lo que los internautas pueden compartir en sus redes, sería dar rienda suelta a esa libertad, pero concienciándolos de que es importante que hagan un análisis previo y comprueben que la información que reciben es verídica antes de compartirla con sus contactos.

Para que esta propuesta idílica pueda prosperar y se proteja la libertad de expresión de los ciudadanos, es necesario que se preserve también el derecho fundamental instaurado en la letra d) del apartado 1º del artículo 20 CE, es decir, el derecho *"a comunicar o recibir libremente información veraz por cualquier medio de difusión"*. Esto es así porque, si los profesionales de la comunicación no tienen libertad para realizar su trabajo, los ciudadanos no estarán recibiendo información totalmente veraz, no podrán contrastarla en varios medios y tampoco podrán hacer uso de su derecho a la libertad de expresión con la garantía de estar bien informados.

5. PREGUNTAS FRECUENTES QUE HAN SURGIDO:

Durante este periodo se han producido varias preguntas ante las circunstancias tan atípicas que se han producido. No se sabía exactamente si se produce alguna excepción en la aplicación de la normativa de datos durante esta pandemia. Aquí encontramos la respuesta con un rotundo no de excepciones, puesto que tanto el reglamento general de protección de datos (RGPD) como la ley organiza de protección de datos y garantía de los derechos digitales (LOPDGDD) son de aplicación a cualquier actividad de tratamiento de datos personales que lleve a cabo una entidad local como consecuencia del tratamiento de datos con fines de gestión de la pandemia. También estas entidades locales deberán aplicar a los tratamientos de datos personales las medidas de seguridad que correspondan de acuerdo con lo previsto en el esquema nacional de seguridad.

Otras de las preguntas más frecuentes es si se puede crear una base de datos de personas vulnerables en la ciudad, que permita a los servicios sociales coordinación con nuestra agencia de salud pública, cubrir aspectos críticos durante la epidemia. La respuesta que encontramos es que si, que nada impide desarrollar actividades legítimas necesarias ni hay obstáculo, pero siempre que se asegure que los datos son tratados en cada caso con pleno respeto al RGPD y a la LOPDGDD.

Si bien se tendrá que tener en cuenta el nuevo marco legal introducido por el decreto de declaración del estado de alarma, a partir de los criterios introducidos de forma específica para esta pandemia por el "statement de la EDPB" y especialmente, por el informe 0017/2020 del gabinete jurídico de la AEPD. Es importante en todo caso que en el registro de actividades de la entidad local se genere un nuevo registro por cada nueva actividad de tratamiento que sea creada, en el que constará la información establecida en el artículo 30 del RGPD y su base legal, y que dicha actividad de tratamiento sea pública y accesible por medios electrónicos para las personas interesadas.

Tenemos que aclarar que es lo que significa exactamente que los datos sean tratados con pleno respeto del RGPD y la LOPDGDD. Esto Significa que la base de datos cumpla los principios básicos de protección de datos y todas las garantías que se establecen para las personas físicas titulares de los datos, como son:

- Con carácter previo se analizará la necesidad de una evaluación de impacto según los criterios de la AEPD. En cualquier caso, aunque no exista la necesidad de evaluación de impacto siempre deberá llevarse a cabo un análisis de riesgos que permita la correcta aplicación de las políticas de seguridad.

- Aplicar el principio de privacidad desde el diseño a la cantidad de datos, a la extensión de su tratamiento, a su accesibilidad y a su plazo de conservación.

- Analizar la base jurídica aplicable y determinar los fines legítimos de tratamiento, los posibles destinatarios y la duración del tratamiento.

- Informar a las personas interesadas cuyos datos son objeto de tratamiento, informando la información a formularios, políticas de privacidad, locuciones telefónicas, envíos postales, u otras formas como enlace a la actividad de tratamiento.

- Aplicar las medidas de seguridad. En este sentido, se dispondrá como marco de referencia las políticas de seguridad corporativas que se hayan establecido para esta situación de emergencia específica que como mínimo garantice los principios de accesibilidad e integridad principalmente soportados sobre servidores corporativos de bases de datos o de ficheros.

En todo caso, el mínimo de las medidas a establecer viene constituido por lo establecido en el artículo 32 del RGPD que exige medidas apropiadas como:

a) la seudonimización y el cifrado de datos personales;

b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;

c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;

d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

- Garantizar en plazo y contenido el ejercicio de los derechos de las personas.

Además, aunque el tratamiento sea novedoso y temporal debería quedar bajo el amparo de las políticas y procedimientos de protección de datos de la entidad local.

Por otro lado, las bases jurídicas del nuevo tratamiento que se generen como consecuencia del COVID-19 serán los siguientes:

El RGPD contiene las salvaguardas y reglas necesarias para permitir legítimamente los tratamientos de datos personales en situaciones, como la presente, en que existe una emergencia sanitaria de alcance general y para estas situaciones el RGPD reconoce que la base jurídica de los tratamientos puede ser múltiple.

Los tratamientos datos personales encuentran en el artículo 6 distintas bases jurídicas legitimadoras, entre otras: el cumplimiento de una obligación legal; proteger intereses vitales del interesado o de otra persona física; cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.

También podrán tratarse categorías especiales de datos de acuerdo con el artículo 9 RGPD cuando el tratamiento sea necesario: para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito de la seguridad y protección social; para proteger intereses vitales del interesado o de otra persona física; por razones de un interés público esencial; para la prestación de asistencia o tratamiento de tipo sanitario o social; por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud; en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento y el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física;

Debemos tener en cuenta que cada una de estas bases jurídicas deben encontrar reconocimiento expreso en la legislación interna y requieren adoptar las debidas cautelas y garantías adecuadas.

Otras de las posibles preguntas es saber los posibles fines que podrían ser de los nuevos tratamientos que se generen como consecuencia del COVID-19, serian del desarrollo de políticas públicas de asistencia social en coordinación con los servicios de salud pública y de control de la crisis sanitaria, como por ejemplo: El suministro de alimentos cocinados compras básicas de alimentación o medicamentos a gente mayor o personas en situación de vulnerabilidad; Atención a menores; Localizar posibles casos de masificación residencial, que puedan constituir un riesgo importante para los residentes y contactos vecinales; Cualquier otro servicio de asistencia domiciliaria a personas vulnerables; Reparto de material de protección; Facilitar la actuación de voluntariado social en la situación de emergencia.

Otro punto que en el que han surgido dudas es si se debe informar a la ciudadanía de las nuevas actividades de tratamiento, por lo que indicamos que en la medida de lo posible si se debe informar. El RGPD indica que ello no será preciso en la medida en que las personas interesadas ya dispongan de la información; la comunicación de dicha información resulte imposible o suponga un esfuerzo desproporcionado, en particular, para el tratamiento con fines de interés público, o en la medida en que la obligación pueda imposibilitar u obstaculizar gravemente el logro de los objetivos de tal tratamiento.

No obstante, en estos casos, la entidad local debe adoptar medidas adecuadas para proteger los derechos, libertades e intereses de las personas interesadas, inclusive haciendo pública la información, por ejemplo, por medios electrónicos en el sitio web municipal. También podría quedar limitada la obligación de informar si la obtención o la comunicación está expresamente establecida por el Derecho de la Unión Europea o nuestro Derecho Interno si establece medidas adecuadas para proteger los intereses legítimos de las personas interesadas.

Los ciudadanos, partido de este estado de alarma se han preguntado si posible llevar a cabo una actividad de video vigilancia, ya sea vía drones o mediante cámaras instaladas por la población urbana para identificar conductas prohibidas por la situación de alarma, es decir, si podrían ser vigilados. La respuesta es clara, sí. Eso sí , siempre y cuando se tenga en cuenta que esta es una actividad de tratamiento propia de la Policía Local exclusivamente y que está sujeta a los mismos principios del RGPD y la LOPDGDD, como cualquier actividad de vigilancia que ya esté llevando a cabo la Policía Local regulada por la normativa específica de seguridad pública, dado que pese a la característica del medio tecnológico de recogida datos al fin y al cabo el dron realiza funciones de captación de imágenes para fines de vigilancia por motivos del COVID19.

Otra de las preguntas más frecuentes es que si se puede geo localizar a las personas para saber dónde se encuentran, si se salta alguna prohibición etc. En primer lugar, entenderemos por geolocalización la ubicación en coordenadas absolutas de un terminal, bien sea mediante el seguimiento de los sistemas GPS integrados o del posicionamiento celular que pueden realizar las compañías operadoras. No debe confundirse con los sistemas de localización próxima que como el Bluetooth que permitiría establecer relaciones de proximidad entre dispositivos, pero no conocer su localización en términos de posición absoluta. La Orden SND/297/2020 de 27 de marzo, regula en su punto segundo encomendar a la Secretaría de Estado de Digitalización e Inteligencia Artificial el estudio de la movilidad de las personas en los días previos y durante el confinamiento siguiendo el modelo agregado y anonimizado ya utilizado previamente por el INE con los datos provenientes de las operadoras del servicio. Asimismo, en el punto tercero, encomienda a dicha Secretaría ser el punto central de la coordinación para la evaluación de otras propuestas tecnológicas por parte de otros organismos y entidades, entre los que deberemos incluir también las posibles propuestas de las EELL. Por lo que cualquier posible tratamiento al respecto, deberá hacerse dentro de este marco, de forma agregada, con las debidas garantías de irreversibilidad del proceso y de acuerdo con la citada Orden.

A raíz de la geolocalización también puede surgir la duda si la entidad local realizar un mapa epidemiológico indicando las zonas de desarrollo de COVID-19 en la población y su porcentaje El derecho a la protección de datos no es incompatible con el monitoreo epidemiológico, enfatizando que los datos anonimizados no están cubiertos por los requisitos de protección de datos, por lo que si se podría. Por lo tanto, el uso de información agregada para señalar zonas de alta, media o baja incidencia de la enfermedad en el territorio municipal no vulnera la normativa de protección de datos. No obstante, el Ayuntamiento deberá tener en cuenta que cuanto mayor sea el grado de información estadística más deben tenerse en cuenta medidas que

aseguren la anonimizarían. En la publicación de información estadística que incluya datos relativos a edad, género, indicadores sociales etc., deberá tenerse muy en cuenta el impacto del tamaño poblacional del área en la identificabilidad de las personas.

Tampoco se sabe si se puede incorporar a las bases de datos municipales información, como teléfonos, datos de contacto u otro, procedente de otras fuentes, como por ejemplo sitios web públicos de internet. La respuesta es que si, que en estos casos, además de que la base jurídica de tratamiento sea legítima, es muy importante informar a la persona interesada de la fuente de la que proceden los datos personales y de cuáles son los datos personales objeto de tratamiento. Esto puede hacerse de acuerdo con las propuestas antedichas en preguntas anteriores. Además, esta información se debería hacer constar en el registro de actividades de tratamiento de la corporación local igualmente. Estas situaciones pueden darse para llevar a cabo actividades especialmente relevantes como, por ejemplo, localizar personas vulnerables cuyos datos de contacto en algún caso no están en las "fuentes administrativas" del Ayuntamiento o no están actualizados, para lo cual hay que hacer cruces con otros servicios de carácter autonómico como los de salud o con operadores privados de telecomunicaciones o incluso, acudiendo a fuentes públicas en internet. En todo caso, en todo momento, deberá optarse por la que represente un menor riesgo para los interesados y con fuentes de finalidades compatibles. En este sentido, la Ley de Servicios Sociales prevé la colaboración entre los servicios sociales municipales y los Centros de Atención Primaria (CAPs) para un tratamiento integral de los pacientes y la actuación con medidas coordinadas, ante problemas de salud pública como el actual, permitiendo el intercambio de datos, especialmente los identificativos o de contacto, presentes en los Registros Centrales de asegurados de los servicios sanitarios de las Comunidades autónomas. En este sentido y atendiendo al principio de minimización de datos y menor riesgo para los derechos y libertades de la persona interesada, es preferible llevar a cabo el intercambio de datos entre las Administraciones públicas antes que el intercambio con otros operadores de índole privada, dado que, en este segundo caso, desde la Administración se podría estar revelando de forma indirecta a estos operadores privados la condición de persona vulnerable, a la hora de solicitar su teléfono.[16]

[16] Dirección general de servicio jurídico y coordinación territorial.

6. PREGUNTAS FRECUENTES DE LA PROTECCIÓN DE DATOS EN LA PANDEMIA RELACIONADAS CON EL TRABAJO:

En este ámbito se han producido diversas preguntas, puesto que los empresarios y encargados no sabían exactamente qué información podían o no dar, o tener ellos mismo. Surgen una serie de preguntas que la agencia española de protección de datos (AEPD)[17].

Lo primero que debemos de saber es si estos empresarios pueden tratar información sobre si las personas que trabajan para él están infectas o no. En aplicación de lo establecido en la normativa sanitaria, laboral y, en particular, de prevención de riesgos laborales, los empleadores podrán tratar, de acuerdo con dicha normativa y con las garantías que establecen, los datos del personal necesarios para garantizar su salud y adoptar las medidas necesarias por las autoridades competentes, lo que incluye igualmente asegurar el derecho a la protección de la salud del resto del personal y evitar los contagios en el seno de la empresa y/o centros de trabajo que puedan propagar la enfermedad al conjunto de la población.

La empresa podrá conocer si la persona trabajadora está infectada o no, para diseñar a través de su servicio de prevención los planes de contingencia que sean necesarios, o que hayan sido previstos por las autoridades sanitarias. Esa información también puede ser obtenida mediante preguntas al personal. Sin embargo, las preguntas deberían limitarse exclusivamente a indagar sobre la existencia de síntomas, o si la persona trabajadora ha sido diagnosticada como contagiada, o sujeta a cuarentena. Resultaría contrario al principio de minimización de datos la circulación de cuestionarios de salud extensos y detallados, o que incluyan preguntas no relacionadas con la enfermedad.

Por lo que entendemos que sí, pero ahora bien ¿podrían transmitir esa información al personal de la empresa? Pero esta información debería proporcionarse sin identificar a la persona afectada a fin de mantener su privacidad, si bien, podría transmitirse a requerimiento de las autoridades competentes, en particular las sanitarias. La información debe proporcionarse respetando los principios de finalidad y proporcionalidad y siempre dentro de lo establecido en las recomendaciones o instrucciones emitidas por las autoridades competentes, en particular las sanitarias.

Por ejemplo, si es posible alcanzar la finalidad de protección de la salud del personal divulgando la existencia de un contagio, pero sin especificar la identidad de la persona contagiada, debería procederse de ese modo. Si, por el contrario, ese objetivo no puede conseguirse con información parcial, o la práctica es desaconsejada por las autoridades competentes, en particular las sanitarias, podría proporcionarse la información identificativa.

Pero ahora bien los trabajadores que estén en cuarentena preventiva o que pueda estar afectado por el coronavirus si tiene una obligación de informar a su empleador de esta circunstancia para que este pueda iniciar un protocolo.

Los trabajadores que, tras haber tenido contacto con un caso de coronavirus, pudieran estar afectados por dicha enfermedad y que, por aplicación de los protocolos establecidos por las Autoridades Sanitarias competentes, se ven sometidos al correspondiente aislamiento preventivo para evitar los riesgos de contagio derivados de dicha situación hasta tanto se disponga del correspondiente diagnóstico, deberán informar a su empleador y al servicio de prevención o, en su caso, a los delegados de prevención (Ley de Prevención de Riesgos

[17] Documento de la agencia española de protección de datos sobre el COVID-19

Laborales) La persona trabajadora en situación de baja por enfermedad no tiene obligación de informar sobre la razón de la baja a la empresa, sin embargo, este derecho individual puede ceder frente a la defensa de otros derechos como el derecho a la protección de la salud del colectivo de trabajadores en situaciones de pandemia y, más en general, la defensa de la salud de toda la población.

Y como última pregunta, y una de las que me parece un tanto interesante, puesto que en mi trabajo y en el de muchas personas que conozco se realiza, es si el personal de seguridad puede tomar la temperatura a los trabajadores con el fin de detectar casos de coronavirus.

Verificar si el estado de salud de las personas trabajadoras puede constituir un peligro para ellas mismas, para el resto del personal, o para otras personas relacionadas con la empresa constituye una medida relacionada con la vigilancia de la salud de los trabajadores que, conforme a la Ley de Prevención de Riesgos Laborales, resulta obligatoria para el empleador y debería ser realizada por personal sanitario. En todo caso, el tratamiento de los datos obtenidos a partir de las tomas de temperatura debe respetar la normativa de protección de datos y, por ello y entre otras obligaciones, debe obedecer a la finalidad específica de contener la propagación del coronavirus, limitarse a esa finalidad y no extenderse a otras distintas, y mantenidos no más del tiempo necesario para la finalidad para la que se recaban.

7. CONCLUSIÓN

Para finalizar este trabajo, realice una encuesta entre personas de diferentes rangos de edad. Realice diferentes preguntas que en algunas de ellas se diferenciaban las respuestas según el tipo de edad. Una de las preguntas que me llamo la atención fue que si durante esta pandemia vieron vulnerados sus derechos y libertades, la gran mayoría respondió que no los vieron vulnerados. Es decir, la mayoría de las personas han sido conscientes que este tipo de derechos, como mencione en el trabajo han tenido que limitarse para poder actuar en esta pandemia. La segunda y última pregunta que voy a destacar es" Tanto en el trabajo como en el colegio si pillas el virus, debes comunicarlo. Debido a ello se lo comunican a las personas que has estado en contacto recientemente ¿estarías de acuerdo que tus datos se expongan? Es decir, que digan que tal persona en este caso tú, has pillado el virus.". Esta pregunta me llamo la atención, todos los respondieron que sí, que ellos querían que dieran sus datos y apellidos, pero como dije durante el trabajo, esta información debería proporcionarse sin identificar a la persona afectada a fin de mantener su privacidad.

Para concluir, esta pandemia por COVID-19 le ha llamado mucho la atención a los ciudadanos para realizar un análisis y aprendizaje para la protección de los derechos individuales y los colectivos respectivamente, y en la confianza de los ciudadanos respecto a los gobiernos de los países cuando se declaró el estado de alarma y limitaron sus derechos.

Como bien sabemos, la restricción de derechos no puede afectar el núcleo fundamental de estos, debe ser temporal, conforme al principio de legalidad, responder a una necesidad perentoria, ser proporcional a esta, no generar discriminación, ni, no mantenerse de forma permanente, no ser arbitrarios, así como estar plenamente justificados. Y hoy día, vamos viendo como la movilidad y muchos derechos que habíamos sido privados, han vuelto puesto que ha pasado un tiempo considerado.

Respecto a la adaptación de los sistemas de protección de datos personales, a los retos que imponen las medidas de salud pública en tiempos de pandemia deben salvaguardar los derechos humanos y responder a las particularidades jurídicas y culturales de cada país, de manera que nadie se vea obligado a elegir entre una respuesta eficaz para el control de la pandemia y la protección de sus derechos fundamentales.

Por último decir, que me ha parecido un trabajo muy interesante sobre todo porque es algo relacionado con l actualidad, y me ha servido para informarme cosas de la actualidad que no me hubiera fijado si no hubiera realizado este trabajo.

8. Bibliografía

- ➔ PARDO FALCON, J. (1992). "Los derechos del artículo 18 de la Constitución española en la jurisprudencia del Tribunal Constitucional". Revista Española de Derecho Constitucional, n.34, pp. 146 y 158.
- ➔ ARENAS RAMIRO, M. (2006). El derecho fundamental a la protección de datos en Europa, Valencia: Tirant lo Blanch, pp. 439-441.
- ➔ ALZAGA VILLAAMIL, O. (2017). Comentario sistemático a la Constitución española de 1978, Madrid: Marcial Pons, pp. 141-142.
- ➔ MARTÍNEZ MARTINEZ, R. (2008). "El Real Decreto 1720/2007, de 21 De diciembre, por el que se aprueba el reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. Aspectos clave." Revista Jurídica de Castilla y León, n. 16, pp. 257-293.
- ➔ APARICIO SALOM, J. (2002). Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal, Navarra: Aranzadi, p. 27.
- ➔ APARICIO SALOM, J. (2002). Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal, Navarra: Aranzadi, p. 39.
- ➔ Art. 35 CC: Son personas jurídicas, las corporaciones, asociaciones y fundaciones de interés público reconocidas por la ley. Y las asociaciones de interés particular, sean civiles, mercantiles o industriales, a las que la ley conceda personalidad propia.
- ➔ ANDREU MARTÍNEZ, M .B. (2013), La protección de datos personales de los menores de edad, Navarra: Aranzadi, pp. 67-92.
- ➔ LESMES SERRANO, C. (2008). La Ley de Protección de Datos: Análisis y comentario de su jurisprudencia. Valladolid: Lex Nova, p 115.
- ➔ Agencia Española de Protección de Datos.
- ➔ La protección de datos de carácter personal en el derecho español. Pág. 120
- ➔ Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).
- ➔ Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.
- ➔ Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.