CNS 2/2022

Dictamen en relación con la consulta formulada por un Ayuntamiento relativa a la conformidad con la normativa de protección de datos del uso de dispositivos de control de presencia en el puesto de trabajo mediante reconocimiento facial

Se presenta ante la Autoridad Catalana de Protección de Datos una consulta de un Ayuntamiento en la que expone que tiene intención de instalar un sistema de control de presencia en el puesto de trabajo mediante reconocimiento facial. El Ayuntamiento solicita conocer la conformidad a la normativa de protección de datos del uso de estos sistemas, y plantea "[...] qué tratamiento se debe dar a los datos de reconocimiento facial necesarios para el correcto funcionamiento del aplicativo, y qué pasos debería seguir el Ayuntamiento para poder ponerlo en marcha [...]".

Analizada la petición, que no se acompaña de más información, vista la normativa vigente aplicable y de acuerdo con el informe de la Asesoría Jurídica, se dictamina lo siguiente:

(...)

II

El Ayuntamiento expone que tiene intención de instalar un nuevo dispositivo de control de presencia mediante reconocimiento facial. Expone que la necesidad de este sistema obedece a diferentes motivos: "[...] seguir las recomendaciones sanitarias con respecto a la Covid-19 para prevenir posibles contagios sustituyendo al sistema de control por huella dactilar, y por otra, poder disponer de una herramienta que de forma centralizada recoja los datos en un servidor central sin la necesidad de que sea necesario acudir a cada centro de trabajo a recoger los datos de cada trabajador para después volcar la información y poder realizar el control horario de forma individualizada, lo que dificulta el correcto seguimiento de las jornadas laborales. El hecho de tener varios centros de trabajo repartidos por diferentes edificios [...] hace que en el caso de usar una tarjeta personal e intransferible, no haya una manera de comprobar que ésta se utiliza de forma adecuada y unipersonal como debería ser para poder (hacer) un buen seguimiento".

El Ayuntamiento considera que el sistema de reconocimiento facial "[...] es un sistema de acreditación fidedigna de la presencia de personal en su puesto de trabajo, los días y horas que corresponden según su calendario de trabajo, y satisface plenamente las necesidades que tiene el ente municipal al respecto."

En relación con las características de este sistema, y su implementación, el Ayuntamiento informa que se instalará un terminal en cada centro de trabajo, que enviará toda la información registrada a un servidor central, en el que quedará almacenada en una base de datos, en formato texto, por un tiempo que no queda definido en la consulta. La información que se registrará en estos dispositivos será la relativa a los trabajadores y funcionarios, incluyendo una imagen de referencia de éstos para la lectura facial, así como los datos relativos a las jornadas. Por lo que respecta al acceso a esta información, el Ayuntamiento manifiesta que será restringido.

El Ayuntamiento también hace referencia a que la empresa instaladora le ha informado de la necesidad de solicitar, por escrito, a todo el personal laboral y funcionario del ente local la conformidad a la cesión de la imagen exclusivamente con el fin de poder realizar el control horario.

III

El Reglamento (UE) 2016/679 del Parlamento y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en cuanto al tratamiento de datos personales ya la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), en adelante RGPD, prevé que sus disposiciones son de aplicación a los tratamientos que se lleven a cabo sobre cualquier información *"sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un número, un número de identificación, datos de localización, un identificador online o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona" (arts.* 2.1 y 4.1).

Por otra parte, el artículo 4.2) del RGPD considera *"tratamiento": cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización , estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción".*

En base a estos preceptos, es evidente que el uso de dispositivos con el fin de control horario o de presencia mediante el reconocimiento facial comporta llevar a cabo un tratamiento de datos personales, el cual está sujeto a los principios y obligaciones que establece 'RGPD.
Además, hay que tener en cuenta que en la medida en que dichos dispositivos utilizarán mecanismos de reconocimiento facial, se tratarán datos biométricos. El artículo 4.14 del RGPD define los datos biométricos como "datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirman la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos".

Esto hace que, tal y como manifestó esta Autoridad en el dictamen CNS 21/2020 (el cual se puede consultar en la web www.apdcat.cat), el tratamiento de datos personales a partir de mecanismos automatizados con el objetivo de confirmar la identificación única de una persona a partir de datos biométricos, como la imagen facial, esté sometido a las previsiones del artículo 9 del RGPD.

El considerante 51 del RGPD hace referencia al tratamiento derivado de la imagen de una persona y pone de manifiesto el carácter restrictivo con el que se puede admitir el tratamiento de las categorías especiales de datos:

"[…] El tratamiento de fotografías no debe considerarse sistemáticamente tratamiento de categorías especiales de datos personales, pues únicamente se encuentran comprendidas en la definición de datos biométricos cuando el hecho de ser tratadas con medios técnicos específicos permita la identificación o la autenticación unívocas de una persona física. Tales datos personales no deben ser tratados, a menos que se permita su tratamiento en situaciones específicas contempladas en el presente Reglamento, habida cuenta de que los Estados miembros pueden establecer disposiciones específicas sobre protección de datos a fin de adaptar la aplicación de las normas del presente Reglamento al cumplimiento de una obligación legal o al cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. Además de los requisitos específicos de este tratamiento, deben aplicarse los principios generales y otras normas del presente Reglamento, sobre todo en lo que se refiere a las condiciones de licitud del tratamiento. Se deben establecer de forma explícita excepciones a la prohibición general de tratamiento de estas categorías especiales de datos personales, entre otras cosas cuando el interesado dé su consentimiento explícito o tratándose de necesidades específicas, en particular cuando el tratamiento sea realizado en el marco de actividades legítimas por determinadas asociaciones o fundaciones cuyo objetivo sea permitir el ejercicio de las libertades fundamentales."

El considerante 52 del RPGD añade:

"Asimismo deben autorizarse excepciones a la prohibición de tratar categorías especiales de datos personales cuando lo establezca el Derecho de la Unión o de los Estados miembros y siempre que se den las garantías apropiadas, a fin de proteger datos personales y otros derechos fundamentales, cuando sea en interés público, en particular el tratamiento de datos personales en el ámbito de la legislación laboral, la legislación sobre protección social, incluidas las pensiones y fines de seguridad, supervisión y alerta sanitaria, la prevención o control de enfermedades transmisibles y otras amenazas graves para la salud. Tal excepción es posible para fines en el ámbito de la salud, incluidas la sanidad pública y la gestión de los servicios de asistencia sanitaria, especialmente con el fin de garantizar la calidad y rentabilidad de los procedimientos utilizados para resolver las reclamaciones de prestaciones y de servicios en el régimen del seguro de enfermedad, o fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos. Debe autorizarse asimismo a título excepcional el tratamiento de dichas datos personales cuando sea necesario para la formulación, ejercicio o defensa de reclamaciones, ya sea por un procedimiento judicial o un procedimiento administrativo o extrajudicial".

Estos considerantes guardan relación con el principio de licitud (art. 5.1.a) del RGPD), a partir del cual cualquier tratamiento de datos personales debe ser lícito, y requiere que concurra alguna de las bases jurídicas establecidas en el artículo 6.1 del RGPD. Y, en la medida en que se traten categorías especiales de datos personales, como en el caso que nos ocupa, debe concurrir también alguna de las excepciones previstas en el artículo 9.2 del RGPD.

Según se desprende de la consulta, el tratamiento pretendido por el Ayuntamiento responde a la necesidad de controlar la presencia del personal al servicio del ente local en el puesto de trabajo. Así, en la medida

que el tratamiento de sus datos personales se realiza dentro de una relación jurídica laboral o administrativa, y tiene como finalidad el control por el personal de sus obligaciones y deberes, en particular, la presencia o cumplimiento de la jornada, sería posible acudir en la base jurídica prevista en el artículo 6.1.b) del RGPD ("el tratamiento es necesario para la ejecución de un contrato en el que el interesado se parte o para la aplicación a petición del mismo de medidas precontractuales").

En cuanto al personal laboral, será necesario tener en cuenta la legislación laboral (artículo 2.4 del Decreto 214/1990, de 30 de julio, por el que se aprueba el Reglamento del personal al servicio de las entidades locales). Y, en este sentido, conviene llevar al análisis la previsión del artículo 20.3 del Estatuto de los Trabajadores, aprobado por Real Decreto Legislativo 2/2015, de 23 de octubre, según el cual:

"El empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad y teniendo en cuenta, en su caso, la capacidad real de los trabajadores con discapacidad"

Y, en particular, el artículo 34.9 del Estatuto de los Trabajadores, que prevé lo siguiente:

"La empresa garantizará el registro diario de jornada, que deberá incluir el horario concreto de inicio y finalización de la jornada de trabajo de cada persona trabajadora, sin perjuicio de la flexibilidad horaria que se establece en este artículo.

Mediante negociación colectiva o acuerdo de empresa o, en su defecto, decisión del empresario previa consulta con los representantes legales de los trabajadores en la empresa, se organizará y documentará este registro de jornada.

La empresa conservará los registros a que se refiere este precepto durante cuatro años y permanecerán a disposición de las personas trabajadoras, de sus representantes legales y de la Inspección de Trabajo y Seguridad Social."

En base a este precepto, en lo que concierne al personal laboral del ente local, el tratamiento relativo al control de la presencia o jornada laboral podría también estar legitimado en base al artículo 6.1.c) del RGPD , es decir, cuando el tratamiento es necesario por el cumplimiento de una obligación legal aplicable al responsable del tratamiento.

Ahora bien, tal y como hemos avanzado, el tratamiento de datos biométricos con el fin de identificar de forma unívoca a una persona física requiere que, además de una base jurídica del artículo 6.1 del RGPD, concurra también alguna de las excepciones previstas en el artículo 9.2 del RGPD.

En caso de que se examina, conviene analizar el supuesto previsto en la letra b) del artículo 9.2 del RGPD, relativo a cuando el tratamiento es necesario para el cumplimiento de obligaciones y ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del derecho laboral y de la seguridad y protección social, en la medida en que lo autorice el derecho de la Unión o de los Estados miembros o un convenio colectivo de acuerdo con el derecho de los estados miembros que establezca garantías adecuadas respecto de los derechos fundamentales y de los intereses del interesado.

Para que concurra esta circunstancia, será necesario:

a) Que el tratamiento sea necesario para el cumplimiento de obligaciones o el ejercicio de derechos específicos del empresario o de la persona interesada en el ámbito del derecho laboral o de la seguridad y protección social, y

b) Que lo autorice el derecho de la Unión o de los Estados miembros o un convenio colectivo, que establezcan garantías adecuadas en lo que respecta al respeto de los derechos fundamentales y los intereses de las personas afectadas.

En cuanto a la habilitación contenida al derecho de los estados miembros, el considerante 41 del RGPD dispone que “cuando el presente Reglamento hace referencia a una base jurídica oa una medida legislativa, esto no exige necesariamente un acto legislativo adoptado por un parlamento ”, pero añade que esto debe entenderse “sin perjuicio de los requisitos de conformidad con el ordenamiento constitucional del Estado miembro de que se trate”. En el caso del Estado Español, de acuerdo con las exigencias constitucionales, la norma que lo prevea, por tratarse del desarrollo de un derecho fundamental, deberá tener rango de ley (artículo 53 CE).

En este sentido, el artículo 88 del RGPD ha establecido que los Estados miembros pueden, a través de disposiciones legislativas o de convenios colectivos, establecer normas más específicas para garantizar la protección de los derechos y libertades en relación con el tratamiento de datos personales de los trabajadores en el ámbito laboral, en particular, entre otros, a efectos del cumplimiento de las obligaciones que establece la ley o el convenio colectivo, la gestión, planificación y organización del trabajo. Estas normas deben incluir medidas adecuadas y específicas para preservar la dignidad humana de los interesados, así como sus intereses legítimos y sus derechos fundamentales, en particular, en relación, entre otros con los sistemas de supervisión en el sitio de trabajo.

De acuerdo con lo avanzado, en el caso del personal sometido al régimen laboral, el Estatuto de los Trabajadores prevé la posibilidad de que el empresario adopte medidas de vigilancia y control para verificar el cumplimiento de las obligaciones laborales de sus trabajadores (art. 20.3), pero para el caso del control de la jornada, establece la necesidad de elaborar un registro diario de las jornadas (art. 34.9).

Sin embargo, conviene tener en cuenta que la normativa no determina el mecanismo que se puede utilizar para registrar la jornada, ni prevé ninguna autorización para utilizar categorías especiales de datos, en concreto, de datos biométricos.

En relación con esta falta de concreción de la norma, debe tenerse en cuenta la sentencia del Tribunal Constitucional 76/2019, de 22 de mayo, en la que el tribunal recuerda que la injerencia estatal en el ámbito de los derechos fundamentales y las libertades públicas requiere una norma con rango de ley y precisa los requisitos indispensables que debe reunir esta norma como garantía de la seguridad jurídica:

“[…] Esta doble función de la reserva de ley se traduce en una doble exigencia: por un lado, la necesaria intervención de la ley para habilitar la injerencia; y, por otro lado, esta norma legal "debe reunir todas aquellas características indispensables como garantía de la seguridad jurídica", esto es, "debe expresar todos y cada uno de los presupuestos y condiciones de la intervención"
(STC 49/1999, FJ 4). En otras palabras, "no sólo excluye apoderamientos a favor de las normas

reglamentarias [...], sino que también implica otras exigencias respecto al contenido de la Ley que establece tales límites" (STC 292/2000, FJ 15).

La segunda exigencia mencionada constituye la dimensión cualitativa de la reserva de ley, y se concreta en las exigencias de previsibilidad y certeza de las medidas restrictivas en el ámbito de los derechos fundamentales. En la STC 292/2000, FJ 15, señalamos que, aun teniendo un fundamento constitucional, las limitaciones del derecho fundamental establecidas por una ley "pueden vulnerar la Constitución si adolecen de falta de certeza y previsibilidad en los propios límites que imponen y su modo de aplicación", pues "la falta de precisión de la Ley en los presupuestos materiales de la limitación de un derecho fundamental es susceptible de generar una indeterminación sobre los casos a los que se aplica tal restricción"; "al producirse este resultado, más allá de toda interpretación razonable, la Ley ya no cumple su función de garantía del propio derecho fundamental que restringe, pues deja que en su lugar opere simplemente la voluntad de quien debe aplicarla". En la misma Sentencia y fundamento jurídico precisamos también el tipo de vulneración que acarrea la falta de certeza y previsibilidad en los propios límites: " no sólo lesionaría el principio de seguridad jurídica (art. 9.3 CE), concebida como certeza sobre el ordenamiento aplicable y expectativa razonablemente fundada de la persona sobre cuál debe ser la actuación del poder aplicando el Derecho (STC 104/2000, FJ 7, por todas), sino que al mismo tiempo dicha Ley estaría lesionando el contenido esencial del derecho fundamental así restringido, dado que la forma en que se han fijado o sobre los límites lo hacen irreconocible e imposibilitan, en la práctica, su ejercicio (SSTC 11/1981, FJ 15; 142/1993, de 22 de abril (RTC 1993, 142), FJ 4, y 341/1993, de 18 de noviembre (RTC 1993, 341), FJ 7)".

Es decir, la afectación por el derecho a la protección de datos que se derive de la norma debe ser previsible. Y en un caso como el que nos ocupa, no se puede considerar previsible la norma si no concreta la posibilidad de utilizar datos biométricos con el fin de realizar el control horario.

Además, en la sentencia también se determina que la norma debe establecer garantías adecuadas, especialmente cuando se traten categorías especiales de datos. En particular, el Tribunal manifiesta lo siguiente:

La exigencia de especial protección de esta categoría de datos está prevista en el Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (RCL 1985, 2704) , de 28 de enero de 1981 (RCL 1985, 2704), ratificado por España el 15 de noviembre de 1985, cuyo artículo 6 establece lo siguiente: "Las datos de carácter personal que revelan el origen racial, las opiniones políticas, las

convicciones religiosas u otras convicciones, así como las datos de carácter personal relativas a la salud oa la vida sexual, no podrán tratarse automáticamente a menos que el derecho interno prevea garantías apropiadas. [...]." […]

Las garantías adecuadas deben velar por que el tratamiento de datos se realice en condiciones que aseguren la transparencia, la supervisión y la tutela judicial efectiva, y deben procurar que las datos no se recojan de forma desproporcionada y no se utilicen para fines distintos de los que justificaron su obtención. La naturaleza y el alcance de las garantías que resulten constitucionalmente exigibles en cada caso dependerán de tres factores esencialmente: el tipo

de tratamiento de datos que se pretende llevar a cabo; la naturaleza de las datos; y la probabilidad y gravedad de los riesgos de abuso y utilización ilícita que, a su vez, están vinculadas al tipo

de tratamiento y en la categoría de datos de que se trate. Así, no plantean los mismos problemas una recogida de datos con fines estadísticos que una recogida de datos con un fin concreto. Tampoco supone el mismo grado de injerencia la recopilación y procesamiento de datos anónimos que la recopilación y procesamiento de datos personales que se toman individualmente y no se anonimizan, como no es lo mismo el tratamiento de datos personales que revelan el origen étnico o racial , las opiniones políticas, la salud, la vida sexual o la orientación sexual de una persona física, que el tratamiento de otro tipo de datos.

El nivel y la naturaleza de las garantías adecuadas no se pueden determinar de una vez para todas, pues, por un lado, deben revisarse y actualizarse cuando sea necesario y, por otro lado, el principio de proporcionalidad obliga a verificar si, con el desarrollo de la tecnología, aparecen posibilidades de tratamiento que resultan menos intrusivas o potencialmente menos peligrosas para los derechos fundamentales."

En la medida en que las categorías especiales de datos tienen especial protección, superior a otros datos personales, "Una protección adecuada y específica frente al tratamiento constituye, en suma, una exigencia constitucional, sin perjuicio de que, como se ha visto, también represente una exigencia derivada del derecho de la Unión Europea. Por tanto, el legislador está constitucionalmente obligado a adecuar la protección que dispensa a dichas datos personales, en su caso, imponiendo mayores exigencias a fin de que puedan ser objeto de tratamiento y previendo garantías específicas en su tratamiento, además de las que puedan ser comunes o generales."

Así, ante la falta de previsibilidad de la normativa, no parece que el tratamiento de control horario mediante el reconocimiento facial pueda basarse en una norma con rango de ley, de acuerdo con la previsión de la letra b) del artículo 9.2 del RGPD.

Por lo que respecta al personal sometido a una relación jurídica administrativa, si bien la normativa relativa a la función pública no recoge previsiones específicas relacionadas con el registro de la jornada del personal, equivalentes a los artículos 20.3 y 34.9 del Estatuto de los Trabajadores, sí encontramos previsiones relacionadas con el cumplimiento de la jornada estipulada (por ejemplo, el artículo 54.3 del Real decreto legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del estatuto básico de empleado público, o el artículo 108.2.g) del Decreto legislativo 1/1997, de 31 de octubre, por el que se aprueba la refundición en un Texto único de los preceptos de determinados textos legales vigentes en Cataluña en materia de función pública), y el régimen disciplinario aplicable en caso de incumplimiento de ésta (como, el artículo 116, apartado .o) yq) (faltas graves) o el artículo el 117.d) (faltas leves) del Decreto legislativo 1/1997, de 31 de octubre.) a partir de los cuales las administraciones públicas pueden adoptar más ras de vigilancia y control de la ejecución de la jornada por parte de los empleados públicos.

Sin embargo, tal y como sucede en el caso del personal laboral, la normativa no prevé que se utilicen datos biométricos para controlar la presencia o ejecución de la jornada.

A falta de previsión legal, cabe recordar que, de acuerdo con lo que prevé el artículo 9.2.b) del RGPD, la autorización puede estar prevista en el marco de un convenio colectivo. Previsión a entender también aplicable a los acuerdos sobre condiciones de trabajo del personal funcionario en el marco de la negociación colectiva. Por ello, en caso de que el convenio colectivo, el pacto o acuerdo resultante de la negociación prevea la utilización de datos biométricos a tal fin y establezca garantías adecuadas respecto a los derechos fundamentales y de los intereses de las personas interesadas, este instrumento permitiría concluir la concurrencia de la excepción prevista en el artículo 9.2.b) del RGPD.

IV

En la consulta, el Ayuntamiento hace referencia a que la entidad instaladora de los dispositivos ha indicado la necesidad de contar con el consentimiento del personal para el tratamiento de su imagen con el fin de control horario. Se entiende que el Ayuntamiento se refiere a la base jurídica del consentimiento (art. 6.1.a del RGPD), que debe ser explícito en el caso de tratamientos sobre categorías especiales de datos (art. 9.2.a) del RGPD).

El artículo 4.11) del RGPD prevé que el consentimiento constituye "[...] toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen".

Asimismo, debe tenerse en cuenta que, en la medida en que el tratamiento pretendido conlleva tratar categorías especiales de datos, el consentimiento debe ser explícito (art. 9.2.a) RGPD). En relación con este requisito, es necesario tener en cuenta las Directrices 5/2020 sobre el consentimiento en el sentido del Reglamento (UE) 2016/679 del Comité Europeo de Protección de Datos (CEPD) (https://edpb.europa.eu/ sites/default/files/files/file1/edpb_guidelines_202005_consent_es.pdf):

"93. El término explícito se refiere al modo en que el interesado expresa el consentimiento. Significa que el interesado debe realizar una declaración expresa de consentimiento. Un modo evidente de garantizar que el consentimiento se explícito sería confirmar de modo expreso dicho consentimiento en una declaración escrita. Cuando proceda, el responsable podría asegurarse de que el interesado firma la declaración escrita, a fin de eliminar cualquier posible duda o falta de prueba en el futuro. […]".

En cuanto al requisito de que el consentimiento sea libre, el considerante 43 del RGPD expone lo siguiente:

"[…] el consentimiento […] no debe constituir un fundamento jurídico válido para el tratamiento de datos de carácter personal en un caso concreto en el que exista un desequilibrio claro entre el interesado y el responsable del tratamiento, en particular cuando dicho responsable sea una autoridad pública y sea por tanto improbable que el consentimiento se haya dado libremente en todas las circunstancias de dicha situación particular."

Al respecto, relativa al carácter libre del consentimiento, hay que tener en cuenta también las Directrices 5/2020 del CEPD. De estas Directrices conviene destacar lo siguiente:

"13. El término «libro» implica elección y control real por parte de los interesados. […] si el sujeto no es realmente libre para elegir, se siente obligado a dar su consentimiento o sufrirá consecuencias negativas si no lo da, entonces el consentimiento no puede considerarse válido.
[…] La noción de desequilibrio entre el responsable del tratamiento y el interesado también se tiene en cuenta en el RGPD.

14. A la hora de valorar si el consentimiento se ha dado libremente, deben considerarse también las situaciones concretas en las que el consentimiento se supedita a la ejecución de contratos oa la prestación de un servicio […]. En términos generales, el consentimiento quedará invalidado por cualquier influencia o presión inadecuada ejercida sobre el interesado (que puede manifestarse de formas muy distinguidas) que impida que éste ejerza su libre voluntad.

[…]

16. El considerando 43 indica claramente que no es probable que las autoridades públicas puedan basarse en el consentimiento para realizar el tratamiento de datos ya que cuando el responsable del tratamiento es una autoridad pública, siempre hay un claro desequilibrio de poder en la relación entre el responsable del tratamiento y el interesado. Queda también claro en la mayoría de los casos que el interesado no dispondrá de alternativas realistas para aceptar el tratamiento (las condiciones de tratamiento) de dicho responsable.

El CEPD considera que existen otras bases jurídicas que son, en principio, más adecuadas para el tratamiento de datos por las autoridades públicas.

17. Sin perjuicio de estas consideraciones generales, el uso del consentimiento como una base jurídica para el tratamiento de datos por parte de las autoridades públicas no queda totalmente excluido en virtud del marco jurídico del RGPD. […]

21. También en el contexto del empleo se produce un desequilibrio de poder. Dada la dependencia que resulta de la relación entre el empleador y el empleado, no es probable que el interesado pueda negar al empleador el consentimiento para el tratamiento de datos sin experimentar temor o riesgo real de que su negativa produzca efectos perjudiciales. Parece poco probable que un empleado pudiera responder libremente a una solicitud de consentimiento del empleador para, por ejemplo, activar sistemas de vigilancia por cámara en el lugar de trabajo o para rellenar impresos de evaluación, sin sentirse presionado a dar su consentimiento.
[…] En el caso de la mayoría de estos tratamientos de datos en el trabajo, la base jurídica no puede y no debe ser el consentimiento de los trabajadores […] debido a la naturaleza de la relación entre empleador y empleado.

22. Sin embargo, esto no significa que los empleadores no puedan basarse nunca en el consentimiento como base jurídica para el tratamiento de datos. Puede haber situaciones en las que el empleador pueda demostrar que el consentimiento se ha dado libremente. Dado el desequilibrio de poder entre un empleador y los miembros de su personal, los trabajadores únicamente pueden dar su libre consentimiento en circunstancias excepcionales, cuando el hecho de que otorguen o no dicho consentimiento no tenga consecuencias adversas".

En base a lo expuesto, y otras cuestiones que también quedan recogidas en las Directrices 5/2020 del CEPD, a las que nos remitimos, no parece que la base jurídica del consentimiento sea adecuada para legitimar el tratamiento de los datos del personal con el fin del control horario del personal, dado que no puede considerarse que en el caso planteado pudiera existir un consentimiento realmente libre. En este sentido, podría considerarse que existe consentimiento libre si el interesado dispone de una alternativa para cumplir con el control horario o controlar su presencia o ejecución del horario, siendo éste quien elige y presta su consentimiento al tratamiento de sus datos biométricos a través de sistemas de reconocimiento facial, pero no parece que sea así en un caso como el descrito en la consulta.

En definitiva, la normativa de protección de datos no admite a todos los efectos el consentimiento como base jurídica legitimadora de los tratamientos llevados a cabo por las administraciones públicas o los empresarios para el control en el entorno laboral, dado el desequilibrio de poder que suele producirse entre las relaciones de aquéllos con los interesados, que impide que el consentimiento pueda considerarse libre.

A tal efecto, debe tenerse en consideración que, de acuerdo con el principio de responsabilidad proactiva (art. 5.2 del RGPD), el responsable del tratamiento, en caso de que nos ocupa el Ayuntamiento, debe ser capaz de demostrar que el consentimiento es válido y que el tratamiento es lícito.

V

Al margen del principio de licitud, cualquier tratamiento debe cumplir también el resto de los principios y obligaciones derivados de la normativa de protección de datos, tales como el principio de minimización (art. 5.1.c) RGPD).

En este sentido, el Dictamen 3/2012 del Grupo de Trabajo del Artículo 29, sobre la evolución de las tecnologías biométricas afirmaba lo siguiente en relación con el análisis del cumplimiento del principio de minimización:

“Al analizar la proporcionalidad de un sistema biométrico propuesto, se preciso considerar previamente si el sistema es necesario para responder a la necesidad identificada, es decir, si es esencial para satisfer esa necesidad, y no sólo lo más adecuado o rentable. Un segundo factor que debe tenerse en cuenta es la probabilidad de que el sistema sea eficaz para responder a la necesidad en cuestión a la luz de las características específicas de la tecnología biométrica que se va a utilizar. Un tercer aspecto a ponderar es si la pérdida de intimidad resultante es proporcional a los beneficios esperados. Si el beneficio es relativamente menor, como una mayor comodidad o un ligero ahorro, entonces la pérdida de intimidad no es apropiada. El cuarto aspecto para evaluar la adecuación de un sistema biométrico se considerar si un medio menos invasivo de la intimidad alcanzaría el fin deseado.”

Parece clara la necesidad de admitir la instalación de sistemas de control del cumplimiento horario por parte del personal, tal y como ha reconocido de forma reiterada esta Autoridad. Sin embargo, no parece tan claro que la utilización de sistemas de control horario basados en datos biométricos deban ser admitidos como medio preferente para llevar a cabo en el control. Más bien lo contrario.
Dada la especial naturaleza de estos datos habrá que optar, en primer lugar, por otros sistemas de

control que, sin utilizar categorías de datos especialmente protegidas, puedan permitir alcanzar la misma finalidad.

Las exigencias derivadas de la protección de datos en el diseño (art. 25.1 RGPD) y, en especial, del principio de minimización, obligan a elegir esa tecnología que resulte menos intrusiva desde el punto de vista de la protección de datos. El principio de minimización no se manifiesta sólo a la hora de optar por alternativas que no impliquen el tratamiento de datos personales, o de llevar a cabo el tratamiento de datos de forma que se empleen los datos mínimos indispensables, sino que también comportar que si se puede alcanzar una determinada finalidad sin tener que tratar datos de categorías especiales, esta opción debe prevalecer ante otras opciones que sí impliquen el tratamiento de este tipo de datos.

Hay que tener en cuenta que los datos biométricos, dado su carácter personal y único, constituyen un medio fiable de identificación (aunque en determinados datos biométricos puede existir un riesgo de no identificabilidad). La fiabilidad como sistema de identificación, pero está condicionada también por la amplitud con la que se puedan utilizar estos sistemas de identificación.
Cuanto mayor sea el número de sistemas de identificación que se basan en unos datos biométricos o en una plantilla obtenida a partir de datos biométricos, mayor es el riesgo de que este dato pueda acabar siendo utilizado de forma inadecuada y dando lugar a un riesgo de usurpación o suplantación de identidad. Este riesgo puede incrementarse claramente en función de cuál sea la tecnología empleada y del tratamiento que se dé a los datos biométricos en bruto u originales.

Por una parte, una pérdida de confidencialidad de estos datos podría permitir, en función de la tecnología utilizada, la suplantación. Sin embargo, es que además, estos datos no son modificables. Es decir, a diferencia de una contraseña, en caso de pérdida no pueden cambiarse.

Por otra parte, también existen riesgos evidentes si la tecnología utilizada no garantiza de forma suficiente que la plantilla obtenida a partir de los datos biométricos no coincidirá con la empleada en otros sistemas similares.

A efectos de determinar los riesgos existentes y las medidas para mitigarlos, pueden ser de ayuda las Directrices 3/2019 sobre el tratamiento de datos personales mediante dispositivos de vídeo del CEPD, en particular el apartado 5.2 relativo a las medidas sugeridas para minimizar los riesgos en el consultable tratar datos biométricas, enlace https://edpb.europa.eu/sites/default/files/files/ al siguiente edpb_guidelines_201903_video_devices_es.pdf.

Es innegable que la utilización de sistemas basados en datos biométricos para llevar a cabo el control horario evita el riesgo de suplantación que puede producirse en algún caso, como apunta la consulta. Ahora bien, no parece ser el único sistema que permita garantizarlo. Por ejemplo, a efectos del control horario, la utilización de tarjetas personales u otros tipos de objetos (token) en un sistema de marcado, la utilización de códigos personales, la visualización directa del punto de marcado o la utilización de sistemas de videovigilancia donde quede constancia de la hora de entrada o salida pueden constituir, por sí mismos o en combinación con alguno de los demás sistemas disponibles, medidas eficaces para llevar a cabo el control.

La consulta, al margen de hacer referencia a la necesidad de evitar el riesgo de suplantación que otros mecanismos de marcaje pueden tener, como por ejemplo el uso de tarjetas individuales, también hace referencia a que uno de los motivos de instalación de estos sistemas es seguir las recomendaciones sanitarias con respecto a la Covid-19 para prevenir posibles contagios sustituyendo al sistema de control por huella dactilar.

Si bien la consulta no concreta a qué recomendación se refiere, se entiende que hace referencia a las recomendaciones de las autoridades públicas en el marco de la pandemia por la Covid-19, como por ejemplo, el Ministerio de Sanidad, el cual a diferentes Órdenes (como, la Orden SND/388/2020, de 3 de mayo; la Orden SND/399/2020, de 9 de mayo, o bien la Orden SND/458 /2020, de 30 de mayo) ha previsto, recogido en diferentes artículos respectivamente, lo siguiente:

"El fichaje con huella dactilar será sustituido por cualquier otro sistema de control horario que garantice las medidas higiénicas adecuadas para la protección de la salud y la seguridad de los trabajadores, o bien se deberá desinfectar el dispositivo de fichaje antes y después de cada uso, advirtiendo a los trabajadores de esta medida."

De entrada, esta recomendación en ningún caso puede constituir una excepción para el tratamiento de categorías especiales de datos a los efectos previstos en el artículo 9.2.b). Pero más allá de esto, existen otras alternativas posibles de aplicación sencilla, sin tener que cambiar el sistema de control, como desinfectar el dispositivo de marcado antes y después de cada uso, o bien que el trabajador disponga de un expendedor de hielo antiséptico cerca del sistema de marcado para ser usado una vez realizado el fichaje con el dedo, tanto de entrada como de salida. Por tanto, la sustitución del sistema de marcación no parece que deba ser la única opción.

Hay que tener presente que el tratamiento de la huella dactilar constituye también un tratamiento de datos biométricos, dado lo que prevé el artículo 4.11 del RGPD. Esto quiere decir que al igual que el tratamiento mediante reconocimiento facial requiere, además de una base jurídica de acuerdo con lo que prevé el artículo 6.1 del RGPD, que concurra alguno de los supuestos que prevé el artículo 9.2 del RGPD, de acuerdo con lo analizado, el tratamiento de la huella dactilar a tal fin también lo requiere en la medida en que se trata de una categoría especial de datos. En cualquier caso, si se dispone de base jurídica para tratar la huella dactilar con finalidad de control horario, pero no para utilizar mecanismos de reconocimiento facial, mientras dure esta situación, debería recurrirse a otro sistema que no comporte el tratamiento de categorías especiales de datos.

Por último, recordar que, con carácter previo a la decisión sobre la puesta en marcha de un sistema de control de este tipo, hay que tener en cuenta que el artículo 35 del RGPD prevé la necesidad de realizar una evaluación del impacto relativa a la protección de datos (AIPD) en aquellos tratamientos, especialmente si utilizan nuevas tecnologías, que comporten un alto riesgo por los derechos y libertades de las personas. A estos efectos, y de acuerdo con el artículo 35.4 del RGPD, esta Autoridad ha publicado una Lista de tipos de tratamientos de datos que requieren evaluación de impacto relativa protección de datos (https://apdcat.gencat.cat /web/.content/02-a la derechos_y_obligaciones/obligaciones/documentos/Lista-DPIA-CAT.pdf), en la que se determina que será necesario realizar una AIPD en la mayoría de los casos en que el tratamiento cumpla con dos o más criterios de la lista. Entre estos criterios, pueden concurrir en caso de que se analiza los siguientes:

"[...] 3. Tratamientos que impliquen la observación, monitorización, supervisión, geolocalización o control del interesado de forma sistemática y exhaustiva, incluida la recogida de datos y metadatos a través de redes, aplicaciones o en zonas de acceso público, así como el procesamiento de identificadores únicos que permitan la identificación de usuarios de servicios de la sociedad de la información como pueden ser los servicios web, TV interactiva, aplicaciones móviles, etc.
[...]
5. Tratamientos que impliquen el uso de datos biométricos con el propósito de identificar de modo único a una persona física.
[...]
10. Tratamientos que impliquen la utilización de nuevas tecnologías o un uso innovador de tecnologías consolidadas, incluyendo la utilización de tecnologías a una nueva escala, con un nuevo objetivo o combinadas con otros, de forma que suponga nuevas formas de recogida y utilización de datos con riesgo por los derechos y libertades de las personas.[...]"

En consecuencia, es necesario realizar una evaluación del impacto relativa a la protección de datos, en la que es necesario evaluar tanto la legitimidad del tratamiento y su proporcionalidad, como la determinación de los riesgos existentes y las medidas para mitigarlos (art. 35 RGPD).

De acuerdo con las consideraciones hechas en estos fundamentos jurídicos en relación con la consulta planteada en relación con la utilización de sistemas de control basados en mecanismos de reconocimiento facial, se hacen las siguientes,

Conclusiones

El consentimiento del personal afectado no puede considerarse una base jurídica adecuada para la implantación de un sistema de control horario mediante reconocimiento facial como el descrito en la consulta.

Sería necesaria la previsión de este sistema de control en una disposición legal o en un convenio colectivo aplicable, o en su caso, en un pacto o acuerdo resultado de la negociación colectiva, circunstancias que no parecen concurrir en el caso analizado. En cualquier caso, antes de la implantación de un sistema de este tipo, es necesario realizar una evaluación del impacto sobre la protección de datos a la vista de las circunstancias concretas en las que se lleve a cabo el tratamiento para determinar su ción y la proporcionalidad, incluido el análisis de la existencia de alternativas menos intrusivas, y establecer las garantías adecuadas.

Barcelona, 2 de febrero de 2022