CNS 2/2022

Dictamen en relació amb la consulta formulada per un Ajuntament relativa a la conformitat a la normativa de protecció de dades de l'ús de dispositius de control de presència al lloc de treball mitjançant reconeixement facial

Es presenta davant l'Autoritat Catalana de Protecció de Dades una consulta d'un Ajuntament en la qual exposa que té intenció d'instal·lar un sistema de control de presència al lloc de treball mitjançant reconeixement facial. L'Ajuntament sol·licita conèixer la conformitat a la normativa de protecció de dades de l'ús d'aquests sistemes, i planteja *"[...] quin tractament cal donar a les dades de reconeixement facial necessàries per al correcte funcionament de l'aplicatiu, i quines passes hauria de seguir l'Ajuntament per poder-lo posar en marxa [...]".*

Analitzada la petició, que no s'acompanya de més informació, vista la normativa vigent aplicable i d'acord amb l'informe de l'Assessoria Jurídica, es dictamina el següent:

I

(...)

II

L'Ajuntament exposa que té intenció d'instal·lar un nou dispositiu de control de presència mitjançant reconeixement facial. Exposa que la necessitat d'aquest sistema obeeix a diferents motius: *"[...] seguir les recomanacions sanitàries pel que fa a la Covid-19 per prevenir possibles contagis substituint el sistema de control per empremta dactilar, i d'altra, poder disposar d'una eina que de manera centralitzada reculli les dades en un servidor central sense la necessitat de que calgui anar a cada centre de treball a recollir les dades de cada treballador per després bolcar la informació i poder fer el control horari de manera individualitzada, cosa que dificulta el seguiment correcte de les jornades laborals. El fet de tenir diversos centres de treball repartits per diferents edificis [...] fa que en el cas d'usar una targeta personal i intransferible, no hi hagi una manera de comprovar que aquesta es fa servir de manera adequada i unipersonal com hauria de ser per poder* (fer) *un bon seguiment".*

L'Ajuntament considera que el sistema de reconeixement facial *"[...] és un sistema d'acreditació fidedigna de la presència de personal al seu lloc de treball, els dies i hores que pertoquen segons el seu calendari de treball, i satisfà plenament les necessitats que té l'ens municipal al respecte."*

En relació amb les característiques d'aquest sistema, i la seva implementació, l'Ajuntament informa que s'instal·larà un terminal a cada centre de treball, el qual enviarà tota la informació registrada a un servidor central, en el qual quedarà emmagatzemada en una base de dades, en format text, per un temps el qual no queda definit a la consulta. La informació que s'enregistrarà en aquests dispositius serà la relativa als treballadors i funcionaris, incloent-hi una imatge de referència d'aquests per a la lectura facial, així com les dades relatives a les jornades. Pel que fa a l'accés a aquesta informació, l'Ajuntament manifesta que serà restringit.

L'Ajuntament també fa referència al fet que l'empresa instal·ladora l'ha informat de la necessitat de sol·licitar, per escrit, a tot el personal laboral i funcionari de l'ens local la conformitat a la cessió de la imatge exclusivament amb la finalitat de poder fer el control horari.

III

El Reglament (UE) 2016/679 del Parlament i del Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades i pel qual es deroga la Directiva 95/46/CE (Reglament general de protecció de dades), d'ara endavant RGPD, preveu que les seves disposicions són d'aplicació als tractaments que es duguin a terme sobre qualsevol informació "*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 nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona*" (arts. 2.1 i 4.1).

Per altra banda, l'article 4.2) de l'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*".

Sobre la base d'aquests preceptes, és evident que l'ús de dispositius amb la finalitat de control horari o de presència mitjançant el reconeixement facial comporta dur a terme un tractament de dades personals, el qual està subjecte als principis i obligacions que estableix l'RGPD.
A més, cal tenir en compte que en la mesura que els dits dispositius empraran mecanismes de reconeixement facial, es tractaran dades biomètriques. L'article 4.14 de l'RGPD defineix les dades biomètriques com *"datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos".*

Això fa que, tal com va manifestar aquesta Autoritat al dictamen CNS 21/2020 (el qual es pot consultar al web www.apdcat.cat), el tractament de dades personals a partir de mecanismes automatitzats amb l'objectiu de confirmar la identificació única d'una persona a partir de dades biomètriques, com ara la imatge facial, estigui sotmès a les previsions de l'article 9 de l'RGPD.

El considerant 51 de l'RGPD fa referència al tractament derivat de la imatge d'una persona i posa de manifest el caràcter restrictiu amb què es pot admetre el tractament de les categories especials de dades:

"[…] 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 con objeto 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 ese 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 esas 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 considerant 52 de l'RPGD afegeix:

"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 con 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 la rentabilidad de los procedimientos utilizados para resolver las reclamaciones de prestaciones y de servicios en el régimen del seguro de enfermedad, o con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos. Debe autorizarse asimismo a título excepcional el tratamiento de dichos datos personales cuando sea necesario para la formulación, el ejercicio o la defensa de reclamaciones, ya sea por un procedimiento judicial o un procedimiento administrativo o extrajudicial".

Aquests considerants guarden relació amb el principi de licitud (art. 5.1.a) de l'RGPD), a partir del qual qualsevol tractament de dades personals ha de ser lícit, i requereix que concorri alguna de les bases jurídiques establertes a l'article 6.1 de l'RGPD. I, en la mesura que es tractin categories especials de dades personals, com en el cas que ens ocupa, ha de concórrer també alguna de les excepcions previstes a l'article 9.2 de l'RGPD.

Segons es desprèn de la consulta, el tractament pretès per l'Ajuntament respon a la necessitat de controlar la presència del personal al servei de l'ens local al lloc de treball. Així, en la mesura

que el tractament de les seves dades personals es realitza dins d'una relació jurídica laboral o administrativa, i té com a finalitat el control pel personal de les seves obligacions i deures, en particular, la presència o compliment de la jornada, seria possible acudir a la base jurídica prevista a l'article 6.1.b) de l'RGPD (*"el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales").*

Pel que fa al personal laboral, caldrà tenir en compte la legislació laboral (article 2.4 del Decret 214/1990, de 30 de juliol, pel qual s'aprova el Reglament del personal al servei de les entitats locals). I, en aquest sentit, convé portar a l'anàlisi la previsió de l'article 20.3 de l'Estatut dels Treballadors, aprovat pel Reial decret legislatiu 2/2015, de 23 d'octubre, segons el qual:

"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"

I, en particular, l'article 34.9 de l'Estatut dels Treballadors, el qual preveu el següent:

"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."

Sobre la base d'aquest precepte, pel que fa al personal laboral de l'ens local, el tractament relatiu al control de la presència o jornada laboral podria també estar legitimat sobre la base de l'article 6.1.c) de l'RGPD, és a dir, quan el tractament és necessari pel compliment d'una obligació legal aplicable al responsable del tractament.

Ara bé, tal com hem avançat, el tractament de dades biomètriques amb la finalitat d'identificar de manera unívoca una persona física requereix que, a més d'una base jurídica de l'article 6.1 de l'RGPD, concorri també alguna de les excepcions que preveu l'article 9.2 de l'RGPD.

En el cas que s'examina, convé analitzar el supòsit que preveu la lletra b) de l'article 9.2 de l'RGPD, relatiu a quan el tractament és necessari per al compliment d'obligacions i exercici de drets específics del responsable del tractament o de l'interessat en l'àmbit del dret laboral i de la seguretat i protecció social, en la mesura que ho autoritzi el dret de la Unió o dels Estats membres o un conveni col·lectiu d'acord amb el dret dels estats membres que estableixi garanties adequades respecte dels drets fonamentals i dels interessos de l'interessat.

Per tal que concorri aquesta circumstància, però, caldrà:

a) Que el tractament sigui necessari per al compliment d'obligacions o l'exercici de drets específics de l'empresari o de la persona interessada en l'àmbit del dret laboral o de la seguretat i protecció social, i

b) Que ho autoritzi el dret de la Unió o dels estats membres o un conveni col·lectiu, que estableixin garanties adequades pel que fa al respecte dels drets fonamentals i els interessos de les persones afectades.

Pel que fa a l'habilitació continguda al dret dels estats membres, el considerant 41 de l'RGPD disposa que *"cuando el presente Reglamento hace referencia a una base jurídica o a una medida legislativa, esto no exige necesariamente un acto legislativo adoptado por un parlamento"*, però afegeix que això s'ha d'entendre *"sin perjuicio de los requisitos de conformidad con el ordenamiento constitucional del Estado miembro de que se trate"*. En el cas de l'Estat Espanyol, d'acord amb les exigències constitucionals, la norma que ho prevegi, per tractar-se del desenvolupament d'un dret fonamental, haurà de tenir rang de llei (article 53 CE).

En aquest sentit, l'article 88 de l'RGPD ha establert que els estats membres poden, a través de disposicions legislatives o de convenis col·lectius, establir normes més específiques per garantir la protecció dels drets i les llibertats en relació amb el tractament de dades personals dels treballadors en l'àmbit laboral, en particular, entre d'altres, a l'efecte del compliment de les obligacions que estableix la llei o el conveni col·lectiu, la gestió, planificació i organització del treball. Aquestes normes han d'incloure mesures adequades i específiques per preservar la dignitat humana dels interessats, així com els seus interessos legítims i els seus drets fonamentals, en particular, en relació, entre d'altres amb els sistemes de supervisió en el lloc de treball.

D'acord amb el que s'ha avançat, en el cas del personal sotmès al règim laboral, l'Estatut dels Treballadors preveu la possibilitat que l'empresari adopti mesures de vigilància i control per verificar el compliment de les obligacions laborals dels seus treballadors (art. 20.3), però pel cas del control de la jornada, estableix la necessitat d'elaborar un registre diari de les jornades (art. 34.9).

No obstant això, convé tenir en compte que la normativa no determina el mecanisme que es pot emprar per registrar la jornada, ni preveu cap autorització per utilitzar categories especials de dades, en concret, de dades biomètriques.

En relació amb aquesta manca de concreció de la norma, cal tenir en compte la sentència del Tribunal Constitucional 76/2019, de 22 de maig, en la qual el tribunal recorda que la ingerència estatal en l'àmbit dels drets fonamentals i les llibertats públiques requereix una norma amb rang de llei i precisa els requisits indispensables que ha de reunir aquesta norma com a garantia de la seguretat 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, esa norma legal "ha de reunir todas aquellas características indispensables como garantía de la seguridad jurídica", esto es, "ha de 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 ha de 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 ha de 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 sus 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)".

És a dir, l'afectació pel dret a la protecció de dades que es derivi de la norma ha de ser previsible. I en un cas com el que ens ocupa, no és pot considerar previsible la norma si no concreta la possibilitat d'utilitzar dades biomètriques amb la finalitat de fer el control horari.

A més, a la sentència també es determina que la norma ha d'establir garanties adequades, especialment quan es tractin categories especials de dades. En particular, el Tribunal manifesta el següent:

"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 (instrumento de ratificación publicado en el Boletín Oficial del Estado núm. 274, de 15 de noviembre de 1985), cuyo artículo 6 establece lo siguiente: "Los datos de carácter personal que revelen el origen racial, las opiniones políticas, las
convicciones religiosas u otras convicciones, así como los datos de carácter personal relativos a la salud o a 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 los 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 los datos; y la probabilidad y la gravedad de los riesgos de abuso y de utilización ilícita que, a su vez, están vinculadas al tipo
de tratamiento y a 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 el procesamiento de datos anónimos que la recopilación y el procesamiento de datos personales que se toman individualmente y no se anonimizan, como no es lo mismo el tratamiento de datos personales que revelen 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 mesura que les categories especials de dades tenen especial protecció, superior a altres dades personals, *"Una protección adecuada y específica frente a su 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 dichos 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."*

Així, davant la manca de previsibilitat de la normativa, no sembla que el tractament de control horari mitjançant el reconeixement facial es pugui basar en una norma amb rang de llei, d'acord amb la previsió de la lletra b) de l'article 9.2 de l'RGPD.

Pel que fa al personal sotmès a una relació jurídica administrativa, si bé la normativa relativa a la funció pública no recull previsions específiques relacionades amb el registre de la jornada del personal, equivalents als articles 20.3 i 34.9 de l'Estatut dels Treballadors, sí que trobem previsions relacionades amb el compliment de la jornada estipulada (com ara, l'article 54.3 del Reial decret legislatiu 5/2015, de 30 d'octubre, pel qual s'aprova el text refós de la Llei de l'estatut bàsic de l'empleat públic, o l'article 108.2.g) del Decret legislatiu 1/1997, de 31 d'octubre, pel qual s'aprova la refosa en un Text únic dels preceptes de determinats textos legals vigents a Catalunya en matèria de funció pública), i el règim disciplinari aplicable en cas d'incompliment d'aquesta (com ara, l'article 116, apartat .o) i q) (faltes greus) o l'article el 117.d) (faltes lleus) del Decret legislatiu 1/1997, de 31 d'octubre.) a partir dels quals les administracions públiques poden adoptar mesures de vigilància i control de l'execució de la jornada per part dels empleats públics.

No obstant això, tal com succeeix en el cas del personal laboral, la normativa no preveu que s'utilitzin dades biomètriques per controlar la presència o l'execució de la jornada.

A manca previsió legal, cal recordar que, d'acord amb el que preveu l'article 9.2.b) de l'RGPD, l'autorització pot estar prevista en el marc d'un conveni col·lectiu. Previsió que cal entendre aplicable també als acords sobre condicions de treball del personal funcionari en el marc de la negociació col·lectiva. Per això, en el cas que el conveni col·lectiu, el pacte o acord resultant de la negociació prevegi la utilització de dades biomètriques amb aquesta finalitat i estableixi garanties adequades respecte dels drets fonamentals i dels interessos de les persones interessades, aquest instrument permetria concloure la concurrència de l'excepció prevista a l'article 9.2.b) de l'RGPD.

IV

A la consulta, l'Ajuntament fa referència a que l'entitat instal·ladora dels dispositius ha indicat la necessitat de comptar amb el consentiment del personal per al tractament de la seva imatge amb la finalitat de control horari. S'entén que l'Ajuntament es refereix a la base jurídica del consentiment (art. 6.1.a de l'RGPD), el qual ha de ser explícit en el cas de tractaments sobre categories especials de dades (art. 9.2.a) de l'RGPD).

L'article 4.11) de l'RGPD preveu que el consentiment constitueix *"[...] 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*".

Alhora, cal tenir en compte que, en la mesura que el tractament pretès comporta tractar categories especials de dades, el consentiment ha de ser explícit (art. 9.2.a) RGPD). En relació amb aquest requisit, cal tenir en compte les *Directrius 5/2020 sobre el consentiment en el sentit del Reglament (UE) 2016/679* del Comitè Europeu de Protecció de Dades (CEPD) (https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_es.pdf):

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

Pel que fa al requisit que el consentiment sigui lliure, el considerant 43 de l'RGPD exposa el següent:

"[…] 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 desequilibro claro entre el interesado y el responsable del tratamiento, en particular cuando dicho responsable sea una autoridad pública y sea por lo tanto improbable que el consentimiento se haya dado libremente en todas las circunstancias de dicha situación particular."

Sobre aquesta qüestió, relativa al caràcter lliure del consentiment, cal tenir en compte també les Directrius 5/2020 del CEPD. D'aquestes Directrius convé destacar-ne el següent:

"13. El término «libre» implica elección y control reales 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 o a 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 distintas) que impida que este 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 hay 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 a su 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 de su 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. No obstante, 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".

Sobre la base del que s'ha exposat, i altres qüestions que també queden recollides a les Directrius 5/2020 del CEPD, a les quals ens remetem, no sembla que la base jurídica del consentiment sigui adient per legitimar el tractament de les dades del personal amb la finalitat del control horari del personal, atès que no es pot considerar que en el cas plantejat pogués haver-hi un consentiment realment lliure. En aquest sentit, podria considerar-se que existeix consentiment lliure si l'interessat disposa d'una alternativa per complir amb el control horari o controlar la seva presència o execució de l'horari, i és aquest qui escull i presta el seu consentiment al tractament de les seves dades biomètriques a través de sistemes de reconeixement facial, però no sembla que sigui així en un cas com el que es descriu a la consulta.

En definitiva, la normativa de protecció de dades no admet amb caràcter general el consentiment com a base jurídica legitimadora dels tractaments duts a terme per les administracions públiques o els empresaris per al control en l'entorn laboral, atès el desequilibri de poder que acostuma a produir-se entre les relacions d'aquells amb els interessats, que impedeix que el consentiment pugui considerar-se lliure.

A tal efecte, cal tenir en consideració que, d'acord amb el principi de responsabilitat proactiva (art. 5.2 de l'RGPD), el responsable del tractament, en el cas que ens ocupa l'Ajuntament, ha de ser capaç de demostrar que el consentiment és vàlid i que el tractament és lícit.

V

Al marge del principi de licitud, qualsevol tractament ha de complir també la resta dels principis i obligacions derivats de la normativa de protecció de dades, com ara el principi de minimització (art. 5.1.c) RGPD).

En aquest sentit, el Dictamen 3/2012 del Grup de Treball de l'Article 29, sobre l'evolució de les tecnologies biomètriques afirmava el següent en relació amb l'anàlisi del compliment del principi de minimització:

"*Al analizar la proporcionalidad de un sistema biométrico propuesto, es preciso considerar previamente si el sistema es necesario para responder a la necesidad identificada, es decir, si es esencial para satisfacer esa necesidad, y no solo el 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 es considerar si un medio menos invasivo de la intimidad alcanzaría el fin deseado*."

Sembla clara la necessitat d'admetre la instal·lació de sistemes de control del compliment horari per part del personal, tal com ha reconegut de manera reiterada aquesta Autoritat. Ara bé, no sembla tan clar que la utilització de sistemes de control horari basats en dades biomètriques hagin de ser admesos com a mitjà preferent per dur a terme al control. Més aviat al contrari. Atesa l'especial naturalesa d'aquestes dades caldrà optar, en primer lloc, per altres sistemes de

control que, sense utilitzar categories de dades especialment protegides, puguin permetre assolir la mateixa finalitat.

Les exigències derivades de la protecció de dades en el disseny (art. 25.1 RGPD) i, en especial, del principi de minimització, obliguen a escollir aquella tecnologia que resulti menys intrusiva des del punt de vista de la protecció de dades. El principi de minimització no es manifesta només a l'hora d'optar per alternatives que no impliquin el tractament de dades personals, o de dur a terme el tractament de dades de manera que s'emprin les dades mínimes indispensables, sinó que també ha de comportar que si es pot assolir una determinada finalitat sense haver de tractar dades de categories especials, aquesta opció ha de prevaldre davant altres opcions que sí que impliquin el tractament d'aquests tipus de dades.

Cal tenir en compte que les dades biomètriques, atès el seu caràcter personal i únic, constitueixen un mitjà fiable d'identificació (tot i que en determinades dades biomètriques pot existir un risc de no identificabilitat). La fiabilitat com a sistema d'identificació, però està condicionada també per l'amplitud amb què es puguin utilitzar aquests sistemes d'identificació. Com major sigui el nombre de sistemes d'identificació que es basen en unes dades biomètriques o en una plantilla obtinguda a partir de dades biomètriques, major és el risc que aquesta dada pugui acabar essent utilitzada de manera inadequada i donant lloc a un risc d'usurpació o suplantació d'identitat. Aquest risc es pot incrementar clarament en funció de quina sigui la tecnologia emprada i del tractament que es doni a les dades biomètriques en brut o originals.

Per una banda, una pèrdua de confidencialitat d'aquestes dades podria permetre, en funció de la tecnologia utilitzada, la suplantació. Però, és que a més, aquestes dades no són modificables. És a dir, a diferència d'una contrasenya, en cas de pèrdua no es poden canviar.

Per altra banda, també existeixen riscos evidents si la tecnologia emprada no garanteix de manera suficient que la plantilla obtinguda a partir de les dades biomètriques no coincidirà amb l'emprada en altres sistemes similars.

A l'efecte de determinar els riscos existents i les mesures per mitigar-los, poden ser d'ajuda les *Directrius 3/2019 sobre el tractament de dades personals mitjançant dispositius de vídeo* del CEPD, en particular l'apartat 5.2 relatiu a les mesures suggerides per minimitzar els riscos al tractar dades biomètriques, consultable al següent enllaç https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_es.pdf.

És innegable que la utilització de sistemes basats en dades biomètriques per a dur a terme el control horari evita el risc de suplantació que es pot produir en algun cas, com apunta la consulta. Ara bé, no sembla que sigui l'únic sistema que permeti garantir-ho. Per exemple, a efectes del control horari, la utilització de targetes personals o altres tipus d'objectes (token) en un sistema de marcatge, la utilització de codis personals, la visualització directa del punt de marcatge o la utilització de sistemes de videovigilància on quedi constància de l'hora d'entrada o sortida poden constituir, per si mateixos o en combinació amb algun dels altres sistemes disponibles, mesures eficaces per dur a terme el control.

La consulta, al marge de fer referència a la necessitat d'evitar el risc de suplantació que altres mecanismes de marcatge poden tenir, com ara l'ús de targetes individuals, també fa referència a què un dels motius d'instal·lació d'aquests sistemes és seguir les recomanacions sanitàries pel que fa a la Covid-19 per prevenir possibles contagis substituint el sistema de control per empremta dactilar.

Si bé la consulta no concreta a quina recomanació es refereix, s'entén que fa referència a les recomanacions de les autoritats públiques en el marc de la pandèmia per la Covid-19, com ara, el Ministeri de Sanitat, el qual a diferents Ordres (com ara, l'Ordre SND/388/2020, de 3 de maig; l'Ordre SND/399/2020, de 9 de maig, o bé l'Ordre SND/458/2020, de 30 de maig*)* ha previst, recollit en diferents articles respectivament, el següent:

"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."

D'entrada, aquesta recomanació en cap cas pot constituir una excepció per al tractament de categories especials de dades als efectes previstos a l'article 9.2.b). Però més enllà d'això, hi ha altres alternatives possibles d'aplicació senzilla, sense haver de canviar el sistema de control, com ara desinfectar el dispositiu de marcatge abans i després de cada ús, o bé que el treballador disposi d'un expenedor de gel antisèptic a prop del sistema de marcatge per ser usat un cop realitzat el fitxatge amb el dit, tant d'entrada com sortida. Per tant, la substitució del sistema de marcatge no sembla que hagi de ser l'única opció.

Cal tenir present que el tractament de l'empremta dactilar també constitueix un tractament de dades biomètriques, atès el que preveu l'article 4.11 de l'RGPD. Això vol dir que de la mateixa manera que el tractament mitjançant reconeixement facial requereix, a més d'una base jurídica d'acord amb el que preveu l'article 6.1 de l'RGPD, que concorri algun dels supòsits que preveu l'article 9.2 de l'RGPD, d'acord amb el que s'ha analitzat, el tractament de l'empremta dactilar amb aquesta finalitat també ho requereix en la mesura que es tracta d'una categoria especial de dades. En qualsevol cas, si es disposa de base jurídica per tractar l'empremta dactilar amb finalitat de control horari, però no per emprar mecanismes de reconeixement facial, mentre duri aquesta situació, caldria recórrer a un altre sistema que no comporti el tractament de categories especials de dades.

Finalment, recordar que, amb caràcter previ a la decisió sobre la posada en marxa d'un sistema de control d'aquest tipus, cal tenir en compte que l'article 35 de l'RGPD preveu la necessitat de fer una avaluació de l'impacte relativa a la protecció de dades (AIPD) en aquells tractaments, especialment si empren noves tecnologies, que comportin un alt risc pels drets i llibertats de les persones. A aquests efectes, i d'acord amb l'article 35.4 de l'RGPD, aquesta Autoritat ha publicat una *Llista de tipus de tractaments de dades que requereixen avaluació d'impacte relativa a la protecció de dades (*https://apdcat.gencat.cat/web/.content/02-drets_i_obligacions/obligacions/documents/Lista-DPIA-CAT.pdf), en la qual es determina que serà necessari fer una AIPD en la majoria dels casos en què el tractament compleixi amb dos o més criteris de la llista. Entre aquests criteris, poden concórrer en el cas que s'analitza els següents:

"[...] 3. Tractaments que impliquin l'observació, monitorització, supervisió, geolocalització o control de l'interessat de forma sistemàtica i exhaustiva, inclosa la recollida de dades i metadades a través de xarxes, aplicacions o en zones d'accés públic, així com el processament d'identificadors únics que permetin la identificació d'usuaris de serveis de la societat de la informació com poden ser els serveis web, TV interactiva, aplicacions mòbils, etc.
[...]
5. Tractaments que impliquin l'ús de dades biomètriques amb el propòsit d'identificar de manera única a una persona física.
[...]
10. Tractaments que impliquin la utilització de noves tecnologies o un ús innovador de tecnologies consolidades, incloent la utilització de tecnologies a una nova escala, amb un nou objectiu o combinades amb altres, de manera que suposi noves formes de recollida i utilització de dades amb risc pels drets i llibertats de les persones.[...]"

En conseqüència, és necessari fer una avaluació de l'impacte relativa a la protecció de dades, en la qual cal avaluar tant la legitimitat del tractament i la seva proporcionalitat, com la determinació dels riscos existents i les mesures per mitigar-los (art. 35 RGPD).

D'acord amb les consideracions fetes en aquests fonaments jurídics en relació amb la consulta plantejada en relació amb la utilització de sistemes de control basats en mecanismes de reconeixement facial, es fan les següents,

Conclusions

El consentiment del personal afectat no pot considerar-se una base jurídica adequada per a la implantació d'un sistema de control horari mitjançant reconeixement facial com el que es descriu a la consulta.

Seria necessària la previsió d'aquest sistema de control en una disposició legal o en un conveni col·lectiu aplicable, o si escau, en un pacte o acord resultat de la negociació col·lectiva, circumstàncies que no sembla que concorrin en el cas analitzat. En qualsevol cas, abans de la implantació d'un sistema d'aquest tipus, cal fer una avaluació de l'impacte sobre la protecció de dades a la vista de les circumstàncies concretes en què es dugui a terme el tractament per determinar-ne la licitud i la proporcionalitat, inclosa l'anàlisi de l'existència d'alternatives menys intrusives, i establir les garanties adequades.

Barcelona, 2 de febrer de 2022