CNS 63/2018

Dictamen en relació amb la consulta formulada per un col.legi professional sobre la utilització de sistemes de control basats en l'empremta dactilar

Es presenta davant l'Autoritat Catalana de Protecció de Dades un escrit d'un col.legi professional en el que es demana que l'Autoritat emeti un dictamen per valorar si la utilització de sistemes de control basats en l'empremta dactilar pot suposar una vulneració de la legislació sobre protecció de dades.

En concret, la consulta es refereix a dues situacions: per una banda, la utilització de sistemes de fixatge mitjançant empremta dactilar amb finalitat de control horari dels treballadors; per altra banda, també es planteja en relació amb l'accés a determinades instal·lacions que la consulta identifica com instal·lacions de seguretat del Col·legi (centres de processament de dades i arxiu).

Analitzada la consulta, que no s'acompanya de cap altra documentació, i d'acord amb l'informe de l'Assessoria Jurídica, emeto el següent dictamen:

I

(...)

II

En relació amb la primera de les qüestions plantejades, la instal·lació d'un sistema de control d'accés i horari basat en la recollida i tractament d'un patró de l'empremta dactilar dels empleats comporta el tractament de les seves dades personals, atès que per dada personal cal entendre "*toda información sobre una persona física identificada o identificable («el interesado»)*" (art. 4.1 del Reglament 2016/679, del Parlament i del Consell, de 27 d'abril, general de protecció de dades (en endavant, RGPD)).

Pel que fa a l'empremta dactilar o al patró de l'empremta dactilar es tracta, a més, d'una dada que ha de ser qualificada com a dada biomètrica, atès que d'acord amb l'article 4.14 RGPD tenen aquesta consideració quan han estat "*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, d'acord amb l'article 9 .1 RGPD, a les dades relatives a les empremtes dactilars se'ls hagi d'aplicar el règim específic previst per a les categories especials de dades previst tant a l'article 9, com a altres articles de l'RGPD.

En aquest sentit, el Considerant 51 de l'RGPD posa de manifest el caràcter restrictiu amb que es pot admetre el tractaments d'aquestes dades:

> *"(51) (...)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.*
>
> *(52) 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.(...)"*

D'acord amb aquestes consideracions, el tractament de dades biomètriques requerirà no només la concurrència d'una de les bases jurídiques establertes a l'article 6 de l'RGPD sinó que, a més, haurà de concórrer alguna de les excepcions previstes a l'article 9.2 de l'RGPD.

Aquesta Autoritat ja ha analitzat, en dictàmens anteriors (per exemple, CNS 9/2009, CNS 22/2009 o 22/2011), l'adequació a la normativa en matèria de protecció de dades personals dels sistemes de control d'accés i horari dels empleats de les administracions públiques mitjançant dades biomètriques (com l'empremta digital o un patró biomètric). Aquests dictàmens, i d'altres, poden ser consultats a la pàgina web www.apd.cat.

De conformitat amb l'article 6.2 de la Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal (LOPD) i amb el principi de qualitat de les dades (article 4 de l'LOPD), aplicables per raons temporals als supòsits que s'analitzaven en aquells dictàmens, l'Autoritat va considerar, en supòsits similars al que s'examina en aquest dictamen, que, en la mesura que la recollida de dades personals dels treballadors públics es realitzava dins d'una relació jurídica laboral o administrativa i tenia com a finalitat el control, precisament, del seu compliment a l'empara del que estableix l'article 20.3 de l'Estatut dels treballadors (ET), el responsable podia tractar i recollir les dades biomètriques consistents en l'empremta digital o el patró biomètric dels seus treballadors sense necessitat de requerir el seu consentiment.

En aquest sentit, es pronunciava la Sentència del Tribunal Suprem, de 2 de juliol de 2007, fonament setè, recalcant que la finalitat perseguida amb aquest sistema *"es plenamente legítima: el control del cumplimiento del horario de trabajo al que viene obligados los empleados públicos. Y, en tanto esa obligación es inherente a la relación que une a estos con la Administración Autonómica, no es necesario obtener previamente su consentimiento ya que el artículo 6.2 de la Ley Orgánica 15/1999 lo excluye en estos casos. Además, no parece que la toma en las condiciones expuestas, de una imagen de la mano, incumpla las exigencias del artículo 4.1. Por el contrario, puede considerarse adecuada, pertinente y no excesiva",* a la qual es remeten altres sentències que enjudicien supòsits similars, com ara, la Sentència del Tribunal Superior de Justícia de la Regió de Múrcia de 25 de gener de 2010 o la Sentència de l'Audiència Nacional de 4 de març de 2010. En el mateix sentit s'assenyalava la Interlocutòria del Tribunal Constitucional de 26 de febrer de 2007, en especial pel que fa als arguments referits a la doctrina de la proporcionalitat.

L'aprovació i la plena aplicabilitat de l'RGPD ha introduït però alguns elements addicionals que afecten l'anàlisi que es pot fer de la utilització de dades biomètriques en l'entorn laboral.

III

Amb l'aprovació de l'RGPD, i des del punt de vista de la base jurídica del tractament, no només és possible acudir a la base jurídica prevista a l'article 6.1.b) de l'RGPD (que el tractament sigui necessari per a l'execució d'un contracte en el qual la persona interessada és part), sinó que també és possible, en el cas de subjectes als quals els sigui aplicable, acudir a la base jurídica establerta a l'article 6.1.f) (que el tractament sigui necessari per satisfer l'interès legítim de l'empleador en la correcta execució de les prestacions derivades del contracte de treball), tal com havia reconegut el Dictamen 3/2012 del Grup de Treball de l'Article 29, sobre l'evolució de les tecnologies biomètriques. Sigui com sigui, l'element clau serà la determinació de la necessitat del tractament. No ja de la necessitat de fer algun tipus de control, sinó de fer-lo a través de la tècnica proposada, això és l'ús de sistemes d'identificació basats en dades biomètriques.

Per altra banda, i tal com posa de relleu el considerant 51 del mateix RGPD, en la mesura que les dades biomètriques han passat a ser considerades com una categoria especial de dades (art. 9.1 RGPD), caldrà que concorri alguna de les excepcions previstes a l'article 9.2 RGPD que permeten aixecar la prohibició general del tractament d'aquests tipus de dades establerta a l'article 9.1.

En aquest punt cal fer especial menció a la lletra b) de l'article 9.2 RGPD, segons la qual la prohibició general de tractament de dades biomètriques no serà d'aplicació quan "*el tratamiento es necesario para el cumplimiento de obligaciones y el 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 así lo autorice el Derecho de la Unión de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado*".

Per tant, per poder aplicar aquesta excepció serà necessària la concurrència de dues condicions:

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

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

Pel que fa a la possibilitat que el dret dels estats membres ho autoritzi, 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.

Cada estat membre ha de notificar a la Comissió les disposicions legals que adopti de conformitat amb l'apartat 1.

En l'ordenament espanyol, l'article 20 del Text refós de l'Estatut dels treballadors (ET), aprovat pel Reial decret legislatiu 2/2015, de 23 d'octubre, preveu la possibilitat que l'empresari adopti mesures de vigilància i control per verificar el compliment de les obligacions laborals dels seus treballadors, però no es refereix en cap moment a una autorització per a la utilització de categories especials de dades o, en concret, de dades biomètriques, amb aquesta finalitat:

> "*3. 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*."

Els articles 87, 89 i 90 de la Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals (LOPDGDD), sí que han previst i han regulat les condicions i garanties amb que pot fer-se el control dels treballadors per part de l'empresari pel que fa a la utilització dels dispositius digitals posats a la seva disposició per part de l'empresari, la utilització de sistemes de videovigilància en el lloc de treball o la utilització de sistemes de geolocalització a l'àmbit laboral, però no contenen cap referència a la possibilitat d'utilització de dades biomètriques en sistemes de control en l'àmbit laboral, com seria el cas del control horari.

Aquesta autorització per implantar sistemes de control seria encara més necessària en el cas de sistemes basats en dades biomètriques, atesa la condició de categoria especial d'aquestes dades, i els termes poc precisos amb que es pronuncia l'actual article 20.3 ET. La manca de previsió expressa d'una autorització en el dret laboral, que ara requereix l'article 9.2.b) de l'RGPD fa que puguin sorgir dubtes pel que fa a l'admissibilitat d'aquest tipus de sistemes de control horari a l'àmbit laboral.

Par altra banda, i al marge d'aquesta qüestió relacionada amb l'exigència que la utilització de les dades biomètriques estigui autoritzada per una norma amb rang de llei, cal tenir en compte que en qualsevol cas el tractament ha de complir amb la resta dels principis i obligacions derivats de la normativa de protecció d dades, en especial, del principi de minimització (art. 5.1.c) RGPD).

Així es desprèn tant de la mateixa redacció de l'article 9.2.b) de l'RGPD, que exigeix que el tractament sigui "necessari", com de la Recomanació CM/Rec(2015) 5 del Consell de Ministres del Consell d'Europa als estatal membres sobre el tractament de dades personals en el context laboral. En concret, el Principi 18 d'aquesta Recomanació estableix el següent:

> *"18.1. La recopilació i posterior processament de les dades biomètriques només s'haurien d'emprendre quan cal protegir els interessos legítims d'empresaris, empleats o tercers, només si no hi ha altres mitjans menys intrusius disponibles i només si s'acompanya de les garanties adequades previstes en el principi 21.*
>
> *18.2. El tractament de les dades biomètriques s'ha de basar en mètodes científicament reconeguts i ha d'estar subjecte als requisits d'estricta seguretat i proporcionalitat."*

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 d'aquest principi:

> *"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 utilizar1. 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 dels treballadors, tal com havia reconegut de manera reiterada aquesta Autoritat, d'acord amb les decisions judicials que s'han esmentat més amunt. Ara bé, un cop les dades biomètriques han passat a ser considerades com a dades especialment protegides, no sembla tan clar que la utilització de sistemes de control horari basats en aquest tipus de dades 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 sembla que 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 pugui existir un risc de no identificabilitat). La fiabilitat com a sistema d'identificació però està condicionada també per l'amplitud amb que 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 mes, 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 la emprada en altres sistemes similars.

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. 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.

En virtut d'aquestes consideracions algunes autoritats de control en matèria de protecció de dades no han admès la utilització de sistemes de control basats en dades biomètriques com a sistema generalitzat de control horari dels treballadors per part de l'empresari. Seria el cas de la Commission Nationale de l'informatique et des libertés (CNIL) de França o del Garante per la protezione dei dati personali d'Itàlia.

En la consulta formulada es fa referència a la informació que s'ofereix a l'apartat de preguntes freqüents de l'AEPD i a una resolució de 19 de desembre de 2016 de l'Agència Basca de Protecció de Dades on s'admetia la utilització d'un sistema descentralitzat de control basat en

dades biomètriques. S'ha de dir però que, si be es fa referència a l'aprovació de l'RGPD, en ambdós casos hi ha una remissió a la jurisprudència anterior a l'RGPD, la qual havia admès, tal com també havia fet aquesta Autoritat en els dictàmens esmentats al principi, la utilització de dades biomètriques per a sistemes de control horari en l'àmbit laboral.

Més enllà d'això, en la consulta no s'exposa quines són les circumstàncies que justificarien aquest tipus de control, ni tampoc quins motius impedirien utilitzar altres sistemes de control que no impliquin el tractament de categories especials de dades i que per tant siguin menys intrusius pel dret a la protecció de dades de les persones afectades.

Ateses aquestes circumstàncies no sembla que es pugui concloure la proporcionalitat de la utilització de l'empremta dactilar per a establir un sistema de control horari en el cas descrit a la consulta.

En qualsevol cas, amb caràcter previ a la decisió sobre la posada en marxa d'un sistema de control d'aquest tipus, tenint en compte les implicacions tecnològiques de la tecnologia emprada, la observació sistemàtica dels hàbits dels treballadors i el tractament de dades d'una categoria especial (biomètriques), caldria dur a terme una avaluació de l'impacte relativa a la protecció de dades de caràcter personal per 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).

IV

En la consulta es planteja encara un altre supòsit, consistent en la utilització de l'empremta dactilar per controlar l'accés a determinades dependències que requereixin una major seguretat. En la consulta s'identifiquen com a tals els centres de processament de dades o els arxius.

A diferència del cas anterior, aquí, si s'accedeix a les dependències de que es tracti, el possible dany que es produeixi, destrucció, alteració, sostracció o accés indegut a la informació o als sistemes d'informació continguts en aquestes dependències, serà difícil de reparar. No es tractaria només de tenir constància de qui accedeix a aquestes dependències sinó d'evitar que persones no autoritzades puguin accedir-hi. Essent així, sistemes com ara la instal·lació de càmeres de videovigilància no serien sistemes eficaços, però en canvi sí que poden haver-hi altres sistemes (claus, codi personal, token) que sí que poden resultar eficaços.

Com en el cas anterior resulta essencial que es compleixi el principi de proporcionalitat o de minimització de les dades personals a l'hora de determinar quin és el sistema de control que s'aplica.

D'entrada sembla plausible que la necessitat d'aplicar sistemes de control d'accés més robustos per l'accés a determinades dependències que poden contenir informació sensible pot aparèixer com a més justificada que en el cas de la finalitat de control horari. No obstant això, tampoc sembla que es pugui concloure de manera automàtica la justificació de la mesura.

D'acord amb el Dictamen 3/2012 del Grup de Treball de l'Article 29, sobre l'evolució de les tecnologies biomètriques, *"Como norma general, el uso de la biometría para las exigencias generales de seguridad de los bienes y las personas no puede considerarse un interés legítimo*

que prevalezca sobre los intereses o los derechos y libertades fundamentales del interesado. Por el contrario, el tratamiento de datos biométricos solo puede justificarse como un instrumento necesario para asegurar los bienes o las personas cuando se disponga de pruebas, sobre la base de las circunstancias objetivas y documentadas, de la existencia de un riesgo considerable. Para ello, el responsable del tratamiento deberá probar que determinadas circunstancias plantean un riesgo considerable específico, que deberá evaluar con especial cuidado. Con el fin de cumplir con el principio de proporcionalidad, el responsable del tratamiento, ante estas situaciones de alto riesgo, deberá verificar si posibles medidas alternativas podrían ser igualmente eficaces pero menos intrusivas en relación con los objetivos perseguidos, y optar por tales alternativas. La existencia de las circunstancias en cuestión también deberá revisarse periódicamente. Sobre la base de esta revisión, las operaciones de tratamiento de datos que no se justifiquen deberán concluirse o suspenderse."

Per tant, caldrà veure, en atenció a la naturalesa de la informació custodiada i les repercussions que podria tenir un accés indegut a aquestes dependències, quins són els riscos que cal afrontar, com també quines són les possibles alternatives. Més enllà d'identificar el tipus de dependències (centres de processament i arxiu), en la consulta no s'ofereix cap altra informació que permeti avaluar els riscos ni analitzar les possibles alternatives.

En qualsevol cas, i per al supòsit que, després de realitzar l'avaluació d'impacte a la qual ens hem referit en el fonament jurídic anterior, es pugui concloure que la mesura resulta proporcionada, d'acord amb el Dictamen 3/2012 del Grup de Treball de l'article 29 sobre l'evolució de les tecnologies biomètriques, i sens perjudici del que resulti de l'anàlisi de riscos que es dugui a terme, convé tenir en compte algunes mesures tècniques per tal de minimitzar els riscos:

a) Convé evitar l'emmagatzematge de dades biomètriques en brut, i conservar només les plantilles obtingudes a partir d'aquelles dades.
b) La plantilla s'ha d'extreure de manera que es pugui preveure que no podrà ser utilitzada per altres responsables del tractament per fins similars.
c) S'ha de donar preferència als sistemes d'emmagatzematge descentralitzats, evitant la creació de bases de dades centralitzades amb aquests tipus de dades. D'acord amb el model descentralitzat que es proposa, les plantilles biomètriques es conservarien exclusivament en poder de les persones interessades mitjançant una targeta o dispositiu, de manera que la pèrdua de les mateixes tindria uns efectes limitats.
d) Les dades s'han de conservar xifrades.

Tot això a banda de la necessitat de facilitar informació transparent a les persones afectades sobre el tractament que es pretén dur a terme de manera que puguin comprendre l'abast i les conseqüències que podria tenir aquest tractament.

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 l'empremta dactilar, es fan les següents,

Conclusions

La inclusió de les dades biomètriques, entre elles les de l'empremta dactilar, entre les categories especials de dades previstes per l'RGPD no permet concloure de manera automàtica que la implantació d'un sistema de control horari basat en la recollida d'aquest tipus de dades pugui considerar-se proporcionat i, per tant, conforme amb el principi de minimització. 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 legitimitat i la proporcionalitat, inclosa l'anàlisi de l'existència d'alternatives menys intrusives, i establir les garanties adequades.

En el cas del control d'accés a dependències o zones que requereixin unes condicions de seguretat reforçades, la utilització d'aquest tipus de sistemes pot resultar justificat en determinats casos, si bé també resulta necessari dur a terme amb caràcter previ l'avaluació de l'impacte en la protecció de dades.

Barcelona,14 de febrer de 2019