

## **Dictamen en relació amb la consulta formulada per la delegada de protecció de dades d'un Ajuntament relativa al tractament de les dades biomètriques amb finalitats de control de presència i control de l'accés a dependències municipals**

### **Antecedents**

Es presenta davant l'Autoritat Catalana de Protecció de Dades una consulta formulada per la delegada de protecció de dades d'un Ajuntament, en relació amb el tractament de les dades biomètriques amb finalitat de control de presència i control de l'accés a dependències municipals.

La consulta sol·licita conèixer el criteri de l'Autoritat respecte de les següents qüestions:

"a- Causa de licitud pel tractament de les dades: En la guia de l'AEPD es determina que l'única causa de licitud del tractament de les dades biomètriques amb finalitats de control de presència i/o de control és el consentiment establert en l'article 6.1.a del Reglament Europeu 2016/679 General de Protecció de dades personals. Però en resolució d'Aquest Autoritat de l'any 2022 es fa menció de la possibilitat de que es puguin tractar si aquest tractament de dades biomètriques es troba recollit de forma expressa en el Conveni col·lectiu de l'entitat a realitzar el tractament.

Aquest Ajuntament ha acordat al respecte: "La jornada realitzada en la modalitat de treball a distància es registrarà mitjançant la incidència "teletreball". La jornada realitzada en règim presencial, es realitzarà mitjançant el sistema de control d'accés i presència amb l'empremta dactilar, que captarà trets característics d'aquestes per diferenciar-les de les altres, sense que es realitzi una reproducció total de l'empremta per garantir la seguretat de les dades i evitar el seu possible ús fraudulent". I per tant, conèixer si incorporat en el conveni col·lectiu aplicable que el control de presència i d'accés dels seus funcionaris i treballadors es realitzarà amb dades biomètriques, seria legítim aquest tractament al donar compliment la causa de licitud establerta en l'article 6.1.c del RGPD

b. Judici de necessitat: en quant al criteri exposat en aquesta Guia de considerar que en tots els casos les dades biomètriques son considerades dades de categories especials encara que no siguin reproduccions completes, el judici de necessitat cobra una gran importància per tal de poder comprovar que es complexi aquest criteri de necessitat. I per aquest motiu, desitgem conèixer quin és el criteri d'aquest Autoritat al respecte i en especial si la seguretat dels nostres treballadors i informació en una administració pública local pot superar aquest judici per tal de garantir els accessos de no tercers en la totalitat dels seus espais com zones d'oficines, comissaries policials, zones d'espais d'alcaldia..., o considera que no aquesta seguretat es pot obtenir per altres medis com accés amb targeta, càmeres de videovigilància, consergeria."

Analitzada la consulta, i vista la normativa vigent aplicable, i d'acord amb l'informe de l'Assessoria Jurídica emeto el següent dictamen:

## Fonaments Jurídics

I

(...)

II

D'acord amb el que s'ha exposat als antecedents, la delegada de protecció de dades (DPD) de l'Ajuntament circumscriu la consulta a dues qüestions: la licitud del tractament de dades biomètriques (empremta dactilar) amb finalitat de control de presència o control d'horari del personal de l'Ajuntament i, l'altre, en relació amb el requisit de necessitat respecte del tractament de dades biomètriques amb finalitat de control d'accessos.

Abans d'analitzar la qüestió plantejada, val a dir que s'entén que la DPD de l'Ajuntament fa referència en la consulta al dictamen número CNS 2/2022 (el qual es pot consultar al web [apdcat.gencat.cat](http://apdcat.gencat.cat)), i en el qual es va donar resposta a una consulta d'un ajuntament relativa a l'ús de dispositius de control de presència al lloc de treball mitjançant reconeixement facial. Si bé en aquesta consulta es feia referència a l'ús de tecnologia de reconeixement facial amb la finalitat de control de presència, cal tenir en compte que les conclusions a les quals es van arribar són plenament aplicables a l'ús de dispositius o sistemes de control de presència mitjançant l'empremta dactilar, en la mesura que ambdós sistemes utilitzen dades biomètriques per a identificar de manera unívoca a una persona física.

Això no obstant, també cal fer referència al fet que aquesta Autoritat ja va emetre un dictamen (el CNS 63/2018, que es pot consultar al web [apdcat.gencat.cat](http://apdcat.gencat.cat)) en relació amb la utilització de sistemes de control basats en l'empremta dactilar, per una banda, amb finalitat de control de compliment de l'horari dels treballadors, i per altra, per al control d'accés a determinades instal·lacions d'un col·legi professional, com ara el centre de processament de dades i arxiu.

Situada la consulta en aquests termes partim de la base que 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 3 transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción".

Alhora, 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".

Sobre la base d'aquests preceptes, l'ús de dispositius amb la finalitat de presència o control de la jornada, així com el control dels accessos, mitjançant l'empremta dactilar, comporta dur a terme el tractament de dades personals el qual està subjecte als principis i obligacions que estableix l'RGPD, com ara, el principi de licitud (art. 5.1.a) de l'RGPD), segons el 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.

Així, en la mesura que el tractament a què fa referència la consulta 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, a més de sobre base jurídica prevista a l'article 6.1.b) de l'RGPD, 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.

I, 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 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, 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.

Ara bé, cal tenir en compte que 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 fa que estigui sotmès a les previsions de l'article 9 de l'RGPD, el qual prohibeix el seu tractament llevat que concorri una de les circumstàncies de l'article 9.2 de l'RGPD.

I, en particular, l'Ajuntament fa referència a la concurrència de la circumstància 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.

A tal efecte, cal tenir en compte que per tal que concorri aquesta circumstància, però, cal 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 a més:

a) Que ho autoritzi el dret de la Unió dels que estableixi garanties adequades pel que fa al respecte dels drets fonamentals i els interessos de les persones afectades, o bé

b) Que ho autoritzi un conveni col·lectiu que estableixi garanties adequades pel que fa al respecte dels drets fonamentals i els interessos de les persones afectades.

### III

Quant a l'habilitació continguda al dret de la Unió dels estats membres, cal fer avinent que aquesta qüestió ha estat prèviament analitzada al dictamen [CNS 2/2022](#), en particular en el fonament jurídic III, al qual ens remetem. No obstant això, convé extraure la conclusió a la qual es va arribar:

"[...] 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."

I, en relació amb aquesta conclusió, la **primera qüestió** que planteja l'Ajuntament és si pot concórrer aquesta circumstància si s'inclou en el conveni col·lectiu (s'entén que, si escau, també en els acords sobre condicions de treball del personal funcionari en el marc de la negociació col·lectiva), la següent previsió:

"La jornada realitzada en la modalitat de treball a distància es registrarà mitjançant la incidència "teletreball". La jornada realitzada en règim presencial, es realitzarà mitjançant el sistema de control d'accés i presència amb l'empremta dactilar, que captarà trets característics d'aquestes per diferenciar-les de les altres, sense que es realitzi una reproducció total de l'empremta per garantir la seguretat de les dades i evitar el seu possible ús fraudulent".

Cal avançar que, si bé la força vinculant dels convenis col·lectius garantida a l'article 37 de la Constitució espanyola, i l'excepció de l'article 9.2.b) de l'RGPD per tractar categories especials de dades, la redacció que proposa incloure l'Ajuntament en el conveni col·lectiu, i si escau els acords pel que fa al personal funcionari, no reuniria els requisits de l'article 9.2.b) de l'RGPD. Tal com s'exposarà, si bé el conveni col·lectiu pot ser instrument suficient per implementar aquesta mesura, la mateixa es troba condicionada a la superació del test de proporcionalitat, a la realització d'una avaluació d'impacte de protecció de dades, i a l'establiment de garanties adequades, extrems que no s'han constatat en la consulta formulada..

En primer lloc, i en termes estrictament teòrics, cal fer avinent que la primera circumstància a què fa referència l'article 9.2.b) de l'RGPD que ha de concórrer és que el tractament de categories especials de dades sigui necessari per al compliment d'obligacions i l'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 relació amb aquesta qüestió, cal tenir en compte que quan l'article 9.2.b) de l'RGPD fa referència a què el tractament és necessari, això no s'ha de confondre en cap cas amb la necessitat de dur a terme el tractament (el registre de la jornada o control horari), el qual ve imposat per la normativa, sinó que es refereix a la necessitat que el registre de la jornada es realitzi a través del mitjà proposat, en aquest cas, la captació de l'empremta dactilar.

La Recomanació CM/Rec(2015) 5 del Consell de Ministres del Consell d'Europa als estats membres sobre el tractament de dades personals en el context laboral, en concret el principi 18, 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 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.”

En relació amb aquesta qüestió, en el dictamen 63/2018, es va considerar el següent:

“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 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 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.[...]"

Això, portat al cas de la consulta plantejada, i sobre la base de la informació que ha estat tramesa, sens perjudici del que a continuació s'exposa, a priori no sembla que l'ús de sistemes de control o registre de la jornada mitjançant l'empremta dactilar sigui un mitjà necessari per complir amb l'obligació legal de dur a terme el registre de la jornada, al qual fa referència l'article 34.9 de l'Estatut dels Treballadors per al personal laboral, o bé per exercir la potestat de les administracions públiques d'adoptar mesures de vigilància i control de l'execució de la jornada per part dels empleats públics d'acord amb la normativa relativa a la funció pública. En aquest sentit, la consulta no justifica raonablement que no hi hagi altres mesures menys intrusives respecte dels drets fonamentals i els interessos de les persones interessades.

En qualsevol cas, tal com s'exposarà més endavant, la força normativa del conveni col·lectiu, en termes de licitud, permetria la implantació d'aquesta mesura, tot i que això no suposa excloure un anàlisi de les opcions a les mesures de control horari que es volen implementar.

En aquesta línia, es desconeix si l'Ajuntament ha dut a terme una avaluació d'impacte en la protecció de dades (AIPD) a què es refereix l'article 35 de l'RGPD (atès que aquest precepte disposa que serà necessària "cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas") en la qual s'hagi analitzat aquesta circumstància i quedi justificada amb criteris objectivables, i no de conveniència. A més, fins i tot, és altament recomanable que es dugui a terme aquesta AIPD en el

procediment d'aprovació del conveni col·lectiu o dels acords pel que fa al personal funcionari, en la mesura que l'article 35.10 de l'RGPD estableix que si en el procediment d'aprovació de la norma se sotmet aquesta a una AIPD després no serà necessari realitzar-la quan es duguin a terme els tractaments que se'n derivin.

En qualsevol cas, val a dir que aquesta Autoritat no disposa d'aquesta informació.

En segon lloc, l'article 9.2.b) de l'RGPD també exigeix que l'autorització en un conveni col·lectiu ha d'establir "[...] garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado".

En relació amb aquesta qüestió, cal tenir en compte que l'autorització a què fa referència l'article 9.2.b) de l'RGPD és respecte del tractament de categories especials de dades per a una determinada finalitat, és a dir, que el dret de la Unió dels Estats membres o un conveni col·lectiu autoritzi el tractament de categories especials de dades per a la finalitat pretesa i, a més, que s'estableixin garanties adequades respecte dels drets fonamentals i els interessos de les persones interessades. Tot això sens perjudici de què hagi de concórrer el requisit de necessitat que ha estat analitzat prèviament.

Per tant, no és suficient amb que el dret de la Unió dels Estats membres o un conveni col·lectiu contempli una previsió que merament determini que un tractament (en aquest cas, el registre de la jornada) es duguin a terme a través d'un mitjà concret o tractant una determinada categoria especial de dades (l'empremta dactilar), sinó que cal que concorrin la resta de condicions, és a dir, que es prevegin garanties adequades de respecte dels drets fonamentals i dels interessos de les persones interessades i, alhora, que el responsable del tractament justifiqui la seva necessitat respecte la finalitat pretesa.

Convé fer referència a la sentència del Tribunal Constitucional 76/2019, de 22 de maig, la qual recorda que la ingerència estatal en l'àmbit dels drets fonamentals i les llibertats públiques requereix una norma amb rang de llei i, alhora, 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)".

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 definitiva, aquesta sentència estableix que (1) és necessari que el tractament de categories especials de dades estigui previst en la norma amb rang legal, sense que es pugui remetre a una norma reglamentària posterior o a les decisions que pugui prendre a posteriori el responsable del tractament, (2) en la qual s'estableixi de manera clara la finalitat del tractament de les dades, sense que sigui suficient una menció genèrica a aquesta finalitat, de manera que detalli les restriccions del dret fonamental (regles clares sobre l'abast i el contingut dels tractaments de dades que autoritza) i, alhora, (3) estableixi garanties adequades per protegir els drets dels interessats, que garanteixin la transparència, la supervisió i la tutela judicial efectiva, que no es recullin de forma desproporcionada i no s'utilitzin per a finalitats diferents de les que van justificar la seva obtenció.

I, en relació amb això últim, el fet que calgui tenir en compte si existeixen possibilitats menys intrusives o potencialment menys perilloses per als drets fonamentals, reforça el requisit de la necessitat el qual hem analitzat anteriorment, i al qual també es refereix el considerant 39 de l'RGPD quan estableix expressament que "[...] Los datos personales solo deben tratarse si la finalidad del tratamiento no pudiera lograrse razonablemente por otros medios", i l'article 5.1.c) de l'RGPD, en relació amb el principi de minimització, pel qual les dades personals han de ser les adequades, pertinents i limitades al que és necessari en relació amb les finalitats per a les quals es tracten.

Per tot el que ha exposat, es considera que la redacció que proposa incloure l'Ajuntament en el conveni col·lectiu (i si escau, en els acords pel que fa al personal funcionari) no reuneix els requisits de l'article 9.2.b) de l'RGPD.

Ara bé, tal com s'ha avançat, si que pot concórrer la circumstància a què fa referència l'article 9.2.b) de l'RGPD si l'Ajuntament du a terme, amb caràcter previ al tractament de categories especials de dades, l'anàlisi de la necessitat de la mesura, i d'acord amb el principi de responsabilitat proactiva (art. 5.2 de l'RGPD) és capaç de poder demostrar la necessitat, i la previsió que s'inclou al conveni col·lectiu estableix les garanties adequades en els termes que ho estableix la doctrina del Tribunal Constitucional a què hem fet referència.

#### IV

La **segona qüestió** a la qual fa referència la consulta se circumscriu a analitzar el requisit de necessitat respecte del tractament de dades biomètriques amb la finalitat de control dels accessos a determinades dependències municipals, com ara la zona d'oficines, comissaries policials, zona d'espai de l'alcaldia, etc.

En particular, la consulta demana que aquesta Autoritat es pronunciï sobre si la seguretat de les persones i la informació custodiada en aquestes dependències justificaria el tractament de dades biomètriques per accedir a aquests espais o si, per contra, es considera que aquesta seguretat es pot obtenir per altres mitjans com ara l'accés amb targeta, càmeres de videovigilància o consergeria.

D'entrada, cal tenir en compte que l'article 24 de l'RGPD estableix que el responsable del tractament, en aquest cas l'Ajuntament, ha d'aplicar les mesures tècniques i organitzatives adequades per garantir i poder demostrar que el tractament és conforme a aquest reglament, tenint en compte la naturalesa, l'àmbit, el context i les finalitats del tractament,

així com els riscos de probabilitat i gravetat diversa per als drets i les llibertats de les persones físiques.

Respecte de la seguretat del tractament, l'article 32.2 de l'RGPD estableix que cal tenir particularment en compte els riscos que presenta el tractament de dades, especialment a conseqüència de la destrucció, la pèrdua o l'alteració accidental o il·lícita de dades personals transmeses, conservades o tractades d'una altra manera, o la comunicació o l'accés no autoritzats a aquestes dades.

I, alhora, quan sigui probable que el tractament, especialment si utilitza noves tecnologies, i tenint en compte la seva naturalesa, abast, context o finalitats, pot comportar un alt risc per als drets i les llibertats de les persones físiques, l'Ajuntament ha d'avaluar l'impacte de les operacions de tractament en la protecció de dades personals (art. 35 de l'RGPD).

D'acord amb aquestes previsions, correspon a l'Ajuntament analitzar les circumstàncies que concorren en cada cas i adoptar les mesures tècniques i organitzatives que siguin adequades per garantir i poder demostrar que el tractament és conforme l'RGPD. Això, entre altres qüestions, implica l'anàlisi i justificació de la necessitat d'adoptar unes determinades mesures, i no d'altres, les quals siguin menys intrusives o potencialment menys perilloses per als drets fonamentals dels interessats, si escau.

Aquesta tasca comporta acreditar que existeix una relació de proporcionalitat entre el fi pretès i la manera en què es tractaran les dades de les persones afectades, així com que no hi ha cap altra mesura més idònia.

Com ha posat de manifest reiterada jurisprudència (per totes, la STC 39/2016, de 3 de març), per tal de comprovar si una mesura restrictiva d'un dret fonamental respecta el principi de proporcionalitat, cal que aquesta compleixi amb tres requisits: que sigui susceptible d'aconseguir l'objectiu proposat (judici d'idoneïtat); que sigui necessària, en el sentit que no existeixi una altra més moderada per a la consecució d'aquest propòsit amb la mateixa eficàcia (judici de necessitat); i, finalment, que sigui ponderada o equilibrada, en derivar-se més beneficis o avantatges per a l'interès general que perjudicis sobre altres béns o valors en conflicte (judici de proporcionalitat en sentit estricte), és a dir, si la ingerència produïda per la dita mesura en el titular del dret objecte de restricció és la mínima per assolir el fi legítim pretès amb la seva adopció.

Aplicant aquest criteri al cas concret, es pot entendre que l'establiment de mesures de control d'accessos mitjançant el tractament de dades biomètriques, a determinats espais municipals que, per raó de la seva singularitat, requereixen un nivell superior de seguretat, podria superar el judici de proporcionalitat, sempre que es valori acuradament i, d'altra banda, no suposi una mesura encoberta de control per a la totalitat dels espais municipals o una part significativa dels mateixos.

Així, als efectes del judici de proporcionalitat, l'Ajuntament ha de ponderar els diferents drets i béns jurídics en joc analitzant, entre d'altres, la necessitat d'utilitzar aquests sistemes, la idoneïtat d'implementar controls d'accessos a través de l'empremta a determinades dependències municipals on han d'haver-ne condicions addicionals d'accés en termes de seguretat per assolir la finalitat perseguida (com podria ser l'armeria de la policia municipal, per exemple), el risc que pot suposar per als drets de les persones, ateses les característiques del sistema que es pretén emprar, l'absència d'altres mecanismes

alternatius que comportin un risc menor, en relació amb possibles intromissions en els drets fonamentals, si les característiques de configuració del sistema permeten assolir la finalitat perseguida de la manera menys intrusiva pels drets de les persones afectades. En qualsevol cas, l'anàlisi de proporcionalitat s'ha de fer atenent a les condicions tècniques dels sistemes o dispositius emprats i, entre d'altres extrems, les pròpies condicions de captació i tractament de les empremtes dactilars.

En el cas que ens ocupa, aquest judici de proporcionalitat hauria d'avaluar:

a) En primer lloc, si la mesura és susceptible d'aconseguir l'objectiu proposat (judici d'idoneïtat). Al respecte, no es pot negar que l'ús de sistemes de control d'accés a través de l'empremta dactilar permetria assolir la finalitat de controlar les persones que accedeixen a determinades dependències.

b) En segon lloc, si la mesura és necessària (judici de necessitat). Sobre la base de raons objectivables, l'Ajuntament només hauria d'optar per aquesta mesura si la finalitat del tractament no pogués aconseguir-se raonablement per altres mitjans que siguin menys intrusius per als drets i llibertats fonamentals dels interessats.

c) I finalment, si la mesura és ponderada o equilibrada, pel fet que de la seva implantació se'n deriven més beneficis o avantatges per a l'interès general que perjudicis per a altres béns jurídics o valors en conflicte (judici de proporcionalitat en sentit estricte). En el cas concret que ens ocupa, tal com s'ha indicat, pot adquirir especial rellevància la dependència concreta en la qual es pretén implementar el control d'accés a través de l'empremta dactilar.

En aquests casos, aquesta ponderació passa a ser l'element decisorí envers la justificació de l'adopció de la mesura. És evident que l'aplicació del sistema de control a través de l'empremta digital és idoni per l'assoliment de l'objectiu a aconseguir, que es pot considerar necessària als efectes de garantir una seguretat superior en els accessos a determinats espais: però especialment s'ha de justificar que, en el cas concret, ha de prevaldre l'adopció d'aquesta mesura, davant fórmules menys invasives de la privacitat.

En aquesta línia, el Tribunal Constitucional ha aplicat el principi de proporcionalitat en sentit estricte com a límit modulador de tota actuació dels poders públics que pugui suposar una ingerència no justificada en l'esfera dels drets i llibertats de les persones.

Es tracta d'una actuació que no deixa de ser complexa i controvertida, i que exigeix una relació equilibrada entre els beneficis que es pretenen amb l'adopció de la mesura limitativa del dret fonamental i la lesió o afectació que es provoca a aquest dret. En definitiva, es tracta d'un judici de resultats, que es mou en el terreny de les conseqüències jurídiques de l'adopció de la mesura restrictiva.

En aquests casos, la fórmula que utilitza el Tribunal Constitucional posa a cada extrem de la balança un dret fonamental i intenta justificar les raons que donen suport a un o altre dret a partir de l'existència de la finalitat legítima que podria arribar a justificar la restricció, la coherència de la restricció amb aquest fi i els resultats precisos que provocaria la lesió d'un dels drets fonamentals. Tot i això, el Tribunal Constitucional tendeix sempre a equilibrar o acomodar ambdós drets, buscant l'equilibri dels avantatges i desavantatges per no arribar a excloure completament el gaudi d'un dret fonamental. Per això no aplica fórmules matemàtiques, sinó que fa una activitat valorativa que parteix de les certes jurídiqes, de

la importància en la satisfacció o preservació de determinats béns constitucionals i de la realitat del cas concret.

En definitiva, l'Ajuntament només ha d'optar per les mesures sense les quals no es pot assolir raonablement la finalitat del tractament o, dit en altres paraules, ha de justificar perquè es descarten altres mesures que també permetin dur a terme la finalitat pretesa i que siguin menys intrusives per als drets i llibertats fonamentals de les persones interessades, i aquesta tasca s'ha d'avaluar cas per cas, prenent en consideració totes les circumstàncies que concorren.

### **Conclusió**

Analitzades les consultes formulades per la delegada de protecció de dades de l'Ajuntament, és necessari que la previsió que es pretén introduir al conveni col·lectiu (i si escau, en els acords pel que fa al personal funcionari), reuneixi els requisits de l'article 9.2.b) de l'RGPD, és a dir, que estableixi les garanties adequades en els termes que ho estableix la doctrina del Tribunal Constitucional a què s'ha fet referència i, a més, que hagi dut a terme amb caràcter previ al tractament de categories especials de dades l'anàlisi de la necessitat de la mesura, i tingui la capacitat de poder demostrar-ho d'acord amb el principi de responsabilitat proactiva (art. 5.2 de l'RGPD).

Pel que fa a l'anàlisi de la necessitat del tractament de dades biomètriques amb la finalitat de control d'accessos, cal que l'Ajuntament analitzi per cadascuna de les dependències municipals, si aquesta mesura supera el judici de proporcionalitat.

Barcelona, 22 d'abril de 2024