Dictamen en relació amb la consulta sobre la utilització d'imatges obtingudes pel sistema de videovigilància.

Antecedents

Es presenta davant l'Autoritat Catalana de Protecció de Dades un escrit dels Delegats de Protecció de Dades de dos entitats en el qual plantegen diverses qüestions en relació amb la utilització d'imatges recollides inicialment per a la finalitat de videovigilància.

En els antecedents de la consulta s'exposa: que una de les entitats (primera entitat) gestiona, i manté el patrimoni i les instal·lacions, d'un edifici on hi conviuen, en qualitat d'arrendataris, entitats dedicades a la investigació i la recerca en el camp de la biomedicina, aquests centres paguen una renda per l'ús de l'espai d'acord amb la seva superfície i tipus, així com diversos serveis del parc.

Segons s'indica, la primera entitat, que gestiona els diferents espais comuns del parc, compta amb un sistema de videovigilància amb la finalitat de garantir la seguretat de les persones i béns així com les seves instal·lacions, en els termes de l'article 22 de la LOPDGDD.

Per la seva banda, s'exposa que una entitat (segona entitat), que ocupa part de l'espai de l'edifici en condició d'arrendatària, va patir la desaparició d'un bé moble de la seva propietat que estava ubicat dins el centre de treball, a la segona planta del parc, on es troben instal·lades dues càmeres de videovigilància situades als accessos del passadís d'aquella planta.

Es posa de manifest que la primera entitat havia col·locat cartells amb el dret d'informació amb les finalitats de l'article 22 LOPDGDD, la identitat del responsable, la possibilitat d'exercir els drets que preveuen els articles 15 a 22 de l'RGPD, i també una adreça a internet amb la resta d'informació que configura l'article 13 de l'RGPD.

La segona entitat va demanar a la primera l'accés a les imatges amb la finalitat d'esbrinar la persona autora del presumpte acte il·lícit sobre el bé moble i, en el cas que fos una persona treballadora, depurar les possibles responsabilitats mitjançant l'obertura d'un expedient disciplinari, d'acord amb el que disposa l'article 89.1 de la LOPDGDD.

Exposat això, el DPD planteja a aquesta Autoritat les qüestions següents:

"Pregunta 1: Respecte dels supòsits previstos a l'article 89.1 de la LOPDGDD, cal entendre aquests com a base de legitimació addicional de les previstes a l'article 6 RGPD o com un reconeixement, iuris et de iure, d'un interès legítim en relació amb el previst a l'article 6.1.f RGPD o bé, una altra de les bases jurídiques previstes al RGPD?

Pregunta 2: Quin és l'abast del concepte acte il·lícit de l'article 89.1 de la LOPDGDD.

Pregunta 3: En relació amb l'anterior, existeix habilitació legal, d'acord amb l'article 89 LOPDGDD, per tal que la primera entitat pugui facilitar les imatges objecte de controvèrsia?

Pregunta 4: En cas afirmatiu a l'anterior pregunta, la segona entitat podrà utilitzar les imatges per a l'obertura d'un expedient disciplinari?

Pregunta 5: Si la segona entitat, en qualitat d'ocupador, incoa un expedient disciplinari en el marc del qual s'acorda la pràctica d'una prova que consistís en l'obtenció de les imatges captades per les càmeres de videovigilància de la primera entitat, aquesta última hauria de facilitar les imatges?

Pregunta 6: Si es fes un acord de corresponsabilitat, entre la primera entitat i els diferents arrendataris del Parc, que complís amb tots els requisits normatius, inclòs el dret d'informació, de manera que el primer, fos responsable del tractament amb la finalitat de videovigilància previst a l'article 22 LOPDGDD (seguretat) i els arrendataris, fossin responsables del tractament amb la finalitat prevista a l'article 89 LOPDGDD (control laboral), aquests últims podrien utilitzar les imatges captades amb finalitats de videovigilància per a les finalitats previstes a l'article 89.1 LOPDGDD?"

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

Fonaments de Dret

I

De conformitat amb allò establert a l'article 5, apartats g) i o) de la Llei 32/2010, de l'1 d'octubre, de l'Autoritat Catalana de Protecció de Dades, correspon a l'Autoritat proporcionar informació sobre els drets de les persones en matèria de tractament de dades personals, així com respondre les consultes que formulin les entitats del seu àmbit d'actuació sobre la protecció de dades de personals en poder de les administracions públiques. L'article 8.2.g) de la Llei 32/2010, de l'1 d'octubre, disposa que és funció de la directora de l'Autoritat respondre les consultes que l'Administració de la Generalitat, els ens locals i les universitats de Catalunya li formulin sobre l'aplicació de la legislació de protecció de dades personals.

En conseqüència, el present dictamen s'emet en base a les esmentades previsions dels articles 5 i 8 de la Llei 32/2010, de l'1 d'octubre, de l'Autoritat Catalana de Protecció de Dades.

II

En la consulta s'exposa que la segona entitat ha sofert la sostracció d'un bé de les seves instal·lacions que previsiblement ha estat captat pel sistema de videovigilància de seguretat de la primera entitat i sol·licita a aquesta l'accés a les imatges per poder determinar el presumpte responsable dels fets.

La imatge i, si escau la veu, captades per un sistema de videovigilància són dades personals, el tractament de les quals, entès com "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, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción"(article 4.2), està sotmès als principis i garanties del 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 (d'ara endavant, RGPD), a la Llei orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals (d'ara endavant LOPDGDD) i, específicament, a la Instrucció 1/2009, de 10 de febrer, de l'Agència Catalana de Protecció de Dades, sobre el tractament de dades de caràcter personal mitjançant càmeres amb fins de videovigilància, en allò que no hagi estat afectada per l'RGPD i l'LOPDGDD.

En aquest sentit, cal tenir present que la utilització de càmeres o sistemes de videovigilància ha de respectar, entre altres, els principis de licitud (article 5.1.a) RGPD), de limitació de la finalitat (article 5.1.b) RGPD) i de minimització de dades (article 5.1.c) RGPD), a partir dels quals només es poden captar i tractar dades a través de sistemes de videovigilància sota l'empara d'una base jurídica, amb finalitats determinades, explicites i legitimes, i cenyint-se a les dades que siguin adequades, pertinents i limitades al necessari en relació amb la finalitat pretesa.

Pel que fa a la licitud del tractament, l'article 5.1.a) RGPD estableix que tot tractament de dades personals ha de ser lícit, lleial i transparent en relació amb l'interessat. Per tal que un tractament sigui lícit cal que concorri alguna de les condicions previstes en l'article 6.1 de l'RGPD.

Com ha fet avinent aquesta Autoritat en altres ocasions (entre d'altres, als dictàmens CNS 37/2022, CNS 4/2022, CNS 42/2021, CNS 33/2021, CNS 21/2021, CNS 26/2019, disponibles al web de l'Autoritat), en l'àmbit de les administracions públiques, la captació d'imatges amb finalitats de videovigilància pot trobar habilitació en la base jurídica de l'article 6.1.e) de l'RGPD.

D'acord amb l'article 6.3 de l'RGPD, la base jurídica del tractament indicat a l'article 6.1.c) i e) RGPD ha d'estar establerta pel Dret de la Unió Europea o pel dret dels Estats membres que s'apliqui al responsable del tractament. En aquest sentit, l'article 8 de la LOPDGG estableix el rang de llei de la norma habilitant per als tractaments que tenen com a base jurídica les lletres c), e) de l'article 6.1 RGPD.

Pel que fa a la videovigilància amb finalitats de seguretat l'article 22 de la LOPDGDD regula el tractament d'imatges a través de sistemes de càmeres i videocàmeres, i estableix condicions específiques per a la seva licitud. Així, estableix:

"1. Les persones físiques o jurídiques, públiques o privades, poden dur a terme el tractament d'imatges a través de sistemes de càmeres o videocàmeres amb la **finalitat de preservar la seguretat de les persones i béns, així com de les seves instal·lacions.**

2. Només es poden captar imatges de la via pública en la mesura en què sigui imprescindible per a la finalitat que esmenta l'apartat anterior. No obstant això, és possible la captació de la via pública en una extensió superior quan sigui necessari per garantir la seguretat de béns o instal·lacions estratègics o d'infraestructures vinculades al

transport, sense que en cap cas pugui suposar la captació d'imatges de l'interior d'un domicili privat.

3. Les dades s'han de suprimir en el termini màxim d'un mes des de la seva captació, **excepte quan s'hagin de conservar per acreditar la comissió d'actes que atemptin contra la integritat de persones, béns o instal·lacions. En aquest cas, les imatges s'han de posar a disposició de l'autoritat competent en un termini màxim de setanta-dues hores des que es tingui coneixement de l'existència de la gravació. No és aplicable a aquests tractaments l'obligació de bloqueig que preveu l'article 32 d'aquesta Llei orgànica.**

4. El deure d'informació que preveu l'article 12 del Reglament (UE) 2016/679 s'entén complert mitjançant la col·locació d'un dispositiu informatiu en un lloc prou visible amb la identificació, almenys, de l'existència del tractament, la identitat del responsable i la possibilitat d'exercir els drets que preveuen els articles 15 a 22 del Reglament (UE) 2016/679. També es pot incloure en el dispositiu informatiu un codi de connexió o una adreça d'Internet amb aquesta informació. En tot cas, el responsable del tractament ha de mantenir a disposició dels afectats la informació a què es refereix el Reglament esmentat.

5. A l'empara de l'article 2.2.c) del Reglament (UE) 2016/679, es considera exclòs del seu àmbit d'aplicació el tractament per part d'una persona física d'imatges que només captin l'interior del seu propi domicili. Aquesta exclusió no comprèn el tractament que dugui a terme una entitat de seguretat privada que hagi estat contractada per a la vigilància d'un domicili i tingui accés a les imatges.

6. El tractament de les dades personals procedents de les imatges i els sons obtinguts mitjançant la utilització de càmeres i videocàmeres per part de les forces i cossos de seguretat i els òrgans competents per a la vigilància i el control als centres penitenciaris i per al control, la regulació, la vigilància i la disciplina del trànsit es regeix per la legislació de transposició de la Directiva (UE) 2016/680, quan el tractament tingui finalitats de prevenció, investigació, detecció o enjudiciament d'infraccions penals o d'execució de sancions penals, incloses la protecció i la prevenció davant de les amenaces contra la seguretat pública. Fora d'aquests supòsits, aquest tractament es regeix per la seva legislació específica i supletòriament pel Reglament (UE) 2016/679 i aquesta Llei orgànica.

7. El que regula aquest article s'entén sense perjudici del que preveuen la Llei 5/2014, de 4 d'abril, de seguretat privada i les seves disposicions de desplegament.

8. El tractament per part de l'ocupador de dades obtingudes a través de sistemes de càmeres o videocàmeres se sotmet al que disposa l'article 89 d'aquesta Llei orgànica."

D'acord amb les condicions establertes per l'article 22 transcrit, es poden considerar lícits els tractaments d'imatges i, si escau veu, duts a terme per persones físiques o jurídiques, públiques o privades quan tinguin com a finalitat preservar la seguretat de les persones, béns i instal·lacions, sempre que no es captin imatges de la via pública (excepte que aquesta captació sigui merament incidental, i es justifiqui per la finalitat perseguida), i es garanteixi el deure d'informació als interessats en els termes de l'apartat quart.

A més, el responsable del tractament ha de suprimir les dades gravades pel sistema de videovigilància en el termini màxim d'un mes des de la seva gravació, excepte que s'hagin de conservar per acreditar la comissió d'actes que "atemptin contra la integritat de persones, béns o instal·lacions".

En el cas que ens ocupa, la primera entitat és el responsable del sistema de videovigilància que ha captat la sostracció d'un bé. La finalitat d'aquest sistema de videovigilància és la seguretat de les persones, béns i instal·lacions i, d'acord amb el que s'indica a la consulta, s'adequa a les previsions de l'article 22 de la Llei orgànica 3/2018, de 5 de desembre, de Protecció de dades personals i garantia dels drets digitals (LOPDGDD).

D'entrada, cal tenir en consideració que en l'escenari plantejat en la consulta no resulta d'aplicació l'article 22.8 de la LOPDGDD en relació amb l'article 89.1 del mateix text legal, que fa referència al tractament per part de l'ocupador de dades obtingudes a través de sistemes de càmeres o videocàmeres. En concret no aplicaria l'excepció prevista en aquest article 89.1 quan estableix: " En el supuesto de que se haya captado la comisión flagrante de un acto ilícito por los trabajadores o los empleados públicos se entenderá cumplido el deber de informar cuando existiese al menos el dispositivo al que se refiere el artículo 22.4 de esta ley orgánica", ja que el responsable del tractament (la primera entitat PRBB) no és l'ocupador i els possibles afectats pel sistema de videovigilància no són els seus treballadors.

La base jurídica del tractament per part del PRBB de les dades del sistema de videovigilància és l'article 6.1.e) de l'RGPD en relació amb l'article 22 de la Llei orgànica 3/2018, de 5 de desembre, de Protecció de dades personals i garantia dels drets digitals (LOPDGDD).

La comunicació de les dades provinents d'un sistema de videovigilància a terceres persones diferents del responsable del tractament -en aquest cas el lliurament de les imatges captades per la videovigilància a la segona entitat-, és també un tractament de dades que requereix una habilitació de les previstes a l'article 6.1 de l'RGPD.

III

Dels termes en els quals es planteja la consulta es dedueix que la segona entitat té la sospita que la sostracció i retorn del bé de les seves instal·lacions l'ha fet un dels seus treballadors, però aquest fet, d'entrada, no es pot corroborar sense el visionament de les imatges del sistema de videovigilància.

En aquest context, escau analitzar si la segona entitat, que és una fundació privada del sector públic de la Generalitat de Catalunya, podria fonamentant la comunicació de les dades en la base jurídica de l'article 6.1.f) de l'RGPD, segons el qual "el tratamiento es necesario para la satisfacción de intereses legitimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y llibertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño."

Tal com estableix el mateix article 6.1 de l'RGPD la lletra f) no serà d'aplicació al tractament realitzat per les autoritats públiques en l'exercici de les seves funcions.

Cal tenir en consideració que la base jurídica de l'interès legítim pot ser utilitzada pel sector públic institucional (en aquest cas per la segona entitat) respecte de les funcions organitzatives i relatives al seu funcionament intern, de manera que la limitació prevista a l'article 6.1 RGPD, s'ha d'entendre que aplica exclusivament respecte de l'exercici de les funcions públiques que tenen encomanades.

Aquest criteri va ser exposat pel grup de treball de l'article 29 en el Dictamen 06/2014 sobre el concepto de interés legítimo del responsable del tratamiento de los datos en virtud del artículo 7 de la Directiva 95/46/CE, en concret plantejava:

> "De cara al futuro, también es importante considerar que la propuesta de Reglamento, en su artículo 6, apartado 1, letra f), estipula de manera específica que el motivo del interés legítimo «no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones». Si esta disposición se promulga y se interpreta de manera amplia, de forma que las autoridades públicas en su conjunto estén excluidas de la aplicación del interés legítimo como fundamento jurídico , entonces los motivos de «interés público» y «poder oficial» del artículo 7, letra e), deberán interpretarse de manera que permitan a las autoridades públicas cierto grado de flexibilidad, al menos con el fin de garantizar su gestión y funcionamiento adecuados, exactamente del mismo modo en que se interpreta el Reglamento nº 45/2001 en la actualidad.
>
> Alternativamente, la última frase del artículo 6, apartado 1, letra f), de la propuesta de Reglamento a la que se hace referencia podría interpretarse de manera que no excluya a las autoridades públicas en su conjunto de la utilización del interés legítimo como fundamento jurídico. En este caso, la frase «tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones» en el artículo 6, apartado 1, letra f) propuesto, deberá interpretarse en sentido estricto. Esta interpretación estricta significaría que el tratamiento para la gestión y el funcionamiento adecuados de estas autoridades públicas se encontraría fuera del ámbito del «tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones». Como consecuencia, el tratamiento para la gestión y el funcionamiento adecuados de estas autoridades públicas podría todavía ser posible en virtud del motivo del interés legítimo."

Ara bé, cal tenir en compte que la base jurídica de l'interès legítim (art. 6.1.f) RGPD) no s'aplica de manera automàtica, sinó que és necessari fer una ponderació que tingui en compte els interessos legítims perseguits pel responsable del tractament o per un tercer, els interessos o els drets i les llibertats fonamentals de l'interessat i les garanties adequades que s'ofereixin.

És a dir, cal valorar si en el supòsit concret objecte d'anàlisi hi ha un interès legítim perseguit pel responsable del tractament o pel tercer o tercers als quals es comuniquin les dades que prevalgui sobre l'interès o els drets i les llibertats fonamentals de l'interessat o si, per contra, aquests drets fonamentals o interessos dels interessats a què es refereixi el tractament de les dades han de prevaler sobre l'interès legítim en què el responsable pretén fonamentar el tractament de dades personals.

Així ho estableix el considerant 47 de l'RGPD quan exposa que:

> "En cualquier caso, la existencia de un interés legítimo requeriría una evaluación meticulosa, inclusive si un interesado puede prever de forma razonable, en el momento y en el contexto de la recogida de datos personales, que pueda producirse el tratamiento con tal fin. En particular, los intereses y los derechos fundamentales del interesado podrían prevalecer sobre los intereses del responsable del tratamiento cuando se proceda al tratamiento de los datos personales en circunstancias en las que el interesado no espere razonablemente que se realice un tratamiento ulterior".

D'aquesta manera, a efectes d'efectuar la necessària ponderació exigida, s'haurà de plantejar si, atenent les circumstàncies concretes que es produeixen en aquest supòsit, l'interès de la segona entitat d'accedir a les dades sol·licitades ha de prevaldre sobre el dret a la protecció de dades dels afectats que siguin objecte de la comunicació.

La segona entitat és responsable de la gestió de l'Hospital del Mar Research Institute, D'acord amb els estatuts de la segona entitat correspon a la gerència "Vetllar pel bon estat i funcionament del patrimoni de la Fundació i fer-ne el seguiment de l'inventari dels béns."(article 35.4.e), així mateix, també li correspon: "Gestionar, d'acord amb les directrius marcades pel Patronat i amb el vist i plau de la persona titular de la Direcció, els recursos humans de la Fundació, la contractació de personal, incidències, separació i rescissió dels contractes laborals i de prestació de serveis; així com la gestió de les beques i ajuts" (article 35.4.c).

En exercici d'aquestes competències la segona entitat podria haver obert un expedient informatiu en relació amb els fets produïts per determinar el responsable o responsables dels fets contra els seus béns, i, en el cas de verificar que el responsable sigui un dels seus treballadors, aplicar les mesures disciplinàries corresponents. En aquest context sembla clara l'existència d'un interès legítim de la segona entitat que li permeti accedir a la informació necessària per determinar el responsable dels fets.

Per altra banda, cal tenir en consideració que l'article 5.1.b) de l'RGPD estableix el principi de limitació de la finalitat de manera que "los datos personales seran recogidos con fines determinados, explícitos i legítimos, y no seran tratados utleriormente de manera incompatible con dichos fines (...)".

Així, per a l'anàlisi de la possibilitat de la comunicació de dades serà necessari determinar si la finalitat per a la qual es van recollir les dades és la mateixa, o en el seu cas, és una finalitat compatible.

Com ens indica el Comitè Europeu de Protecció de Dades (CEPD) en les Directrius 3/2019, sobre el tractament de dades personals mitjançant dispositius de vídeo: "La transmisión de imágenes de vídeo a terceros con fines distintos de aquellos para los que se han obtenido los datos es posible en virtud de las reglas del artículo 6, apartado 4.RGPD (...)"

L'article 6.4 de l'RGPD estableix que:

> "Cuando el tratamiento para otro fin distinto de aquel para el que se recogieron los datos personales no esté basado en el consentimiento del interesado o en el Derecho de la Unión o de los Estados miembros que constituya una medida necesaria y proporcional en una sociedad democrática para salvaguardar los objetivos indicados en el artículo 23, apartado 1, el responsable del tratamiento, con objeto de determinar si el tratamiento con

> otro fin es compatible con el fin para el cual se recogieron inicialmente los datos personales, tendrá en cuenta, entre otras cosas:
>
> a) cualquier relación entre los fines para los cuales se hayan recogido los datos personales y los fines del tratamiento ulterior previsto;
>
> b) el contexto en que se hayan recogido los datos personales, en particular por lo que respecta a la relación entre los interesados y el responsable del tratamiento;
>
> c) la naturaleza de los datos personales, en concreto cuando se traten categorías especiales de datos personales, de conformidad con el artículo 9, o datos personales relativos a condenas e infracciones penales, de conformidad con el artículo 10;
>
> d) las posibles consecuencias para los interesados del tratamiento ulterior previsto;
>
> e) la existencia de garantías adecuadas, que podrán incluir el cifrado o la seudonimización."

Per a determinar la compatibilitat del tractament posterior de les dades del sistema de videovigilància cal analitzar, en primer lloc, qualsevol relació entre la finalitat per a la qual es van recollir les dades i la finalitat del tractament ulterior previst. En el cas que ens ocupa hi ha una clara relació entra la finalitat de seguretat de les persones, béns i instal·lacions que perseguia el tractament inicial, amb la finalitat d'investigació dels fets per tal de , si fos el cas, dirimir les responsabilitats disciplinàries relacionades amb la presumpta comissió d'un il·lícit sobre els béns de l'empresa per part d'una persona treballadora.

En segon lloc, s'ha d'analitzar el context en el qual s'han recollit les dades personals. En el cas que ens ocupa les dades personals provenen del sistema de videovigilància de les instal·lacions que, segons s'indica a la consulta, s'adequa a les previsions de l'article 22 de la LOPDGDD i compta amb els dispositius d'informació a les persones afectades en els termes de l'article 22.4 de la LOPDGDD. Per tant, en el context de la recollida de les dades les persones afectades ja disposen d'unes expectatives que les seves dades personals seran recollides pel sistema de videovigilància.

En tercer lloc, cal tenir en consideració la naturalesa de les dades personals i en concret si es tracta de categories especials de dades de conformitat amb l'article 9 o dades relatives a condemnes i infraccions penals.

Pel que fa a la naturalesa de les dades consistents en la imatge i la veu de persones físiques, en principi, d'acord amb l'RGPD no han de considerar-se categories especials de dades. El considerant 51 de l'RGPD especifica que "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".

És a dir, la imatge i, si escau la veu, de les persones que podrien ser susceptibles de ser captats per un sistema de videovigilància, en principi i pel sol fet de ser captades, no han de considerar-se un tractament de dades biomètriques (categories especials de dades), sempre que aquestes dades no es tractin amb mitjans tècnics específics per tal d'identificar o

autenticar de manera unívoca les persones afectades, el que no sembla que concorri en el supòsit referent a la consulta formulada.

Finalment, cal analitzar les possibles conseqüències per als interessats del tractament ulterior previst i l'existència de garanties adequades. En aquest sentit, si l'entitat destinatària de les dades en aplicació del principi de minimització identifica l'interval de temps en el qual es pot haver produït la sostracció i reposició del bé, de tal manera que no es produeix un accés indiscriminat i continu a la informació, sinó exclusivament al moment exacte en que es produeixen els fets, l'afectació als interessats es pot considerar mínima. Per altra bada, i en quant a les garanties adequades, el destinatari podria garantir la implementació de mesures tècniques i organitzatives per garantir que l'accés a la informació només es produirà per les persones competents per a la tramitació de l'expedient informatiu i, que només es conservaran durant el període de temps necessari per a la nova finalitat.

És a dir, amb caràcter general, i d'acord amb l'anàlisi efectuat es pot concloure que la comunicació de les dades objecte de la consulta no persegueix una finalitat incompatible, amb la finalitat per a la qual es van recollir.

També cal tenir en compte que l'article 5.1.c) del RGPD recull el principi de "minimització de les dades", de manera que "Les dades personals seran adequades, pertinents i limitades al que és necessari en relació amb els fins per als que són tractats"

Això suposa que la comunicació haurà de limitar-se al mínim necessari o imprescindible per a la finalitat pretesa, cosa que en aquest cas ens porta a concloure que la "visualització" pretesa només seria conforme amb aquest principi si no s'estén més enllà del necessari perquè la segona entitat pogués determinar exclusivament allò relacionat amb l'incident concret i específic a què es refereix la seva petició, però res més.

Per això, i tenint en compte els termes en què està plantejada la consulta, cal apuntar que correspon al responsable del tractament (la primera entitat), determinar en primer lloc, mitjançant la visualització de les imatges, la informació imprescindible i necessària perquè el tercer (la segona entitat) pugui veure satisfeta la finalitat de la consulta, però sense que es pugui estendre a res més del necessari. Per tant, aquest "visionat" haurà de limitar-se exclusivament a les imatges que tinguin relació amb els supòsits per als quals se sol·licita la informació, però no a cap altra imatge en què puguin existir dades personals no relacionades amb els motius exposats a la consulta.

En els termes exposats, es pot considerar que la comunicació de les dades del sistema de videovigilància del la primera entitat a la segona entitat, és un tractament lícit emparat en l'article 6.1.f) de l'RGPD i que s'adequa a la resta de principis de l'RGPD.

IV

Qüestió diferent a la plantejada en els fonaments anteriors seria que la segona entitat fos el responsable del tractament d'un sistema de videovigilància amb finalitats de seguretat a l'empara de l'article 22 de la LOPDGDD i volgués emprar les imatges captades pel seu

sistema de videovigilància, en els termes de l'article 89.1 de la mateixa LOPDGDD per haver captat la comissió flagrant d'un acte il·lícit per un dels seus treballadors.

Pel que fa a la videovigilància amb finalitats de control laboral, l'article 22.8 de l'LOPDGDD concreta els termes en què el tractament de càmeres de videovigilància amb fins laborals pot tenir habilitació legal, tot establint que *"el tratamiento por el empleador de datos obtenidos a través de sistemas de cámaras o videocámaras se somete a lo dispuesto en el artículo 89 de esta ley orgánica"* (apartat 8).

L'article 89 a què ens remet aquest precepte legal disposa el següent:

> *"1. Los **empleadores podrán tratar las imágenes obtenidas a través de sistemas de cámaras o videocámaras para el ejercicio de las funciones de control de los trabajadores o los empleados públicos** previstas, respectivamente, en el artículo 20.3 del Estatuto de los Trabajadores y en la legislación de función pública, **siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo**. Los empleadores habrán de informar con carácter previo, y de forma expresa, clara y concisa, a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de esta medida.*
> *En el supuesto de que se haya captado la comisión flagrante de un acto ilícito por los trabajadores o los empleados públicos se entenderá cumplido el deber de informar cuando existiese al menos el dispositivo al que se refiere el artículo 22.4 de esta ley orgánica.*
> *2. En ningún caso se admitirá la instalación de sistemas de grabación de sonidos ni de videovigilancia en lugares destinados al descanso o esparcimiento de los trabajadores o los empleados públicos, tales como vestuarios, aseos, comedores y análogos.*
> *3. La utilización de sistemas similares a los referidos en los apartados anteriores para la **grabación de sonidos en el lugar de trabajo se admitirá únicamente** cuando resulten relevantes los riesgos para la seguridad de las instalaciones, bienes y personas derivados de la actividad que se desarrolle en el centro de trabajo y siempre respetando el principio de proporcionalidad, el de intervención mínima y las garantías previstas en los apartados anteriores. La supresión de los sonidos conservados por estos sistemas de grabación se realizará atendiendo a lo dispuesto en el apartado 3 del artículo 22 de esta ley."*

Segons l'article 20.3 del Text refós de la Llei de l'Estatut dels Treballadors (ET), aprovat pel Reial decret legislatiu 2/2015, de 23 d'octubre, *"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."*

Destacar també que la disposició addicional tretzena de l'LOPDGDD afegeix un nou article 20 bis a l'ET, amb el següent contingut:

> *"Artículo 20 bis. Derechos de los trabajadores a la intimidad en relación con el entorno digital y a la desconexión.*

*Los **trabajadores tienen derecho a la intimidad** en el uso de los dispositivos digitales puestos a su disposición por el empleador, a la desconexión digital y a la intimidad **frente al uso de dispositivos de videovigilancia** y geolocalización en los términos establecidos en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales."*

En el mateix sentit, la disposició final catorzena de l'LOPDGDD, afegeix una nova lletra j bis) a l'article 14 del Text refós de la Llei de l'Estatut bàsic del treballador públic (TRLEBEP), aprovat per Reial decret legislatiu 5/2015, de 30 d'octubre, amb la següent redacció:

*"**Los empleados públicos tienen los siguientes derechos** de carácter individual en correspondencia con la naturaleza jurídica de su relación de servicio:*
(...)
*j bis) **A la intimidad** en el uso de dispositivos digitales puestos a su disposición y **frente al uso de dispositivos de videovigilancia** y geolocalización, así como a la desconexión digital en los términos establecidos en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales."*

Aquestes previsions normatives habiliten, en el marc de les relacions laborals, al responsable del tractament per a poder dur a terme un tractament de les imatges captades a través de sistemes de videovigilància per a finalitats de control laboral, sempre, però, que es respecti la intimitat de les persones treballadores.

Cal tenir en consideració, però, que en l'àmbit de la videovigilància, no és suficient amb una base jurídica que habiliti el tractament, sinó que és necessari també que aquesta mesura resulti proporcionada a la finalitat perseguida.

Com ha posat de manifest reiterada jurisprudència (per totes, la STC 39/2016, de 3 de març), i com fa avinent també la Instrucció 1/2009, 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.

En aquest sentit, el dictamen CNS 37/2022, d'aquesta Autoritat que es pot consultar en el següent enllaç, posa de manifest que partint d'aquest judici de proporcionalitat, els tribunals han considerat (per exemple, STS de 5 de març de 2020 o la STSJC de 22 de març de 2018) que la mesura de vigilància mitjançant càmeres de manera contínua per al control de l'activitat laboral, que abasti el conjunt de persones treballadores, i sense fer esment de cap risc en particular, resultaria desproporcionada, atès que comportaria un veritable monitoratge de les persones treballadores, un control de tots i cadascun dels seus comportaments, en definitiva, un excés del poder directiu de què disposa l'empresari (article 20.3 ET).

També la Instrucció 1/2009 fa avinent que pot resultar no-adequada al principi de proporcionalitat *"la utilització de sistemes de videovigilància en l'àmbit laboral amb la finalitat exclusiva de controlar el rendiment de les persones treballadores"* (article 7.3.b)).

En conseqüència, el judici de proporcionalitat que ha d'acompanyar qualsevol mesura restrictiva de drets, en aquest cas el de la videovigilància dels treballadors ha de determinar clarament, entre altres qüestions, la finalitat concreta pretesa per la mesura, la ubicació i camp de visió de les càmeres de tal manera que es garanteixi que el tractament no resulta desproporcionat.

Per altra banda, l'article 89 de LOPDGDD regula una excepció en el supòsit que el sistema de videovigilància hagués captat la comissió flagrant d'un acte il·lícit pels treballadors o empleats públics, en quin cas l'ocupador podria tractar les imatges tot i que la informació als treballadors s'hagués efectuat en els termes de l'article 22.4 LOPDGDD.

Sobre aquesta qüestió, el Tribunal Constitucional en la Sentència de 119/2022 de 29 de setembre de 2022, en recurs d'empara per vulneració del dret a la tutela judicial efectua (article 24.1 CE), analitza la normativa sobre protecció de dades en l'àmbit laboral i avala la utilització per a ús disciplinari de les imatges captades pel sistema de seguretat de l'empresa. En aquest sentit ell Tribunal exposa:

> "La nueva regulación ha supuesto un cambio de paradigma normativo, superando el sistema de registros o ficheros, para inspirarse en el principio de proactividad de los responsables del tratamiento de datos, lo que supone la obligación de aplicar medidas técnicas y organizativas apropiadas, acordes con la naturaleza, ámbito y fines del tratamiento, para garantizar y acreditar el cumplimiento de la normativa vigente en protección de los derechos de los titulares de esos datos.
> En el ámbito concreto de las relaciones laborales, la Ley Orgánica 3/2018 ha previsto expresamente una serie de criterios generales para el tratamiento de los datos derivado del uso de dispositivos de videovigilancia y de grabación de sonidos. Estos criterios se desprenden de la interpretación y aplicación conjunta de los arts. 22 y 89 de la Ley Orgánica 3/2018, en el marco general descrito en el art. 20 del Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del estatuto de los trabajadores (en adelante, LET).
>
> En lo que ahora interesa, el art. 20.3 LET dispone, con carácter general, que 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». Más en concreto, el art. 20 bis LET señala que los trabajadores «tienen derecho a la intimidad […] frente al uso de dispositivos de videovigilancia y geolocalización en los términos establecidos en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales». Por lo tanto, la normativa laboral básica se remite, en esta materia, a lo dispuesto en la Ley Orgánica 3/2018.
>
> A su vez, el art. 22.8 de la Ley Orgánica 3/2018 establece que el «tratamiento por el empleador de datos obtenidos a través de sistemas de cámaras o videocámaras se somete a lo dispuesto en el artículo 89 de esta ley orgánica». Por su parte, el art. 89 de la Ley Orgánica 3/2018 señala, en sus dos primeros apartados, lo siguiente:
> (...)

Y, finalmente, el art. 22.4 de la Ley Orgánica 3/2018 cierra el círculo de remisiones normativas señalando que el deber de información que corresponde al responsable de un tratamiento de datos con fines de videovigilancia «se entenderá cumplido mediante la colocación de un dispositivo informativo en lugar suficientemente visible identificando, al menos, la existencia del tratamiento, la identidad del responsable y la posibilidad de ejercitar los derechos previstos en los artículos 15 a 22 del Reglamento (UE) 2016/679».

En consecuencia, en el marco general del control del cumplimiento de un contrato de trabajo, y a estos solos fines, el empresario podrá instalar un sistema de videovigilancia. La instalación y uso del sistema no requerirá el consentimiento de los trabajadores, pero sí exige un deber de informar a estos con carácter previo y de forma expresa sobre su existencia y finalidad. La ubicación de las cámaras habrá de respetar la intimidad propia de los lugares destinados al descanso o esparcimiento, o que tengan un carácter reservado. No obstante, la utilización de las imágenes captadas para verificar o acreditar la comisión flagrante de un acto ilícito no exigirá el previo deber de información, que podrá entenderse cumplido cuando se haya colocado en lugar visible un distintivo informativo de la existencia del sistema, de su responsable y de su finalidad.

El marco normativo vigente, por tanto, resulta coherente con la doctrina jurisprudencial de este tribunal y del Tribunal Europeo de Derechos Humanos, lo que permite abordar la resolución de este recurso.
(...)

De la doctrina jurisprudencial expuesta y de la normativa aplicable se deduce que, para la adecuada resolución de este recurso de amparo, se hace necesario analizar, en primer lugar, si la instalación del sistema y su uso con fines disciplinarios se ajustó o no a la normativa sobre protección de datos y, en el caso de que así fuera, procedería, en segundo lugar, valorar su posible repercusión desde la perspectiva del derecho a la intimidad del trabajador.

Todo lo anterior sería determinante, a su vez, de la licitud o no de la prueba y, por lo tanto, de la vulneración o no del derecho a la tutela judicial efectiva (art. 24.1 CE), en relación con el derecho a utilizar los medios de prueba y a un proceso con todas las garantías (art. 24.2 CE).

(...)

En base a aquestes consideracions l'enjudiciament del cas conclou:

b) Sobre el derecho a la protección de los datos personales del trabajador: inexistencia de vulneración.

El consentimiento del titular de los datos y el consiguiente deber de información sobre su tratamiento se configuran como elementos determinantes del contenido esencial del derecho a la protección de los datos personales reconocido en el art. 18.4 CE. Por lo que se refiere a la instalación de sistemas de videovigilancia y la utilización de las imágenes para fines de control laboral, el tratamiento de esos datos no exige el consentimiento expreso del trabajador, porque se entiende implícito por la mera relación contractual. Pero, en todo caso, subsiste el deber de información del empresario, como garantía ineludible del citado derecho fundamental. En principio, este deber ha de cumplimentarse

de forma previa, expresa, clara y concisa. Sin embargo, la norma permite que, en caso de flagrancia de una conducta ilícita, el deber de información se tenga por efectuado mediante la colocación en lugar visible de un distintivo que advierta sobre la existencia del sistema, su responsable y los derechos derivados del tratamiento de los datos. El fundamento de esta excepción parece fácilmente deducible: no tendría sentido que la instalación de un sistema de seguridad en la empresa pudiera ser útil para verificar la comisión de infracciones por parte de terceros y, sin embargo, no pudiera utilizarse para la detección y sanción de conductas ilícitas cometidas en el seno de la propia empresa. Si cualquier persona es consciente de que el sistema de videovigilancia puede utilizarse en su contra, cualquier trabajador ha de ser consciente de lo mismo.

El hecho de que las cámaras hubieran sido utilizadas para la misma finalidad en el año 2014 no puede ser valorado en perjuicio de la empresa, como hace la sala de lo social del Tribunal Superior de Justicia del País Vasco. Para la sala, la infracción del deber específico de información implica una vulneración del derecho a la intimidad del trabajador. Frente a este planteamiento, conviene precisar, en primer lugar, que el incumplimiento del deber de información afectaría, en esencia, al derecho a la protección de datos de carácter personal, no a la intimidad. Pero, sobre todo, lo que pone de manifiesto ese hecho es que el trabajador, con una antigüedad en la empresa desde el año 2007, conocía y era consciente de la existencia de las cámaras y de su eventual utilización para fines laborales disciplinarios. Con ello, no se quiere excluir la responsabilidad de la empresa en el incumplimiento de su deber de información, pero de ese dato no se puede deducir la invalidez de la utilización de esas imágenes en los casos de conducta ilícita flagrante, porque la mayor o menor flagrancia de la conducta no depende de la existencia o no de un hecho acreditado con anterioridad a través de esa misma medida.

En el caso concreto, los elementos fácticos no controvertidos ponen de manifiesto que no se ha producido vulneración alguna de la normativa sobre protección de datos de carácter personal y, por lo tanto, del derecho fundamental correspondiente. La empresa había colocado el correspondiente distintivo en lugar visible, ajustado a las previsiones legales en materia de protección de datos. Las cámaras se utilizaron para comprobar un hecho concreto, que resultó flagrante, y sobre la base de una sospecha indiciaria concreta, como era la irregularidad manifiesta de guardar un producto de la empresa dentro de una bolsa con el logotipo de una empresa de la competencia, en un lugar no habilitado a tal efecto, del que desapareció al día siguiente. En ese contexto, resultaba válida la utilización de las imágenes captadas para verificar una conducta ilícita cometida por un trabajador."

En base a les consideracions efectuades podem concloure que les previsions de l'article 89.1 de la LOPDGDD, no constitueixen una base legitimadora addicional a les previstes a l'article 6 de l'RGPD, sinó una concreció dels requisits de licitud que ha de reunir un sistema de videovigilància laboral en relació amb alguna de les bases legitimadores de l'article 6 de l'RGPD, com podrien ser, en el cas de les administracions públiques el compliment d'una missió realitzada en interès públic o en l'exercici de poders públics (6.1.e) o l'execució d'un contracte (6.1.b) en el cas dels ocupadors privats, en el marc de les facultats de control empresarial que reconeix l'article 20.3 de l'ET.

Així mateix, les previsions de l'article 89.1 de la LOPDGDD tampoc s'han d'entendre com "un reconeixement iuris et de iure, d'un interès legítim en relació amb el previst a l'article

6.1.f)" (emprant els termes de la consulta), ja que l'aplicació de l'article 6.1.f) requereix necessàriament efectuar la ponderació de cada cas concret per determinar-ne l'existència de l'interès legítim, i aquesta ponderació no es pot suplir per una disposició normativa perquè aniria en contra de les previsions de l'RGPD. Així ho va posar de manifest el Consell d'Estat en el seu informe sobre l'Avantprojecte de Llei Orgànica de Protecció de Dades de Caràcter Personal, de data 26 d'octubre de 201, quan analitza el Titol IV de l'avantporjecte de llei, anomenat "Disposiciones aplicables a tratamientos concretos" i on està ubicat l'actual article 22 de la LOPDGDD, respecte del qual efectua les consideracions següents:

> "El Título IV del Anteproyecto (artículos 20 a 28) contempla una serie de disposiciones aplicables a tratamientos concretos.
>
> Algunos de ellos se consideran como lícitos al amparo del artículo 6.1.f) del Reglamento Europeo y, más concretamente, de la previsión del artículo 9.3 del propio Anteproyecto de Ley Orgánica, por ser necesarios para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, sin que sobre dichos intereses prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales.
>
> **Deben darse aquí por reproducidas, por tanto, las observaciones formuladas en el cuerpo del presente dictamen en relación con el artículo 9.3 del Anteproyecto, que llevan a concluir a la imposibilidad de llevar a cabo un desarrollo en el ordenamiento jurídico nacional del supuesto de licitud del tratamiento contemplado en el citado artículo 6.1.f), en la medida en que el mismo suponga congelar a nivel legislativo una ponderación de intereses que debe hacerse, tal y como viene reiterando la jurisprudencia, en consideración a las circunstancias del caso en particular** (SSTJUE, ya citadas, ASNEF, apartado 47; y Breyer, apartado 62). En la medida en que los preceptos de ese Título IV, por tanto, se han amparado en la habilitación general contenida en el artículo 9.3 del Anteproyecto no pueden tampoco mantenerse (en los términos en que actualmente aparecen redactados).

V

Finalment, la consulta planteja la possibilitat de fer un acord de corresponsabilitat entre el la primera entitat i els diferents arrendataris del Parc, de manera que el primer, fos responsable del tractament amb la finalitat de videovigilància previst a l'article 22 LOPDGDD (seguretat) i els arrendataris, fossin responsables del tractament amb la finalitat prevista a l'article 89 LOPDGDD (control laboral), i en aquest escenari si aquests últims podrien utilitzar les imatges captades amb finalitats de videovigilància per a les finalitats previstes a l'article 89.1 LOPDGDD.

Respecte d'aquesta qüestió cal analitzar, en primer lloc si el sistema de videovigilància existent es pot utilitzar per a una finalitat de control laboral en el sentit que es superi el judici de proporcionalitat de la mesura. I, en segon lloc si es donen les circumstàncies per a considerar que existeix corresponsabilitat en el tractament per part d'ambdós organismes.

Pel que fa a la primera qüestió, com s'ha exposat, l'article 22.8 en relació amb l'article 89 de l'LOPDGDD, concreten els termes en què el tractament de càmeres de videovigilància amb

fins laborals pot tenir habilitació legal en relació amb alguna de les bases jurídiques de l'article 6.1 de l'RGPD.

En el cas que la segona entitat es plantegés la implantació d'un sistema de videovigilància amb finalitat de control laboral hauria d'efectuar la corresponent anàlisi de proporcionalitat i de justificació de la mesura que hauria de quedar recollida en la Memòria a què fa referència la Instrucció 1/2009, de 10 de febrer.

Així mateix, d'acord amb l'article 89.1 de la LOPDGDD, la segona entitat hauria d'informar amb caràcter previ i de forma, expressa, clara i concisa a les persones treballadores i als seus representants, sobre la mesura de videovigilància que es vol implantar.

Pel que fa a la possibilitat d'emprar el sistema de videovigilància de la primera entitat, existent a les instal·lacions, mitjançant un acord de corresponsabilitat, cal tenir en consideració l'article 26 de l'RGPD, que estableix que quan dos o més responsables determinen conjuntament els objectius i els mitjans del tractament són considerats corresponsables del tractament.

Com ha fet avinent aquesta Autoritat (a tall d'exemple, en el dictamen CNS 24/2018, disponible al següent enllaç del seu web), l'element clau per atribuir el rol de responsable del tractament és la capacitat de decidir o determinar la finalitat, el contingut, l'ús o els mitjans del tractament, és a dir, la capacitat de prendre decisions sobre què fer i com tractar les dades personals des del moment en què aquestes es recullen fins a la seva destrucció, és a dir, durant tot el cicle del tractament de les dades (article 4.2) RGPD).

La determinació de la corresponsabilitat en el tractament requereix una anàlisi detallada de les circumstàncies concretes que concorren en el cas.

Les Directrius 7/2020 sobre els conceptes de responsable del tractament i d'encarregat del tractament en l'RGPD del CEPD (disponible en aquest enllaç del seu web) aporten elements que es poden tenir en consideració a l'hora de determinar si existeix corresponsabilitat en el tractament .

Segons el CEPD, el criteri general per a l'existència de la corresponsabilitat del tractament és la participació conjunta de dos o més ens en la determinació de les finalitats i els mitjans del tractament. Ara bé, l'avaluació de la corresponsabilitat s'ha de basar en una anàlisi fàctica de la influència real sobre les finalitats i els mitjans del tractament, perquè no totes les operacions de tractament en les quals participen varis ens donen lloc a una situació de corresponsabilitat.

Les Directrius 7/2020, indiquen que no ha d'haver-hi necessàriament una responsabilitat idèntica entre els diferents participants involucrats en el tractament, sinó més aviat al contrari i en aquest sentit recorda que "el TJUE ha aclarado que las partes pueden participar en distintas fases del tratamiento y en distinto grado. Por tanto, el nivel de responsabilidad de cada una debe evaluarse en función de todas las circunstancias pertinentes del caso concreto" (apartat 58).

Pel que fa als objectius el CEPD també indica que "en vista de la jurisprudencia del TJUE, es posible determinar la corresponsabilidad cuando los participantes persigan unos fines

estrechamente vinculados o complementarios, aunque no compartan un mismo fin en el tratamiento" (aparat 60).

En relació amb els mitjans del tractament, el CEPD puntualitza, "También puede darse el caso de que uno de los participantes proporcione los medios para el tratamiento y los ponga a disposición de otros para que estos lleven a cabo las actividades de tratamiento de datos personales. El ente que decide utilizar dichos medios para poder tratar los datos personales para un fin concreto también participa en la determinación de los medios del tratamiento" (apartat 64).

D'acord amb l'article 26 RGPD els corresponsables han de determinar de manera transparent i de mutu acord les seves responsabilitats respectives en el compliment de les obligacions imposades pel RGPD, en particular quant a l'exercici dels drets de l'interessat i de les seves respectives obligacions del subministrament de la informació a què es refereixen els articles 13 i 14 de l'RGPD.

A tal efecte, l'acord entre els corresponsables del tractament ha de reflectir degudament les funcions i les relacions respectives d'aquests en relació amb els interessats (l'article 26.1. RGPD)

Com explicita el CEPD, pel que fa a la relació entre els corresponsables del tractament, l'acord, també ha de "abarcar otras obligaciones del responsable del tratamiento relacionadas, por ejemplo, con los principios generales de protección de datos, la base jurídica, las medidas de seguridad, la obligación de notificar las violaciones de la seguridad de los datos, las evaluaciones de impacto relativas a la protección de datos, el recurso a encargados del tratamiento, las transferencias a terceros países, y los contactos con los interesados y las autoridades de control" (Resum executiu Directrius).

Si bé l'RGPD no especifica la forma jurídica que ha de tenir l'acord, respecte d'aquesta qüestió el CEPD recomana " En aras de la seguridad jurídica y a fin de asegurar la transparencia y la responsabilidad proactiva, el CEPD recomienda que dicho acuerdo se suscriba por medio de un documento vinculante,como un contrato, u otro acto jurídico vinculante en virtud del Derecho de la Unión o del Derecho de los Estados miembros que se les aplique."

En definitiva, si ambdues institucions consideren que compleixen els requisits de corresponsabilitat, en els termes de l'article 26.1 de l'RGPD, han de signar el corresponent acord que el reguli, establint les obligacions concretes que corresponen a cadascú. Ara bé, correspondria a la segona entitat informar a les persones treballadores i als seus representants, amb caràcter previ a la utilització del sistema de videovigilància per a la finalitat de control laboral, i de forma, expressa, clara i concisa, sobre la mesura que es vol implantar.

Conclusió

En l'escenari plantejat en la consulta no resulta d'aplicació l'article 22.8 de la LOPDGDD en relació amb l'article 89.1 del mateix text legal, que fa referència al tractament per part de l'ocupador de dades obtingudes a través de sistemes de càmeres o videocàmeres. En concret no aplicaria l'excepció prevista en aquest article 89.1 quan estableix: " En el

supuesto de que se haya captado la comisión flagrante de un acto ilícito por los trabajadores o los empleados públicos se entenderá cumplido el deber de informar cuando existiese al menos el dispositivo al que se refiere el artículo 22.4 de esta ley orgánica", ja que el responsable del tractament (la primera entitat) no és l'ocupadora i els possibles afectats pel sistema de videovigilància no són els seus treballadors.

En canvi, la base jurídica de l'interès legítim (article 6.1.f) RGPD, podria habilitar la comunicació de les imatges del sistema de videovigilància de la primera entitat a la segona entitat per tal que aquest adopti les mesures oportunes en relació amb els fets enregistrats.

Igualment, pel que fa a l'obertura d'un expedient disciplinari en base a dites imatges, des del punt de vista procedimental, ha d'existir una actuació prèvia, com podria ser la incoació d'una informació reservada per part de l'òrgan competent, que habiliti i documenti els termes concrets de la petició de comunicació.

Si es fes un acord de corresponsabilitat, entre la primera i la segona entitats, que complís amb tots els requisits normatius, inclòs el dret d'informació, de manera que el primer, fos responsable del tractament amb la finalitat de videovigilància previst a l'article 22 LOPDGDD (seguretat) i la segona entitat, fos responsable del tractament amb la finalitat prevista a l'article 89 LOPDGDD (control laboral) es podria considerar que el tractament s'adequa a la normativa de protecció de dades.

Barcelona, 1 de juliol de 2024