

PRIVACIDADE E DATOS PERSOAIS DOS TRABALLADORES: CONVERXENCIA DAS SOLUCIÓNS LEXISLATIVAS E XURISPRUDENCIAIS EN EUROPA

PRIVACY AND PERSONAL DATA PROTECTION OF WORKERS:
CONVERGENCE OF LEGAL AND JUDICIAL SOLUTIONS IN
EUROPE

DAVID ORDÓÑEZ SOLÍS

Maxistrado

Red de Especialistas en Derecho de la Unión Europea (REDUE)

Comisión Iberoamericana de Ética Judicial

d.ordonez@poderjudicial.es

RESUMO

Os traballadores tamén teñen dereito a que na súa relación laboral se respecte a súa vida privada e se protexan os seus datos persoais. Como se fose unha carreira fronte a unhas tecnoloxías cada vez máis invasivas, a lexislación e, en particular, a xurisprudencia do Tribunal Europeo de Dereitos Humanos e do Tribunal de Xustiza da Unión Europea están a achegar solucións. A lexislación europea, especialmente a partir da aplicación do Regulamento xeral de protección de datos, resulta de gran importancia e así se deduce da aprobación de leis nacionais complementarias. Na aplicación deste marco normativo, integrado por normas europeas e nacionais, os tribunais deben ter en conta esta retroalimentación entre lexislación e xurisprudencia nun ámbito onde se deixa en mans dos xuíces a tarefa de garantir adecuadamente o equilibrio dos dereitos en xogo do traballador e do empregador.

Palabras chave: novas tecnoloxías, empregador, traballador, dereito á vida privada, dereito á protección de datos, Tribunal Europeo de Dereitos Humanos, Tribunal de Xustiza da Unión Europea, tribunais nacionais.

RESUMEN

Los trabajadores también tienen derecho a que en su relación laboral se respete su vida privada y se protejan sus datos personales. Como si fuese una carrera frente a unas tecnologías cada vez más invasivas, la legislación y, en particular, la jurisprudencia del Tribunal Europeo de Derechos Humanos y del Tribunal de Justicia de la Unión Europea están aportando soluciones. La legislación europea, especialmente a partir de la aplicación del Reglamento General de Protección de Datos, resulta de gran importancia y así se deduce de la aprobación de leyes nacionales complementarias. En la aplicación de este marco normativo, integrado por normas europeas y nacionales, los tribunales deben tener en cuenta esta retroalimentación entre legislación y jurisprudencia en un ámbito donde se deja en manos de los jueces la tarea de garantizar adecuadamente el equilibrio de los derechos en juego del trabajador y del empleador.

Palabras clave: nuevas tecnologías, empleador, trabajador, derecho a la vida privada, derecho a la protección de datos, Tribunal Europeo de Derechos Humanos, Tribunal de Justicia de la Unión Europea, tribunales nacionales.

ABSTRACT

Workers are entitled to protect their rights in the working relations, notably the right to privacy and the right to protect their personal data. As a competition facing the new technologies' intrusion, European legislation and case-law, notably the European Court of Human Rights and the Court of Justice of the European Union, are focused on these issues. Especially after the entry into force of the General Data Protection Regulation, European legislation is of great interest in order to adopt complementary national norms. When implementing this legal framework, composed of European and national laws, national Courts must understand this feed-back between legislation and case-law where judges are committed to strike a fair balance between workers' and employers' rights at stake.

Keywords: new technologies, worker, employer, right to privacy, right to personal data protection, European Court of Human Rights, Court of Justice of the European Union, National Courts.

1. INTRODUCCIÓN. INTIMIDADE, PRIVACIDADE E TRABALLADORES NUN CONTEXTO TECNOLÓXICO AVANZADO

A aparición de novas tecnoloxías facilitou unha alarmante invasión da vida privada das persoas ata o punto de acelerar, en resposta, a creación dun novo dereito fundamental, complementario do dereito á privacidade, como é a protección dos datos persoais.

No ámbito laboral a aplicación deste novo dereito fundamental veu matizado pola necesidade de ter en conta a especial relación que se produce entre empregador e empregado que, en realidade, pode esixir unha ponderación apropiada dos intereses en xogo. Esta relación especial debilita, en gran medida, a eficacia do consentimento do traballador para o tratamento dos datos persoais polo empregador, pero non exime a este de respectar un ámbito íntimo do traballador e sometelo a un procedemento de información e de xustificación da intromisión na súa vida privada.

Nestes momentos resulta relevante comprobar como se producen os cambios na formulación constitucional, na adopción de normas lexislativas e, en fin, nas solucións xurisprudenciais adoptadas. Para iso sería importante tomar como referencia a experiencia española, desenvolvida no marco europeo, onde se tentan cumprir as obrigas europeas sobre privacidade e protección de datos no ámbito laboral e ver como os tribunais, en particular o Tribunal Constitucional e os tribunais do social e do contencioso-administrativo, tratan de establecer parámetros claros de actuación.

Na primeira parte, examino a regulación da Unión Europea e a súa aplicación normativa en España; e na segunda parte explico cal foi o alcance das intervencións dos tribunais europeos, do Tribunal Europeo de Dereitos Humanos e do

Tribunal de Xustiza da Unión Europea, e a actitude dos tribunais españois.

2. A REGULACIÓN DA PROTECCIÓN DA VIDA PRIVADA E OS DATOS PERSOAIS DOS TRABALLADORES NA UNIÓN EUROPEA E EN ESPAÑA

O Consello de Europa estableceu en 2015 uns principios aplicables tanto ao emprego privado como ao público baseados na dignidade humana e os dereitos e liberdades fundamentais, á vez que marcaba as pautas a empregadores e traballadores en canto a almacenamento dos datos, ao seu uso interno, á súa comunicación, á súa transmisión, aos datos sensibles dos traballadores ou ás formas particulares de procesamento dos datos (uso da internet e comunicacións electrónicas, videovixilancia e control, localización, datos biométricos etc.)¹.

O 25 de maio de 2018 entrou en vigor o Regulamento xeral de protección de datos (RXP)² que se aplica en todos os ámbitos excepto no penal, onde rexe a regulación especial da Directiva (UE) 2016/680 que debía incorporarse ás lexislacións nacionais e entrar en vigor o 6 de maio de 2018³.

¹ Comité de Ministros do Consello de Europa (2015). [*Recommendation CM/Rec \(2015\) 5 on the processing of personal data in the context of employment*](#), 1 de abril de 2015, at the 1224th meeting of the Ministers' Deputies), Estrasburgo.

² Regulamento (UE) 2016/679 do Parlamento Europeo e do Consello, do 27 de abril de 2016, relativo á protección das persoas físicas no que respecta ao tratamento de datos persoais e á libre circulación destes datos e polo que se derroga a Directiva 95/46/CE (Regulamento xeral de protección de datos) (DOUE nº L 119, 4.5.2016, p. 1).

³ Directiva (UE) 2016/680 do Parlamento Europeo e do Consello, do 27 de abril de 2016, relativa á protección das persoas físicas no que respecta ao tratamento de datos persoais por parte das autoridades competentes para fins de prevención, investigación, detección ou axuízamento de infraccións penais ou de execución de sancións penais, e á libre circulación dos devanditos datos e pola que se derroga a Decisión Marco 2008/977/JAI do Consello (DOUE nº L 119, 4.5.2016, p. 89).

En España e ata o de agora a única medida lexislativa que completa o RGPD é a Lei española de protección de datos persoais e garantía dos dereitos dixitais, en vigor dende o 7 de decembro de 2018⁴. En cambio, a Directiva de protección de datos no ámbito penal segue pendente de transposición en España⁵.

En canto se refire á protección da vida privada e os datos persoais dos traballadores, haberá que estar ao marco normativo establecido polo RGPD que, con todo, confía nunha colaboración dos lexisladores nacionais, mediante leis e outras normas, e dos interlocutores sociais, a través de regulacións convencionais.

2.1. A REGULACIÓN EUROPEA E A SÚA APLICACIÓN NO ÁMBITO LABORAL A PARTIR DE 2018

O RXPd refírese expresamente á regulación normativa ou convencional do tratamento dos datos persoais dos traballadores no ámbito a laboral e ofrece unha enumeración de ámbitos afectados que reproduce cumpridamente tanto nos seus considerandos como na parte dispositiva.

Así, no seu considerando 155 o RXPd fai referencia aos ámbitos nos que poden operar as normas e os convenios

⁴ Lei orgánica 3/2018, do 5 de decembro, de protección de datos persoais e garantía dos dereitos dixitais (LOPD 2018) (BOE núm. 294, do 06/12/2018).

⁵ O 25 de xullo de 2019 a Comisión Europea iniciou un procedemento por incumprimento contra España e pediu ao Tribunal de Xustiza da Unión Europea «que impoña sancións financeiras en forma dunha suma a tanto alzado de 21.321 euros ao día entre o día posterior ao vencemento da data límite do prazo de transposición que se establece na Directiva e a data de cumprimento por parte de España, ou ben a data de pronunciamento da sentenza prevista no artigo 260, apartado 3, do TFUE, cun importe mínimo a tanto alzado de 5.290.000 euros e unha multa diaria de 89.548,20 euros dende o día da primeira sentenza ata alcanzar o pleno cumprimento ou ata a segunda sentenza do Tribunal» (véxase o comunicado de prensa en IP/19/4261). O recurso por incumprimento foi interposto ante o Tribunal de Xustiza o 4 de setembro de 2019, Comisión Europea / España, C-658/19.

colectivos, a saber, «en relación coas condicións nas que os datos persoais no contexto laboral poden ser obxecto de tratamento sobre a base do consentimento do traballador, os fins da contratación, a execución do contrato laboral, incluído o cumprimento das obrigas establecidas pola lei ou por convenio colectivo, a xestión, planificación e organización do traballo, a igualdade e seguridade no lugar de traballo, a saúde e seguridade no traballo, así como aos fins do exercicio e goce, sexa individual ou colectivo, de dereitos e prestacións relacionados co emprego e a efectos da rescisión da relación laboral».

O artigo 88 RXPd refírese ao tratamento no ámbito laboral e, en esencia, recoñece a facultade das autoridades nacionais para adoptar, mediante disposicións legislativas ou convenios colectivos, «normas máis específicas para garantir a protección dos dereitos e liberdades en relación co tratamento de datos persoais dos traballadores no ámbito laboral, en particular a efectos de contratación de persoal, execución do contrato laboral, incluído o cumprimento das obrigas establecidas pola lei ou polo convenio colectivo, xestión, planificación e organización do traballo, igualdade e diversidade no lugar de traballo, saúde e seguridade no traballo, protección dos bens de empregados ou clientes, así como a efectos do exercicio e gozo, individual ou colectivo, dos dereitos e prestacións relacionados co emprego e a efectos da extinción da relación laboral».

O artigo 88.2 RXPd refírese aos límites que se impoñen a tales regulacións do modo seguinte:

As ditas normas incluírán medidas adecuadas e específicas para preservar a dignidade humana dos interesados así como os seus intereses lexítimos e os seus dereitos fundamentais, prestando especial atención á transparencia do tratamento, á transferencia dos datos persoais dentro dun grupo empresarial ou dunha unión de empresas dedicadas a unha actividade económica conxunta e aos sistemas de supervisión no lugar de traballo.

O artigo 9.2.h) RXPd consagra unha excepción á prohibición do tratamento de datos persoais relativos á saúde cando:

O tratamento é necesario para fins de medicina preventiva ou laboral, avaliación da capacidade laboral do traballador, diagnóstico médico, prestación de asistencia ou tratamento de tipo sanitario ou social, ou xestión dos sistemas e servizos de asistencia sanitaria e social, sobre a base do Dereito da Unión ou dos Estados membros ou en virtude dun contrato cun profesional sanitario e sen prexuízo das condicións e garantías contempladas no apartado 3;

No artigo 9.3 RXDP permítese este tratamento cando sexa realizado por un profesional suxeito á obriga de secreto profesional, ou baixo a súa responsabilidade, de acordo co Dereito da Unión ou dos Estados membros ou coas normas establecidas polos organismos nacionais competentes.

A Comisión Europea impulsou, primeiro a través do Grupo de Traballo sobre protección de datos do artigo 29 e agora a través da Comité Europeo de Datos Persoais, o exame da dimensión laboral da privacidade e da protección de datos persoais.

No Ditame 2/2017 sobre o tratamento de datos no traballo, do 8 de xuño de 2017, o Grupo do artigo 29 «volve a avaliar o equilibrio entre os intereses lexítimos dos empresarios e as expectativas razoables de privacidade dos traballadores, describindo os riscos que ocasionan as novas tecnoloxías e avaliando a proporcionalidade dunha serie de escenarios nos que poderían aplicarse»⁶.

Para ese efecto, o Ditame 2/2017 realiza un exame dos escenarios onde estarían en xogo os dereitos dos traballadores, en particular, o tratamento de datos persoais durante o proceso de selección (consulta de perfís dispoñibles da internet), os derivados do exame no emprego, a vixilancia do uso das novas tecnoloxías da información no lugar de traballo e fóra del, o emprego do tempo e a presenza no traballo, a videovixilancia, o control

⁶ Neste ditame faise referencia a *Ditame 8/2001 sobre o tratamento de datos persoais no contexto laboral*, WP48, 13 de setembro de 2001, e ao *Documento de traballo relativo á vixilancia das comunicacións electrónicas no lugar de traballo*, WP55, 29 de maio de 2002.

de vehículos da empresa utilizados polo traballador (a través do GPS, de vídeos etc.), a comunicación dos datos dos traballadores a terceiros (por exemplo, facilitando a foto do repartidor aos clientes) ou as transferencias internacionais destes datos.

Neste Ditame 2/2017 do Grupo do artigo 29 subliñase reiteradamente a escasa operatividade do consentimento de traballador para que o seu empregador utilice os seus datos porque: «Os traballadores case nunca están en condicións de dar, denegar ou revogar o consentimento libremente, tendo en conta a dependencia que resulta da relación empresario/traballador. Dado o desequilibrio de poder, os traballadores só poden dar o seu libre consentimento en circunstancias excepcionais, cando a aceptación ou o rexeitamento dunha oferta non ten consecuencias» (apartado 6.2).

En definitiva, dende a perspectiva europea apuntáronse os problemas máis específicos da protección da privacidade e dos datos persoais dos traballadores, á vez que se encomenda aos lexisladores nacionais e aos interlocutores sociais a súa regulación específica.

2.2. A REGULACIÓN ESPAÑOLA APLICABLE EN MATERIA LABORAL

A Constitución española de 1978 adiviñou a importancia das novas tecnoloxías pero só deixou apuntada a necesidade de regular tal cuestión: «A lei limitará o uso da informática para garantir a honra e a intimidade persoal e familiar dos cidadáns e o pleno exercicio dos seus dereitos».

O ordenamento constitucional español contén unha versión limitada ou embrionaria do dereito á protección de datos persoais ao referirse ao dereito á intimidade persoal e familiar nestes termos: «Garántese o dereito á honra, á intimidade persoal e familiar e á propia imaxe». En 1978 era difícil aventurar a deriva que tería o vertixinoso desenvolvemento tecnolóxico e os seus efectos na vida privada dos cidadáns.

En todo caso, a lexislación española foi a remolque da harmonización lexislativa europea a partir da Directiva

95/46/CE e, dende logo, a partir da unificación lexislativa levada a cabo a partir de 2018 polo RXPd.

Nestes momentos a Lei española de protección de datos persoais e garantía dos dereitos dixitais (2018) consagrou unha serie de dereitos de gran interese no ámbito laboral referidos ao uso de dispositivos dixitais, o dereito á desconexión dixital, o uso de dispositivos de videovixilancia e de gravación de sons no lugar de traballo ou os sistemas de xeolocalización.

Os dereitos consagrados aplícanse a todo tipo de traballadores e empregados públicos. De feito, a Lei de 2018 modifica simultaneamente o Estatuto dos traballadores e o Estatuto básico do empregado público coa mesma finalidade.

A propia Lei de 2018 modifica o Estatuto dos traballadores, engadindo un artigo 20bis, co fin de introducir unha regulación específica dos dereitos dos traballadores á intimidade en relación co ámbito dixital e á desconexión.

Tamén a Lei de 2018 modifica o Estatuto básico do empregado público co fin de consagrar, no artigo 14.jbis), o dereito «á intimidade no uso de dispositivos dixitais postos á súa disposición e fronte ao uso de dispositivos de videovixilancia e xeolocalización, así como á desconexión dixital nos termos establecidos na lexislación vixente en materia de protección de datos persoais e garantía dos dereitos dixitais».

En primeiro lugar e polo que se refire ao uso de dispositivos dixitais, o artigo 87 recoñece o dereito á protección da intimidade fronte a eles e ao empregador. Con todo, prevé o acceso do empregador «aos contidos derivados do uso de medios dixitais facilitados aos traballadores co único propósito de controlar o cumprimento das obrigas laborais ou estatutarias e de garantir a integridade dos devanditos dispositivos».

Este acceso esixe dos empregadores que establezan «criterios de utilización dos dispositivos dixitais respectando en todo caso os estándares mínimos de protección da súa intimidade de acordo cos usos sociais e os dereitos recoñecidos constitucional e legalmente. Na súa elaboración deberán participar os representantes dos traballadores».

Tamén se prevé a necesidade de especificar os usos autorizados e esixe que se establezan garantías para preservar a intimidade dos traballadores, tales como, no seu caso, a determinación dos períodos en que os dispositivos poderán utilizarse para fins privados. Así mesmo, a Lei española dispón: «os traballadores deberán ser informados dos criterios de utilización».

O artigo 88 proclama o dereito á desconexión dixital no ámbito laboral co fin de «garantir, fóra do tempo de traballo legal ou convencionalmente establecido, o respecto do seu tempo de descanso, permisos e vacacións, así como da súa intimidade persoal e familiar».

O alcance deste dereito depende de «a natureza e obxecto da relación laboral» e con el preténdese potenciar «o dereito á conciliación da actividade laboral e a vida persoal e familiar e suxeitaranse ao establecido na negociación colectiva ou, na súa falta, ao acordado entre a empresa e os representantes dos traballadores».

O procedemento de regulación corresponde ao empregador quen, previa audiencia dos representantes dos traballadores, elaborará unha política interna dirixida a traballadores, incluídos os que ocupen postos directivos, na que definirán as modalidades de exercicio do dereito á desconexión e as accións de formación e de sensibilización do persoal sobre un uso razoable das ferramentas tecnolóxicas que evite o risco de fatiga informática. En particular, preservárase o dereito á desconexión dixital nos supostos de realización total ou parcial do traballo a distancia así como no domicilio do empregado vinculado ao uso con fins laborais de ferramentas tecnolóxicas.

O artigo 89 da Lei española pretende unha regulación do uso de dispositivos de videovixilancia e de gravación de sons no lugar de traballo.

Por unha banda, permite aos empregadores «tratar as imaxes obtidas a través de sistemas de cámaras ou videocámaras para o exercicio das funcións de control dos traballadores ou os empregados públicos previstas, respectivamente, no artigo 20.3 do Estatuto dos traballadores e na lexislación de función pública, sempre que estas funcións se exerzan dentro do seu marco legal e

cos límites inherentes a este. Os empregadores haberán de informar con carácter previo, e de forma expresa, clara e concisa, aos traballadores ou os empregados públicos e, no seu caso, aos seus representantes, acerca desta medida».

Por outra banda, a Lei española resolve un caso especial que enuncia nestes termos: «No caso de que se captase a comisión flagrante dun acto ilícito polos traballadores ou os empregados públicos entenderase cumprido o deber de informar cando existise polo menos o dispositivo ao que se refire o artigo 22.4 desta lei orgánica». A efectividade de tales probas esixe que, polo menos, se colocase un dispositivo informativo en lugar suficientemente visible que identifique a existencia do tratamento, a identidade do responsable e a posibilidade de exercer os dereitos, podendo facelo mediante un código de conexión ou dirección da internet a esta información.

Agora ben, a Lei española establece un límite absoluto á «instalación de sistemas de gravación de sons [ou] de videovixilancia»: cando se trate de «lugares destinados ao descanso ou espaxeamento dos traballadores ou os empregados públicos, tales como vestiarios, aseos, comedores e análogos».

Tamén se establecen garantías adicionais de modo que «a utilización de sistemas similares aos referidos nos apartados anteriores para a gravación de sons no lugar de traballo admitirase unicamente cando resulten relevantes os riscos para a seguridade das instalacións, bens e persoas derivados da actividade que se desenvolva no centro de traballo e sempre respectando o principio de proporcionalidade, o de intervención mínima e as garantías previstas nos apartados anteriores. A supresión dos sons conservados por estes sistemas de gravación realizarase atendendo ao disposto no apartado 3 do artigo 22 desta lei».

Por último, o artigo 90 refírese á utilización de sistemas de xeolocalización no ámbito laboral que poden instalar os empregadores baixo certas condicións.

Por unha banda, o tratamento dos datos obtidos a través de sistemas de xeolocalización para o exercicio das funcións de control dos traballadores ou empregados públicos previstas,

respectivamente, no artigo 20.3 do Estatuto dos traballadores e na lexislación de función pública, debe realizarse sempre dentro do seu marco legal e cos límites inherentes.

Por outra banda, requírese a información previa por parte dos empregadores de forma expresa, clara e inequívoca aos traballadores ou os empregados públicos e, no seu caso, os seus representantes, acerca da existencia e características destes dispositivos. Igualmente deberán informalos acerca do posible exercicio dos dereitos de acceso, rectificación, limitación do tratamento e supresión.

O artigo 91 deixa un ámbito de regulación á negociación colectiva de modo que «os convenios colectivos poderán establecer garantías adicionais dos dereitos e liberdades relacionados co tratamento dos datos persoais dos traballadores e a salvagarda de dereitos dixitais no ámbito laboral».

3. A XURISPRUDENCIA EUROPEA SOBRE A PROTECCIÓN DA VIDA PRIVADA E OS DATOS PERSOAIS DOS TRABALLADORES NO MARCO TECNOLÓXICO ACTUAL

O desenvolvemento vertixinoso das novas tecnoloxías permite rastrexar nos últimos anos unha evolución da xurisprudencia europea e da xurisprudencia dos tribunais españois en materia de privacidade e datos persoais dos traballadores en xeral e dos empregados públicos en particular. De feito, compróbanse as titubeantes respostas dos tribunais nos distintos niveis, europeo e nacional, e a atención do lexislador para resolvelos con opcións lexislativas claras.

O exame debe ter en conta os desenvolvementos en Estrasburgo a cargo do Tribunal Europeo de Dereitos Humanos, en Luxemburgo por obra do Tribunal de Xustiza da Unión Europea e nos tribunais españois.

3.1. A XURISPRUDENCIA DO TRIBUNAL EUROPEO DE DEREITOS HUMANOS

O Tribunal Europeo de Estrasburgo elaborou unha xurisprudencia sólida en materia de protección da

privacidade e dos datos persoais que é aplicable no ámbito laboral.

Recentemente adoptáronse dúas sentenzas de particular transcendencia: *sentenza Bărbulescu c. Romanía* (2017)⁷ e *sentenza López Ribalda e outros c. España* (2019)⁸. Nestes dous casos móstrase a división existente no propio Tribunal de Estrasburgo que, primeiro, nunha Sala, considera que houbo violación de dereitos fundamentais ou que non a houbo, mentres que, a continuación, a Gran Sala chega á interpretación contraria.

Na *sentenza Bărbulescu c. Romanía* a Gran Sala corrixe en 2017 a sentenza de 2016 da Sala. Na primeira sentenza dise que non houbo violación do artigo 8 por seis votos a un; en cambio, a Gran Sala considerou que houbo violación do dereito á vida privada por 11 votos fronte a 6. Sumando os votos de ambas as instancias pódese comprobar que, en teoría, habería empate entre os xuíces que participaron na deliberación de ambas as sentenzas.

Os feitos refírense ao despedimento dun enxeñeiro dunha empresa romanesa polo uso de Yahoo Messenger durante o traballo para o intercambio de mensaxes que mantivera coa súa noiva e co seu irmán.

A Sala apoiouse, fundamentalmente, na comisión dunha falta disciplinaria do traballador ao utilizar Yahoo Messenger para usos privados.

A Gran Sala matiza, en cambio, a súa resposta para chegar á conclusión de que houbo violación do artigo 8 CEDH. O seu punto de partida é a existencia dun contrato de traballo, a falta de consenso nas lexislacións nacionais para resolver esta cuestión e a rápida evolución neste ámbito.

⁷ TEDH (Gran Sala), sentenza do 5 de setembro de 2017, *Bărbulescu c. Romanía*, procedemento nº 61496/08 (despedimento do empregado polo uso dun servizo de mensaxería en liña da empresa). A Sala pronunciouse neste asunto en virtude da sentenza do 12 de xaneiro de 2016.

⁸ TEDH (Gran Sala), sentenza do 17 de outubro de 2019, *López Ribalda e outros c. España*, procedementos nº 1874/13 e 8567/13 (videovixilancia de empregados sen ser advertidos). A Sala pronunciouse na primeira sentenza o 9 de xaneiro de 2018.

O contrato de traballo determina que se manteña, por unha banda, o dereito do traballador ao respecto da súa vida privada; pero, a xuízo do Tribunal Europeo, ha de terse en conta o dereito de control, incluídas as prerrogativas disciplinarias, que exerce o empregador para asegurar o bo funcionamento da empresa (§ 124).

Neste sentido, conclúe o Tribunal Europeo: «as instrucións dun empregador non poden reducir á nada o exercicio da vida privada social no lugar de traballo. O respecto da vida privada e da confidencialidade das comunicacións continúa esixíndose, mesmo se estas últimas poden limitarse na medida que sexa necesario» (§ 80).

A tal fin, o Tribunal Europeo procedeu a unha sistematización dos criterios que debía ter en conta para axuizar estes casos nos seguintes termos:

- 1) O empregado debe ser informado claramente e con carácter previo á súa instalación da posibilidade de que o empregador adopte medidas de vixilancia da súa correspondencia e as súas comunicacións.
- 2) É importante a amplitude da vixilancia do empregador e o grao de inxerencia na vida privada do empregado, debendo distinguirse entre o fluxo de comunicación e o seu contido.
- 3) Corresponde ao empregador a xustificación dos motivos lexítimos do uso da vixilancia e do seu alcance e dos seus límites.
- 4) Debe analizarse a posibilidade de alcanzar o fin lexítimo a través de medios e de medidas menos invasivas para o contido das comunicacións do traballador.
- 5) Deben terse en conta as consecuencias da vixilancia para o empregado, podendo controlarse a súa proporcionalidade, é dicir, a utilización que, para o fin pretendido, faga o empregador de tales datos.
- 6) O empregador debe ofrecer ao traballador garantías adecuadas especialmente se as medidas son invasivas (§ 121).

No exame do caso concreto a Gran Sala subliña os defectos que observa no axuizamento dos tribunais romaneses, a saber e por unha banda, non verificaron se o traballador

fora advertido con carácter previo da posibilidade de vixiar as súas comunicacións de Yahoo Messenger; e, por outra, o traballador non fora informado da natureza nin do alcance da vixilancia. Ademais, os tribunais romaneses tampouco determinaron as razóns que xustificaban a aplicación de medidas de control, nin se o empregador podería utilizar medidas menos invasivas para a vida privada e a súa correspondencia, nin, en fin, se o acceso ao contido das comunicacións fose posible sen o seu coñecemento (§ 140). Agora ben, a Gran Sala non concede indemnización ningunha ao traballador senón que, simplemente, considera que a constatación da violación supón unha satisfacción suficiente do dano moral que se lle causara.

No *asunto López Ribalda* expúñase a cuestión da vulneración dos dereitos das empregadas dun supermercado videovixiado sen que fosen advertidas do alcance do control, dado que algunhas das cámaras estaban ocultas. O propio Tribunal Europeo refírese a un antecedente propio, a *decisión Köpke* (2010) referida a un suposto similar en Alemaña⁹.

Ante os tribunais españois, cinco caixeiros dun supermercado de Mercadona en Granollers (Barcelona) foron despedidas por comprobarse, despois de que a empresa colocase videocámaras, algunhas visibles pero outras ocultas; estas últimas enfocaban as caixas sen que se advertise as traballadoras, que escaneaban os produtos e logo cancelaban as compras de clientes, compañeiros e as súas propias ou deixaban saír cos produtos sen pagar. As traballadoras despedidas recoñeceron os feitos pero alegaron a vulneración do seu dereito á intimidade no traballo.

⁹ TEDH, decisión do 5 de outubro de 2010, *Karin Köpke c. Alemaña*, recurso nº 420/07 (cámara oculta nun supermercado para detectar se se produciron furtos). Neste caso acordouse a inadmisibilidade do recurso e considerouse, en esencia, que os tribunais alemáns ponderaran o dereito de propiedade do empregador, que non tiña outro medio efectivo de protexerse contra os furtos no establecemento da súa propiedade, en relación co dereito da empregada a que se respectase a súa vida privada.

O Xulgado do Social de Granollers e a Sala do social do Tribunal Superior de Xustiza de Cataluña desestimaron as demandas fronte aos despedimentos; a Sala do social do Tribunal Supremo e o Tribunal Constitucional inadmitiron a casación e o recurso de amparo.

En cambio, a primeira sentenza de 2018 do Tribunal Europeo condenou a España baseándose no axuizamento realizado polos xuíces españois; con todo, en 2019 a sentenza da Sala cambia de criterio e desestima o recurso.

En ambas as sentenzas, o Tribunal Europeo lembra a súa xurisprudencia sobre o dereito á vida privada conforme á cal «a expectativa razoable dunha persoa respecto a súa intimidade é un factor revelador pero non necesariamente concluínte».

Así mesmo, no caso concreto, o Tribunal de Estrasburgo subliña que «a videovixilancia encuberta dun empregado no seu lugar de traballo debe considerarse, en si mesma, como unha importante intromisión na súa vida privada».

En fin, o Tribunal Europeo comproba que a lexislación española xa obrigaba a informar os clientes e os traballadores sobre o uso da videovixilancia encuberta por un tempo prolongado. Con todo, a xuízo do Tribunal Europeo a utilización no procedemento xudicial do material gravado en segredo non se opón ás esixencias de equidade garantidas polo artigo 6.1 do Convenio.

Agora ben, na sentenza de 2018 o Tribunal Europeo reprocha aos tribunais españois non alcanzar un equilibrio equitativo entre o dereito das traballadoras ao respecto da súa vida privada consonte o artigo 8 do Convenio e o interese do seu empregador na protección dos seus dereitos patrimoniais. Desta solución discrepou o xuíz Dedov ao considerar que «o fallo da maioría contradí o principio xeral do dereito: non se debe permitir que os demandantes se beneficien legalmente dos seus propios actos ilícitos». O Tribunal de Estrasburgo concede a cada unha das cinco empregadas unha indemnización por danos morais de 4.000 euros. Con todo, dous dos sete xuíces europeos consideraron que a propia sentenza sería satisfacción bastante.

En cambio, a sentenza de 2019 da Gran Sala chega á conclusión contraria, por 14 votos a 3, de modo que decide que España non vulneraría o artigo 8 do Convenio.

O Tribunal Europeo baséase expresamente na *decisión Köpke* e na *sentenza Bărbulescu* e, seguindo as mesmas indicacións, volve repetir os elementos que deben determinar a proporcionalidade das medidas de videovixilancia:

- 1) O empregado debe ser informado claramente e con carácter previo á súa instalación da posibilidade de que o empregador adopte medidas de videovixilancia.
- 2) Resulta importante ter en conta a amplitude da videovixilancia do empregador e o grao de inxerencia na vida privada do empregado: lugares máis ou menos privados, límites espaciais e temporais, e número de persoas que teñen acceso aos datos.
- 3) É necesaria a xustificación polo empregador dos motivos lexítimos do uso da videovixilancia e do seu alcance, de tal modo que canto máis invasiva sexa a videovixilancia, máis esixente debe ser a súa xustificación.
- 4) Debe considerarse a posibilidade de alcanzar o fin lexítimo a través de medios e de medidas menos invasivas na vida privada do asalariado.
- 5) Deberan terse en conta as consecuencias da videovixilancia para o empregado podendo controlar a utilización que faga o empregador de tales datos en función da finalidade perseguida.
- 6) O empregador debe ofrecer ao empregado as garantías adecuadas, directamente, a través dos seus representantes, baixo o control dun organismo independente ou se hai posibilidade de presentar reclamacións, especialmente cando as medidas son invasivas (§ 116).

Finalmente, a Gran Sala do Tribunal Europeo chega á conclusión de que non houbo violación do artigo 8 do Convenio, debido ás garantías que ofrecía a normativa española, tendo en conta o axuizamento detallado feito polo Xulgado de Granollers e pola Sala do social de Barcelona, do

que se deducía a xustificación e proporcionalidade das medidas de videovixilancia e, en fin, en atención ás vías de recurso ante a Axencia Española de Protección de Datos e ante outros tribunais que, con todo, as empregadas non utilizaron (§ 137).

En cambio, o voto disidente que pretendía constatar a violación do artigo 8 reprochaba á lexislación española que non previse máis que unha única garantía específica ao réxime de videovixilancia, a obriga de advertir os empregados con carácter previo da instalación e utilización da vixilancia, sen que se establecese ningunha outra excepción (§ 4); o que non se produciría no caso das cámaras ocultas e, en consecuencia, determinaría, di o voto discrepante, a vulneración por España do dereito fundamental á privacidade dos traballadores.

En suma, pode observarse que a xurisprudencia de Estrasburgo é oscilante e non termina por decantarse por unha solución única. Con todo, os elementos fundamentais da xurisprudencia están xa deseñados.

3.2. A XURISPRUDENCIA DO TRIBUNAL DE XUSTIZA DA UNIÓN EUROPEA

A Unión Europea respondeu lexislativamente dunha maneira apropiada fronte aos desafíos das novas tecnoloxías na vida privada e na protección de datos persoais. Agora ben, no caso dos traballadores, a xurisprudencia de Luxemburgo non é, ata o de agora, particularmente significativa. Con todo, ofrece algúns elementos que merecen destacarse.

Na *sentenza Österreichischer Rundfunk e outros* (2003) o Tribunal de Xustiza aborda a cuestión da conformidade co dereito á protección de datos do control que corresponde ao Tribunal de Contas e outros organismos públicos sobre os ingresos de determinados empregados da televisión pública austríaca e outros entes territoriais e empresas públicas¹⁰.

¹⁰ TXCE, sentenza do 20 de maio de 2003, *Österreichischer Rundfunk e outros*, C-465/00, C-138/01 e C-139/01, EU:C:2003:294 (divulgación de datos sobre os ingresos de empregados de entidades suxeitas ao control financeiro externo).

O Tribunal de Xustiza considera que cabe unha ampla divulgación do importe dos ingresos anuais e, cando estes superan un límite determinado, do nome das persoas empregadas polas entidades suxeitas ao control do Tribunal de Contas, se é necesaria e apropiada para lograr o obxectivo de boa xestión dos recursos públicos.

A *sentenza Worten* (2013) pronúnciase sobre as cuestións do rexistro do tempo de traballo, coa indicación das horas en que cada traballador inicia e finaliza a xornada e as pausas de descanso, e considera que está comprendido no concepto de «datos persoais», aplicándose a lexislación europea para o efecto, naquel entón a Directiva 95/46/CE¹¹. A cuestión prejudicial exposta por un tribunal de traballo portugués pretendía saber se era conforme co Dereito da Unión europea a imposición dunha multa a unha empresa que non permitira que a Inspección laboral procedese á consulta inmediata do rexistro do tempo de traballo dos traballadores dun establecemento da empresa Worten.

A pesar das garantías en materia de protección de datos, a lexislación europea non impide que se aplique a Directiva 2003/88/CE, relativa a determinados aspectos da ordenación do tempo de traballo. A efectividade desta Directiva pode establecer a obriga do empregador de proporcionar a unha autoridade de control laboral o acceso inmediato ao rexistro do tempo de traballo, dado que esta obriga pode resultar necesaria se contribúe a unha aplicación máis eficaz da normativa en materia de condicións de traballo.

Este enfoque foi confirmado pola *sentenza Federación de Servizos de Comisións Obreiras (CCOO) / Deutsche Bank* (2019), na medida en que o Tribunal de Xustiza considera necesario garantir o efecto útil dos dereitos recollidos na Directiva 2003/88 e no artigo 31.2 da Carta de todo traballador á limitación da duración máxima do traballo e a períodos de descanso diarios e semanais, así como a un

¹¹ TXCE, sentenza do 30 de maio de 2013, Worten — Equipamentos para o Lar, SA / Autoridade para as Condições de Trabalho (ACT), C-342/12, EU:C:2013:355 (acceso da inspección de Traballo para a supervisión das condicións de traballo).

período de vacacións anuais retribuídas, de tal modo que as autoridades nacionais están obrigadas a «impoñer aos empresarios a obriga de implantar un sistema obxectivo, fiable e accesible que permita computar a xornada laboral diaria realizada por cada traballador»¹².

A *sentenza Nowak* (2017) aplica a Directiva 95/46 a un exame profesional feito no Colexio de censores xurados de contas de Irlanda¹³. A xuízo do Tribunal de Xustiza, «as respostas por escrito dadas por un aspirante nun exame profesional e as eventuais anotacións do examinador referentes a esas respostas son datos persoais» (apartado 62).

Con todo, o Tribunal de Xustiza considera que, transcorrido un prazo determinado, pode haber interese en que tales exames se destrúan tendo presentes os dereitos de terceiros. En efecto, o Tribunal de Xustiza subliña expresamente que un aspirante tería dereito a solicitar ao responsable do tratamento de datos que, transcorrido un determinado período de tempo, se supriman as súas respostas ao exame e as correspondentes anotacións do examinador, é dicir, que se destrúan. Ao que engade o Tribunal de Xustiza: «tendo en conta a finalidade das respostas do aspirante nun exame e das correspondentes anotacións do examinador, a súa conservación nunha forma que permita a identificación do aspirante xa non parece necesaria *a priori*, unha vez que o procedemento de exame está definitivamente concluído e non pode ser obxecto de recurso, de tal modo que tales respostas e anotacións perderon calquera valor probatorio» (apartado 55).

E de maneira moi clara o Tribunal de Xustiza insiste nas limitacións que tanto a Directiva 95/46 como o

¹² TXUE (Gran Sala), sentenza do 14 de maio de 2019, Federación de Servizos de Comisións Obreiras (CCOO) / Deutsche Bank, SAE, C-55/18, EU:C:2019:402 (sistema de rexistro da xornada laboral diaria realizada polos seus traballadores).

¹³ TXUE, sentenza do 20 de decembro de 2017, Nowak, C-434/16, EU:C:2017:994 (anotacións nun exame profesional como datos persoais).

Regulamento 2016/679, que substituíu á dita Directiva, establecen a eses dereitos (apartado 59).

Os desenvolvementos noutros ámbitos do dereito á protección de datos persoais e o uso da internet¹⁴ ou a protección de datos biométricos¹⁵ poden clarificar o ámbito propiamente das relacións entre empregadores e traballadores.

3.3. A XURISPRUDENCIA DOS TRIBUNAIS ESPAÑÓIS

En España as cuestións relativas aos dereitos de privacidade e de protección de datos dos traballadores resólvense tanto na xurisdición social, cando coñece dos litixios entre traballadores e empresarios, como na xurisdición contencioso-administrativa cando quedan afectados os empregados públicos (o acceso de todos ao emprego público, incluído o persoal laboral, e as vicisitudes laborais dos funcionarios e do persoal estatutario).

Todo parece indicar unha converxencia nas solucións da xurisdición social e da xurisdición contencioso-administrativa producida non só pola xurisprudencia europea antes referida senón tamén pola xurisprudencia constitucional. De feito, o Tribunal Constitucional, intérprete supremo da Constitución e que protexe de maneira especial determinados dereitos fundamentais por vía de amparo, en particular tal como resultan do artigo 18 da Constitución, actúa como punto de referencia das xurisdicións implicadas.

¹⁴ TXUE (Gran Sala), sentenza do 24 de setembro de 2019, Google / Comisión Nacional de Informática e Liberdades de Francia, C-507/17, EU:C:2019:772 (alcance territorial do dereito ao esquecemento na internet); TXUE (Gran Sala), sentenza do 1 de outubro de 2019, Planet49, C-673/17, EU:C:2019:801 (consentimento sobre datos persoais na internet e *cookies*); TXUE, sentenza do 3 de outubro de 2019, Eva Glawischnig-Piesczek / Facebook Ireland Limited, C-18/18, EU:C:2019:821 (obrigas dunha rede social a bloquear ou a suprimir datos almacenados e declarados xudicialmente ilícitos).

¹⁵ TXUE, sentenza do 3 de outubro de 2019, Staatssecretaris van Justitie en Veiligheid / A e outros, C-70/18, EU:C:2019:823 (registro de datos biométricos de traballadores turcos).

Non é posible un exame exhaustivo da xurisprudencia dos tribunais españois, polo que se elixiron algunhas sentenzas que marcan a tendencia na xurisdición constitucional e na xurisdición ordinaria, social e contencioso-administrativa.

3.3.1 Tribunal Constitucional

O Tribunal Constitucional pronunciouse na sentenza 39/2016 nun recurso de amparo formulado por unha traballadora dunha tenda de moda Bershka, do Grupo Inditex en León, que fora despedida como consecuencia das imaxes captadas por unha cámara de videovixilancia instalada sen comunicación previa á traballadora, aínda que había aviso na tenda de instalación de cámaras, e das que se deducían que se apropiou de 189,92 euros da caixa¹⁶. Tanto o Xulgado como a Sala do social desestimaron a impugnación do despedimento disciplinario da traballadora. Sobre este particular, o Tribunal Constitucional refírese, en primeiro lugar, ao consentimento e sinala: «No ámbito laboral o consentimento do traballador pasa, por tanto, como regra xeral a un segundo plano, pois o consentimento enténdese implícito na relación negocial, sempre que o tratamento de datos de carácter persoal sexa necesario para o mantemento e o cumprimento do contrato asinado polas partes». Con todo, precisa: «o consentimento dos traballadores afectados si será necesario cando o tratamento de datos se utilice con finalidade allea ao cumprimento do contrato».

En segundo lugar, o Tribunal Constitucional pronúnciase sobre o deber de información que pesa sobre o empregador neste sentido: «O deber de información previa forma parte do contido esencial do dereito á protección de datos, pois resulta un complemento indispensable da necesidade de consentimento do afectado».

En terceiro lugar, o Tribunal Constitucional prevé excepcións aos dous supostos anteriores nestes termos: «o

¹⁶ TC (Pleno), sentenza 39/2016, do 3 de marzo, relator: Roca Trías (despedimento baseado nas imaxes captadas por unha cámara de videovixilancia instalada sen comunicación previa á traballadora de Bershka).

incumprimento do deber de requirir o consentimento do afectado para o tratamento de datos ou do deber de información previa só supoñerá unha vulneración do dereito fundamental á protección de datos tras unha ponderación da proporcionalidade da medida adoptada».

No caso concreto, o Tribunal Constitucional desestima o recurso de amparo por considerar que se respectou o principio de proporcionalidade nas súas tres dimensións (xuízo de necesidade, xuízo de idoneidade e proporcionalidade en sentido estrito), a saber:

A medida de instalación de cámaras de seguridade que controlaban a zona de caixa onde a demandante de amparo desempeñaba a súa actividade laboral era unha medida xustificada (xa que existían razoables sospeitas de que algún dos traballadores que prestaban servizos na devandita caixa estaba a apropiarse de diñeiro); idónea para a finalidade pretendida pola empresa (verificar se algúns dos traballadores cometía efectivamente as irregularidades sospeitadas e en tal caso adoptar as medidas disciplinarias correspondentes); necesaria (xa que a gravación serviría de proba de tales irregularidades); e equilibrada (pois a gravación de imaxes limitouse á zona da caixa), polo que debe descartarse que se producise lesión algunha do dereito á intimidade persoal consagrado no art. 18.1 CE (FJ 5).

A esta sentenza formuláronse dous votos particulares, asinados por tres dos once maxistrados do Tribunal Constitucional, nos que propoñen a solución contraria. Por unha banda, o voto subscrito polo maxistrado Valdés Dal-Ré, catedrático de Dereito do Traballo, considera: «o despedimento debeu cualificarse como nulo, por non cumprirse o deber de información que impón ao empresario o art. 18.4 CE» que renega enerxicamente por unha interpretación na que «nin os poderes ou facultades empresariais son, sen excepción e de maneira universal, expresións directas e indefectibles dos arts. 33 e 38 CE que caiba confrontar de maneira mecánica e sen maior fundamentación cos dereitos fundamentais dos

traballadores; nin, en fin, as facultades do empresario e, menos aínda se se exercen de modo irregular ou desviado, como máis adiante terei ocasión de razoar, poden restrinxir aqueles dereitos no ámbito das organizacións produtivas, incluídos, está claro, os formulados no art. 18 CE».

O outro voto particular, do maxistrado Xiol Ríos, adopta a mesma postura e insiste en que a información ao público non é suficiente senón que debe informarse os traballadores. Ademais, o seu voto revela o axustado da solución ao propoñer que se estimase o amparo pero se mantivesen as sentenzas previas dado que «tanto en primeira instancia como en suplicación se fai constar polos respectivos tribunais que existen outros elementos de proba independentes da videovixilancia suficientes para entender probados os feitos que deron lugar ao despedimento».

O sentido da sentenza responde, con toda probabilidade, á influencia da solución dada na primeira *sentenza Bărbulescu* (2016), que non apreciara a violación do dereito á vida privada. Aínda que debe lembrarse que á luz da segunda *sentenza Bărbulescu* (2017), ditada seis meses despois, a sentenza podería ser estimatoria. En cambio, á luz da primeira *sentenza López Ribalda* (2018), a solución do Tribunal Constitucional sería máis controvertida que dende a perspectiva da segunda *sentenza López Ribalda* (2018) en que a solución de Estrasburgo e de Madrid parecen sincronizarse.

Aínda cando non sexa no ámbito laboral, é importante ter en conta a sentenza 97/2019, onde o Tribunal Constitucional se refire ao uso de datos da denominada *lista Falciani*¹⁷ e confirma as sentenzas de instancia e de casación que condenaran por delito contra a Facenda pública na declaración do imposto da renda de 2005 e na de 2006 a un empresario domiciliado en Madrid¹⁸.

¹⁷ TC (Pleno), sentenza 97/2019, do 17 de xullo de 2019, relator: Montoya Melgar (uso de datos da *lista Falciani* para a persecución de delitos de defraudación tributaria).

¹⁸ TS (Sala 2ª), sentenza do 23 de febreiro de 2017, recurso nº 1281/2016, ES:TS:2017:471, relator: Marchena Gómez (delito fiscal e *lista Falciani*).

O Tribunal Constitucional denega o amparo porque «os datos que son utilizados pola Facenda Pública española se refiren a aspectos periféricos e inocuos da chamada “intimidade económica”. Non se introduciron dentro do proceso penal datos, como poderían ser os concretos movementos de contas, que poidan revelar ou que permitan deducir os comportamentos ou hábitos de vida do interesado [...] Os datos controvertidos son, exclusivamente, a existencia da conta bancaria e o importe ingresado nesta. O resultado da intromisión na intimidade non é, por tanto, de tal intensidade que esixa, por si mesmo, estender as necesidades de tutela do dereito substantivo ao ámbito do proceso penal, tendo en conta que, como xa se dixo, este non ten conexión instrumental ningunha co acto de inxerencia verificado entre particulares».

Estas dúas vías de aproximación, o carácter máis ou menos periférico e inocuo dos datos tidos en conta, así como a existencia dun ilícito previo, especialmente se é grave, determinan en gran medida as solucións que deben alcanzar os tribunais.

3.3.2 A xurisprudencia social e contencioso-administrativa do Tribunal Supremo

En primeiro lugar e polo que se refire á xurisdición social, a sentenza do 2 de febreiro de 2017, do Pleno da Sala Social acepta a lexitimidade de probas videográficas obtidas na entrada e espazos comúns dun ximnasio sen que o Tribunal Supremo esixa comunicar que o seu uso podería facer en procedementos disciplinarios¹⁹.

Un traballador fora despedido, entre outras razóns por coar a clientes sen entrada, pero tanto o Xulgado como a Sala do social de Barcelona declararan a improcedencia do despedimento polas probas de que se valeu o empregador.

¹⁹ TS (Sala 4ª, Pleno), sentenza do 2 de febreiro de 2017, recurso nº 554/2016, ES:TS:2017:817, relator: Calvo Ibarlucea (validez de probas videográficas na entrada e espazos públicos sen que se avisase aos traballadores do seu uso a efectos disciplinarios).

En cambio, o Tribunal Supremo aceptou as probas videográficas e considerou que «o uso da videocámara revestiu carácter razoable e proporcionado ao seu obxecto sen que polo lugar da súa instalación exista risco para a vulneración do dereito á honra á intimidade persoal e familiar nin polas circunstancias de tempo e oportunidade o haxa tampouco para o pleno exercicio dos seus dereitos ao actuar o demandante como o fixo sendo coñecedor de que a súa conduta estaba a ser gravada e de que polo que respecta ás cámaras da entrada o acceso indebido con auxilio interno xa fora obxecto de sanción».

O Tribunal Supremo acolle, na súa sentenza do 23 de febreiro de 2017 a *xurisprudencia Barbulescu* no ámbito social considerando que está en sintonía coa xurisprudencia constitucional²⁰. A cuestión expúñase respecto do rexeitamento de determinadas probas que xustificaran o despedimento dun traballador.

En suplicación, a Sala de Galicia refugara as probas ilicitamente obtidas a través do control do correo electrónico do traballador de Inditex, aínda que, á vista doutras probas, confirmou o despedimento.

En cambio, a Sala do social do Tribunal Supremo reforza o poder de control do empresario nun suposto no que «se non hai dereito a utilizar o computador para usos persoais, non haberá tampouco dereito para facelo nunhas condicións que impoñan un respecto á intimidade ou ao secreto das comunicacións, porque, ao non existir unha situación de tolerancia do uso persoal, tampouco existe xa unha expectativa razoable de intimidade e porque, se o uso persoal é ilícito, non pode esixirse ao empresario que o soporte e que ademais se absteña de controlalo». Para ese efecto, o Tribunal Supremo reproduce os mesmos argumentos do Tribunal Europeo e refírese resumidamente aos criterios establecidos en Estrasburgo e que xiran ao

²⁰ TS (Sala 4ª), sentenza do 8 de febreiro de 2018, recurso nº 1121/2015, ES:TS:2018:594, relator: De Castro Fernández (plena validez procesual da proba utilizada por Inditex e derivada do exame do correo electrónico existente en computador do traballador).

redor dos seguintes elementos: «a) o grao de intromisión do empresario; b) a concorrencia de lexítima razón empresarial xustificativa da monitoraxe; c) a inexistencia ou existencia de medios menos intrusivos para a consecución do mesmo obxectivo; d) o destino dado pola empresa ao resultado do control; e) a previsión de garantías para o traballador».

Polo que se refire á xurisprudencia contencioso-administrativa do Tribunal Supremo, non é moi abundante en relación coa protección da vida privada e dos datos persoais dos empregados públicos (funcionarios e persoal estatutario).

A sentenza do 2 de xullo de 2007 refírese á protección dos dereitos fundamentais de integridade física e datos persoais fronte á implantación dun sistema de control horario para empregados públicos en Cantabria mediante a lectura biométrica da man²¹.

O Tribunal Supremo considera que se trata de datos persoais cuxo rexistro está sometido á normativa aplicable na materia; con todo, ao seu xuízo «a finalidade perseguida mediante a súa utilización é plenamente lexítima: o control do cumprimento do horario de traballo ao que veñen obrigados os empregados públicos».

4. CONCLUSIÓN

A resposta aos desafíos que as novas tecnoloxías representan para a privacidade e a protección dos datos persoais dos traballadores baséase nunha decantación do dereito fundamental á vida privada e á protección dos datos persoais.

A Constitución española apenas puido adiviñar en 1978 os cambios que produciría a técnica. Con todo, foron a adopción da Carta dos dereitos fundamentais e o seu desenvolvemento lexislativo pola Unión Europea, especialmente a través do vixente Regulamento xeral de

²¹ TS (Sala C-A , Sección 7ª), sentenza do 2 de xullo de 2007, recurso nº 5017/2003, É:TS:2007:5200, relator: Lucas Murillo de la Cueva (control de horario mediante a captación da imaxe tridimensional da man en Cantabria).

protección de datos, os que estableceron un marco normativo apropiado que, con todo, está en constante desenvolvemento. Neste sentido será preciso confiar unha maior participación dos interlocutores sociais na adopción de normas convencionais que clarifiquen o alcance do poder de autoorganización dos empregadores e o ámbito íntimo irredutible dos traballadores.

A xurisprudencia europea, especialmente dende Estrasburgo, reflexionou sobre esta cuestión que, en realidade, se revela especialmente difícil como se deduce das sentenzas *Bărbulescu* e *López Ribalda*, con solucións contraditorias e debates especialmente controvertidos entre os mesmos xuíces do Tribunal Europeo.

Dende España a atención e o seguimento desta xurisprudencia europea foron especialmente intensos sen que, neste momento, se determinase unha solución unívoca. Con todo, parece que haberá unha converxencia entre as solucións adoptadas polos xuíces españois do laboral e do contencioso-administrativo por efecto da xurisprudencia europea e da xurisprudencia constitucional.

Agora ben, todo parece indicar que, aínda que o consentimento do traballador non é relevante neste ámbito, a maior ou menor información dos traballadores sobre o alcance do control do empresario xustificará determinadas invasións e limitacións na privacidade e na protección dos datos dos traballadores. Certamente, será necesario superar un enfoque exclusivamente procedemental para ter en conta os aspectos substantivos da vida privada dos traballadores. Neste sentido, a maior ou menor afectación da intimidade dos traballadores será un elemento decisivo para determinar a legalidade da actuación empresarial porque, como sinala o Tribunal Europeo de Dereitos Humanos: «as instrucións dun empregador non poden reducir a cero o exercicio da vida privada social no lugar de traballo»²².

²² TEDH (Gran Sala), sentenza do 5 de setembro de 2017, *Bărbulescu c. Romanía*, procedemento nº 61496/08, antes citada, § 80; a versión inglesa di literalmente: «an employer's instructions cannot reduce private social life in the workplace to zero»; a

5. BIBLIOGRAFÍA

- Comité de Ministros del Consejo de Europa (2015). [*Recommendation CM/Rec \(2015\) 5 on the processing of personal data in the context of employment*](#), 1 de abril de 2015, at the 1224th meeting of the Ministers' Deputies), Estrasburgo.
- Delgado Martín, J. (2019), "Reflexiones sobre la protección de datos personales en la Administración de Justicia", *Diario La Ley* Nº 9363, Madrid.
- González González, C. (2019). "Control empresarial de la actividad laboral mediante la videovigilancia y colisión con los derechos fundamentales del trabajador. Novedades de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales", *Revista Aranzadi Doctrinal* Nº. 4, Navarra.
- Grupo de Trabajo sobre Protección de Datos del Artículo 29 (2017). *Dictamen 2/2017 sobre el tratamiento de datos en el trabajo, de 8 de junio de 2017*, [Comisión Europea](#), WP 249, Bruselas.
- Jiménez Asensio, R. (2019). *Introducción al nuevo marco normativo de la protección de datos personales en el sector público*, Instituto Vasco de Administración Pública, Oñate.
- Mangan, D. (2019). "Beyond Procedural Protection: Information Technology, Privacy and the Workplace", *European Law Review*, August, pp. 559-571.
- Ordóñez Riaño, M. (2019). "Los derechos fundamentales de los trabajadores y el impacto de las nuevas tecnologías", *Diálogos Jurídicos 2019. Anuario de la Facultad de Derecho de la Universidad de Oviedo*, Universidad de Oviedo, Thomson Reuters Aranzadi, Navarra, pp. 217-232.
- Ordóñez Solís, D. (2014). *La protección judicial de los derechos en Internet en la jurisprudencia europea*, Editorial Reus, Madrid.

versión francesa reza así: «les instructions d'un employeur ne peuvent pas réduire à néant l'exercice de la vie privée sociale sur le lieu de travail».

- Pérez Miras, J. (2019). *El derecho a la protección de datos y a la privacidad: una perspectiva comparada entre la Unión Europea y Estados Unidos*, Tesis doctoral dirigida por Marycruz Arcos Vargas (dir. tes.). Universidad de Sevilla (2019).
- Rallo Lombarte, A. (2019). *Tratado de protección de datos. Actualizado con la Ley orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales*, Tirant lo Blanch, Valencia.
- Rodríguez Escanciano, S (2019). "Videovigilancia empresarial: límites a la luz de la Ley Orgánica 3/2018, de 5 diciembre, de protección de datos personales y garantía de los derechos digitales", *Diario La Ley* Nº 9328, Madrid.
- Rojas Rosco, R. y López Carballo, D. (2018). "El impacto del RGPD en el ámbito del control laboral y la era de la innovación", *Actualidad civil* Nº 5, 2018 (Ejemplar dedicado a: Protección de datos: entre el RGPD y la nueva LOPD), Madrid.