

AUTODETERMINACIÓN INFORMATIVA: UN DEREITO EN ALZA

CARMEN SÁNCHEZ TRIGUEROS

Catedrática de Dereito do Traballo e da Seguridade Social
Universidade de Murcia
carmenst@um.es

MARÍA ELISA CUADROS GARRIDO

Avogada. Profesora Asociada (acred. Axudante Doutora)
Universidade de Murcia
mariaelisa.cuadros@um.es

RESUMO

A protección de datos é un dereito fundamental que permaneceu larvado, pero a partir da STC 29/2013 emerxeu con forza, someténdose a diversos vaivéns xurisprudenciais que ao final viñeron a consagralo como un dereito máis potente que a propia intimidade ou o secreto das comunicacións, impoñendo os seus principios de actuación moito máis esixentes e formalistas que os que serviran ata agora para limitar outros dereitos fundamentais. A súa concepción está en pleno crecemento polo que non é posible pechar a súa delimitación, e iso xera problemas de interpretación e constante readaptación.

Palabras chave: Liberdade informática; dereitos dixitais; protección de datos.

RESUMEN

La protección de datos es un derecho fundamental que ha permanecido larvado, pero a partir de la STC 29/2013 ha emergido con fuerza, sometándose a diversos vaivenes jurisprudenciales que al final han venido a consagrarlo como un derecho más potente que la propia intimidad o el secreto de las comunicaciones, imponiendo sus principios de actuación mucho más exigentes y formalistas que lo que habían servido hasta ahora para limitar otros derechos fundamentales. Su concepción está en pleno crecimiento

por lo que no es posible cerrar su delimitación, y ello genera problemas de interpretación y constante readaptación.

Palabras clave: Libertad informática; derechos digitales; protección de datos.

ABSTRACT

Data protection is a fundamental right that has remained latent and since STC 29/2013 it has emerged with strength, submitting to various jurisprudential swings that in the end have come to consecrate it as a more powerful right than the privacy or secrecy of communications, imposing its principles of action much more demanding and formalist than what had served until now to limit other fundamental rights. It is not risky to affirm that its conception is in full growth so it is not possible to close its delimitation, and this generates problems of interpretation and continuous readjustment.

Keywords: Computer freedom; digital rights; Data Protection.

SUMARIO

1. DELIMITACIÓN.- 1.1. CONCEPTO.- 1.1.1. DELIMITACIÓN FRONTE AO DEREITO Á INTIMIDADE.- 1.1.2. DELIMITACIÓN FRONTE AO DEREITO AO SECREDO DAS COMUNICACIÓNS.- 1.2. UN DEREITO EN EVOLUCIÓN.- 2. O ART. 8 DO CONVENIO EUROPEO DE DEREITOS HUMANOS.- 2.1. OS CASOS HALFORD E COPLAND.- 2.2. O CASO BARBULESCU.- 2.3. O CASO LÓPEZ RIBALDA.- 3. O REGULAMENTO XERAL DE PROTECCIÓN DE DATOS.- 3.1. ÁMBITO DO RXPD.- 3.2. DEREITO AO ESQUECEMENTO. 3.3. DEREITO Á PORTABILIDADE DOS DATOS. 4. A LEI ORGÁNICA DE PROTECCIÓN DE DATOS E GARANTÍA DE DEREITOS DIXITAIS.- 4.1. IDEA XERAL.- 4.2. USOS E DISPOSITIVOS DIXITAIS NO ÁMBITO LABORAL.- 4.3. DEREITO Á DESCONEXIÓN DIXITAL NO ÁMBITO LABORAL.- 4.4. DISPOSITIVOS DE VIDEOVIXILANCIA E DE GRAVACIÓN DE SONS.- 5. EVOLUCIÓN DA XURISPRUDENCIA CONSTITUCIONAL.- 5.1. PRIMEIRA ETAPA.- 5.2. SEGUNDA ETAPA.- 5.3. TERCEIRA ETAPA.- 5.4. CUARTA

ETAPA.- 5.5. QUINTA ETAPA.- 5.6. SEXTA ETAPA.- 6.
REFLEXIÓN CONCLUSIVAS.- 7. BIBLIOGRAFÍA.

1. DELIMITACIÓN

1.1. CONCEPTO

O noso lexislador constitucional foi pioneiro ao recoñecer o dereito fundamental á protección de datos persoais, pero o seu alcance e interpretación no sistema español como dereito fundamental¹ é unha creación xurisprudencial², en boa medida obra do noso Tribunal Constitucional³.

O perfil do dereito analizado é marcadamente formalista, xa que garante á persoa o control activo das informacións que lle afectan, e o dereito a non ser instrumentalizado a través do coñecemento adquirido de aspectos da súa personalidade, na medida en que supón ser informado de quen posúe os seus datos persoais, a qué uso se están sometendo e o dereito a opoñerse, no seu caso, a unha posesión ilexítima ou uso ilícito; é a potestade de control sobre o uso dos datos propios.

O TC vén considerar este dereito⁴ como *unha facultade de control sobre os datos relativos á propia persoa*, engadindo

¹ O artigo 18.4 CE, establece en realidade, un mandato ao lexislador e non un dereito fundamental en sentido propio, así dispón o seguinte: *a lei limitará o uso da informática para garantir a honra e a intimidade persoal e familiar dos cidadáns e o pleno uso dos seus dereitos*. A redacción do precepto constitucional non é afortunada, xa que limitar o uso da informática, ademais de pouco factible, é pouco desexable, cousa distinta, que é sen dúbida o que o constituínte quixo dicir, é *poñer coto* aos eventuais abusos no emprego das novas tecnoloxías. O mandato constitucional é, sen dúbida, unha garantía para a plena eficacia doutros dereitos como son a honra e a intimidade. Neste sentido, sobre o lexislador pesa o deber de regular o tratamento de datos de maneira que esa actividade se realice de forma respectuosa cos dereitos fundamentais.

² As vulneracións á autodeterminación informativa por parte dos particulares teñen relevancia constitucional e por conseguinte tamén se consideran violacións do artigo 18.4 CE e isto significa, na práctica, que son susceptibles de protección vía recurso de amparo.

³ Así, o Tribunal Constitucional amparou aos traballadores fronte á utilización empresarial non xustificada de información sobre afiliación sindical (STC 11/1998, do 12 de febreiro) ou fronte á creación polo empresario sen o consentimento dos afectados dun ficheiro sobre absentismo con baixa médica (STC 202/1999, do 8 de novembro).

⁴ Neste punto, SEMPERE NAVARRO e SAN MARTÍN MAZZUCCONI advirten que o Tribunal Constitucional se afana *en deslindar* a liberdade informática

que a chamada *liberdade informática*⁵ é o dereito para controlar o uso dos mesmos datos insertos nun programa informático, *habeas data*⁶, e comprende a oposición do cidadán a que determinadas informacións persoais sexan utilizadas para fins distintos do lexítimo que xustificou a súa obtención.

Para establecer unha correcta análise e delimitación temos que mencionar os outros dous dereitos que en materia de control de TIC poden resultar afectados; o dereito á intimidade e o dereito ao segredo das comunicacións.

1.1.1. Delimitación fronte ao dereito á intimidade

Segundo reiterada xurisprudencia constitucional, o dereito á intimidade persoal, en canto derivación da liberdade e dignidade da persoa, art. 10.1 CE, implica a existencia dun ámbito propio e reservado fronte á acción e o coñecemento dos demais, necesario segundo as pautas da nosa cultura, para manter unha mínima calidade de vida humana. A fin de resgardar ese espazo reservado, este dereito confire á persoa o poder xurídico de impoñer a terceiros o deber de absterse de toda intromisión na esfera íntima e a prohibición de facer uso do así coñecido (STC 196/2004, do 15 de novembro). Por tanto, *o atributo máis importante da intimidade, como núcleo central de personalidade, é a facultade de exclusión dos demais da abstención de inxerencias por parte doutro, tanto no que se refire á toma de coñecementos intrusiva, como á divulgación ilexítima destes datos* (STC 142/1993, do 22 de abril).

respecto do dereito á intimidade, pero tacitamente, recoñece que a escisión non pode ser absoluta, porque o dereito á protección de datos comprende o dereito á intimidade, aínda que o exceda. V. SEMPERE NAVARRO, A. V. e SAN MARTÍN MAZZUCCONI, C.: *Nuevas tecnologías y Relaciones Laborales, Aranzadi, 2002*, páx. 120.

⁵ STC 202/1999 do 8 novembro (RTC 1999\202).

⁶ Segundo a RAE o dereito á propia intimidade informática, que confire ao seu titular un dereito de control sobre os datos (acceso, rectificación e cancelación destes), intervindo o Estado na súa protección con axencias ou comisarios para a protección dos datos.

1.1.2. Delimitación fronte ao dereito ao segredo das comunicacións

O segredo das comunicacións, expresamente proclamado no art. 18.3 CE, ten un significado instrumental respecto da liberdade, pois se garante o segredo das comunicacións para que estas poidan desenvolverse con liberdade. Así podemos realizar unha serie de precisións:

- Só a comunicación que ha de valerse dalgún medio técnico está cuberta polo art. 18.3 CE. Non o está, con todo, a directa.
- Protéxese o soporte e o contido.
- O segredo non rexe entre os propios comunicantes, e en consecuencia a gravación da propia conversación non vulnera o segredo das comunicacións.

1.2. UN DEREITO EN EVOLUCIÓN

Para certo sector da doutrina constitucionalista encabezado por CORDOBA CASTROVERDE e Díez Pícazo, o art. 18.4 CE supón un dereito cunha tremenda forza irresistible, pois aínda que permaneceu larvado durante un gran lapso de tempo, actualmente converteuse nun *buraco negro que o absorbe todo e non deixa escapar nada do seu ámbito*. E mesmo á luz dos amplos conceptos de datos persoais e tratamento, estes autores consideran que calquera acto de comunicación baseado en medios automáticos, como as telecomunicacións, o correo electrónico ou as redes sociais, relativo a unha persoa física, constitúe unha interferencia putativa tal deste dereito fundamental que require de xustificación⁷.

En parecido sentido, pronúncianse dentro da doutrina social GARCÍA-PERROTE ESCARTÍN e MERCADOR UGUINA ao afirmar que a protección de datos comeza a ocupar os espazos da privacidade impoñendo os seus principios de actuación moito máis esixentes e rigorosos que os que

⁷ CORDOBA CASTROVERDE, D. e Díez- PÍCAZO GIMÉNEZ, L. M.: Reflexiones sobre los retos de la protección de la privacidad en un entorno tecnológico en AA. VV. Asociación de Letrados del Tribunal Constitucional (Coord.): *el derecho a la privacidad en un nuevo entorno tecnológico*. XX Jornadas de la Asociación de Letrados del Tribunal Constitucional, CEPC, 2016, páxs. 99-122.

serviran ata agora para limitar o dereito á intimidade⁸. Chegándose mesmo a afirmar que estamos ante un dereito en construción, de perfís non completamente acabados, e que por iso mesmo non hai que descartar que nun futuro máis ou menos próximo presente novidades ou aspectos que hoxe en día puidesen sorprendernos ou, cando menos, que non somos capaces de adiviñar⁹.

O obxecto do dereito fundamental á protección de datos dende a perspectiva das relacións laborais persegue garantir á persoa un poder de control sobre os seus datos persoais, o seu uso e o seu destino, co propósito de impedir un tráfico ilícito e lesivo para a dignidade do traballador afectado. A súa concepción abarca calquera tipo de dato persoal, sexa ou non íntimo, cuxo coñecemento ou emprego poida afectar os dereitos da persoa, sexan ou non fundamentais.

Dende unha perspectiva laboral, o contrato de traballo é, sen dúbida, unha zona *particularmente sensible*¹⁰ respecto das ameazas que para a vida privada dos traballadores poden derivar do control dos datos persoais, ou dadas as características propias da relación laboral que fan que existan dificultades e excepcións á hora de transplantar o réxime xurídico propio da protección de datos de carácter persoal ao ámbito da empresa.

⁸ GARCÍA-PERROTE ESCARTÍN, I. e MERCADOR UGUINA, J. R.: La protección de datos se come a la intimidad: la doctrina de la sentencia del Tribunal Europeo de Derechos Humanos del 5 de septiembre de 2017 (caso Bărbulescu v. Rumania; nº 61496/08; Gran Sala), *Revista de Información Laboral*, núm. 10, 2017.

⁹ GARCÍA MURCIA, J, e RODRÍGUEZ CARDO, I. A.: La protección de datos personales en el ámbito de trabajo: una aproximación desde el nuevo marco normativo, *Revista Española de Derecho del Trabajo*, núm. 216, 2019 (BIB 2019\1432).

¹⁰ O perigo denunciado multiplícase polo desequilibrio das posicións de poder na relación de traballo, dentro da cal, o traballador ten menor capacidade de resistencia ás pretensións de control informativo. Vide. CUADROS GARRIDO, M.E.: *Trabajadores Tecnológicos y Empresas Digitales*, Aranzadi, 2018, páx. 135.

2. O ART. 8 DO CONVENIO EUROPEO DE DEREITOS HUMANOS

2.1. OS CASOS HALFORD E COPLAND

A autodeterminación informativa atópase de maneira implícita dentro dos dereitos protexidos polo art. 8¹¹ do Convenio Europeo para a salvaguardia dos Dereitos Humanos e as Liberdades Fundamentais (CEDH)¹², e nalgúns arranques puntuais desta doutrina xurisprudencial nos casos *Huvig e Krsuling v. Francia* do 24 de abril de 1990¹³. Faise necesario por iso aludir a dúas importantes sentenzas do Tribunal Europeo de Dereitos Humanos, consideradas como *leading case*, nos termos que establecen as SSTDH do 25 de xuño de 1997 -caso HALFORD- e do 3 de abril de 2007 -sentenza COPLAND- para valorar a existencia dunha lesión do art. 8 do Convenio Europeo para a Protección dos Dereitos Humanos; e a través deste pasou a formar parte da xurisprudencia da Sala IV do Tribunal Supremo e posteriormente da do Tribunal Constitucional. O caso *Halford contra o Reino Unido*¹⁴, constitúe o primeiro no que levou a cabo unha utilización explícita da doutrina da *expectativa de privacidade*¹⁵. Os feitos que se declararon probados na sentenza son os seguintes:

¹¹ Artigo 8 sobre o dereito ao respecto á vida privada e familiar, cuxa literalidade é a seguinte: «1. Toda persoa ten dereito ao respecto á súa vida privada e familiar, do seu domicilio e da súa correspondencia; 2. Non poderá haber inxerencia da autoridade pública no exercicio deste dereito, senón sempre que esta inxerencia estea prevista pola lei e constitúa unha medida, que nunha sociedade democrática, sexa necesaria para a seguridade nacional, a seguridade pública, o benestar económico do país, a defensa da orde e a prevención do delito, a protección da saúde ou da moral ou a protección dos dereitos e liberdades dos demais».

¹² Convenio Europeo para a Protección dos Dereitos Humanos e as liberdades fundamentais feito en Roma o 4 de novembro de 1950. Protocolo adicional ao Convenio feito en París o 20 de marzo de 1952.

¹³ STDH 24 de abril de 1999 (TEDH 1990, 2).

¹⁴ STDH do 25 de xuño de 1997 (TEDH 1997, 37).

¹⁵ O referido criterio podería definirse coa seguinte máxima: un cidadán non pode ser sometido a unha inxerencia sobre a súa privacidade coa que non puidese contar en termos razoables. Os seus antecedentes atópanse en EEUU e parten da interpretación dada pola Supreme Court á Cuarta Emenda da Constitución Americana, que contempla a protección contra persecucións e investigacións irracionais, e serviu de base para sentar o criterio da expectativa razoable de intimidade, coñecido tamén como

- A demandante, chamada Alinson Halford, era inspectora xeral da policía británica de Merseyside.
- Antes do proceso ante o TEDH, presentou unha demanda por vulneración do principio de igualdade ante un tribunal de traballo, debido a que se rexeitou en sucesivas ocasións a súa candidatura a un ascenso; e, con todo, segundo sostíña, concedeuse a colegas con menos méritos, pero todos de sexo masculino.
- Halford tiña dereito a un despacho para o seu uso exclusivo e nel facía uso de dous teléfonos, un dos cales era para as súas comunicacións privadas e outro de traballo (estes teléfonos formaban parte dun sistema interno de comunicacións da policía, independente da rede pública).
- A inspectora tivo coñecemento de que se interceptaron as súas chamadas telefónicas e solicitou á comisión competente no seu país en materia de interceptacións de comunicacións, que abrise unha investigación debido a que consideraba que tal medida se realizou para obter información que sería utilizada contra ela no curso do procedemento en materia de discriminación. Como o amparo se lle denegou no país inglés esgotadas todas as vías legais no mesmo, acudiu ao TEDH.

O TEDH considerou que a interceptación das chamadas da demandante representaba unha violación do art. 8 do CEDH. Para o Tribunal despréndese claramente da súa xurisprudencia que as chamadas telefónicas que proceden de locais profesionais, do mesmo xeito que as procedentes do domicilio, poden incluírse nos conceptos de «vida privada» e de «correspondencia» citados no apartado 1 do art. 8 do Convenio de Roma. Non hai probas de que á Sra. Halford se lle avisase, en calidade de usuaria da rede

expectation of privacy test. O Tribunal Supremo estadounidense, ao longo dunha extensa e gradual xurisprudencia, considerou implícito un «*right to privacy*» na garantía da Cuarta Emenda fronte a rexistros e requisas arbitrarias (*unreasonable searches and seizures*), que limita a intrusión do goberno nas persoas, domicilios, documentos e efectos persoais, incluíndose non só os supostos de invasión material (*physical trespass*) senón tamén de vixilancia electrónica.

interna de telecomunicacións da policía, de que as chamadas efectuadas mediante esta podían ser interceptadas. O Tribunal considera que ela podía razoablemente esperar que se recoñecese o carácter privado deste tipo de chamadas.

No caso *Copland contra o Reino Unido*¹⁶, o TEDH estima que o almacenamento da información persoal sobre o teléfono da demandante, o seu correo electrónico e o uso que fai da internet sen o seu consentimento supoñía unha interferencia co seu dereito á vida privada do art. 8 da CEDH. Durante o seu emprego nun colexio estatal, o teléfono da demandante, o seu correo electrónico e o uso da internet estivo suxeito a monitoraxe por parte dunha institución británica ante as sospeitas de que a recorrente estaba a realizar un abuso de tarificación dende os terminais telefónico e informático. O TEDH declara o quebranto da expectativa razoable de privacidade, porque a recorrente vivía nun ambiente de permisividade co que se manexaba no seu posto de traballo, o que a levaba á crenza de que estaba libre do escrutinio das súas comunicacións por parte do empregador.

En suma: cando existe un hábito social xeneralizado de certa tolerancia co uso moderado dos medios informáticos e de comunicación, facilitados pola empresa, créase unha expectativa xeral de confidencialidade que pode entrar en conflito co control empresarial, de aí a necesidade de regulación mediante convenio colectivo; faise necesario que os representantes dos traballadores negocien previamente unhas regras de uso que poidan ser asumidas polas partes.

2.2. O CASO BARBULESCU

A STEDH do 5 de setembro de 2017¹⁷ coñecida como *Barbulescu II*¹⁸, regula o abano de protección do dereito á

¹⁶ STDH do 3 de abril de 2007 (TEDH 2007, 23).

¹⁷ STEDH do 5 de setembro de 2017 (TEDH 2017, 61).

¹⁸ A Sala Cuarta do STEDH do 12 de xaneiro de 2016, nunha primeira sentenza coñecida como caso *Barbulescú vs. Romania*, avalou o despedimento dun traballador de profesión enxeñeiro, por realizar un uso particular da conta de mensaxería de Yahoo Messenger, baseando a súa fundamentación en que se demostrou que incumpriu o código interno de conduta que estaba establecido na empresa, respecto a a utilización das

autodeterminación informativa, marca doutrina xeral non sobre mensaxería instantánea senón sobre TIC en xeral no marco do contrato do traballo e das pautas de control a seguir polo empresario pois constrúe unha técnica argumental de razoamento xenérico para enfrontarse a este tipo de problemas.

O TEDH considera que os tribunais nacionais romaneses omitiron datos fundamentais para resolver o suposto. Por unha banda, verificar se o traballador fora advertido con carácter previo polo seu empresario da posibilidade de que as súas comunicacións fosen vixiadas, e, doutra banda, a

tecnoloxías da información e da comunicación. En consecuencia, podíase entender que o empresario podía controlar as comunicacións electrónicas profesionais dos seus empregados, sen vulnerar por iso o seu dereito á intimidade, recollido no art. 8 do CEDH. Os antecedentes do caso son os seguintes: un empregador informou a un traballador que realizara un control da actividade da súa conta de mensaxería instantánea e comprobara que a usaba para fins particulares, prohibidos polo protocolo sobre uso de novas tecnoloxías establecido na empresa, polo cal procedeu ao seu despedimento disciplinario. No acto de xuízo achegouse como proba documental dos feitos unha transcripción das comunicacións da devandita mensaxería instantánea, na que constaban intercambios de mensaxes entre o demandado e varias persoas e mesmo algúns de natureza sexual. O demandante negou que *de facto* se cumprise o protocolo da empresa, pois, na práctica había unha situación de tolerancia respecto ao uso persoal da conta profesional de mensaxería e alegou que co rexistro desta violouse o seu dereito ao secreto da correspondencia. Os tribunais romaneses estimaron a procedencia do despedimento, por considerar que este se realizou conforme á lexislación local aplicable, así como a inexistencia de vulneración do dereito á intimidade do traballador, por canto este fora informado da normativa interna da empresa e o rexistro da súa conta de mensaxería era a única forma de comprobar se se respectou esa normativa. O TEDH nunha primeira Sentenza coñecida logo como *Barbulescû I*, concluíu que os tribunais internos mantiveron un equilibrio apropiado entre o dereito do actor ao respecto á súa vida privada e á da súa correspondencia electrónica conforme ao art. 8 do Convenio e os intereses do seu empregador. Por tanto, non se apreciou unha vulneración do devandito precepto. Se unha Sala do TEDH emite unha sentenza as partes poden solicitar a remisión do asunto ante a Gran Sala para unha nova consideración, tal posibilidade é excepcional e dela fixo uso o demandante, solicitou que o asunto fose remitido á Gran Sala; sendo aceptada esta pretensión o 6 de xuño de 2016 e procedéndose a ditarse STEDH o 5 de setembro de 2017, coñecida como *Barbulescû II*. O labor da Gran Sala, integrada por 15 maxistrados, foi revisar a sentenza baseándose nas excepcionais obxeccións alegadas polo recorrente, para reiterar ou non o fallo daquela.

ausencia de información previa e clara xa que o traballador non fora informado nin da natureza, nin do alcance da vixilancia da que fora obxecto, así como do grao de intromisión na súa vida privada e na súa correspondencia. Para a maioría da Sala, dos feitos declarados probados da sentenza non pode extraerse a conclusión de que a parte agora recorrente fose informada «por anticipado da extensión e da natureza da vixilancia levada a cabo polo seu empregador», nin tampouco de que este tivese posibilidade de «acceso ao contido das súas comunicacións». O que conduce á Gran Sala a considerar que o art. 8 do CEDH é aplicable ao suposto debatido.

O TEDH reflexiona sobre varios aspectos para resolver sobre se se vulnerou ou non o referido artigo. Xorde así unha serie de interrogantes que configuran o “test Barbulescu”:

- Informouse ao empregado da posibilidade de que o empresario tome medidas para controlar a súa correspondencia e outras comunicacións, así como da aplicación desas medidas? A información debe en principio ser clara en canto á natureza da vixilancia e anterior á súa posta en práctica e no suposto axuizado non o foi.

- Cal foi o alcance da vixilancia levada a cabo polo empregador e o grao de intromisión na vida privada do traballador? Non se detalla se o empresario puido valerse de medios menos intrusivos de fiscalización da conta do traballador, pois se afirma que existen varios tipos de control, uns moi intrusivos sobre o contido das comunicacións electrónicas e outros menos invasores que analizan o tráfico xerado sobre o número das comunicacións. Non se xustifica por que se opta pola vixilancia máis intrusiva e non se explica se se puido chegar ao mesmo resultado con outros métodos menos invasivos. Non se especifica tampouco durante canto tempo se levou a cabo a vixilancia e cantas persoas puideron acceder ao contido de tales informacións.

- Existiron motivos lexítimos, debidamente acreditados polo empregador, para xustificar a vixilancia e o acceso aos

contidos das comunicacións? Afírmase que non se xustifica cales son as razóns concretas que determinan a fiscalización e a monitoraxe da conta do traballador, doutra banda, tampouco e, en fin, se o acceso ao contido das comunicacións sería posible sen o seu coñecemento.

Os tribunais nacionais romaneses non verificaron se o traballador fora advertido con anterioridade da vixilancia que ía levar a cabo das súas comunicacións electrónicas efectuadas dende a conta profesional, nin tampouco ata que punto se produciu unha intromisión na vida privada do traballador no ámbito da relación de traballo que puidese alcanzarse por vías menos invasivas. Como argumento de peche, razoa a sentenza que non se protexeu de maneira adecuada o dereito do traballador respecto da súa vida privada, e dende ese momento, non realizaron unha ponderación xusta dos intereses en xogo e vulneraron o art. 8 CEDH.

2.3. O CASO LÓPEZ RIBALDA

Coa STEDH do 9 de xaneiro de 2018¹⁹ coñecida como *López Ribalda* reafírmase a doutrina anterior *Barbulescu II*, o TEDH estima que a videovixilancia encuberta ás traballadoras no seu posto de traballo é unha inxerencia no seu dereito á vida privada xa que o empresario non cumpriu coa súa obrigaón de informar as titulares dos datos da existencia da videovixilancia e os fins da recollida e tratamento dos seus datos persoais ²⁰.

O caso López Ribalda e outras contra o Reino de España, resolve sobre unha pretendida vulneración do art. 8 CEDH por lesionar a proba videográfica o dereito á privacidade das cinco demandantes, antigas empregadas de MERCADONA, no seu día despedidas, por cometer diversos furtos.

Os feitos transcorren do seguinte modo: nun supermercado da cadea antes mencionada, na provincia de Barcelona, en Granollers, realizouse unha auditoría dos últimos meses de facturación que desprende un importante descuadre

¹⁹ STEDH 9 de xaneiro de 2018 (TEDH 2018, 1).

²⁰ PRECIADO DOMENECH, C.H.: «Comentario de urgencia a la STEDH del 9 de enero de 2018. Caso López Ribalta y otras c. España», *Revista de Información Laboral*, núm. 1, 2018.

contable. Para detectar a orixe das anomalías, decidiuse instalar varias cámaras de vixilancia oculta na liña de caixa, para fiscalizar a actividade dos empregados, que ás cámaras permanentes na área de entrada e de cuxa existencia coñecían os traballadores, fiscalizaron a totalidade da actividade do persoal. Do visionado das gravacións constatouse que varias caixeiras cometían pequenos furtos. Antes de proceder aos correspondentes despedimentos disciplinarios, as afectadas foron convocadas a unha reunión con presenza dun representante dos traballadores. No transcurso das entrevistas, todas recoñeceron os feitos e, mesmo, tres das empregadas asinaron a súa renuncia para impugnar en sede xudicial o despedimento; a cambio diso, a empregadora ofreceu non instar accións penais contra elas.

Procesalmente ínstanse dous procesos, nun deles, figuraba como parte accionante unha única traballadora, a señora López Ribalda e, no outro procedemento, como parte demandante, catro traballadoras. Ambas demandas postulan a nulidade da proba por falta da información previa.

Respecto ao art. 8 CEDH, declárase o evidente incumprimento do seu contido, posto que o dereito ao respecto á vida privada e familiar, implica un coñecemento previo da fiscalización da actividade das traballadoras a través da videovixilancia, e respecto das cámaras instaladas *ad hoc*, non existía pois non se facilitou información previa. O Tribunal parte do dereito do empregador a velar polo correcto funcionamento da súa empresa, exercendo as correspondentes facultades de control que correspondan, pero sempre salvagardando un xusto equilibrio cos dereitos dos traballadores, o que no suposto obxecto de axuízamento non se cumpre, argumenta o TEDH.

Na fase de alegacións, o Reino de España alegou que era certo que non existía coñecemento das cámaras ocultas pero que tal omisión non supoñía unha vulneración do art. 18.4 CE xa que tal medida superara o xuízo de proporcionalidade a través da regra do triplo test. O TEDH discrepa desta afirmación, entendendo que non se salvagardou o correspondente canon de equilibrio xusto

entre as partes, o que provocou unha situación de menoscabo cara aos dereitos lexítimos das traballadoras.

Por tanto, o dereito do art. 8 CEDH, ha de interpretarse de maneira aberta, sen prestarse a unha definición exhaustiva senón dunha *forma dinámicamente ampla* como sinala CASAS BAAMONDE²¹. Efectivamente, na configuración do mencionado dereito existe unha dobre faceta, negativa e positiva: por unha banda, o deber de non inxerencia, e doutra banda, a obrigación positiva de efectividade do dereito tal e como advirte MOLINA NAVARRETE²².

Por último, con respecto a esta sentenza por parte da avogacía do Estado representando ao Reino de España, solicitouse que o asunto sexa analizado en Gran Sala polos 15 maxistrados do TEDH, e tal pretensión foi aceptada, polo que vai ditarse unha *López Ribalda II*, que cabe esperar que reafirme a doutrina da *López Ribalda I*.

3. REGULAMENTO XERAL DE PROTECCIÓN DE DATOS

3.1. ÁMBITO DO RXPD

Nun eido globalizado como o tecnolóxico, a aplicación extraterritorial das normas constitúe un verdadeiro desafío, pois non tería demasiado sentido limitalas a un determinado espazo, polo principio de aplicación territorial da Lei, ou, a un concreto conxunto de persoas, por imperativo do principio de personalidade. Fronte ao escaso desenvolvemento que a normativa de protección de datos experimentou no ámbito laboral no noso país, a nivel europeo o Regulamento Xeral sobre Protección de Datos

²¹ CASAS BAAMONDE, E.: «Informar antes de vigilar, ¿tiene el Estado la obligación positiva de garantizar un mínimo de vida privada a los trabajadores en la empresa en la era digital? La necesaria intervención del legislador laboral», *Revista de Derecho de las Relaciones Laborales*, núm. 2, 2018, páx. 104.

²² MOLINA NAVARRETE, C.: «De "Barbulescu II" a "López Ribalda" ¿que hay de nuevo en la protección de datos de los trabajadores? Comentario a la Sentencia del Tribunal Europeo de Derechos Humanos del 9 de enero de 2018, caso López Ribalda "et alii" vs. España», *Estudios Financieros, Revista de Trabajo y seguridad social: comentarios casos prácticos: recursos humanos*, núm. 419, 2018, páx. 127.

(RXPDP)²³ abre a posibilidade de intervir neste ámbito, ata hai pouco ignorado pola normativa estatal.

O RXPDP establece unha normativa única, válida en toda a UE e aplicable ao tratamento de datos persoais no contexto das actividades dun establecemento do responsable ou do encargado do tratamento na Unión, independentemente de que o tratamento teña lugar na Unión ou non.

Deste xeito, o RXPDP incorpora novas regras sobre extraterritorialidade das normas e aplicárase fóra da Unión Europea cando o tratamento de datos persoais de interesados residentes na Unión se efectúe por responsables ou encargados do tratamento non establecidos na Unión e as actividades de tratamento estean relacionadas con dous ámbitos:

- A oferta de bens ou servizos a eses interesados na Unión, independentemente de se se require un pago por parte do interesado.
- O control da súa conduta, na medida en que esta teña lugar na Unión Europea.

No ámbito laboral, os aspectos máis relevantes do RXPDP son os seguintes:

1. O tratamento de datos está prohibido cando revelen a orixe étnica ou racial, as opinións políticas, as conviccións relixiosas ou filosóficas, ou a afiliación sindical, e o tratamento de datos xenéticos, datos biométricos dirixidos a identificar de maneira unívoca a unha persoa física, datos relativos á saúde ou datos relativos á vida ou a orientación sexual dunha persoa física²⁴.

2. O Regulamento dá a posibilidade aos Estados membros de establecer normas máis específicas, a través de disposicións lexislativas ou de convenios colectivos, para

²³ Regulamento 2016/679 do Parlamento Europeo e do Consello do 27 de abril de 2016, relativo á protección de persoas físicas no que respecta ao tratamento de datos persoais e libre circulación deses datos, DOCE 4 de maio de 2016.

²⁴ Esta prohibición ten algunhas condicións en relación ao tratamento, v. art. 9.2 do RXPDP.

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 obrigacións 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 goce, individual ou colectivo, dos dereitos e prestacións relacionados co emprego e a efectos da extinción da relación laboral.

3. As normas que establezan os Estados deben incluír 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.

4. A figura do *Delegado de Protección de Datos*, foi altamente debatida en todo o proceso regulatorio. Existe a obrigatoriedade na designación desa figura, pero só para determinados casos concretos, como:

- Administracións públicas.
- Entidades cuxa principal actividade leve aparelada a monitoraxe de datos persoais ou o tratamento de datos persoais a gran escala.
- Entidades cuxa principal actividade comporte o tratamento de datos especialmente protexidos a gran escala, así como de antecedentes penais.

Con respecto aos dereitos dos interesados, existen dous novos dereitos que son recoñecidos a favor de todos os cidadáns que constitúen unha das principais novidades do RXPd; o dereito ao esquecemento e o dereito á portabilidade, que á súa vez constitúen as dúas indicacións máis interesantes que xorden respecto da aplicación no

ámbito laboral, aspectos, que, pola súa importancia, se analizan en dous epígrafes separados.

3.2. DEREITO AO ESQUECIMENTO

O *dereito ao esquecemento* é unha vertente do dereito á protección de datos persoais fronte ao uso da informática e é tamén un mecanismo de garantía para a preservación dos dereitos á intimidade e á honra, cos que está intimamente relacionado, aínda que se trate dun dereito autónomo²⁵.

O art. 31.2 RPD establece que en calquera momento un interesado pode solicitar ao responsable dun ficheiro ou tratamento que se cancelen os datos que lle concirnen, ben porque desexa revogar o consentimento outorgado con anterioridade ou ben porque entende que o tratamento se está efectuando sen o seu consentimento previo ou porque non se lle informou dos extremos que a normativa esixe; así o dereito de cancelación dará lugar á supresión dos datos que resulten inadecuados ou excesivos.

Dende que se publicou a coñecida STXUE do 13 de maio de 2014²⁶ na que se estimaba a pretensión dun cidadán español que pedía a cancelación de resultados obtidos ao buscar o seu nome en Google, pois mostraba unha información desactualizada, foise configurando o «dereito ao esquecemento»²⁷ e foise concretado o seu exercicio. O TXUE recoñeceu nesta importante sentenza *un certo dereito a ser esquecidos na internet*²⁸, dereito do interesado a solicitar que a información sobre a súa persoa non se poña a disposición do público en xeral mediante a súa inclusión na lista de resultados dos buscadores da internet, pero non supón un dereito á supresión dos datos publicados na Rede. É importante resaltar que a sentenza só se refire aos

²⁵ STC (Sala Pleno), núm. 58/2018, do 4 xuño (RTC 2018,58). Constitúe a primeira sentenza sobre a materia sobre dereito ao esquecemento do TC.

²⁶ STXUE de 13 maio 2014 Caso Google Spain, S.L., contra Axencia Española de Protección de Datos (TXCE 2014, 85).

²⁷ No sentido de «desindexación»; alude ao dereito da persoa para deixar de ter un perfil en liña, é dicir, a eliminar da Rede a súa pegada dixital.

²⁸ GOÑI SEIN, J. L.: «Los límites de las potestades empresariales vs. Derecho de la intimidad de las personas trabajadoras en el entorno de las TIC. El control empresarial en el espacio virtual. Problemática laboral en las redes sociales», *Actum social*, 2015.

buscadores, non comporta o dereito para borrar información do soporte orixinal, porque a información persoal non se elimina das webs de orixe.

O RXPd foi un pouco máis aló e configurou, por vez primeira, o dereito ao esquecemento como un dereito autónomo aos denominados «dereitos ARCO» (acceso, rectificación, cancelación e oposición)²⁹, no seu art. 17. Este dereito expón dificultades importantes de orixe práctica, xa que existen serias restricións, unha delas é a imposibilidade de modificar a información contida nos boletíns oficiais, dado que son inalterables unha vez transcorrido o prazo para recorrer, outra é a imposibilidade técnica de facer desaparecer determinadas fotos ou noticias unha vez que son compartidas en redes sociais, que posteriormente se difunden a outros aloxamentos web.

Na práctica, este dereito ten unha dimensión dual: por unha banda, supón para o cidadán un recoñecemento da pretensión de suprimir de inmediato a información afectada no sitio web, así como de absterse de dar difusión a esta información sempre que o titular dos datos o solicite. Doutra parte, tamén resulta relevante destacar que este dereito incide na esfera do responsable do tratamento, isto é, a entidade, corporación, sitio web ou rede social que trata os datos. O responsable do tratamento deberá optar entre limitar o tratamento do art. 18 RXPd, ou ben suprimir sen demora a información, art. 17 RXPd, ponderando caso por caso o alcance deste dereito co dereito á liberdade de expresión, a saúde pública, o deber de conservación dos datos para dar cumprimento a unha obriga legal e o interese público.

3.3. DEREITO Á PORTABILIDADE DOS DATOS

Un segundo límite que non debe descoñecerse no tratamento dos datos no ámbito laboral é o *dereito a opoñerse á elaboración de perfís virtuais*, este dereito non tivo uns antecedentes xurisprudenciais tan amplos como os do esquecemento dixital e suscitouse principalmente por

²⁹ DIAZ DÍAZ, E.: «El nuevo Reglamento General de Protección de Datos de la Unión Europea y sus consecuencias jurídicas para las instituciones», *Revista Aranzadi Doctrinal*, núm. 6, 2016 (BIB 2016, 3067).

razóns de interoperabilidade técnica. Conságrase o dereito á portabilidade no art. artigo 20 do RXPD Regulamento (UE) 2016/679³⁰, débese facilitar a transmisión de datos persoais dun proveedor de servizos, como unha rede social, a outro nun formato estruturado e de uso habitual e de lectura mecánica. Este dereito aumentará a protección en materia de autodeterminación informativa e tamén mellorará a competencia efectiva entre provedores de servizos.

Este artigo permite ao interesado controlar a súa dispoñibilidade en liña, dereito perfectamente aplicable aos datos subxectivos procedentes de avaliacións ou xuízos subxectivos realizados sobre os candidatos a postos de traballo ou sobre os propios traballadores. Na práctica, o exercicio do dereito non está exento de complexidades, porque non é nada fácil saber polo momento quen posúe esas análises de datos persoais (avaliacións e xuízos subxectivos)³¹.

³⁰ Di o seguinte:

1. *O interesado terá dereito a recibir os datos persoais que lle incumban, que facilítase a un responsable do tratamento, nun formato estruturado, de uso común e lectura mecánica, e a transmitilos a outro responsable do tratamento sen que o impida o responsable ao que llos facilitou, cando: a) o tratamento estea baseado no consentimento segundo o artigo 6, apartado 1, letra a), ou o artigo 9, apartado 2, letra a), ou nun contrato segundo o artigo 6, apartado 1, letra b), e b) o tratamento se efectúe por medios automatizados.*
2. *Ao exercer o seu dereito á portabilidade dos datos de acordo co apartado 1, o interesado terá dereito a que os datos persoais se transmitan directamente de responsable a responsable cando sexa tecnicamente posible.*
3. *O exercicio do dereito mencionado no apartado 1 do presente artigo entenderase sen prexuízo do artigo 17. Tal dereito non se aplicará ao tratamento que sexa necesario para o cumprimento dunha misión realizada en interese público ou no exercicio de poderes públicos conferidos ao responsable do tratamento.*
4. *O dereito mencionado no apartado 1 non afectará negativamente os dereitos e liberdades doutros.*

³¹ GOÑI SEIN, J. L.: «Los límites de las potestades empresariales vs. Derecho de la intimidad de las personas trabajadoras en el entorno de las TIC. El control empresarial en el espacio virtual. Problemática laboral en las redes sociales», *op. cit.*

4. A LEI ORGÁNICA DE PROTECCIÓN DE DATOS E GARANTÍA DE DEREITOS DIXITAIS

4.1. IDEA XERAL

A aprobación da Lei orgánica de protección de datos e garantía de dereitos dixitais (LOPDGDD)³² supón unha novidade respecto da anterior normativa xa que estende o seu ámbito material ás relacións de traballo. Da propia literalidade do nome da Lei e da súa Exposición de Motivos, desvélese que son obxecto de protección o *dereito á autodeterminación informativa* (art. 18.4 CE) e os *dereitos dixitais* que podemos definilos como dereitos e liberdades recoñecidos a todos os cidadáns predicables ao ámbito da internet³³.

Con tal regulación expresa veuse a colmar a lagoa existente na materia³⁴ e así mesmo a DF 13ª da LO 3/2018 introduce un novo artigo 20 *bis* ao ET, co seguinte contido:

«Os traballadores teñen dereito á intimidade no uso dos dispositivos dixitais postos á súa disposición polo empregador, á desconexión dixital e á intimidade fronte ao uso de dispositivos de videovixilancia e xeolocalización nos termos establecidos na lexislación vixente en materia de protección de datos persoais e garantía dos dereitos dixitais».

³² O 3/2018, do 5 de decembro. BOE/BOE núm. 294, do 6 de decembro de 2018, páxinas 119788 a 119857.

³³ A palabra non se atopa na RAE, a definición é transcripción literal da Exposición de Motivos da Lei. Por dereitos dixitais entendemos un elenco heteroxéneo de dereitos: gran parte deles carecen dunha relación directa coa protección de datos persoais e conéctanse máis ben con outros dereitos fundamentais das persoas, como a igualdade e non discriminación, a liberdade de expresión, a intimidade, a honra ou a dignidade (neutralidade da internet, acceso universal á Rede, rectificación na internet ou educación dixital) e outros dereitos dixitais, forman parte do núcleo duro do dereito de autodeterminación informativa, como o dereito ao esquecemento, o dereito de portabilidade en servizos de redes sociais e servizos equivalentes ou o dereito ao testamento dixital. V. GARCÍA MURCIA, J. e RODRÍGUEZ CARDÓ. I. A.: La protección de datos personales en el ámbito de trabajo: una aproximación desde el nuevo marco normativo, *Revista Española de Derecho del Trabajo*, op. cit.

³⁴ Ata a data o terreo era anómico cun único artigo que regulaba de maneira manifestamente insuficiente 20.3 ET.

En definitiva, segundo o novo art. 20 *bis* ET para saber en que consisten estes dereitos de intimidade e desconexión dixital, teremos que acudir á LOPDGDD, así como á posibilidade de establecer garantías adicionais a través da negociación colectiva³⁵.

Nesta regulación da LOPDGDD tal e como establece nos seus artigos 87 a 91 dentro do capítulo X, *Garantía dos Dereitos Dixitais*³⁶, veñen a considerar lícitos os medios de control empresarial a través das TIC sempre que respecten os dereitos constitucionais superando determinados requisitos. O alcance de aplicación no ámbito laboral é o seguinte:

4.2. USO DE DISPOSITIVOS DIXITAIS NO ÁMBITO LABORAL

A Lei recoñece expresamente o dereito dos traballadores á protección da súa intimidade no uso dos dispositivos dixitais postos a disposición pola empresa. Restrinxe o acceso do empregador aos seus contidos aos únicos efectos de controlar obrigacións laborais ou estatutarias e de garantir a integridade dos dispositivos. Establece o mandato ao empregador de fixar os criterios de uso dos dispositivos coa participación dos representantes dos traballadores, sendo os traballadores informados deses criterios.

Como aspecto positivo, hai que destacar a correcta elección do termo *dispositivo dixital*, cuxa amplitude fai referencia a

³⁵ GARCÍA MURCIA, J. e RODRÍGUEZ CARDO, I. A.: "La protección de datos personales en el ámbito de trabajo: una aproximación desde el nuevo marco normativo", *op. cit.*

³⁶ Dentro do Capítulo X, entrelázanse cuestións laborais relativas á intimidade dos traballadores no ámbito dixital, con cuestións relativas ao dereito de acceso a Internet, a seguridade dixital, o dereito á educación dixital, o dereito de portabilidade en servizos de redes sociais e equivalentes, ou o dereito ao testamento dixital, materias todas elas. Pero esta cuestión non é do capítulo, senón que o *totum revolutum* impera en toda a LO, existe unha mestura de dereitos dixitais dentro dunha lei dedicada á protección de datos. O único nexo en común que forza o lexislador, fixando o ferrete no extremo do cabo para evitar que este se esfiaíe é, precisamente, que os dereitos e liberdades da Constitución son plenamente aplicables na internet. V. QUILEZ QUÑONERO, J.M.: La garantía de Derechos Digitales en el ámbito laboral: el nuevo artículo 20 bis del Estatuto de los Trabajadores, *Revista Española del Derecho del Trabajo*, núm. 179, 2019.

que se entenden incluídos no mesmo tanto os dispositivos dixitais actuais en uso (computadores, teléfonos móbiles, tablets etc.), como os posibles futuros.

Como primeiro punto crítico, apuntar que non se recollen de maneira expresa os dereitos fundamentais do art. 18.3 e da 18.4 CE, como dereitos de especial protección dado que tamén potencialmente xunto á 18.1 CE poden resultar vulnerados. Como segunda obxección, deixáronse fóra de regulación dispositivos propiedade do traballador que cada vez levan máis ao traballo e son usados con fins laborais, de acordo con tendencia anglosaxoa BYOD³⁷.

4.3. DEREITO Á DESCONEXIÓN DIXITAL NO ÁMBITO LABORAL

A desconexión dixital laboral ou o dereito á desconexión laboral é a facultade dos traballadores para desconectar do traballo por medios dixitais unha vez finalizada a xornada laboral convida³⁸. Como precedentes destacables, poñer de manifesto que a figura se atopaba xa regulada no Dereito francés dende 2016³⁹. É o suposto de dereitos dixitais máis

³⁷ Siglas de Bring Your Own Device (Trae o teu propio dispositivo). Con este acrónimo, descríbese unha nova tendencia tecnolóxica na que a política empresarial permite aos traballadores utilizar os seus propios dispositivos persoais para usos profesionais. Así mesmo, cando o empregado ademais utiliza e comparte aplicacións e tratamentos poñéndoo a «traballar» nas funcións da súa actividade na empresa o termo se amplía e fálase de BYOT que abarca programas, aplicacións, plataformas propias ou compartidas no concepto de utilización en común etc.

En España, moitas empresas por política de aforro eliminan os móbiles corporativos e substitúenos por subvencións aos empregados polo uso do seu móbil persoal para fins profesionais (uso de voz e datos), tendencia que vai en aumento, e que se trata dunha práctica xeneralizada no mundo anglosaxón.

³⁸ PURCALLA BONILLA, M.A.: Control tecnolóxico de la prestación laboral y derecho a la desconexión de los empleados: Notas a propósito de la Ley 3/2018, del 5 de diciembre, *Revista Española de Derecho del Trabajo*, núm.218, 2019.

³⁹ Lei número 2016-1088, do 8 de agosto de 2016, relativa ao traballo, a modernización do diálogo social e ao aseguramento das carreiras profesionais (Journal Officiel, núm. 0184, do 9 de agosto de 2016). V. BARRIOS BAUDOR, G.L.: El derecho a la desconexión digital en el ámbito laboral español: primeras aproximaciones, *Revista Aranzadi Doctrinal*, núm. 1, 2019.

mediático, a pesar de que é unha norma aberta, pois remite á negociación colectiva⁴⁰ e en todo caso á autorregulación do empregador, por iso cualificouse como *un dereito formalmente novo*⁴¹.

Cabe matizar que estamos ante un dereito dixital non relacionado co núcleo duro de autodeterminación informativa. Respecto á aplicabilidade, esténdese a calquera forma de traballo incluído o teletraballo.

Son varios os factores que motivan a existencia deste dereito: por unha banda, a conciliación da vida persoal e a familiar; doutra banda, a dicotomía entre tempo de traballo e de descanso; e, finalmente, a prevención do tecnoestrés.

4.4. DISPOSITIVOS DE VIDEOVIXILANCIA E DE GRAVACIÓN DE SONS

O art. 89.1 distingue dous tipos de videovixilancia: a permanente, respecto á que se esixe información previa expresa, clara e inequívoca; e a encuberta⁴², que se permite unicamente nos supostos de flagrante delito. Os dereitos constitucionais que resultan afectados son o 18.1 CE e 18.4 CE, aínda que este último non é aludido de maneira expresa. O lexislador permite o uso da videovixilancia

⁴⁰ Regúlase o “dereito á desconexión dixital no ámbito laboral” (art. 88) para traballadores e empregados públicos, adaptado á natureza e obxecto da relación e suxeito ao acordado colectivamente. O empregador, previa audiencia dos representantes dos traballadores, elaborará unha política interna a este respecto. Xa TALENS VISCONTI vaticinou o importante papel da negociación colectiva nesta materia afirmando que a regulación legal non supoñería máis que unha breve aproximación a un deber empresarial cuxo contido específico sería aconsellable deixar en mans da negociación colectiva. Argumentaba que non cabía descoñecer que a obrigada desconexión dixital non afectaba de igual modo nin na mesma intensidade a todas as actividades laborais, polo que debían de ser os actores legitimados para impulsar a negociación colectiva os que o dotasen de contido. V. TALENS VISCONTI, E.E. La desconexión digital en el ámbito laboral: un deber empresarial y una nueva oportunidad de cambio para la negociación colectiva, *Revista de información Laboral*, núm.4, 2018.

⁴¹ SEMPERE NAVARRO, A. e HIERRO HIERRO, F.J.: Disposiciones Laborales al cierre de 2018, *Aranzadi Digital*, núm. 1, 2019.

⁴² No caso de que se captase a comisión flagrante dun acto ilícito polos traballadores entenderase cumprido o deber de informar cando existise polo menos o cartel informativo conforme á instrución núm.1/2006 da AEPD.

fundamentando o procesamento de imaxes no art. 20.3 ET, como ata entón viña facendo a xurisprudencia.

Tal distinción entre dous niveis informativos distintos produce posturas contrarias: certo sector da doutrina opina que con tal regulación se recolle a xurisprudencia europea⁴³, outra tendencia considera que ao validar a videovixilancia sen información detallada o que se fai é desatender o mandato do lexislador europeo baseándose no preceptuado no RXPd e na doutrina López Ribalda e Barbulescu II⁴⁴.

O art. 89.2 prohibe expresamente a instalación de dispositivos de videovixilancia en lugares de descanso ou entretemento.

O art. 89.3 regula a posibilidade da gravación do son para supostos excepcionais unicamente cando resulten relevantes os riscos para a seguridade das instalacións, bens e persoas derivados da actividade.

⁴³ RODRÍGUEZ ESCANCIANO, S.: 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, *La Ley*, 15103/2018.

⁴⁴ SXS núm. 3 de Pamplona do 18 de febreiro de 2019 (AS 2019\1014) O maxistrado Carlos González González considera que a inadmisión da práctica da proba videográfica está motivada pola ausencia de información previa, os feitos que motivaron o despedimento disciplinario en setembro de 2018 quedaron acreditados por unha testemuña polo que se considera o despedimento procedente. A LOPD entrou en vigor despois, pero realiza unha crítica da actual regulación, que considera incompatible coa regulación comunitaria que ha de primar; así a sentenza recolle:

"O art. 89 LOPDRDD expón moitos interrogantes e o primeiro deles xira ao redor da determinación dos límites inherentes ao exercicio das funcións de control empresarial e ao significado da expresión "acerca desta medida" ao regular o deber de informar o traballador ("Os empregadores haberán de informar con carácter previo, e de forma expresa, clara e concisa aos traballadores ou aos empregados públicos e, no seu caso, aos seus representantes, acerca desta medida"). Tampouco se concreta se é esixencia legal específica a finalidade para a que se implantan as medidas de control empresarial e se inclúe a finalidade sancionadora no caso de que se graven incumprimentos laborais. Outra omisión sería a relativa ao concepto de acto ilícito".

En iguais termos, GONZÁLEZ GONZÁLEZ, C.: Control empresarial de la actividad laboral mediante la videovigilancia y colisión con los derechos fundamentales del trabajador. Novedades de la Ley Orgánica 3/2018, del 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, *Aranzadi digital*, núm. 1, 2019.

A norma non determina que se entende por tal risco, quizais o lexislador podía concretar especificando que determinadas actividades son de risco, pénsese en determinadas zonas restrinxidas dunha central nuclear, por exemplo.

Lembremos a doutrina respecto diso da STC 98/2000, do 10 de abril, a gravación do son constitúe unha intromisión *na propia esfera de desenvolvemento do individuo*⁴⁵; quizais sirva para interpretar o precepto.

- *Art. 90 Dereito á intimidade ante a utilización de sistemas de xeolocalización no ámbito laboral.*

Establécese un deber de información previo á fiscalización do GPS, que detalle de maneira expresa, clara e inequívoca. Recoñécense os dereitos de acceso, rectificación, limitación do tratamento e supresión.

O dereito que resulta máis afectado aquí é a autodeterminación informativa (18.4 CE), pola súa relación instrumental co dereito á intimidade este segundo dereito (18.1 CE) tamén é obxecto de protección, pero non dunha maneira colateral polo que a redacción do precepto non é afortunada de todo.

- *Art. 91. Dereitos dixitais de negociación colectiva.*

Dispón que os convenios colectivos poderán establecer garantías adicionais, polo que a negociación colectiva adquire un papel relevante para a salvagarda destes dereitos.

⁴⁵ En el caso de las grabaciones de Casino de la Toja, o TC considerou que tal gravación supoñía unha *intromisión ilexítima no dereito á intimidade*, pois a empresa co sistema de audición e gravación captaba comentarios privados dos clientes e dos traballadores, que eran alleos ao interese empresarial e por tanto irrelevantes dende a perspectiva de control das obrigacións laborais. A actividade que se pretendía controlar por parte da empresa, declarou o TC, atopábase no que denominou a *propia esfera de desenvolvemento do individuo* polo cal se pasan as funcións de control na prestación laboral, que legalmente lle concede o ET.

5. EVOLUCIÓN DA XURISPRUDENCIA CONSTITUCIONAL

5.1. PRIMEIRA ETAPA

Durante bastante tempo, o respecto á dignidade do traballador, imposto polo art. 20.3 ET como límite ao exercicio do control sobre o uso dos medios electrónicos na empresa, quedou confinado á intimidade e, nalgún caso, ao segredo das comunicacións. A conformidade constitucional dos medios de control examinouse só dende este prisma, relegando a un segundo plano, cando non obviando, a amálgama de informacións obtidas do traballador consideradas como «*datos persoais*». Por tanto, nesta fase, a protección de datos concíbese como unha función de garantía do dereito á intimidade.

5.2. SEGUNDA ETAPA

Na década dos noventa do s. XX empeza a cambiar a formulación coa STC 254/1993, do 20 de xullo⁴⁶, ditada nun recurso onde a protección de datos se concibe como «*un instituto de garantía doutros dereitos*», fundamentalmente, «*a honra e a intimidade*», pero tamén «*un instituto que é en si mesmo un dereito ou liberdade fundamental*».

O TC procede a estimar o recurso de amparo exposto, por considerar que foi vulnerado o dereito do recorrente pola decisión xudicial que declarou axustada a Dereito a denegación presunta do gobernador civil de Guipúscoa e do ministro do Interior de solicitude de información dos datos de carácter persoal existentes en ficheiros automatizados da Administración do Estado. Da opinión maioritaria disente un membro do tribunal, que considera que a pretensión do actor solicitando que se poñan determinados datos persoais, non é amparable en virtude do Convenio do Consello de Europa do 28 de xaneiro de 1981, ratificado por España.

5.3. TERCEIRA ETAPA

No inicio do século XXI, o proceso de recoñecemento do dereito á protección de datos como autónomo, marca un precedente importante, coas SSTC 290/2000 e 292/2000.

⁴⁶ STC 254/1993, do 20 de xullo (RTC 1993, 254).

Por unha banda, a STC 290/2000, do 30 de novembro⁴⁷, pronunciouse sobre a constitucionalidade da xa entón derogada Lei orgánica reguladora do tratamento automatizado de datos de carácter persoal de 1992 (LORTAD). Aínda que non aborda cuestións sustantivas sobre o dereito, é moi interesante o voto particular do maxistrado Jiménez de Parga, no que se expresan as razóns polas cales, ao seu xuízo, *debeu afirmarse de modo explícito, na súa argumentación, que o noso Tribunal recoñece e protexe agora un dereito fundamental, o dereito de liberdade informática, que non figura na Táboa do texto de 1978*.

Pola súa banda a STC 292/2000, do 4 de xaneiro⁴⁸, parte do recoñecemento dun dereito fundamental específico, dereito á protección de datos ou liberdade informática, que coexiste con outros dereitos. Para o Tribunal Constitucional *«a garantía da vida privada e da reputación ten hoxe unha dimensión positiva que excede o ámbito propio do dereito fundamental á intimidade»*. E que se traduce nun dereito de control sobre os datos relativos á propia persoa.

O TC declara a inconstitucionalidade dos incisos *«cando a comunicación fose prevista polas disposicións de creación de ficheiro ou por disposición de superior rango que regule o seu uso»* do art. 21.1, *«impida ou dificulte gravemente o cumprimento das funcións de control e verificación das Administracións Públicas»* e *«ou administrativas»* do art. 24.1, e todo o apartado 2 da LO 15/1999, 13 de decembro, de protección de datos de carácter persoal.

Entende a Sala que o límite establecido polo art. 21.1 LOPD, ao permitir que unha norma de rango inferior á Lei autorice a cesión de datos entre Administracións sen previo consentimento do afectado, supón unha restrición que só podería establecer unha Lei, contrariando a reserva legal establecida polo art. 53.1 CE; que a posibilidade de que, segundo o art. 24.1 LOPD, a Administración poida privar ao interesado de información relativa ao ficheiro e aos seus datos, invocando os prexuízos que semellante información

⁴⁷ STC 290/2000, do 30 de novembro (RTC 2000, 290).

⁴⁸ STC 292/2000, do 30 de novembro (RTC 2000, 292).

poida carrexar á persecución dunha infracción administrativa, supón unha grave restrición dos dereitos á intimidade e á protección de datos do art. 18.4 CE, e que ademais *«pode causar grave indefensión ao interesado»*.

O constituínte quixo garantir mediante o actual art. 18.4 CE, non só un ámbito de protección específico senón tamén máis idóneo que o que poderán ofrecer por si mesmos os dereitos fundamentais garantidos no apartado 1 do precepto.

A peculiaridade deste dereito fundamental á protección de datos respecto do dereito fundamental á intimidade radica na súa distinta función, o que aparella por conseguinte que tamén *«o seu obxecto e contido difiran»*. Insiste despois con respecto a este extremo, subliñando que *a función do dereito fundamental á intimidade do art. 18.1 CE é a de protexer fronte a calquera invasión que poida realizarse naquel ámbito da vida persoal e familiar que a persoa desexa excluír do coñecemento alieo e das intromisións de terceiros en contra da súa vontade (por todas, STC 144/1999, do 22 de xullo). En cambio, o dereito fundamental á protección de datos persegue garantir a esa persoa un poder de control sobre os seus datos persoais, sobre o seu uso e destino, co propósito de impedir o seu tráfico ilícito e lesivo para a dignidade e dereito do afectado... Pero ese poder de disposición sobre os propios datos persoais nada vale se o afectado descoñece que datos son os que se posúen por terceiros, quen os posúe, e con que fin (FJ 5.º)*.

5.4. CUARTA ETAPA

Vén marcada pola STC 29/2013, do 11 de febreiro⁴⁹, coñecida como *caso Universidade de Sevilla*, que constituíu

⁴⁹ STC 29/2013, do 11 de febreiro (RTC 2013, 29). O Tribunal Constitucional anulou as sancións impostas a un subdirector técnico sancionado por unha institución universitaria tras ser controlado con respecto ao cumprimento horario coa gravación das cámaras de videovixilancia que foron instaladas nos lugares comúns para seguridade das instalacións, para coñecer se cumpría coa súa xornada laboral. A Sala considerou lesionado o seu dereito á protección de datos. Afirmou que a actuación da Universidade de Sevilla non podía xustificarse polo feito de que houbese distintivos para advertir da instalación de cámaras, senón que

un fito por dous motivos fundamentais; o primeiro, porque estableceu un canon de control de constitucionalidade máis ríxido que o que a xurisprudencia constitucional viña aplicando respecto ao outros dereitos fundamentais como o dereito á intimidade; como segundo motivo, porque por primeira vez e unicamente fundamentándose no art. 18. 4 CE se rexeitou o control laboral da prestación de traballo. Denegouse a existencia de norma legal nas relacións laborais que autorizase restricións do dereito á información sobre o tratamento de datos persoais, non considerando hábil a tal fin o art. 20. 3 ET. Dende esta máxima, por tanto, negada a validez constitucional de restricións ao dereito fundamental dos traballadores ex art. 18.4 CE, quedaba en consecuencia impedida a ponderación da medida empresarial, se non había unha información aos traballadores previa e expresa sobre a finalidade de control da actividade laboral á que esa captación de imaxes podía ser dirixida.

5.5. QUINTA ETAPA

Está determinada pola STC 39/2016, do 3 de marzo, coñecida como *caso Bershka*⁵⁰, que modifica moi

era necesario que se informase aos traballadores de forma previa, precisa e clara das gravacións e do seu obxectivo. Na base da súa fundamentación aparece o seguinte relato: *No caso axuízado, as cámaras de videovixilancia instaladas no recinto universitario reproduciron a imaxe do recorrente e permitiron o control da súa xornada de traballo; captaron, por tanto, a súa imaxe, que constitúe un dato de carácter persoal, e empregáronse para o seguimento do cumprimento do seu contrato. Dos feitos probados despréndese que a persoa xurídica titular do establecemento onde se atopan instaladas as videocámaras é a Universidade de Sevilla e que ela foi quen utilizou ao fin descrito as gravacións, sendo a responsable do tratamento dos datos sen informar ao traballador sobre esa utilidade de supervisión laboral asociada ás capturas da súa imaxe. Vulnerou, dese xeito, o art. 18.4 CE (FJ 8.º).*

⁵⁰ STC 39/2016 de 3 marzo (RTC 2016, 39). Versa sobre o despedimento dunha traballadora dunha empresa do grupo INDITEX (Bershka), que despediu a unha traballadora por transgresión da boa fe contractual porque sostíña que se viña apropiando de efectivo da caixa da tenda, en diferentes datas e de forma habitual. Os feitos que deron lugar ao despedimento foron coñecidos como consecuencia da instalación de videovixilancia oculta. Para proceder a tal instalación de cámaras ocultas, a empresa argumentou que, por mor da instalación dun novo sistema de control

substancialmente a doutrina aplicable, declárase que pode haber sistemas sorpresivos ou non informados de tratamento, polo que a protección da 18.4 CE nesta materia presenta perfís difusos. Con esta sentenza reformúlase a natureza da autorización que recolle a LOPD, que pasa a ser indirecta, e non persoal, a pesar de que estamos ante persoas perfectamente individualizables coas que existe unha relación contractual.

Prodúcese, pois, un descenso no grao de protección do dereito fundamental do art. 18.4 CE, que se engade ao dato previo de que a lei xa estableceu que non é preciso nestes casos o consentimento, co cal a información constituía a peza clave do contido esencial do mencionado dereito e se entendía cumprido coa existencia dun mero cartel informativo conforme á Instrución núm. 1/2006 da AEPD⁵¹.

5.6. SEXTA ETAPA

Co ronsel da STEDH do 5 de setembro de 2017⁵², volve ampliar o abano de protección do dereito á autodeterminación informativa, márcase doutrina xeral non sobre mensaxería instantánea senón sobre TIC en xeral no marco do contrato do traballo e das pautas de control a seguir polo empresario pois constrúe unha técnica

informático de caixa, detectara que na tenda e, en concreto, na caixa onde prestaba os seus servizos a traballadora existían múltiples irregularidades, polo que entendía que había indicios para poder presumir unha posible apropiación dineraria por parte dalgún dos traballadores que operaban nesa caixa. Por tal motivo encargaron a unha empresa de seguridade que instalase unha cámara de videovixilancia na tenda onde prestaba os seus servizos a demandante e que controlase a mencionada caixa en cuestión. A cámara instalouse non comunicando aos traballadores a instalación, aínda que no escaparate do establecemento, nun lugar visible, colocouse o distintivo informativo. Denégase o amparo ao validar a proba de videovixilancia na que estaba baseado.

⁵¹ A Instrución núm. 1/2006, do 8 de novembro, da AEPD sobre tratamento de datos persoais con fins de vixilancia a través de cámaras ou videocámaras, es pecifica que se debe colocar nas zonas videovigiladas polo menos un distintivo informativo, situado nun lugar suficientemente visible, tanto en espazos abertos como pechados, así mesmo ten que haber a disposición dos interesados impresos nos que se detalle a información en materia de protección de datos vixente.

⁵² STEDH do 5 de setembro de 2017 (TEDH 2017, 61).

argumental de razoamento xenérico para enfrontarse a este tipo de problemas.

Coa STEDH do 9 de xaneiro de 2018⁵³ coñecida como *López Ribalda* reafírmase a doutrina anterior do TEDH e con respecto a este particular medio de control procédese a deslexitimar todo tipo de videovixilancia encuberta⁵⁴.

Pero a influencia das dúas sentenzas⁵⁵ vai máis a alá, implica unha modificación a nivel de teoría xeral destacándose por un sector da doutrina científica do noso país a súa marcada *vocación xeneralista*, que non se cingue obviamente a videovixilancia nin a mensaxería instantánea, senón que supón aplicar a protección do dereito á privacidade a nivel de TIC, o que supón que se incorpora un plus de protección aos traballadores, que se logrou coa STC 29/2013, pero que se perdeu coa STC 39/2016. A doutrina xudicial que emana destas sentenzas está chamada a ter importantes consecuencias na configuración e interpretación dos dereitos fundamentais e en concreto respecto ao art. 18.4 CE, xa que supón poder dispoñer dos datos persoais con independencia do seu carácter íntimo ou non, o que se concreta xuridicamente na facultade de acceso a eses datos, a un ulterior tratamento, así como o seu uso ou posibles usos por un terceiro xa sexa o Estado ou un particular⁵⁶.

Así mesmo, dentro desta doutrina, cabe destacar a STC núm. 25/2019, do 28 de febreiro de 2019⁵⁷, que aínda que

⁵³ STEDH 9 de xaneiro de 2018 (TEDH 2018, 1).

⁵⁴ PRECIADO DOMENECH, C.H.: «Comentario de urgencia a la STEDH del 9 de enero de 2018. Caso López Ribalta y otras c. España», *Revista de Información Laboral*, núm. 1, 2018.

⁵⁵ A doutrina *López Ribalda*, séguena: STSX de Cataluña de 8 xaneiro de 2019 (AS 2019\911) STSX Madrid 28 setembro de 2018 (JUR 2018\323429) STXS núm.9 de Sevilla 9 de xullo de 2018 (AS 2018\2107) STSX Cataluña 12 de xullo de 2018 (JUR 2018\281030) STSX Cataluña 25 de xuño de 2018 (JUR 2018\227264) STSJ Castela e León 11 de abril de 2018 (AS 2018\1211) STSX Castela-A Mancha 12 de xaneiro de 2018 (AS 2018\566). STSX País Vasco 27 de febreiro de 2018 (AS 2018\1200) e a doutrina *Barbulescu*: STS 8 de febreiro de 2018 (RJ 2018\666), STSX Andalucía do 3 de maio de 2018 (JUR 2018\210331) e STSX 28 de marzo de 2019 (ECLI: É:TSXAND:2019:1355)

⁵⁶ CUADROS GARRIDO, M.E.: «La mensajería instantánea y la STEDH del 5 de septiembre de 2017», *Revista Aranzadi Doctrinal*, núm. 11, 2017.

⁵⁷ STC núm.25/2019 do 28 de febreiro de 2019 RTC 2019\25

non pertence ao ámbito das relacións laborais, aplica criterios xerais aplicables a todas as xurisdicións. O precedente da sentenza cabe situalo no arranque na doutrina da expectativa na xurisprudencia constitucional, que tivo lugar coa publicación das SSTC 12/2012 do 30 de xaneiro⁵⁸ e 74/2012 do 16 de abril⁵⁹, referidas ambas a unha reportaxe xornalística de investigación oculta, rodada no interior dunha clínica sospeitosa de intrusismo profesional. Resolveuse o caso concreto dando a razón ao titular do dereito á intimidade, afirmando o TC que, conforme ao criterio de expectativa razoable de non ser escoitado ou observado por terceiras persoas, resulta patente que unha conversación mantida nun lugar especificamente ordenado a asegurar a discreción do falado, como ocorre por exemplo no despacho onde se realizan as consultas profesionais, pertence ao ámbito da intimidade. O suposto axuizado na STC núm. 25/2019, do 28 de febreiro de 2019, é moi similar ao anterior, trátase dunha reportaxe xornalística sobre un pretendido sanador que como parte do que ofertaba daba a posibilidade de dar unha copia en DVD dos servizos prestados, pero, ademais, os xornalistas infiltrados como supostos clientes utilizaron cámaras ocultas⁶⁰. O TS estima en parte o recurso e casa a

⁵⁸ STC 12/2012, do 30 de xaneiro (RTC 2012, 12). Versa sobre unha reportaxe que a televisión autonómica valenciana emitiu, que foi producido por Canal Mundo Producciones, no que se utilizaban imaxes obtidas mediante cámara oculta. A canle de televisión e a produtora foron condenados por intromisión á intimidade e vulneración do dereito á propia imaxe. A sentenza recolle a xurisprudencia do Tribunal Europeo de Dereitos Humanos, facéndose eco da teoría da expectativa razoable. Deste xeito, conclúe que a conversación mantida nun lugar especificamente destinado a asegurar a discrecionalidad do falado –neste caso concreto unha consulta profesional– pertence ao ámbito da intimidade. En consecuencia, desestímase o recurso de amparo interposto.

⁵⁹ STC 74/2012, do 16 de abril (RTC 2012, 74).

⁶⁰ O 3 de decembro de 2010, dous xornalistas acudiron un despacho dunha persoa que exercía como *coach*, mentor e consultor persoal, facéndose pasar por clientes e finxindo un deles que padecía cancro, e gravaron a visita con cámara oculta. Ao día seguinte os xornalistas regresaron ao mesmo despacho para recoller a gravación da visita xa que o curador gravaba á súa vez todas as visitas e proporcionaba unha copia aos seus clientes: os xornalistas tamén gravaron esa nova visita con cámara oculta. O día 15 de decembro de 2010 emitíronse fragmentos das gravacións das

STS pois considera que con respecto á gravación das imaxes encubertas lesionouse o dereito do recorrente á intimidade persoal, a propia imaxe e a honra ao centrarse os programas televisivos na persoa do demandante de amparo e difundir un material insuficientemente concluínte de seu e escasamente relevante para contribuír a un debate xeral. Polo que a intromisión na súa intimidade, non só careceu do, en principio, necesario consentimento previo do titular do dereito para realizar a videograbación na consulta profesional, senón que, nas circunstancias do caso, a súa divulgación constituíu tamén un exercicio desproporcionado da liberdade de información.

O TC afirma que non pode obviarse a circunstancia de que a información fose captada subrepticamente nun ámbito privado como é unha consulta profesional, en cuxo seo se desenvolven relacións de natureza profesional que están tamén protexidas polo dereito á intimidade, e nas que, por conseguinte, existe igualmente unha lexítima expectativa de miramento fronte á intromisión de terceiros.

Doutra banda, considera o TC que o feito de que o recorrente proporcionase unha gravación da mesma sesión que os xornalistas filmaron con cámara oculta, non emenda en absoluto a ausencia de consentimento para realizar a gravación subrepticia e divulgar as imaxes así obtidas, nin implica un consentimento expreso, válido e eficaz para difundir publicamente nun medio de comunicación social as imaxes contidas na gravación proporcionada; pola contra,

visitas obtidas con cámara oculta no programa Espejo Público da entidade mercantil Antena 3 de Televisión, S.A. No programa os citados xornalistas debateron coa condutora do programa e outros colaboradores sobre as visitas realizadas e sobre a actuación e o modo de proceder do demandante de amparo. O debate centrouse en mostrarlle como un "sanador" que non tendo titulación algunha relacionada coa saúde atribuíase aptitude para curar todo tipo de enfermidades; así mesmo, cualificóuselle de "mullereiro" e imputóuselle incluír nas terapias "algo máis que caricias". Así mesmo, no programa 3 D da mesma entidade Antena 3 emitíuse unha reportaxe titulada "Un falso gurú da felicidade?" sobre o demandante de amparo no que se mesturaban vídeos gravados por el mesmo con entrevistas e material propio da cadea. Tamén se reproduciron fragmentos da reportaxe noutros programas de noticias de Antena 3 e na páxina web da mesma cadea televisiva baixo o titular "O presunto sanador de Mallorca, ao descuberto. Acudimos á súa consulta en Mallorca".

pon de manifesto que a gravación oculta que levaron a cabo os xornalistas, así como a súa posterior difusión, non foi necesaria para obter a información e difundila.

Deste xeito, o TC fai propia a esencia mesma do concepto de expectativa *razoable de privacidad*; reside en derivar os contornos mesmos do dereito fundamental concernido do ámbito da privacidad, non tanto na súa configuración formal, como nese poder que todo cidadán ten de facelo valer, fronte aos poderes públicos ou ao resto da sociedade, o chamado *dereito de exclusión*.

Por último, dentro desta etapa cabe mencionar a recente STS do 10 de abril de 2019⁶¹. Os feitos axuizados nela son os seguintes: unha empresa multinacional de telemarketing que realiza servizos de *contact center*, inclúe nunha das cláusulas do contrato de traballo⁶² a autorización expresa para gravar mediante a cámara web ou dispositivo análogo a imaxe do traballador co fin do correcto desenvolvemento da prestación laboral. Tal uso da imaxe non era habitual senón puntual, reservado para determinadas actividades promocionais, nas que se solicitaba unha autorización específica aos traballadores. Coa introdución da cláusula xenérica pretendíase eludir a petición de autorizacións *ad hoc* cada vez que fose necesario.

O sindicato CGT presente na empresa impugna a referida cláusula ante a Audiencia Nacional suscitando un conflito colectivo, á demanda adhírense o resto dos sindicatos con representación na empresa. A AN estima a demanda e declara a nulidade da cláusula de cesión da imaxe por non ser válida por violar o dereito á propia imaxe do empregado. Non conforme co fallo, a empresa recorre a decisión ao TS en casación e o recurso é estimado e, por tanto, a sentenza da Audiencia anulada. O TS entende que a restrición do dereito é viable cando o obxecto do contrato o

⁶¹ STS do 10 de abril de 2019 (ECLI: É:TS:2019:1436).

⁶² "O traballador consente expresamente, conforme á LO 1/1982, do 5 de maio, RD 1720/2007 de Protección de Datos de carácter persoal e Lei Orgánica 3/1985, do 29 de maio, á cesión da súa imaxe, tomada mediante cámara web ou calquera outro medio, sempre co fin de desenvolver unha actividade propia de telemarketing e cumprir, por tanto, co obxecto do presente contrato e os requirimentos do contrato mercantil do cliente".

sobrentende, como ocorre no presente caso, dado que a execución é a realización de labores de telemarketing mesmo con videollamadas. Polo que esta maior intrusión se tolera polo especial obxecto do contrato de traballo, e dadas as especiais características, a diferenza dun contrato de traballo ordinario.

O debate xurídico que expón a STS do 10 de abril de 2019 lévanos a partir de que o telemarketing leva implícito que se graven as conversacións. Dende o punto de vista do traballador, a gravación da conversación pode ser moito máis sensible que outro tipo de seguimentos por parte do empresario, supoñer unha maior invasión da intimidade que unha imaxe, porque pode relevar pensamentos ou sentimentos internos que o outro medio non proporciona, neste sentido o art 89.3 da LOPDGDD. O feito certo é que, se as conversacións non puidesen ser gravadas, e no seu caso controladas, a prestación tampouco podería ser dirixida e vixiada polo empresario, polo que o control das conversacións é indispensable pola propia lóxica do contrato, hase de realizar nunhas condicións que minimicen a eventual lesión da esfera da intimidade, a través dos xa controis aleatorios. A STS do 5 de decembro de 2003⁶³ marcou un fito nesta materia e da súa doutrina temos que partir para interpretar o suposto comentado. O TS considera que o dereito á propia imaxe ao que se refire a AN atópase tutelado no art. 18.4 CE, dado que a imaxe é un dato persoal e, baseándose niso, dada a redacción da anterior LOPD e o RXPD⁶⁴, non é necesario solicitar o consentimento

⁶³ STS do 5 de decembro de 2003 (RJ 2004, 313). Nela o Tribunal Supremo non atopou ningún inconveniente para non permitir ao empregador intervir o contido das conversacións telefónicas mantidas polos traballadores cando existía unha finalidade lexitima que xustificase a intromisión, como o era, nun suposto de telemarketing, analizar as técnicas comerciais dos traballadores para impartir as oportunas instrucións para melloralas. Desestimouse que existise unha lesión do dereito á intimidade, pola gravación de conversacións entre os traballadores (asesores comerciais de Telefónica) e os seus clientes, aplicando o principio de ponderación, pois a medida é idónea para a finalidade pretendida, necesaria e equilibrada.

⁶⁴ Respecto ao RXPD o TS precisa que *a nova normativa coincide coa anterior e, aínda que rigoriza certas cuestións, flexibiliza e fai máis clara a aplicación doutros principios como o do consentimento do interesado, que non é preciso que se preste expresamente cando o tratamento do dato é*

do traballador, debido a que se trata dunha das exclusións que marcan ambos textos lexislativos. O feito de gravar a imaxe é algo puntual, cando as esixencias das actividades promocionais o requiran, pero en todo caso forma parte do propio contrato de traballo, polo que cabe concluír que a cláusula controvertida non é abusiva, senón, máis ben, informativa e á vez receptora dun consentimento expreso que non era preciso requirir.

A continuación, para dar máis forza ao argumento tráese a colación a doutrina da STC 99/1994, do 11 de abril⁶⁵, que considera aplicable, respectouse, no caso axuizado o principio de indispensabilidade ou de estrita necesidade da limitación, con base no cal o equilibrio entre as obrigacións derivadas do contrato para o traballador e o ámbito da súa liberdade constitucional ha de producirse na medida estritamente imprescindible para o correcto e ordenado desenvolvemento da actividade produtiva.

Por último, o TS precisa que non se está ante un suposto de videovixilancia, senón ante *videochamadas* nas que quen chama, grazas a unha cámara webcam que instala a empresa, ve a quen lle atende e conversa co seu interlocutor. Ese é o dato que se lle cede e facilita, pero que logo non pode tratar facendo unha gravación e outras operacións, pois iso está expresamente prohibido de maneira xenérica como principio xeral no art 5-1-b RXPd.

6. REFLEXIÓNS CONCLUSIVAS

PRIMEIRA. É conveniente establecer unha política empresarial admonitiva e preventiva sobre o uso dos dispositivos dixitais postos a disposición da empresa, tendo en conta o seguinte:

necesario para a execución dun contrato subscrito polo interesado, artigos 6-1-b) e 9-2-b) do Regulamento Comunitario.

⁶⁵ STC 99/1994, do 11 de abril (RTC 1994, 99). Coñecida como o caso do *cortador de xamón*, estimou lesivo o dereito ao uso da propia imaxe do traballador que foi despedido pola súa negativa a obedecer a orde empresarial que lle obrigaba a exhibir en público a súa habilidade profesional como desosador de xamóns nun acto promocional con presenza dos medios de comunicación.

- Antes do inicio da relación laboral, hanse de establecer previamente as regras do xogo; informarase de maneira clara suficiente ao traballador da política da empresa respecto ao uso das novas tecnoloxías e o seu posible uso disciplinario.

- Unha vez iniciada a relación laboral, hase de usar a tecnoloxía informática de maneira preventiva, para evitar “fugas de información”.

-Non son aconsellables as prohibicións absolutas, senón un uso das TIC social moderado.

- Durante o transcurso da relación laboral, realizaranse de maneira esporádica controis aleatorios para non converter en tolerancia certas prácticas ou malos hábitos que puidesen existir (se se prohíbe, pero non se controla, pódese crear un clima de permisividade).

SEGUNDA. O dereito do art 18.4 CE atópase en construción debido a que os seus límites son difusos e non están aínda determinados.

TERCEIRA. A regulación por parte da LOPDGDD en materia laboral cos arts. 97 a 91, supón un gran avance significativo, pero non respondeu ás expectativas. O papel da negociación colectiva nesta materia adquire o rol de protagonista, nunha tarefa que cabe vaticinar que non vai ser fácil.

CUARTA. A nivel xeral en materia de protección de datos, a lei insta a confusión, en ocasións, pois parece que entende que a intimidade equivale a autodeterminación informativa. E tampouco distingue dunha maneira clara entre dereitos dixitais e protección de datos, pois ás veces trata os termos como sinónimos.

7. BIBLIOGRAFÍA

BARRIOS BAUDOR, G.L: «El derecho a la desconexión digital en el ámbito laboral español: primeras

- aproximaciones», *Revista Aranzadi Doctrinal*, núm. 1, 2019.
- CASAS BAAMONDE, M.E.: «Informar antes de vigilar, ¿tiene el Estado la obligación positiva de garantizar un mínimo de vida privada a los trabajadores en la empresa en la era digital? La necesaria intervención del legislador laboral», *Revista de Derecho de Las Relaciones Laborales*, núm. 2, 2018.
- CÓRDOBA CASTROVERDE, D. e DÍEZ-PICAZO GIMENÉZ, L. M.: «Reflexiones sobre los retos de la protección de la privacidad en un entorno tecnológico», XX Jornadas de la Asociación de Letrados del Tribunal Constitucional/coord. por Asociación de Letrados del Tribunal Constitucional (España), 2016.
- CUADROS GARRIDO, M.E.:
-*Trabajadores Tecnológicos y Empresas Digitales*, Aranzadi, 2018.
-«La mensajería instantánea y la STEDH de 5 de septiembre de 2017», *Revista Aranzadi Doctrinal*, núm. 11, 2017.
- DÍAZ DÍAZ, E.: «El nuevo Reglamento General de Protección de Datos de la Unión Europea y sus consecuencias jurídicas para las instituciones», *Revista Aranzadi Doctrinal*, núm. 6, 2016.
- GARCÍA MURCIA, J. e RODRÍGUEZ CARDÓ, I.A.: «La protección de datos personales en el ámbito de trabajo: una aproximación desde el nuevo marco normativo», *Revista Española de Derecho del Trabajo*, núm. 216, 2019.
- GARCÍA-PERROTE ESCARTÍN, I. e MERCADER UGUINA, J. R.: «La protección de datos se come a la intimidad: la doctrina de la sentencia del Tribunal Europeo de Derechos Humanos de 5 de septiembre de 2017 (caso Bărbulescu v. Rumania; nº 61496/08; Gran Sala)», *Revista de Información Laboral*, núm. 10, 2017.
- GONZÁLEZ GONZÁLEZ, C.: «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», *Aranzadi digital*, núm. 1, 2019.
- GOÑI SEIN, J.L.: «Los límites de las potestades empresariales vs. Derecho de la intimidad de las personas trabajadoras en el entorno de las TIC. El control empresarial en el espacio virtual. Problemática laboral en las redes sociales», *Actum social*, 2015.
- MOLINA NAVARRETE, C.: «De "Barbulescu II" a "López Ribalda" ¿qué hay de nuevo en la protección de datos de los trabajadores? Comentario a la Sentencia del Tribunal Europeo de Derechos Humanos de 9 de enero de 2018, caso López Ribalda "et alii" vs. España», *Estudios Financieros, Revista de Trabajo y seguridad social: comentarios casos prácticos: recursos humanos*, núm. 419, 2018.
- PRECIADO DOMENECH, C.H.: «Comentario de urgencia a la STEDH de 9 de enero de 2018. Caso López Ribalda y otras c. España», *Revista de Información Laboral*, núm. 1, 2018.
- PURCALLA BONILLA, M. A.: «Control tecnológico de la prestación laboral y derecho a la desconexión de los empleados: Notas a propósito de la Ley 3/2018, de 5 de diciembre», *Revista Española de Derecho del Trabajo*, núm.218, 2019.
- RODRÍGUEZ ESCANCIANO, S.: «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», *La Ley*, 15103/2018.
- SEMPERE NAVARRO, A.V. e HIERRO HIERRO, F.J.: «Disposiciones Laborales al cierre de 2018», *Aranzadi Digital*, núm. 1, 2019.
- SEMPERE NAVARRO, A. V. y SAN MARTÍN MAZZUCCONI, C.: «Nuevas tecnologías y Relaciones Laborales», *Aranzadi*, 2002.
- TALENS VISCONTI, E.E. «La desconexión digital en el ámbito laboral: un deber empresarial y una nueva

oportunidad de cambio para la negociación colectiva», *Revista de información Laboral*, núm. 4, 2018.