



Universidad de Valladolid



Facultad de Derecho

MÁSTER de ACCESO a la ABOGACÍA

Sobre una hipotética demanda ante el TEDH en relación con el control de los correos electrónicos en el ámbito laboral

Presentado por:

Javier Revilla Rodríguez

Tutelado por:

Juan María Bilbao Ubillos

Valladolid, 30 de diciembre de 2020

RESUMEN

El presente Trabajo de Fin de Máster consiste en un dictamen jurídico acompañado de un análisis de la más reciente doctrina y jurisprudencia relativa a la protección del derecho al respeto a la vida privada y familiar (artículo 8 CEDH), tanto en el entorno jurídico español, como en el del Consejo de Europa. Para ello, se ha tomado en cuenta la doctrina relativa al control de correos electrónicos por parte de la empresa en el entorno laboral.

PALABRAS CLAVE

Vida Privada – Artículo 8 CEDH – Correo electrónico – Intimidad – Secreto de las comunicaciones
Proceso equitativo – Artículo 6 CEDH – Jurisdicción social – Derechos fundamentales

ÍNDICE

1.	INTRODUCCIÓN	4
2.	DICTAMEN JURÍDICO.....	5
2.1	Objeto del dictamen.....	5
2.2	Antecedentes de hecho.....	6
2.3	Fundamentos, normativa y jurisprudencia	9
2.3.1	El artículo 8 del CEDH: el derecho a la vida privada en la jurisprudencia del TEDH.....	9
2.3.2	Límites del derecho a la vida privada en el ámbito laboral a la luz de la jurisprudencia del TEDH.....	12
2.3.2.1	Incidencia de la jurisprudencia del TEDH en la jurisprudencia española	22
2.3.3	Vulneración del artículo 6 CEDH y doctrina jurisprudencial del TEDH al respecto.....	26
2.3.4	Aplicación de la doctrina establecida por el TEDH al despido de mi cliente.....	28
2.4	Íter procesal.....	34
2.5	Cuestiones adicionales	35
3.	CONCLUSIONES.....	36
4.	BIBLIOGRAFÍA.....	38
4.1	Doctrina	38
4.2	Fuentes normativas	40
4.3	Jurisprudencia.....	41

1. INTRODUCCIÓN

El objeto del presente Trabajo de Fin de Máster, en esencia, no va a ser otro que trasladar a un supuesto práctico de carácter hipotético (una situación en la que se ve afectado el derecho a la vida privada en el ámbito laboral) la jurisprudencia del Tribunal Europeo de Derechos Humanos (en adelante, TEDH) en relación con la especial protección de dicho derecho, según lo previsto en el artículo 8¹ del Convenio Europeo de Derechos Humanos².

Para ello, en primer lugar, haré un análisis de la jurisprudencia del TEDH en torno a este precepto, pasando en un segundo momento a estudiar los límites del derecho a la vida privada en el ámbito laboral. Será en este punto donde se hará una breve referencia al conocido como “caso Barbulescu”³, génesis del cambio en el criterio jurisprudencial por parte del Tribunal de Estrasburgo. A continuación se dará cuenta del impacto que dicha alteración tuvo en el ordenamiento jurídico nacional, incidiendo especialmente en los criterios seguidos desde entonces tanto por el Tribunal Supremo como por el Tribunal Constitucional, así como las discrepancias que surgen en su aplicación en relación con los órganos judiciales de niveles inferiores de la jurisdicción social.

En tercer lugar, se planteará el caso hipotético con unos clientes ficticios, de características similares al caso previamente expuesto, a fin de estudiar su situación, y sopesar las posibilidades de éxito de una demanda a nivel supranacional, esto es, en el TEDH. En este punto serán objeto de estudio asimismo los requisitos de admisibilidad fijados por este Tribunal, cuyo afianzamiento deriva precisamente del caso Barbulescu.

A modo de conclusión, y una vez estudiados los antecedentes y la jurisprudencia relativa a la protección del derecho a la vida privada en el ámbito laboral, procederé a establecer un guion a seguir para mis mandantes, en relación con la viabilidad o no de acudir en defensa de sus intereses ante el TEDH.

¹ Artículo 8 CEDH: “1. *Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.*
2. *No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás*”.

² Convenio Europeo de Derechos Humanos, de 4 de noviembre de 1950, modificado por las disposiciones del Protocolo n° 14 (STCE n° 194) a partir de su entrada en vigor el 1 de junio de 2010.

³ STEDH de 12 de enero de 2016 y STEDH (Gran Sala) de 5 de septiembre de 2017

2. DICTAMEN JURÍDICO

El presente dictamen jurídico versa sobre un caso ficticio creado expresamente al objeto de ser analizado en el presente Trabajo de Fin de Máster.

2.1 Objeto del dictamen

El objetivo que se persigue con la elaboración y análisis del dictamen no es otro que apreciar la incidencia que ha tenido en el sistema judicial español la STEDH (Gran Sala), de 5 de septiembre de 2017 (*Barbulescu II*). Para ello, se ha intentado recrear una situación similar a la que tuvo lugar en los antecedentes de hecho del caso Barbulescu, en la que un trabajador fue despedido debido a que la empresa en la que desarrollaba sus funciones advirtió que usaba los medios informáticos de la misma con fines distintos a los laborales. El estudio se va a centrar en el refuerzo que supone el cambio en la doctrina del TEDH para la protección del derecho al respeto a la vida privada y familiar (artículo 8 CEDH). Se hará también especial hincapié en la amplitud de dicha protección en lo referente a las nuevas tecnologías, especialmente a los correos electrónicos.

En un primer momento se expondrán los antecedentes de hecho, a fin de conocer cuál es la situación que ha provocado que mi cliente se plantee llevar su caso al TEDH. A continuación, se procederá a considerar la normativa, doctrina y jurisprudencia que puedan sernos de utilidad a la hora de defender de los intereses de mi patrocinado. Tras ello, se expondrán los fundamentos jurídicos que avalan las pretensiones de mi mandante, finalizando con una breve síntesis referente al íter procesal, donde se recogerán las distintas instancias judiciales a las que se ha acudido, así como un apartado sumario de cuestiones adicionales.

Mi mandante es D. Álvaro Lesmes Plaza, empleado de la mercantil “LIA S.L.”, sita en Palencia, en la cual desarrollaba sus funciones como administrativo hasta el pasado 16 de octubre de 2017, momento en el que se le comunica su despido. A continuación, se exponen los antecedentes de hecho, basándome en una reunión mantenida en mi despacho profesional con el cliente, en la que me relata cómo se desarrollan los acontecimientos.

2.2 Antecedentes de hecho

PRIMERO.- Mi mandante, D. Álvaro Lesmes Plaza, viene prestando sus servicios en la empresa “LIA S.L.”, sita en Palencia, con una antigüedad reconocida desde el 17 de marzo de 2002, a través de contrato indefinido a tiempo completo.

SEGUNDO.- D. Álvaro ha prestado sus servicios para la empresa como administrativo/contable.

TERCERO.- En fecha 13 de octubre de 2018, mi mandante acude a su puesto de trabajo con puntualidad, como acostumbra a hacer. Al llegar a su oficina, comprueba que la CPU de su ordenador de sobremesa no se encuentra allí. Ante tal sorpresa, acude a hablar con la jefa de personal, quien le comunica que el director de la empresa quiere reunirse con él a la mayor brevedad posible. Tras ello, acude al instante al despacho, donde el director, D. Carlos Girón Melendo, le comunica que está suspendido de empleo y sueldo hasta nuevo aviso, sin darle más explicaciones, y que no acuda a trabajar de nuevo hasta que reciba una llamada suya.

CUARTO.- En fecha 16 de octubre de 2018, D. Álvaro recibe una llamada de D. Carlos, comunicándole que debe presentarse en la sede de la empresa inmediatamente. Al llegar al lugar, es nuevamente la jefa de personal la que le dice que acuda al despacho del director. Es en ese momento cuando D. Carlos le traslada a mi representado que ha sido objeto de una investigación debido al mal uso de los medios aportados por la empresa, ya que se ha averiguado que ha utilizado el correo de trabajo para comunicarse con otra sociedad que es competencia directa de LIA S.L. para concretar una reunión tras recibir una oferta de trabajo que mejora sus condiciones laborales, según se deduce del contenido de los mensajes. Además, se advirtió asimismo que D. Álvaro usaba el ordenador de la empresa para navegar en sus redes sociales, consultar los movimientos bancarios de su cuenta personal, e incluso para hacer compras online. En la propia reunión se le facilita a D. Álvaro una carpeta repleta de fotocopias, en las que aparecen transcritos los correos electrónicos, así como los movimientos de su cuenta bancaria y sus pedidos pendientes en una web online.

D. Álvaro era consciente de que no podía utilizar los medios de la empresa para fines distintos de los estrictamente laborales, ya que cuando firmó su contrato, en uno de los anexos se prohibía expresamente. A pesar de ello, en dicho documento no se explicita en ningún apartado que los trabajadores puedan ser objeto de investigaciones por parte de la

empresa en ese sentido, y mucho menos que pueda accederse al contenido de los mensajes de carácter privado intercambiados por los empleados. Por supuesto, tampoco se contempla la posibilidad de que la empresa supervise las transacciones bancarias de sus asalariados.

En el desarrollo de la reunión, el director le espeta de malas maneras que está muy disgustado con su actitud, e incluso le llega a manifestar lo siguiente: “*Vete a esa mi**da de empresa, a ver si te hundes tú con ella*”. Tras ello, le insta a irse de su despacho, diciéndole que recoja sus pertenencias y que no vuelva por allí. Esa misma tarde, mi mandante recibe un mensaje de texto del INSS, en el que se certifica el despido.

Tras esta primera reunión con mi mandante, y una vez recabados los datos necesarios, procedo a presentar papeleta de conciliación ante el Servicio de Mediación, Conciliación y Arbitraje de Palencia, como paso previo y preceptivo a la vía judicial laboral. El acto de conciliación, al que mi mandante prefiere no acudir tras otorgarme mediante poder su representación, concluye sin avenencia, puesto que D. Carlos, que acude a la misma como representante de la empresa requerida, no reconoce los hechos.

En fecha 18 de noviembre de 2018 se procede a interponer demanda ante los Juzgados de lo Social de Palencia, recayendo el asunto en el Juzgado de lo Social número 2. En dicha demanda se alega que se ha producido un despido del trabajador con vulneración de los derechos fundamentales; en concreto se entienden vulnerados los artículos 18.3 y 18.4 de la Constitución Española (así como el artículo 8 del Convenio Europeo de Derechos Humanos, lo cual tendrá relevancia en última instancia en la demanda que se presentará ante el TEDH).

La Sentencia del Juzgado de lo Social Número 2 de Palencia, de fecha 22 de febrero de 2019, desestima las pretensiones esgrimidas por esta parte, por lo que dentro del plazo otorgado a tales efectos, se viene a interponer recurso de suplicación ante el Tribunal Superior de Justicia de Castilla y León (Sala de lo Social). En esta ocasión, se procede por su parte a ratificar lo expresado en la Sentencia del Juzgado de lo Social, en fecha 17 de junio de 2019.

Tras consultar a mi mandante, y ante las dudas suscitadas por el nulo éxito obtenido en las anteriores instancias, me confirma que desea continuar luchando por lo que él cree que es justo, y en base a ello se interpone Recurso de Casación en fecha 25 de junio de 2019 (artículo 205 de la LJS⁴), el cual es de igual manera inadmitido.

⁴ Ley 36/2011, de 10 de octubre, reguladora de la jurisdicción social, cuyo artículo 205.1 expresa lo siguiente: “La

Entendiendo que existe efectivamente una vulneración de derechos fundamentales, como ya se ha expresado con anterioridad en este propio apartado (artículos 18.3 y 18.4 CE, así como el manido artículo 24), se interpone recurso de amparo ante el Tribunal Constitucional en fecha 14 de diciembre de 2019. Igualmente, el mismo es inadmitido el 2 de febrero de 2020 mediante Auto, arguyendo que no se aprecia tal vulneración de derechos fundamentales en nuestro asunto.

Ante tales hechos, me reúno de nuevo con mi mandante, exponiendo cuáles son las vías que nos quedan en última instancia. Una vez expuesta la doctrina en casos similares a los de mi mandante, D. Álvaro me autoriza para interponer demanda ante el Tribunal Europeo de Derechos Humanos, tras explicarle que es el órgano jurisdiccional europeo que vela por la protección de los derechos y libertades fundamentales plasmados en el Convenio Europeo para la protección de los Derechos Humanos, en base al principio de subsidiariedad, ya que solo puede intervenir cuando los Estados miembros no han cumplido con su obligación. Para ello, se invoca el artículo 34 CEDH⁵, interponiendo la demanda en fecha 13 de junio de 2020, aprovechando las medidas excepcionales adoptadas por el TEDH en materia de plazos para la presentación de solicitudes⁶.

Sala de lo Social del Tribunal Supremo conocerá, en los supuestos y por los motivos establecidos en esta Ley, de los recursos de casación interpuestos contra las sentencias y otras resoluciones dictadas en única instancia por la Salas de lo Social de los Tribunales Superiores de Justicia y por la Sala de lo Social de la Audiencia Nacional”.

⁵ Artículo 34 CEDH: “El Tribunal podrá conocer de una demanda presentada por cualquier persona física, organización no gubernamental o grupo de particulares que se considere víctima de una violación por una de las Altas Partes Contratantes de los derechos reconocidos en el Convenio o sus Protocolos. Las Altas Partes Contratantes se comprometen a no poner traba alguna al ejercicio eficaz de este derecho”.

⁶ El artículo 35 CEDH establece que no se puede recurrir al Tribunal hasta que se hayan agotado las vías de recurso internas, y en el plazo de seis meses desde la decisión interna definitiva. En este sentido, ante la situación de pandemia imperante en el mundo, y en concreto también en el continente europeo, se decidió prorrogar excepcionalmente el plazo por un periodo de un mes a partir del 16 de marzo de 2020, y posteriormente por dos meses más a partir del 16 de abril de , y hasta el 15 de junio de 2020, inclusive.

2.3 Fundamentos, normativa y jurisprudencia

2.3.1 El artículo 8 del CEDH: el derecho a la vida privada en la jurisprudencia del TEDH

En pleno siglo XXI, a nadie se le escapa que estamos en una convulsa etapa de cambios en la sociedad. La irrupción de las conocidas como TIC (Tecnologías de Información y Comunicación) ha supuesto un gran avance a nivel social, trayendo consigo un desarrollo únicamente comparable en la Historia reciente al acontecido a finales del siglo XVIII con la Revolución Industrial.

El Derecho, como no puede ser de otra manera, ha venido adaptándose progresivamente a toda esta batería de cambios, siempre a un ritmo diferente, con la cautela propia que caracteriza a la rama legislativa, ya que se limita a regular las novedades una vez que las mismas se hallan bien asentadas entre la ciudadanía, a fin de lograr el equilibrio entre todos los agentes que intervienen en el sector implicado.

En la situación concreta que nos atañe, nos centraremos en el tratamiento y protección de datos personales (y la libre circulación de los mismos), así como de la intimidad, de la vida privada y del secreto de las comunicaciones. En el ámbito comunitario, el Reglamento de la UE 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril, es el encargado de regular dicha materia, en sustitución de la derogada Directiva 95/46/CE (Reglamento General de Protección de Datos). La intención del legislador europeo al promulgar esta normativa no es otra que “...*impulsar un imponente desarrollo específico, legislativo y convencional, en el ámbito de las relaciones de trabajo para cada Estado miembros...*”⁷.

El artículo 88 del referido Reglamento⁸ viene a otorgar a los Estados miembros la capacidad de establecer normas más específicas para garantizar la protección de los derechos

⁷ Molina Navarrete, C: : “El derecho a la vida privada del trabajador en el Tribunal Europeo de Derechos Humanos: ¿diálogo o conflicto con la jurisprudencia nacional?”, *Temas Laborales*, n° 145, 2018, pp. 143 y ss.

⁸ Reglamento 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos y por el que se deroga la Directiva 95/46/CE

y libertades en relación con el tratamiento de datos personales de los trabajadores en el ámbito laboral a través de disposiciones legislativas, o bien mediante convenios colectivos, con especial incidencia en la transparencia del tratamiento, transferencia de datos dentro de grupos empresariales o UTE y en los sistemas de supervisión en el lugar de trabajo (siendo este último punto de especial relevancia para el supuesto que posteriormente se analizará pormenorizadamente, al igual que ya lo fuera en el caso “López Ribalda contra España”⁹).

El TEDH está erigiéndose como gran protagonista a la hora de velar por la protección de la esfera privada de los trabajadores. Si bien es cierto que el CEDH prevé en su artículo 8 que “...*toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia...*”, no se incluye ningún apartado específico relativo a los datos personales. El Consejo de Europa, a diferencia de la Unión Europea, ha optado por la opción de las denominadas “recomendaciones sectoriales”, que carecen de fuerza jurídica vinculante, encontrándonos aquí con una específica en materia de trabajo, que no es otra que la Recomendación CM/Rec (2015)5, de 1 de abril de 2015, relativa al tratamiento de datos personales en el entorno laboral. Pese a las carencias mencionadas, el TEDH se ha convertido en la punta de lanza en lo relativo a la protección de los datos personales y la vida privada en su conjunto, a base de asimilar como propia la evolución experimentada en tanto en la sociedad, como en los ordenamientos jurídicos de los Estados miembros.

Es preciso puntualizar que la tendencia a acotar detalladamente los límites del derecho que aquí nos ocupa ha ocasionado conflicto con los altos tribunales a nivel nacional, no siendo así con la máxima autoridad jurisdiccional comunitaria. En el caso concreto del Estado español, el Tribunal Constitucional y el Tribunal Supremo tienden a difuminar los límites de la esfera de la vida privada, ya que no se ha llegado a fijar un criterio uniforme a la hora de garantizar su protección, optando en unas ocasiones por una postura garantista, mientras que en otras se tiende a ampliar las facultades de vigilancia de quien por cuestión de su cargo las ostenta. A pesar de ello, en los estratos inferiores de nuestro orden jurisdiccional acostumbran a seguir la posición garantista del TEDH, ex artículo 10.2 y 96 CE. Esto suele traducirse en un especial amparo a la vida privada del trabajador, delimitando así el control del empresario, basándose siempre en el carácter especial de las relaciones de trabajo, y teniendo en cuenta en todo momento la subordinación de una parte respecto de la otra. Estas diferencias de criterios provocan modificaciones sustanciales en las sentencias cuando las mismas llegan a las más altas instancias a nivel nacional, por lo que la doctrina a

⁹ STEDH Caso López Ribalda contra España de 9 de enero de 2019 (Sala) y STEDH de 17 de octubre de 2019. Caso López Ribalda contra España (Gran Sala)

menudo advierte que sería conveniente fijar un criterio convergente, a fin de garantizar el respeto al derecho a la tutela judicial efectiva al evitar a las partes variaciones tan drásticas en función de la discrecionalidad de los distintos tribunales.

El artículo 8 CEDH consagra el derecho al respeto a la vida privada y familiar, estableciéndose en el segundo apartado del mismo que solo podrá verse limitado mediante intervención de la autoridad pública, y siempre que esté prevista en la ley en pro de la seguridad nacional, la seguridad pública, la protección de la salud...Es importante reseñar que el concepto de familia que actualmente contempla el TEDH se ha ampliado con el paso del tiempo, ya que se aleja del concepto de “familia tradicional”, ampliándolo a cualquier relación en la que se generen lazos de mutua dependencia análogos a los familiares. Por tanto, y como se analizará en un momento ulterior, se entiende que de acuerdo con la doctrina fijada por el TEDH en relación con la salvaguarda de este derecho, no existe motivo tasado alguno para que pueda producirse una intromisión del calibre de la ejecutada por LIA S.L. a la hora de controlar el contenido del correo electrónico de D. Álvaro.

Es habitual el consenso entre doctrina y jurisprudencia a la hora de afirmar que el objetivo primordial del artículo 8 CEDH no es otro que proteger a la persona frente a las injerencias arbitrarias de los poderes públicos. Dicha protección no se limita exclusivamente a un aspecto negativo, sino que es preceptivo tener en cuenta de igual forma las obligaciones positivas relativas al respeto a la vida privada. El Estado disfruta de cierto margen de apreciación a la hora de decantar la balanza en la batalla jurídica que se disputa entre los intereses en liza.

2.3.2 Límites del derecho a la vida privada en el ámbito laboral a la luz de la jurisprudencia del TEDH

En el supuesto de hecho que aquí nos ocupa, nos hallamos ante lo que comienza como un control rutinario por parte de la empresa respecto del uso de los medios que ésta aporta a los trabajadores, a fin de chequear que efectivamente solo son usados con fines laborales. Esta práctica es habitual en cualquier tipo de compañía, ya que se trata de probar el tiempo efectivo de trabajo de los empleados, comprobando que no se distraen consultando páginas ajenas a lo estrictamente relacionado con su desempeño profesional. A pesar de ello, estos controles acostumbra a no ser tan estrictos como en un primer momento podrían parecer, dado que frecuentemente los empleados aprovechan sus tiempos de descanso para consultar el correo personal u otras páginas web (ej.: prensa, redes sociales...), por lo que los controles tienden a ser laxos, y solo se llama al orden a los trabajadores que sobrepasan los límites de lo puramente ordinario.

Es importante reseñar que los trabajadores deben acceder desde un primer momento a que los medios electrónicos que la empresa pone a su disposición puedan ser objeto de control por parte de la misma. A pesar de que la existencia de esta nota de ajeneidad, es necesario que exista el consentimiento expreso a la hora de efectuar la supervisión. Esto es así debido a que, como señalan tanto la jurisprudencia nacional como la europea, armonizadas en este punto, el trabajador no abandona sus derechos relativos a la vida privada y a la intimidad “...en la puerta de la empresa...” cuando comienza su jornada laboral, sino que se trata de derechos inherentes a la persona.

Análisis de los límites

En lo que al ámbito laboral se refiere, no nos encontramos con un número elevado de mecanismos que pongan en jaque la intimidad o el derecho al disfrute de la vida privada del trabajador, lo que no es óbice para mencionar que el ejercicio del mismo puede verse modulado “...en la medida estrictamente imprescindible para el correcto y ordenado desenvolvimiento de la actividad productiva...”, según Sentencia del Tribunal Constitucional 99/1994, de 11 de abril. En palabras de Wilfredo Sanguinetti, “...la vigencia de los derechos fundamentales del ciudadano-trabajador constituye más un punto de partida que de llegada”. A pesar de los esfuerzos de la doctrina por delimitar el contenido laboral de los derechos fundamentales previstos en la Constitución, se trata de una tarea harto complicada, precisamente por tratarse de derechos con una estructura abierta e indeterminada. La actual jurisprudencia constitucional apuesta

en esta pugna entre dos pretensiones constitucionales por “...determinar cuál lo es más, por suponer una aplicación más intensa de los contenidos de la Constitución, estableciendo entre ambas (...) una jerarquía axiológica móvil, en tanto que referida al caso y susceptible, por tanto, de verse alterada en otro distinto”¹⁰. Esto es lo que hoy en día se conoce como test de proporcionalidad.

El uso no controlado y para fines personales de los medios facilitados por el empresario provoca cuantiosos daños al empresario: por un lado, un lucro cesante, ya que todo el tiempo que el trabajador dedica a esos fines no los está dedicando al trabajo propiamente dicho, y además puede provocar también distracciones en los compañeros. Además, estas conductas pueden perjudicar a la imagen de la empresa, especialmente cuando se envían correos desde direcciones corporativas y cuyo contenido no se corresponde con materia estrictamente laboral (puede ponerse incluso en jaque la seguridad de la empresa, si el correo contiene información confidencial que no debe ser conocida por la competencia o por posibles ciberdelincuentes que intervengan la información). En definitiva, “...con independencia de cuál sea el daño concreto que se valore, el interés del empresario puede verse comprometido por el uso irregular y abusivo de instrumentos informáticos y en sí misma dicha conducta constituir una transgresión de la buena fe contractual y un abuso de la confianza depositada en el trabajador, frente al cual se le reconoce al empresario capacidad de reacción, con medidas disciplinarias al uso (...), pero también la facultad de prevenir dichas conductas, mediante el ejercicio del poder de control de la actividad productiva”¹¹.

En cuanto a la relación existente entre la protección de la esfera privada de las personas y la repercusión que ello puede tener a la hora de contratar o despedir a un trabajador, la jurisprudencia del TEDH es uniforme en el sentido de tomar como referencia el puesto desempeñado por el mismo (esta característica tiene especial relevancia en los casos en los que existe una colisión de este derecho con la libertad religiosa, estableciéndose en el ámbito europeo que las empresas privadas pueden conminar al trabajador a cumplir una serie de exigencias profesionales relacionadas con su propia deontología, sin que ello impida en un momento posterior el preceptivo control por parte de la Justicia, en caso de que se denuncie una extralimitación en este sentido).

El contenido del artículo 8 abarca igualmente, en la esfera laboral, todas las llamadas telefónicas recibidas o efectuadas en el puesto de trabajo, como así lo establece la Sentencia del TEDH de 25 de junio de 1997 (caso Halford contra Reino Unido), y en relación con el

¹⁰ Sanguineti, W.: "Poderes empresariales y derechos de la persona del trabajador: el difícil equilibrio", Trabajo y Derecho, n° 7, 2018, pág. 3

¹¹ Cardona Rubert, M.B.: "Intimidad del trabajador y comunicaciones electrónicas según el Tribunal Constitucional", Revista Jurídica de los Derechos Sociales Lex Social, vol. 5, núm. 2/2015, pág. 36

desarrollo tecnológico anteriormente expuesto, la jurisprudencia viene a extender de igual manera dicha protección a los correos electrónicos, teniendo siempre en mente lo especial de la relación contractual, que permite al empresario realizar una serie de injerencias habilitadas por el carácter subordinado del trabajador frente al empleador, y que serían impensables en otros órdenes jurisdiccionales¹². Dentro del ámbito de protección se incluyen no solo los archivos de carácter personal del trabajador que se ubican en el ordenador, sino también los archivos de carácter temporal¹³.

El empresario es el titular de los medios de producción, y por ello se encuentra habilitado para establecer cuál es el uso que sus empleados deben darles, así como para fijar las sanciones que estime oportunas en el caso de que se produzcan irregularidades relacionados con su utilización, siempre ciñéndose al marco normativo imperante, a fin de evitar intromisiones relativas a derechos fundamentales de los trabajadores. Éstos deben de guardar en todo momento una “...*expectativa razonable de confidencialidad*...”¹⁴ respecto de sus comunicaciones, y es por ello por lo que son necesarias las advertencias previas cuando vaya a existir cualquier tipo de control sobre los medios de trabajo utilizados por los trabajadores y aportados por la empresa. En caso de no existir dicha advertencia, no puede llegar a derivarse “...*una anuencia tácita del control o el conocimiento de esa potestad de supervisión*...”¹⁵.

En este sentido, la Ley prevé una batería de límites en el ejercicio de la supervisión de la empresa, a fin de preservar la intimidad de los empleados en el uso de dispositivos electrónicos, así como frente a la utilización de sistemas de videovigilancia, de grabación de sonido en el puesto de trabajo, o incluso de sistemas de geolocalización. A este respecto, la propia Ley reconoce el derecho a la desconexión laboral, en consonancia con el artículo 18.4 CE¹⁶, además de la Sentencia del Tribunal Constitucional 94/1998, de 4 de mayo, y la 292/2000, de 30 de noviembre.

Hoy en día, las recomendaciones de los expertos en protección de datos para evitar

¹² STEDH, de 12 de enero de 2017, caso Saumier contra Francia

¹³ Aquí se incluyen las denominadas “cookies”, que permiten acelerar y agilizar la carga de las páginas web una vez que se han producido varias visitas, lo cual produce también injerencias en el ámbito de la privacidad, ya que es habitual que las compañías publicitarias rastreen las páginas que han visitado los usuarios, y con ello dirijan publicidad específica según sus preferencias.

¹⁴ Lluç Corell, F.J.: “El secreto de las comunicaciones en la empresa: el control empresarial del correo electrónico que utiliza el trabajador”, Elderecho.com, Tribuna 17 de enero de 2017, recuperado el 20 de diciembre de 2020 de <https://elderecho.com/el-secreto-de-las-comunicaciones-en-la-empresa-el-control-empresarial-del-correo-electronico-que-utiliza-el-trabajador>

¹⁵ Rodríguez Escanciano, S.: “Posibilidades y límites en el control de los correos electrónicos de los empleados públicos a la luz de la normativa de protección de datos”, en Revista Vasca de Gestión de Personas y Organizaciones Públicas, n.º. 16, 2019, pág.120

¹⁶ “La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos”.

sanciones o que las pruebas sean consideradas como no válidas por los tribunales se encaminan en el sentido de aconsejar a las empresas que acrediten que los empleados efectivamente conocen que su correo profesional puede ser revisado, mediante el envío periódico de recordatorios en los que se comunique la falta de confidencialidad de las comunicaciones mantenidas a través de este medio. En lo referido al acceso propiamente dicho, se aconseja “... no hacer una búsqueda indiscriminada en el correo que se esté revisando. En su lugar la compañía puede utilizar términos específicos de búsqueda o palabras clave que permitan encontrar lo que se está buscando¹⁷”.

Todos los avances tecnológicos han tenido igualmente una enorme influencia en el ámbito del empleo público. Desde la Administración pública tratan de aprovechar los mismos en aras de una mejoría en el funcionamiento y la transparencia de los servicios públicos, lo cual implica en la mayoría de ocasiones que los propios empleados públicos utilicen datos personales en el ámbito laboral (ej.: firma electrónica). Esto no hace sino provocar que sea realmente complejo discernir a la hora de separar la esfera privada y la pública. La situación política que atraviesa nuestro país impide un normal desarrollo legislativo en el Parlamento, por lo que muchas de las novedades que se propugnan en Europa en relación con la presente materia caen en saco roto al llegar a nuestro país, puesto que a la inestabilidad política se le suma ahora la crisis sanitaria, lo cual ralentiza sobremanera la adaptación de nuestro ordenamiento jurídico a las disposiciones que provienen de Europa. Pese a ello, la aprobación de la Ley Orgánica 3/2018¹⁸ extendió las recomendaciones comunitarias al ámbito laboral (incluyendo el funcionariado). Los principales principios y garantías establecidos en materia de protección de datos son: licitud, transparencia, finalidad, adecuación, pertinencia, exactitud y actualización, temporalidad, seguridad a través de la confidencialidad, cifrado, evaluación de impacto y responsabilidad proactiva. Dicha ley no hace sino consolidar la anhelada fijación de límites expresos al ámbito de control de los responsables administrativos, añadiendo dicha previsión en el artículo 14 del EBEP¹⁹.

La creciente importancia de las tecnologías en el ámbito laboral ha provocado incertidumbre en las partes implicadas en él, dado que los conflictos entre ellas son relativamente habituales en lo que a control empresarial y privacidad del empleado se refiere. En el contexto actual, el recelo al control se acentúa más si cabe. Todo ordenamiento

¹⁷ Cortés Domínguez, I.: “¿En qué casos puede la empresa revisar el “email” corporativo de sus empleados?”, Cinco Días, 19 de agosto de 2019

¹⁸ Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales

¹⁹ Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público

jurídico correspondiente a un país desarrollado como el nuestro posee, por supuesto, elementos que equilibran la ya de por sí desigual relación empleador-empleado, a fin de proteger al sujeto más débil. A pesar de ello, nuestro sistema, como la mayoría, es claramente deficitario, y la regulación habida en los convenios colectivos no hace sino agravar dicha problemática, ya que incluso en algunos sectores no hacen si ampliar la esfera de actuación del patrón. La ley no debe de velar solo por el respeto a la vida privada y las comunicaciones de los trabajadores, sino que debe de ampliar el espectro y custodiar todos y cada uno de los derechos fundamentales, a fin de evitar la instrumentalización del empleado, no abusando de las necesidades de la persona a cambio de aceptar condiciones abusivas a la hora de desempeñar el trabajo.

El trabajador, a la hora de desenvolverse en el ámbito laboral, debe preguntarse si, tomando como referencia la información que le ha facilitado el empleador, puede confiar en que se esté respetando su vida privada con todas las garantías. En el supuesto de que la política de la empresa excluyera de forma taxativa el uso para asuntos personales de un instrumento facilitado por la misma, informándole incluso de que existen elementos de control para verificarlo, la privacidad quedaría entonces aparcada, pero de una forma justificada.

El caso Barbulescu y el test Barbulescu

En lo referente a los límites del derecho a la vida privada en el ámbito laboral, es imprescindible citar la Sentencia del TEDH de 3 de abril de 2007²⁰, en la que se estima que, pese a que los dispositivos electrónicos cedidos a los trabajadores sean propiedad del empleador y se utilicen durante el tiempo de trabajo, los empleados mantienen en plenitud su derecho a la intimidad, exceptuando las injerencias consentidas por estos, y siempre que las mismas hayan sido debidamente informadas con anterioridad o cuenten con el adecuado fundamento normativo para su aplicación.

El supuesto de hecho del caso Barbulescu es el siguiente: el demandante, el señor Barbulescu, un ingeniero rumano, creó una cuenta de correo a petición de su empresa a fin de atender a preguntas realizadas por los clientes. Este empleado ya poseía con anterioridad, como es habitual, una cuenta de correo, pero de carácter personal. La política de la empresa prohibía el uso de los aparatos informáticos y electrónicos para fines personales, circunstancia que era conocida por Barbulescu, ya que firmó el Reglamento donde así se

²⁰ Sentencia del Tribunal Europeo de Derechos Humanos de 3 de abril de 2007, caso Copland contra Reino Unido

atestiguaba. Posteriormente, la empresa accedió al correo de empresa del empleado en cuestión, y le citaron a fin de que explicara por qué había usado los equipos de la empresa con fines distintos a los estrictamente laborales. Él esgrimió que solo los utilizó con fines profesionales, pero la empresa demostró (sin informarle de que habían accedido al contenido de las comunicaciones) que la mayoría de mensajes tenían como destinatarios a su novia y a su hermano. Por este motivo fue despedido.

Tras llevar el asunto a los tribunales rumanos y llegar hasta el TEDH, en una primera sentencia (STEDH de 12 de enero de 2016), conocida como *Barbulescu I*, se estimó que, efectivamente, una empresa podía vigilar e incluso leer los mensajes intercambiados por correo electrónico por sus trabajadores a través de aparatos propios de la sociedad, siempre que el objetivo fuera constatar que estos estaban cumpliendo las funciones encomendadas. Se entendía que sí que había existido una intromisión en la vida privada del señor Barbulescu, pero sin llegar a vulnerar el contenido del art. 8 del CEDH, entendiéndose que el control fue limitado y proporcionado. Este fallo causó una gran conmoción, puesto que se podía interpretar que se otorgaba al empresario una libertad aún mayor que la existente previamente a la hora de inmiscuirse en los derechos de los trabajadores. El voto particular emitido llegaba incluso a hablar de “*retroceso en la protección de los derechos fundamentales*” (Juez Pinto de Albuquerque).

Tras instar una revisión, la Gran Sala del TEDH modificó la línea seguida hasta dicho momento en relación con esta materia (STEDH, Gran Sala, de 5 de septiembre de 2017), en la llamada sentencia *Barbulescu II*, estimando las pretensiones del demandante por entender vulnerado el derecho a la vida privada y el secreto de las comunicaciones. A pesar de reafirmarse en el hecho de que la empresa puede revisar el contenido de los mensajes de los trabajadores en horario laboral siempre que estos sean emitidos o recibidos a través de medios de la empresa, y siempre que medie un aviso previo o una prohibición de uso personal, como era el caso. En el asunto concreto, los tribunales previos no habían entrado a examinar el hecho de que no fue avisado de la actividad de vigilancia concreta a la que fue sometido, solo conocía la prohibición general de no usar medios de la empresa para fines personales. Asimismo, tampoco se le comunicó al señor Barbulescu el motivo que originó la toma de medidas. Tampoco se tuvo en cuenta el hecho de que el empleador pudo haber utilizado medios menos intrusivos a la hora de acceder a las comunicaciones, ni que la acción con la que reaccionó la empresa fue la más rigurosa de todas, como fue el despido. A modo de conclusión, se argumenta que el derecho a la vida privada no se abandona en la puerta de la empresa cuando comienza la jornada laboral: si bien es cierto que puede ser limitado,

nunca pueden reducirlo a su mínima expresión (“*las instrucciones de un empleador no pueden reducir a la nada, anular, el ejercicio de la vida privada social en el lugar de trabajo*”)²¹.

La nota más positiva que se deduce de la sentencia *Barbulescu II* es la introducción, o mejor dicho consolidación, de un “instrumento técnico-jurídico”, el conocido como Test Barbulescu, de gran utilidad tanto para el legislador como para el juzgador nacional a la hora de fijar los requisitos para que una empresa pueda vigilar de forma legal las comunicaciones de sus trabajadores, basándose en los siguientes principios:

- Principio de transparencia: debe estar garantizada la información previa y concreta al empleado relativa a la posibilidad del empleador de supervisar la correspondencia y comunicaciones. Dicha comunicación debe ser siempre previa a la adopción de las medidas.
- Principio de causalidad real y seria: el empleador debe justificar los motivos en los que se ampara a la hora de adoptar las medidas de vigilancia.
- Principio de proporcionalidad: como ya se ha mencionado con anterioridad, debe ponderarse el nivel de intrusión en los derechos del trabajador que implican las medidas adoptadas. En esta línea, siempre debe optarse por la opción menos intrusiva, basándose en criterios de efectividad, y no de simplicidad a la hora de su ejecución. Asimismo, deben reservarse las sanciones más graves para situaciones extremas, en aras de preservar los derechos fundamentales del trabajador.
- Principio de efectividad de tutela: deben cumplirse las debidas garantías respecto del empleado, en especial si se trata de medidas intrusivas.

El TEDH reafirma en esta Sentencia su doctrina referida a las obligaciones positivas de los Estados miembros, ya que a pesar de que los hechos afectan a una sociedad de carácter privado, debe en todo momento garantizarse la expectativa de privacidad del ciudadano, incluyendo el ejercicio de la actividad profesional. En este sentido, y citando de nuevo la STEDH del caso Copland, se confirma que los correos electrónicos enviados o recibidos desde un medio proporcionado por el empresario también forman parte de la vida privada del empleado (“*comprende también la información derivada del seguimiento del uso personal de Internet*”). A pesar de que en el caso Barbulescu se había informado al trabajador

²¹ Bilbao Ubillos, J.M.: “La vida privada en el ámbito laboral”, en F.J. Matía / G. López de la Fuente (dirs), De la intimidad a la vida privada y familiar. Un derecho en construcción, Tirant lo Blanch, 2020, pág. 172

de que no podía utilizar el correo electrónico con fines privados, en ningún momento se le advirtió de que el contenido del mismo fuera a ser objeto de una investigación exhaustiva, ya que llegar a este extremo reduciría la vida privada y la intimidad del trabajador a la mínima expresión. El fin perseguido por la normativa empresarial a la hora de restringir el uso de los medios electrónicos cedidos a los asalariados para fines distintos de los laborales debe ser incentivar la productividad y el buen hacer de los trabajadores, evitando las distracciones que a menudo suele ocasionar el hecho de estar conectado a Internet (redes sociales, compras online, consultar la prensa...), así como “evitar un ataque a los sistemas informáticos de la empresa en caso de una actividad ilícita en la red”²². Esta supervisión no puede ser ilimitada, porque en ese caso el empresario estaría atentando contra la libertad y la intimidad de los trabajadores, pese a encontrarse bajo su dirección mientras dure la jornada laboral. En el caso concreto de Barbulescu, en ningún momento se llega a probar que el ingeniero pusiera en peligro la seguridad de su empresa.

Los objetivos perseguidos a la hora de fijar los criterios del test Barbulescu son los siguientes:

- Cada Estado miembro debe decidir unilateralmente los criterios que establece a la hora de proteger la vida privada de sus ciudadanos, si bien es competencia del Tribunal de Estrasburgo fijar las líneas maestras a seguir en lo referente a la naturaleza y al ámbito de aplicación de las obligaciones contraídas por los Estados miembros (“...al Tribunal le compete clarificar la naturaleza y el campo de aplicación de las obligaciones positivas de los mismos...”).
- Reforzar el respeto al derecho a la vida privada en las relaciones interpersonales y proteger los intereses que están en juego, a fin de que se dé cumplimiento a las obligaciones mencionadas en el apartado anterior (“... tales obligaciones no se cumplirán adecuadamente a menos que se asegure el respeto a la vida privada en las relaciones entre particulares y que se tengan en cuenta los intereses variados que deben ser objeto de protección...”).
- Los Estados miembros tienen la capacidad y la libertad de elegir el marco jurídico que va a reglar la capacidad de control del empresario en relación con las comunicaciones de carácter personal de sus subordinados mientras los mismos se encuentren en su puesto de trabajo, primando siempre el

²² Bilbao Ubillos, J.M.: “La vida privada en el ámbito laboral”, en F.J. Matía / G. López de la Fuente (dirs), De la intimidad a la vida privada y familiar. Un derecho en construcción, Tirant lo Blanch, 2020, pág. 171

respeto a las garantías mínimas establecidas para evitar los abusos derivados de la desigual relación entre las partes implicadas (“...ha de reconocérsele a los Estados un amplio margen de decisión para evaluar la necesidad de establecer un marco legal específico que regule las condiciones en las cuales un empresario puede decidir sobre las comunicaciones, electrónicas o no, de contenido personal de sus trabajadores en el centro de trabajo, pero la discrecionalidad del empresario no puede ser absoluta...”)²³.

La conclusión a la que llega la Gran Sala del TEDH es que las relaciones laborales deben basarse en la existencia de una confianza mutua entre los intervinientes, así como que el trabajador, en el momento en el que se le comunica que sus comunicaciones han sido objeto de una investigación, pueda cerciorarse de que dicho control ha sido realizado con las suficientes garantías, y que de no ser así, podrá acudir a los Tribunales en defensa de sus intereses.

A raíz de la consolidación de la nueva doctrina que se dio con la publicación de la sentencia del caso Barbulescu, el TEDH ha afianzado el uso del test en sucesivas ocasiones, como puede ser el caso Libert²⁴, en el que el denunciante, empleado de la sociedad francesa de ferrocarriles, se percató durante un periodo de tiempo en el que había sido suspendido de empleo y sueldo de que su ordenador había sido inspeccionado por la persona que le sustituyó, y que en dicho chequeo se había encontrado material pornográfico. En este supuesto, la intromisión había sido llevada a cabo por la propia autoridad pública, por lo que había que tener en cuenta las obligaciones positivas y negativas de Francia como Estado. Pese a que la normativa francesa impide cualquier tipo de injerencia en la vida privada de los trabajadores, quedó probado que la carpeta que contenía el contenido pornográfico tenía el nombre de “risas”, por lo que se entendió por parte del Tribunal que sí que era legítima una inspección de dicha carpeta, puesto que el fin último era comprobar que el contenido de ésta no guardaba ninguna relación con el desempeño propiamente dicho de su labor profesional, como finalmente sucedió. Así pues, se dictaminó que no existía una vulneración del artículo 8 del CEDH. Esta Sentencia también ha tenido una repercusión notable, dado que se entiende que el hecho de consultar los archivos “personales” (y no “privados”) del empleado no constituye una violación del respeto al derecho a la vida privada, precisamente por no ser identificados

²³ Cabeza Pereiro, J.: “El necesario cambio en la jurisprudencia constitucional sobre videovigilancia y control de mensajería electrónica de los trabajadores a la vista de la doctrina del TEDH”, Temas Laborales, nº 141, 2018, p. 30

²⁴ STEDH de 22 de febrero de 2018, caso Libert contra Francia

adecuadamente como privados, escudándose en la normativa interna francesa para diferenciar ambos conceptos. Lo que ha provocado dicha resolución es un paso atrás respecto de lo logrado con la Sentencia Barbulescu II, ya que parece que el trabajador queda a priori más expuesto con este nuevo cambio de criterio del Tribunal, dado que el uso del test encamina la doctrina a una solución más restrictiva.

La postura actual del TEDH es por tanto intermedia entre dos variantes contrapuestas, que no son otras que la que por una parte propugna que el control empresarial del uso de los medios es plenamente lícito, ya que se autoriza por parte del trabajador a ser objeto del mismo en el momento de la firma del contrato, y la que por otro lado esgrime que no puede exigirse un control pleno sobre las comunicaciones de los empleados, no siendo posible establecer una prohibición general de uso. Se determina por tanto por el Tribunal que para eliminar la expectativa de confidencialidad es preciso, “...*además del impedimento, la advertencia del control previa y clara en cuanto a la naturaleza de la supervisión, la existencia de motivos justificativos de dicho control y, cómo no en tanto materialización del principio de proporcionalidad, la utilización de aquellos medios menos intrusivos para la intimidad o el secreto de las comunicaciones*”²⁵.

La conclusión que se obtiene del análisis pormenorizado del cambio en la doctrina del TEDH es que el Tribunal de Estrasburgo ha optado por una vía más exigente a la hora de supervisar el control ejercido por los empleadores y por los propios Estados. En el caso concreto de nuestro país, es el legislador quien recibe una suerte de toque de atención, ya que a nadie se le escapa la excesiva laxitud presente en el artículo 20.3 del Estatuto de los Trabajadores, en lo que respecta a la escasa autoridad que infunden los Códigos de buenas prácticas desarrollados de forma interna por las empresas, así como el poco margen de maniobra que se deja en manos de la negociación colectiva. Escudándose en el pretexto de buscar una mejora en la confianza y en la credibilidad de la empresa, ésta se constituye como “...*la única fuente de legitimación (...) de la proyección que pueden alcanzar los derechos fundamentales en la empresa...*”²⁶, dando así origen en la mayoría de los casos a un margen de “*libertad residual*” del trabajador respecto del empresario. Así pues, el objetivo del TEDH es ahondar en la protección de los derechos de los trabajadores, en especial los referidos a la vida privada y el secreto de los comunicaciones, en una era patentemente

²⁵ Rodríguez Escanciano, S.: “Posibilidades y límites en el control de los correos electrónicos de los empleados públicos a la luz de la normativa de protección de datos”, en Revista Vasca de Gestión de Personas y Organizaciones Públicas, n.º. 16, 2019, pág.118

²⁶ Goñi Sein, J.L.: “Los derechos fundamentales inespecíficos en la relación laboral individual: ¿necesidad de una reformulación?”, en AA.VV.: Los derechos fundamentales inespecíficos en la relación laboral y en materia de protección social. XXIV Congreso Nacional de Derecho del Trabajo y de la Seguridad Social, Cinca, 2014, p. 44 y ss.

digital, lo cual acarrea y acarreará un copioso foco de conflictos a resolver por los tribunales nacionales²⁷.

2.3.2.1 Incidencia de la jurisprudencia del TEDH en la jurisprudencia española

Por lo general, un uso inadecuado del ordenador cedido por la empresa por parte del trabajador se constituye como causa de despido, según la jurisprudencia nacional. Pese a ello, los tribunales han venido fijando una serie de límites a la acción del empresario, en relación con una posible violación del artículo 18.3 CE, que a priori requiere autorización judicial previa en caso de querer realizar una intervención. Como regla general, son preferibles los controles indirectos, ya que “...*puede resultar suficiente un control de los datos externos como el destinatario o el asunto o de las horas totales de navegación atendiendo a la tarea profesional encomendada...*”²⁸, todo ello a fin de evitar intromisiones innecesarias o desproporcionadas en relación con las opciones de control de las que dispone el empleador. Asimismo, la sanción debe ser acorde a la gravedad de los hechos (afectación de la productividad, lapso de tiempo que abarcan las visitas...), y además debe existir el previo aviso al trabajador. En este sentido se pronuncia la Sentencia de la Sala de lo Social del TS²⁹, de 26 de septiembre de 2007, al declarar como improcedente el despido de un trabajador cuyo ordenador había sido objeto de control, y al que se le había detectado la existencia de virus informáticos “...*como consecuencia de la navegación por páginas poco seguras de Internet...*”, ya que “...*la empresa no podía recoger la información obrante en los archivos temporales y utilizarla con la finalidad que lo ha hecho...*”³⁰.

Pese a ello, tanto la Sentencia del TS 241/2012, de 17 de diciembre como la STS 170/2013, de 7 de octubre, entienden que el control del correo electrónico por parte del empleador es proporcional, y desestima los recursos de dos trabajadores. En la primera de ellas, dos trabajadoras instalaron una aplicación de mensajería en un ordenador de la empresa para verter comentarios despectivos hacia otros trabajadores, descubriéndose posteriormente su instalación y uso de forma casual. En esta ocasión la empresa llegó a acceder al contenido íntegro de los mensajes, por lo que podría existir una extralimitación en sus funciones de acuerdo a los criterios doctrinales actuales, pero en aquel momento no se entendió así, escudándose en la prohibición de instalar ese tipo de aplicaciones y en que

²⁷ Molina Navarrete, C.: “El poder empresarial de control digital: ¿nueva doctrina del TEDH o mayor rigor aplicativo de la precedente?” *IusLabor*, 3/2017, pp. 295 y 296

²⁸ Bilbao Ubillos, J.M.: op. cit., pág. 176

²⁹ Sentencia del Tribunal Supremo 6128/2007

³⁰ Bilbao Ubillos, J.M.: op. cit., pág. 178

el ordenador era de uso común para todos los trabajadores. En la segunda de las sentencias, se despidió a un trabajador que envió información delicada a la competencia mediante el correo de la empresa, al entender que el control del empresario era “previsible” y que no se trató de una medida desproporcionada, ya que existían “...*sospechas de un comportamiento irregular del trabajador...*”³¹.

Una vez expuestos los antecedentes, y a fin de examinar la repercusión que ha tenido la doctrina Barbulescu en nuestro país, se pasa a analizar someramente algunas de las sentencias más relevantes dictadas tras la sentencia Barbulescu II:

- Sentencia del Tribunal Supremo 594/2018, de 8 de febrero de 2018 (Sala de lo Social), caso Inditex: primera sentencia de entidad dictada por el Tribunal Supremo español, referenciando que los criterios defendidos por el TEDH en la sentencia Barbulescu II son coincidentes con los del propio TS en lo referido al control en el ámbito laboral: elementos de control, obligatoriedad de preaviso, alcance de la medida, causa, posibles alternativas menos lesivas o intrusivas para los intereses del asalariado, y consecuencias derivadas para el mismo. Pese a tratarse de una Sentencia en la que se estima que la conducta empresarial pasa holgadamente los requisitos que el TEDH exige para considerar como legítimo el control de la actividad de un trabajador, no se trata de un supuesto de hecho idéntico al de mi cliente, pues entiendo que en el caso de mi mandante sí se han sobrepasado los límites, por llevar a cabo no solo un control del contenido de los mensajes del correo electrónico, sino también de cuentas bancarias y de webs de comercio electrónico de carácter personal. Al margen de ello, el mero control de los contenidos sin que medie previo aviso podría ya sobrepasar los límites del derecho.
- Sentencia del Tribunal Supremo 489/2018, de 23 de octubre (Sala de lo Social): en este supuesto se considera como nula la prueba aportada por la empresa por no existir una advertencia previa del control al que iba a ser sometido, pese a demostrarse la existencia de un delito de apropiación indebida por parte de un empleado. El TS estima que la empresa podía haber advertido al trabajador de diversas maneras: una instrucción expresa que

³¹ Bilbao Ubillos, J.M.: op. cit., pág. 182

limitara el uso de medios, una previsión en el convenio colectivo, o la obtención del consentimiento del propio implicado. Dado que no se empleó ninguna de estas fórmulas, la expectativa de intimidad del demandado era mucho mayor de la que finalmente existió, por lo que a pesar de que existieran motivos para sospechar que la medida de control era adecuada y que se trataba de la medida menos invasiva, faltó uno de los elementos esenciales, que no es otro que el previo aviso al trabajador.

- Sentencia del TSJ de Castilla-La Mancha 1735/2019, de 11 de julio (Sala de lo Social): en el presente caso, la empresa interviene el ordenador corporativo de uno de sus trabajadores a fin de averiguar si lo utilizaba para fines distintos de los estrictamente profesionales. Pese a probar que navegaba en páginas de banca personal, restaurantes o noticias, no existió previo aviso referente a la medida de control efectuada por la empresa, la cual previamente no había abonado a este mismo empleado una paga extraordinaria, hecho por el cual fue demandada en otro procedimiento, y que a juicio del trabajador, fue lo que motivó que se practicara de forma tan repentina la medida de vigilancia.
- Sentencia del Juzgado de lo Social nº 2 de Palma de Mallorca 3055/2019, de 30 de agosto: en este caso, el juzgador avala el despido de una empleada que utilizaba en reiteradas ocasiones el ordenador de la empresa para acceder a sus redes sociales y para otros fines no laborales, mediando en este caso una prohibición expresa por parte de la empleadora mediante Anexo al contrato, así como el reparto de una circular informativa (comunicación constante con los trabajadores). La medida supera el filtro del test Barbulescu, toda vez que se entiende que era necesaria una comprobación exhaustiva de los accesos para averiguar si efectivamente llevaba a cabo un uso inadecuado. Además, únicamente se accede al historial de internet, y en unas fechas concretas. Al ser la empleada consciente de que su actividad puede estar siendo vigilada, y que lo que hace constituye una transgresión de la política de la empresa, no puede albergar una expectativa elevada de intimidad.

Queda claro que la sentencia del TEDH no ha supuesto una revolución doctrinal, sino que solo va a obligar a tener más en cuenta “...*el juicio de valoración, y exigir que los límites,*

*tanto al Estado como a los empleadores, sean reales, efectivos...*³². El TC y el TS no han hecho propios los condicionantes originarios del test de transparencia y proporcionalidad. La doctrina del TC aún asume que el consentimiento contractual es suficiente para crear una expectativa de control, así como que la existencia de una norma que prohíbe el uso personal del correo electrónico de la empresa supone la habilitación para un férreo control por parte del empresario, sin entrar en una ponderación casuística, como dictaminó el TEDH. A pesar de ello, el TC debe comprobar que “...”*se cumplen los tres escalones (necesidad, idoneidad y equilibrio sacrificio-garantía), de forma concreta, no abstracta...*”). De esta forma se garantiza, además de la protección de derechos fundamentales del empleado, la seguridad jurídica, favoreciendo en este sentido también al empresario a la hora de que éste puede conocer dónde se fijan los límites, lo cual no hace sino fomentar las buenas prácticas dentro de la relación contractual.

³² Molina Navarrete, C.: op. cit., pág. 294

2.3.3 Vulneración del artículo 6 CEDH y doctrina jurisprudencial del TEDH al respecto

En segundo lugar, se estudia una posible infracción del derecho al proceso equitativo (art. 6 CEDH³³), dado que los medios de prueba de los que se ha servido la parte contraria en la defensa de sus intereses son, a mi juicio, plenamente ilícitos, toda vez que en ningún momento se cumplió con el deber de información impuesto tanto en la ley nacional como por la propia jurisprudencia a nivel interno y europeo. La Sentencia del TEDH en el caso Zherdev contra Ucrania³⁴ estipula que no se puede excluir de una forma taxativa o absoluta las pruebas obtenidas vulnerando derechos fundamentales, sino que es preciso ahondar en un análisis de las circunstancias en cada supuesto, teniendo en cuenta asimismo el Derecho interno de cada Estado. En este sentido aporta mucha luz también la Sentencia del TEDH del caso Jalloh contra Alemania³⁵, en la que se establece el siguiente criterio: *“No le corresponde al tribunal determinar, como cuestión de principio, qué tipos concretos de pruebas (...) pueden ser admitidas o no (...). La pregunta a responder es si el procedimiento en su conjunto, incluida la forma en que se obtuvo la prueba, fue equitativo (...)”*.

Es en este punto donde entra en juego también el ya mencionado “test Barbulescu”, relativo a la admisibilidad o no de las pruebas en materia de vigilancia a los trabajadores en el ámbito laboral.

En lo que respecta al artículo 6.1 CEDH, el TEDH parte de que existe la posibilidad de excluir una prueba que se estima ilícita si se considera que no ha existido un proceso equitativo, pero sin que ello pueda ser considerado como un mandato. Es preceptivo que el Tribunal averigüe si el proceso en su conjunto ha sido equitativo, y es en este punto donde se valoran los métodos de obtención de las pruebas. En un primer nivel, el Tribunal analiza si en la obtención se ha vulnerado alguno de los derechos previstos en el Convenio (en el caso que nos ocupa, se estudiaría una afectación del artículo 8). En un segundo momento, se examina si la admisión o utilización de las pruebas ha afectado al derecho a un proceso

³³ Artículo 6.1 CEDH: *“Toda persona tiene derecho a que su causa sea oída equitativa, públicamente y dentro de un plazo razonable, por un Tribunal independiente e imparcial, establecido por ley, que decidirá los litigios sobre sus derechos y obligaciones de carácter civil o sobre el fundamento de cualquier acusación en materia penal dirigida contra ella. La sentencia debe ser pronunciada públicamente, pero el acceso a la sala de audiencia puede ser prohibido a la prensa y al público durante la totalidad o parte del proceso en interés de la moralidad, del orden público o de la seguridad nacional en una sociedad democrática, cuando los intereses de los menores o la protección de la vida privada de las partes en el proceso así lo exijan o en la medida en que sea considerado estrictamente necesario por el tribunal, cuando en circunstancias especiales la publicidad pudiera ser perjudicial para los intereses de la justicia”*.

³⁴ Sentencia del Tribunal Europeo de Derechos Humanos, de 27 de abril de 2017, caso Zherdev contra Ucrania

³⁵ Sentencia del Tribunal Europeo de Derechos Humanos, de 11 de julio de 2006, caso Jalloh contra Alemania

equitativo, incluyendo en este momento el análisis de los parámetros del ordenamiento jurídico nacional en cuestión, así como su adecuado manejo.

El Tribunal, en este momento, valora tres niveles de riesgo para el derecho a un proceso equitativo: *low risk* (riesgo bajo, donde se incluyen las violaciones del derecho a la intimidad, como en el presente supuesto), *high risk* (riesgo alto, que recoge la obtención de pruebas a través de tratos degradantes o inhumanos) y *so high risk* (grupo de riesgo más alto, referente a las pruebas obtenidas mediando torturas). Solo en el último de los supuestos se entiende que en todo momento se pone en jaque la equidad en el juicio, mientras que en los dos niveles inferiores, es necesario ponderar caso a caso (*balancing test*). En dicho test se ponderan factores relativos al desarrollo de los juicios en el ámbito nacional, como el medio de obtención de la prueba, la capacidad de defensa del perjudicado, la fiabilidad, la manera en que fue utilizada, la existencia de otras pruebas, o la gravedad del delito.

El artículo 6.1 del Convenio garantiza que el proceso judicial en el que se encuentran inmersas las partes sea equitativo, sin que existan dilaciones indebidas. La jurisprudencia del TEDH es pacífica en lo que respecta a acudir a este tribunal pretendiendo que se invaliden ciertos medios de prueba que se han considerado como adecuados en las instancias nacionales.

Como ya se ha mencionado previamente, el Tribunal no se considera competente a la hora de juzgar sobre hipotéticos errores de hecho o de derecho que hayan acontecido en el iter procesal nacional, salvo que, como se menciona en la STEDH⁷ de 27 de abril de 2017 (caso Zherdev contra Ucrania), exista una vulneración de derechos fundamentales. Todo ello guarda relación con la vulneración del artículo 8 CEDH, dado que si el Tribunal considera que los medios de prueba que se han utilizado en cualquier fase del procedimiento han vulnerado los derechos fundamentales de cualquiera de las partes (en el caso que nos ocupa los de la demandante), puede entrar a valorar cuán equitativo ha sido el procedimiento, y en base a ello, modificar la decisión judicial.

2.3.4 Aplicación de la doctrina establecida por el TEDH al despido de mi cliente

Una vez que nos encontramos ante el Tribunal de Estrasburgo, es importante fijar en el petitum las pretensiones de mi cliente. En primer lugar, y en consonancia con lo argumentado en las sucesivas instancias ante los Tribunales nacionales, se pide que se analice si efectivamente ha existido una transgresión del derecho al respeto a la vida privada (artículo 8.1 CEDH).

A continuación, se va a proceder a someter al ya archiconocido “test Barbulescu” el supuesto de hecho de mi mandante, D. Álvaro Lesmes Plaza:

1. ¿Ha sido informado el empleado de la posibilidad de que el empleador tome medidas para supervisar su correspondencia y otras comunicaciones?

Como ya se mencionó en los antecedentes de hecho, D. Álvaro era consciente en todo momento de que no podía utilizar los medios de la empresa para fines personales, dado que firmó un anexo en el que expresamente se contemplaba este punto. De lo que en ningún momento fue informado es de que el empresario podía utilizar medios con el objetivo de llevar a cabo este control, y menos sin que mediara ningún tipo de previo aviso. Llegados a este extremo, considero que no solo se ha excedido la sociedad en lo referente a la supervisión de uso por no existir el preceptivo aviso, sino que además ha superado con creces los límites de control del empresario, por haber supervisado conversaciones privadas, movimientos de la cuenta personal de mi mandante, sus webs de pedidos online, e incluso sus redes sociales, perteneciendo todos estos elementos a la esfera privada del demandante.

El Tribunal entiende que “...*la advertencia debe ser clara en cuanto a la naturaleza de la supervisión...*” y que “...*se debe informar sobre el establecimiento de la medida, con anterioridad a ser implementada...*”. Por tanto, no se ha cumplido por parte de la empresa con ninguno de los dos requisitos exigidos en este sentido.

2. ¿Cuál fue el alcance de la supervisión del empleador y el grado de intrusión en la vida privada del empleado?

A riesgo de ser repetitivo, se insiste en el desmesurado alcance de la supervisión llevada a cabo por la empresa, toda vez que el objetivo perseguido en origen no es otro que comprobar que el empleado únicamente utiliza los medios puestos a su disposición para fines estrictamente relacionados con el trabajo. Al descubrir durante la indagación, ya de por

sí indebida, que el empleado en concreto podría salir de la empresa para reforzar a la competencia, se produce un ánimo de venganza por parte de la mercantil a fin de provocar su despido antes de que él decida marcharse (extremo que por cierto nunca se llegó a verificar por parte de la empresa, ya que nunca preguntaron a mi cliente si deseaba cambiar de empresa). Es a raíz de estos hechos cuando se produce la mayor de las intromisiones en la vida privada de mi patrocinado, cuando no dándose por satisfechos con las averiguaciones efectuadas en relación con el correo electrónico, proceden a investigar los movimientos de la cuenta bancaria, las redes sociales y los pedidos efectuados online, lo cual está fuera de toda lógica, ya que ninguna relación guarda con los hechos que en su génesis iban a ser objeto de investigación.

El criterio seguido en Estrasburgo guarda relación con la parte de las comunicaciones que ha sido objeto de supervisión (en este caso ha excedido con creces lo que pudiera entenderse como normal en un control de este tipo), la extensión en el tiempo (hecho que se desconoce por esta parte, ya que en los informes aportados de contrario solo constan averiguaciones efectuadas en un día, pero no conocemos si se han efectuado en más días, y simplemente por no haber sido de interés a la hora de acreditar el despido, no fueron aportadas en la reunión mantenida entre el director y el empleado), así como el número de personas que han tenido acceso a los resultados de la investigación (a esta parte le consta que al menos el director y la jefa de personal conocen el contenido de la información obtenida).

3. ¿Ha presentado el empleador argumentos legítimos para justificar la vigilancia de las comunicaciones y el acceso a su contenido?

Nuevamente ahondamos en la teoría de que el empleador no ha justificado en ningún momento los motivos que le han llevado a ejercer un control de estas características, simplemente porque entendemos que no existen, más allá del enfado originado tras descubrir en un control ya de por sí excesivo que mi cliente había recibido una oferta de la competencia que no podía ser igualada por LIA S.L. Desconoce esta representación si era habitual que por parte de la empresa se realizaran controles en los correos electrónicos de los trabajadores, ya que como se ha mencionado con anterioridad, esta supervisión ya excede del hecho de comprobar si los empleados usan los medios facilitados por la compañía para fines personales, puesto que esta es la única habilitación con la que contaban por su parte. De los hechos se deduce que de una averiguación casual, a la par que ilegal, se descubren acontecimientos privados que provocan la ira y la frustración del empresario.

El Tribunal entiende que la vigilancia de las comunicaciones ya es de por sí una metodología muy invasiva en relación con los derechos de los trabajadores, requiriendo para ello justificaciones bien cimentadas, extremo que como se deduce no ha sido en ningún caso probado por la empresa.

4. ¿Era posible un sistema de vigilancia basado en medidas menos intrusivas que el acceso directo a las comunicaciones del empleado?

En este caso, el empleador únicamente podía controlar que los medios aportados por la propia empresa no se utilizaran para fines ajenos al desempeño profesional en sí mismo, por lo que el simple hecho de revisar el historial habría bastado para comprobar este extremo. Existen programas informáticos capaces de recopilar el historial a pesar de que el usuario lo borre, por lo que entiende esta parte que un cribado de este tipo habría sido eficaz para alcanzar el fin deseado por la sociedad. Es importante hacer hincapié en el hecho de que mediante las medidas de vigilancia no solo se rastrean datos de navegación o los destinatarios de los mensajes de correo electrónico, sino que se accede al contenido propiamente dicho de los mismos, lo cual queda traspassa claramente los límites de control de la empresa. Las medidas tomadas son claramente intrusivas en lo que respecta a la vida privada del trabajador, porque se ha superado la barrera del consentimiento otorgado por el empleado al entrometerse en aspectos pertenecientes a la vida privada del demandante en estas actuaciones. No solo se produjo una supervisión telemática y no comunicada de los movimientos efectuados con el ordenador por mi mandante, sino que días antes de ser despedido, incluso se le interviene físicamente la CPU del dispositivo, privándole además de poder ejercer las funciones propias de su cargo profesional.

5. ¿Cuáles fueron las consecuencias de la supervisión para el trabajador afectado? ¿Fue dicha consecuencia proporcional a la invasión que dicha supervisión supone al ejercicio de la libertad protegida? ¿Sirvieron los resultados para alcanzar el objetivo declarado en relación con la medida?

En primer lugar, y en referencia a la primera cuestión planteada, la consecuencia fue en primer lugar la suspensión de empleo y sueldo a mi representado en los días que su equipo informático fue intervenido, sin que en ningún momento conociera cuáles eran los hechos que habían ocasionado tal sanción. Tras producirse la reunión con el director de la empresa, se le comunica que ha sido despedido: a nadie se le escapa que dicha medida es la más gravosa que puede tomarse contra un empleado, toda vez que conlleva la privación de ejercer su derecho al trabajo, así como de percibir el salario asociado a dicho desempeño. Tanto en

el Estatuto de los Trabajadores, como en cualquier convenio, esta medida se contempla como último extremo, en caso de que se haya apreciado, y lo que es más importante aún, probado, una infracción de carácter muy grave por parte del trabajador. En el presente caso, mi cliente no ha hecho sino cumplir con su cometido con la oportuna diligencia: si bien es cierto que en ocasiones utilizaba el ordenador para consultar su correo o su cuenta del banco, incluso para hacer pedidos a través de Internet, como ya se ha mencionado con anterioridad, es una práctica habitual entre los trabajadores de oficina en los descansos de los que disfrutaban, por lo que en ningún caso se puede tachar como muy grave esta conducta. Es más, al entender esta parte que el motivo real que provoca el despido es el hecho de haber recibido una oferta de trabajo por parte de la competencia, la actuación del empresario sería aún más grave si cabe, puesto que mi patrocinado no solo no puede controlar qué remitentes pueden ponerse en contacto con él a través del correo electrónico, sino que como ya se ha referido, en ningún momento comunicó a la empresa su intención de aceptar la oferta transmitida.

En relación con la última de las cuestiones, me corresponde poner de manifiesto que es obvio que no se ha cumplido con el objetivo perseguido de contrario con la vigilancia planeada. Por un lado, al entender que el fin de la empresa era castigar de alguna forma el hecho de que D. Álvaro recibiera ofertas por parte de otras compañías rivales, no han conseguido su objetivo, puesto que en la actualidad se encuentra desempeñando su profesión en una de ellas, y con mejores condiciones, dicho sea de paso. Por otro lado, si el propósito perseguido era efectivamente controlar el uso de los ordenadores por parte de los trabajadores, se podría aceptar que sí consiguieron su meta, pero sin imponer de ninguna manera una sanción acorde a los hechos castigados, toda vez que como ya se ha expuesto, es una práctica habitual entre los empleados, y este es un hecho que los propios empresarios conocen, y en ningún caso mi mandante excedía el tiempo de uso para fines alternativos de los medios de la empresa, ya que en todo momento desarrolló sus funciones de manera ejemplar, sin constar en su expediente sanción alguna hasta el momento del despido, en una trayectoria de casi 17 años en LIA S.L.

En relación con las pruebas, entiendo que teniendo en cuenta los hechos, el Tribunal declare como nulas las presentadas de contrario en las instancias nacionales para justificar el despido del trabajador, y no por el hecho de que las mismas sean extremadamente dañosas en relación con los intereses y derechos de mi mandante, que pudiera entenderse que lo son (se entrará a valorar en profundidad en el siguiente apartado), sino por el hecho de que existía la posibilidad de realizar el control deseado de una forma mucho menos invasiva y

lesiva. El objetivo de la empresa era comprobar si D. Álvaro estaba utilizando los medios de la empresa para fines distintos de los estrictamente relacionados con su trabajo, y efectivamente comprobaron que así era, pero no contentos con ello, decidieron extralimitarse y analizaron el contenido de su correo, advirtiéndolo que había recibido una suculenta oferta de trabajo por parte de la competencia directa. En este momento la empresa se adentró en un peligroso camino, que no es otro que el de inmiscuirse en la vida privada del empleado, lo cual queda fuera del ya de por sí, a mi juicio, amplio poder de control del empresario. El colmo de tal vulneración fue imprimir el contenido de las conversaciones revisadas, y de los movimientos de banca efectuados de forma personal por mi representado, algo que a todas luces carece de sentido, y que constituye una vulneración plena del derecho al respeto a la vida privada, así como de la intimidad, por haberse adentrado de la misma forma en las redes sociales de mi patrocinado.

6.¿Al empleado se le ofrecieron garantías adecuadas, teniendo en cuenta que las medidas de intervención tenían carácter intrusivo?

En ningún momento se ha presentado ninguna clase de garantía al empleado, más allá de que en el momento en que firmó su contrato, allá por el año 2002, consintió que la empresa pudiera supervisar que los medios facilitados por la misma no se utilizaran para fines distintos del propio trabajo, sin que ello habilitara al empresario a controlar ni el contenido del correo electrónico, ni mucho menos de cuentas personales de ningún tipo. El empleado ha visto totalmente expuestos y vulnerados sus derechos al respeto a la vida privada y a la intimidad desde el momento en que por parte del director se ha procedido a acceder al contenido de mensajes de carácter privado, así como a movimientos de cuentas bancarias, siendo esta una intromisión de especial relevancia, por todo lo que conlleva conocer la situación financiera de una persona sin su consentimiento, así como poder comprobar cuáles son sus ingresos, y en qué se gasta el dinero. Además, al haber accedido a sus redes sociales, ha podido igualmente leer conversaciones privadas de todo tipo sin que mediara permiso, pudiendo conocer datos íntimos y comprometidos de D. Álvaro.

En el supuesto de hecho en el que nos encontramos, la empresa, parte demandada en el presente caso, accedió al correo electrónico de D. Álvaro, por aquel entonces administrador contable de la misma, sin que en ningún momento mediase previo aviso. Tras ello, procedieron a analizar el contenido de los mensajes intercambiados, advirtiéndolo que mi

mandante había recibido una oferta de trabajo de la competencia, la cual mejoraba sustancialmente sus condiciones de trabajo y los consiguientes emolumentos. A juicio de la persona que suscribe estas líneas, la empresa, herida en su orgullo, decidió buscar cualquier resquicio que permitiera justificar el despido del trabajador, y procedió a examinar sus redes sociales, sus movimientos de la cuenta bancaria, e incluso las compras efectuadas en una página web. En el momento de la reunión con el empleado, intentando justificar el despido en un mal uso de los medios de la empresa, incluso llegaron a imprimir mensajes privados y un listado con los movimientos financieros privados de su asalariado.

Poniendo como ejemplo el ya aludido “caso Inditex”, en el que un empleado recibió importantes sumas de dinero por parte de un cliente de la multinacional a modo de recompensa, se encuentra una diferencia sustancial a la hora de aportar medios de prueba: mientras que la empresa LIA S.L. hizo una averiguación ex profeso del contenido del correo de mi mandante, para posteriormente ampliar la misma a todo su historial de búsqueda, en el supuesto de Inditex se trató de una averiguación fortuita por parte de otro empleado. Por tanto, en dicha ocasión sí que se entienden como adecuados los medios de prueba, toda vez que no se ha traspasado la barrera de la vulneración de derechos fundamentales, como pueden ser el derecho al respeto a la vida privada o el derecho a la intimidad.

Queda plenamente constatado que la intromisión en la vida privada de mi representado es plenamente injustificada y contraria a Derecho, por lo que el despido es contrario a la normativa vigente en el ámbito europeo, por existir una vulneración manifiesta de los derechos fundamentales, y más en concreto del respeto a la vida privada y de la intimidad de mi mandante, así como del secreto de las comunicaciones.

De esta forma, el objetivo perseguido al llegar a tan elevada instancia judicial es reforzar lo establecido en la sentencia *Barbulescu II*, en aras de afianzar la posición del trabajador frente a la injerencias indebidas del empresario, buscando una modificación a nivel legislativo en el Ordenamiento Jurídico español que por fin establezca unas garantías tasadas a la hora de respaldar el derecho a la intimidad y a la vida privada del empleado, más allá de lo ya previsto en la Constitución Española.

2.4 Íter procesal

1. En fecha 16 de octubre de 2018, el INSS comunica a D. Álvaro su despido por parte de la empresa LIA S.L.

2. En fecha 26 de octubre de 2018 se presenta la preceptiva papeleta de conciliación ante el Servicio de Mediación, Conciliación y Arbitraje de la Junta de Castilla y León, concretamente en la Oficina Territorial de Trabajo de Palencia, dentro del plazo de 20 días hábiles concedido a tales efectos por la Ley en materia de despidos

3. Una vez celebrada la conciliación sin avenencia entre las partes, se interpone demanda ante los Juzgados de lo Social de Palencia en fecha 18 de noviembre de 2018, por ser esta ciudad el lugar de prestación de los servicios (así como el domicilio del demandado), cumpliendo con el mandato del artículo 10.1 de la Ley Reguladora de la Jurisdicción Social³⁶

4. En fecha 22 de febrero de 2019 se desestiman las pretensiones del demandante por parte del Juzgado de lo Social nº 2 de Palencia

5. En fecha 3 de marzo de 2019 se presenta recurso de suplicación ante el Tribunal Superior de Justicia de Castilla y León (Sala de lo Social, con sede en Burgos)

6. En fecha 17 de junio de 2019, el TSJCyL ratifica la sentencia del Juzgado de lo Social de Palencia

7. En fecha 25 de junio de 2019 se presenta Recurso de Casación ante la Sala de lo Social del Tribunal Supremo

8. En fecha 26 de septiembre de 2019 se comunica a esta parte la inadmisión del Recurso presentado ante el TS

9. En fecha 14 de diciembre de 2019 se interpone Recurso de Amparo ante el Tribunal Constitucional

10. En fecha 2 de febrero de 2020 se nos notifica que el Recurso ha sido igualmente inadmitido

11. En fecha 13 de junio de 2020 procedo a interponer demanda ante el Tribunal Europeo de Derechos Humanos

³⁶ Artículo 10.1 LRJS: “La competencia de los Juzgados de lo Social se determinará de acuerdo con la siguientes reglas: 1. Con carácter general será juzgado competente el del lugar de prestación de los servicios o el del domicilio del demandado, a elección del demandante(...)”.

2.5 Cuestiones adicionales

Consta en el Anexo, como Documento número 1, formulario de demanda ante el Tribunal Europeo de Derechos Humanos.

3. CONCLUSIONES

La doctrina más reciente del Tribunal Europeo de Derechos Humanos en referencia tanto a la obtención de medios de prueba y su ulterior validez, como a la protección del derecho al respeto a la vida privada y a la intimidad, en relación con el secreto de las comunicaciones, hace que recomiende a mi cliente presentar una demanda por entender que ha existido una vulneración de derechos previstos en el Convenio. Para ello he basado mi defensa en la jurisprudencia más reciente emanada desde Estrasburgo, tomando como elemento clave para mi caso el hecho de que mi mandante en ningún momento autorizó el acceso ni a su correo ni a las demás cuentas que fueron objeto de vigilancia por parte del empresario, lo cual es contrario a la línea seguida más recientemente en el ámbito europeo. Este tipo de injerencias no pueden tomarse a la ligera por los tribunales, dado que es habitual, y así lo han puesto de manifiesto numerosas sentencias, que en el panorama judicial nacional se tienda aún a proteger en exceso el poder de control del empresario sobre sus trabajadores. Es muy importante que se produzca un equilibrio entre los implicados, partiendo de que existe una relación de subordinación del asalariado respecto del empleador. El ejercicio del control por parte de éste último no puede entenderse, como diría Molina Navarrete, como una *“patente de corso, un auténtico poder general, casi indiscriminado, de acceso a los correos electrónicos de las personas empleadas, (...) como un genuino aval para el espionaje empresarial...”*³⁷ adaptada al mundo laboral, sino que es preciso remar, en mi opinión, en la dirección en la que lo están haciendo los tribunales europeos, que no es otra que la de ampliar el espectro de protección del trabajador en lo que a su intimidad se refiere en el momento en el que comienza su jornada laboral.

Esta reflexión me suscita no obstante numerosas dudas en el panorama actual, dado que la situación de pandemia ha provocado un aumento exponencial de personas que prestan sus servicios mediante el teletrabajo, incluyendo un cuantioso número de funcionarios. Me preocupa cuáles pueden ser los mecanismos de control que se pueden incorporar a la hora de supervisar la labor de los trabajadores cuando estos no acuden personalmente al puesto de trabajo, más si cabe cuando especialmente en nuestro país no estábamos preparados para un cambio tan drástico en el modelo productivo, toda vez que la legislación referida a esta materia se encuentra a mi juicio en una fase muy temprana de desarrollo, a pesar de que en los últimos meses se ha intentado acelerar a marchas forzadas su progresión.

³⁷ Molina Navarrete, C.: op. cit., pág. 290

Volviendo al tema central que es objeto del presente Trabajo, el objetivo perseguido llegando a una instancia tan inusual, y a priori cuasi desconocida para el letrado de a pie, es consolidar la doctrina en materia de admisión de pruebas cuando el proceso de obtención de las mismas suscita numerosas dudas, pero que en las instancias nacionales a menudo no son tenidas en consideración. Entiendo que la línea a seguir hoy en día, en un siglo XXI en el que afortunadamente la violencia y las torturas van quedando atrás, es la de no admitir como medios de prueba aquellos que de algún modo violentan cualquier clase de derecho fundamental. En el caso concreto, estimo que inequívocamente el Tribunal debe dar como cierto que los métodos utilizados por la demandada quiebran a la hora de ser considerados como legítimos, toda vez que únicamente gracias a ellos se justifica el despido de mi mandante. No puede admitirse que mecanismos de vigilancia que en origen persiguen alcanzar una finalidad digna, como puede ser la supervisión del adecuado uso de los medios informático facilitados por las empresas, acaben convirtiéndose en instrumentos orwellianos de represión, en un arma que el trabajador jamás pensaría en ver esgrimida por su propia empresa en aras de conseguir un despido que jamás debió darse, y que únicamente encuentra su verdadera base en una oferta de trabajo procedente de la competencia a un trabajador, y que nunca fue comunicada, pero tampoco aceptada.

En conclusión, entiendo que la demanda tiene todos los visos de ser estimada en su totalidad, a la vista de la reciente doctrina y jurisprudencia que propugna una protección ampliada de los derechos de intimidad, protección de la vida privada y de secreto de las comunicaciones, por lo que recomiendo a mi cliente plantearla ante el TEDH por considerar vulnerados los artículos 6.1 y 8 del Convenio Europeo de Derechos Humanos.

4. BIBLIOGRAFÍA

4.1 Doctrina

- Bilbao Ubillos, J.M.: “La vida privada en el ámbito laboral”, en F.J. Matía / G. López de la Fuente (dirs), De la intimidad a la vida privada y familiar. Un derecho en construcción, Tirant lo Blanch, 2020, pp. 165-185
- Cabeza Pereiro, J.: “El necesario cambio en la jurisprudencia constitucional sobre videovigilancia y control de mensajería electrónica de los trabajadores a la vista de la doctrina del TEDH”, Temas Laborales, nº 141, 2018, pp. 30-34
- Cardona Rubert, M.B.: “Intimidad del trabajador y comunicaciones electrónicas según el Tribunal Constitucional”, Revista Jurídica de los Derechos Sociales Lex Social, vol. 5, núm. 2/2015, pp. 33-51
- Cortés Domínguez, I.: “¿En qué casos puede la empresa revisar el “email” corporativo de sus empleados?”, Cinco Días, 19 de agosto de 2019
- Goñi Sein, J.L.: “Los derechos fundamentales inespecíficos en la relación laboral individual: ¿necesidad de una reformulación?”, en AA.VV.: Los derechos fundamentales inespecíficos en la relación laboral y en materia de protección social. XXIV Congreso Nacional de Derecho del Trabajo y de la Seguridad Social, Cinca, 2014, p. 44 y ss.
- Lluch Corell, F.J.: “El secreto de las comunicaciones en la empresa: el control empresarial del correo electrónico que utiliza el trabajador”, Elderecho.com, Tribuna 17 de enero de 2017, recuperado el 20 de diciembre de 2020 de <https://elderecho.com/el-secreto-de-las-comunicaciones-en-la-empresa-el-control-empresarial-del-correo-electronico-que-utiliza-el-trabajador>
- Madrid-Boquín, Christa M.: “La prueba prohibida ante el Tribunal Europeo de Derechos Humanos: luces y sombras del Caso Zherdev c. Ucrania”, Revista de Estudios Europeos, nº extraordinario monográfico nº 1, 2017, pp. 78-93
- Molina Navarrete, C.: “El derecho a la vida privada del trabajador en el Tribunal Europeo de Derechos Humanos: ¿diálogo o conflicto con la jurisprudencia nacional?”, Temas Laborales, nº 145, 2018, pp. 143 y ss.

- Molina Navarrete, C.: El poder empresarial de control digital: ¿nueva doctrina del TEDH o mayor rigor aplicativo de la precedente? *IusLabor*, 3/2017, pp. 287-297
- Rodríguez Escanciano, S.: “Posibilidades y límites en el control de los correos electrónicos de los empleados públicos a la luz de la normativa de protección de datos”, en *Revista Vasca de Gestión de Personas y Organizaciones Públicas*, nº. 16, 2019, págs. 117-120
- Sanguinetti, W.: "Poderes empresariales y derechos de la persona del trabajador: el difícil equilibrio", *Trabajo y Derecho*, nº 7, 2018, pp. 1-7

4.2 Fuentes normativas

Nacionales

- Constitución Española (BOE número 311, de 29 de diciembre de 1978)
- Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial
- Ley 36/2011, de 10 de octubre, reguladora de la jurisdicción social
- Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores
- Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales

Europeas

- Convenio Europeo de Derechos Humanos, de 4 de noviembre de 1950, modificado por las disposiciones del Protocolo nº 14 (STCE nº 194) a partir de su entrada en vigor el 1 de junio de 2010
- Reglamento 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos y por el que se deroga la Directiva 95/46/CE

4.3 Jurisprudencia

Nacional

- Sentencia del Tribunal Supremo 6128/2007, de 26 de septiembre de 2007 (Sala de lo Social)
- Sentencia del Tribunal Supremo 594/2018, de 8 de febrero de 2018 (Sala de lo Social)
- Sentencia del Tribunal Supremo 489/2018, de 23 de octubre de 2018 (Sala de lo Social)
- Sentencia del TSJ de Castilla-La Mancha 1735/2019, de 11 de julio de 2019 (Sala de lo Social)
- Sentencia del Juzgado de lo Social nº 2 de Palma de Mallorca 3055/2019, de 30 de agosto de 2019

Comunitaria

- Sentencia del Tribunal Europeo de Derechos Humanos, de 11 de julio de 2006, caso Jalloh contra Alemania
- Sentencia del Tribunal Europeo de Derechos Humanos de 3 de abril de 2007, caso Copland contra Reino Unido
- Sentencia del Tribunal Europeo de Derechos Humanos de 12 de enero de 2016, caso Barbulescu I
- Sentencia del Tribunal Europeo de Derechos Humanos, de 12 de enero de 2017, caso Saumier contra Francia
- Sentencia del Tribunal Europeo de Derechos Humanos, de 27 de abril de 2017, caso Zherdev contra Ucrania
- Sentencia del Tribunal Europeo de Derechos Humanos (Gran Sala) de 5 de septiembre de 2017, caso Barbulescu II
- Sentencia del Tribunal Europeo de Derechos Humanos de 22 de febrero de 2018, caso Libert contra Francia
- Sentencia del Tribunal Europeo de Derechos Humanos, Caso López Ribalda contra

España de 9 de enero de 2.019 (Sala)

- Sentencia del Tribunal Europeo de Derechos Humanos de 17 de octubre de 2019, Caso López Ribalda contra España (Gran Sala)