

## Tribunal Europeo de Derechos Humanos

### TEDH (Gran Sala) Caso Barbulescu contra Rumania. Sentencia de 5 septiembre 2017

**DERECHO AL SECRETO DE LAS COMUNICACIONES: Secreto de las comunicaciones en el ámbito laboral: vigilancia en el marco de un proceso disciplinario de despido: interceptación y transcripción de mensajes electrónicos instantáneos personales en el lugar de trabajo constando prohibición expresa por parte de la empresa: falta de comprobación por los tribunales internos de si el empresario había notificado previamente al demandante la posibilidad de que sus comunicaciones en Yahoo Messsenger iban a ser controladas y de si había sido informado de la naturaleza y alcance de la vigilancia a la que iba a ser sometido así como del grado de intrusión en su vida privada y correspondencia: falta de justificación de los motivos concretos para la introducción de las medidas de control y si hubiera sido posible utilizar otras medidas menos intrusivas o el acceso al contenido de las comunicaciones sin su conocimiento: ausencia del justo equilibrio entre los intereses del empleador y el derecho del demandante al respeto de su vida privada: violación existente. OPINIONES DISIDENTES.**

ECLI:ECLI:CE:ECHR:2017:0905JUD006149608 Jurisdicción: Protección Europea de Derechos Humanos Demanda 61496/2008

El Tribunal Europeo de Derechos Humanos estima la demanda interpuesta por ciudadano rumano contra la República de Rumanía y revoca la sentencia dictada por la Sección Cuarta de este Tribunal en fecha 12 de enero de 2016 por considerar que ha existido violación del secreto de las comunicaciones en el despido del demandante por la utilización de mensajería instantánea para uso personal en el centro de trabajo.

En el asunto Bărbulescu contra Rumanía, El Tribunal Europeo de Derechos Humanos, reunido en Gran Sala compuesta por los siguientes jueces, Guido Raimondi, presidente, Angelika Nußberger, Mirjana Lazarova Trajkovska, jueces, Luis López Guerra, juez ad hoc, Ledi Bianku, Işıl Karakaş, Nebojša Vučinić, André Potocki, Paul Lemmens, Dmitry Dedov, Jon Fridrik Kjølbro, Mārtiņš Mits, Armen Harutyunyan, Stéphanie Mourou-Vikström, Georges Ravarani, Marko Bošnjak, Tim Eicke, jueces, así como Søren Prebensen, secretario adjunto de la Gran Sala,

Tras haber deliberado en Sala del Consejo el 30 de noviembre de 2016 y 8 de junio de 2017, Dicta la siguiente,

#### SENTENCIA

##### Procedimiento

1.- El caso tiene su origen en una demanda (núm. 61496/08) dirigida contra Rumanía, presentada ante el Tribunal el 15 de diciembre de 2008, por un ciudadano rumano, el señor Bogdan Mihai Bărbulescu (“el demandante”), en virtud del artículo 34 del Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales (RCL 1999, 1190, 1572) (“el Convenio (RCL 1999, 1190, 1572) ”)

2.- El demandante está representado por los señores E. Domokos-Hâncu y O. Juverdeanu, abogados ejercientes en Bucarest. El Gobierno rumano (“el Gobierno”) está representado por su agente, la señora C. Brumar, del Ministerio de Asuntos Exteriores.

3.- El demandante se queja, en particular, de que la decisión de su jefe de poner fin a su contrato se basó en una vulneración de su derecho al respeto de su vida privada y correspondencia,

garantizado por el artículo 8 del Convenio, y de que los tribunales nacionales no protegieron ese derecho.

4.- La demanda fue atribuida a la Sección Cuarta del Tribunal (artículo 52.1 del Reglamento del Tribunal (“el Reglamento”). El 12 de enero de 2016 (TEDH 2016, 1), una sala de dicha sección, compuesta por András Sajó, président, Vincent A. De Gaetano, Boštjan M. Zupančič, Nona Tsotsoria, Paulo Pinto de Albuquerque, Egidijus Kūris y Iulia Motoc, jueces, así como por Fatoş Araci, secretaria adjunta de sección declaró por unanimidad la admisibilidad de la queja en virtud del artículo 8 del Convenio (RCL 1999, 1190, 1572) . La opinión disidente del juez Pinto de Albuquerque se adjuntó a la sentencia de la sala.

5.- El día 12 de abril de 2016 el demandante solicitó la remisión del asunto a la Gran Sala en virtud de los artículos 43 del Convenio (RCL 1999, 1190, 1572) y 73 del Reglamento. El 6 de junio de 2016 el panel de la Gran Sala admitió dicha solicitud.

6.- La composición de la Gran Sala fue definida de conformidad con los artículos 26.4 y 26.5 del Convenio (RCL 1999, 1190, 1572) y 24 del Reglamento. Tras la recusación de Iulia Motoc, jueza electa por Rumanía (artículo 28 del Reglamento), Luis López Guerra fue designado por el Presidente para sentarse en calidad de juez ad hoc (artículo 26.4 del Convenio y artículo 29.1 del Reglamento).

7.- Tanto el demandante como el Gobierno, presentaron sus observaciones escritas complementarias (artículo 59.1 del Reglamento).

8.- Además se recibieron observaciones del gobierno francés y de la Confederación europea de sindicatos, a quienes el Presidente de la Gran Sala había autorizado a participar en el procedimiento escrito (artículos 36 .2 del Convenio (RCL 1999, 1190, 1572) y 44. 3 del Reglamento).

9.- Una audiencia pública se celebró en el Palacio de los Derechos Humanos de Estrasburgo el día 30 de noviembre de 2016 (artículo 59.3 del Reglamento)

Comparecieron:

- por el Gobierno

Sra. C. BRUMAR, agente,

Sr. G.V. GAVRILĂ, magistrado adjunto a la dirección del agente del Gobierno, asesor

Sra. L.A. RUSU, ministra plenipotenciaria a la representación permanente de Rumanía ante el Consejo de Europa, asesora ;

- por el demandante

Sres. E. DOMOKOS-HÂNCU, abogado,

O. JUVERDEANU, abogado, asesores.

Fueron oídas por el TEDH las declaraciones de los Sres Domokos-Hâncu y Juverdeanu, Sra. Brumar y Sr. Gavrilă así como sus respuestas a las preguntas planteadas por los jueces.

## **Hechos**

### **I. Circunstancias del asunto**

10.- El demandante nació en 1979 y reside en Bucarest.

11.- Del 1 de agosto de 2004 al 6 de agosto de 2007, trabajó para una empresa privada (de aquí en adelante “la empresa empleadora”) como ingeniero de ventas. A petición de su empresa, creó una cuenta Yahoo Messenger (servicio de mensajería en línea que ofrece una transmisión de texto en tiempo real en internet) con el fin de recibir y responder a preguntas de los clientes. El ya disponía de otra cuenta Yahoo Messenger personal.

12 El reglamento interno de la empresa prohibía la utilización por parte de los empleados de los recursos de la empresa en los siguientes términos:

#### **Artículo 50**

“Está estrictamente prohibido perturbar el orden y la disciplina en el recinto de la empresa y particularmente:

(...)

- (...) usar los ordenadores, fotocopiadoras, teléfonos, el télex y la máquina de fax con fines personales.”

13.- Este reglamento no incluía ninguna mención sobre la posibilidad de la empresa de vigilar las comunicaciones de sus empleados.

14.- Se desprende de los documentos presentados al expediente por el Gobierno que el demandante había sido informado del reglamento interno de la empresa, y lo había firmado, tras haberlo leído en fecha 20 de diciembre de 2006.

15.- El 3 de julio de 2007, la oficina de Bucarest recibió y distribuyó a todos los empleados una nota informativa (“la nota informativa”) redactada y enviada el 26 de junio de 2007 por la oficina central de Cluj. La empresa pidió a los empleados que leyeran la nota y la firmaran. En sus partes aplicables, la nota decía:

“1. (...) El tiempo que se pasa en la empresa debe ser tiempo de calidad para todo el mundo!!. Acudid al trabajo para ocuparos de los problemas de la empresa y profesionales, y no de los problemas privados!!. No paséis el tiempo en internet, hablando por teléfono o haciendo fotocopias de cuestiones que no competen a vuestro trabajo ni vuestras funciones. Estáis obligados a ello por [la educación elemental], el buen sentido y la ley!. La empresa se ve en la obligación de verificar y vigilar el trabajo de los empleados y de tomar las medidas oportunas contra los trabajadores en falta!

Vuestras faltas serán en la alternativa vigiladas y castigadas!

2. Debido a las continuadas faltas [de indisciplina cometidas] en contra de su superior, [así como] a la utilización que hizo de internet, del teléfono y de la fotocopiadora con fines privados, su negligencia e incumplimiento de sus funciones, la Sra. B.A. ha sido despedida por motivos disciplinarios! Tomad nota de este ejemplo negativo! No cometáis los mismos errores!

3. Leed atentamente el convenio colectivo, el reglamento interno de la empresa la descripción de vuestro puesto de trabajo y el contrato de trabajo que habéis firmado! Estos son la base de nuestra colaboración! Aquella entre la empresa y el trabajador!(...)”

16.- Asimismo, se desprende de los documentos presentados al expediente por el Gobierno, entre otros el registro de presencia de la empresa, que el demandante tuvo conocimiento de esta nota y la firmó entre el 3 y el 13 de julio de 2007.

17.- Se desprende asimismo, que, entre los días 5 y 13 de julio de 2007, la empresa registró en tiempo real las conversaciones del demandante en Yahoo Messenger.

18.- El 13 de junio de 2007 a las 16 h. 30, el demandante fue convocado por su director. La convocatoria le informaba de que se habían supervisado sus conversaciones en Yahoo Messenger y que ciertos elementos indicaban que había utilizado internet con fines personales, contrariamente al reglamento interno. Se adjuntaban gráficas que indicaban que su navegación por internet era superior a la del resto de sus colegas. En este momento no fue informado si la supervisión de sus comunicaciones también afectaba a su contenido. La convocatoria estaba redactada en los siguientes términos:

“Deberá explicar por qué utiliza los recursos de la empresa con fines personales (conexión a internet, Messenger) durante las horas de trabajo, tal y como demuestran los gráficos que se adjuntan.”

19.- Ese mismo día, el demandante respondió por escrito a su director que sólo había utilizado el Yahoo Messenger con fines profesionales.

20.- A las 17 h. 20 fue convocado por segunda vez. La convocatoria estaba redactada en los siguientes términos:

“Explique por qué toda la correspondencia intercambiada entre los días 5 y 12 de julio de 2007 utilizando el identificador en internet de S. Bucarest era de interés privado, como lo demuestran las 45 páginas que se adjuntan.”

21.- Las 45 páginas mencionadas en la convocatoria correspondían a la transcripción de las comunicaciones que el demandante había mantenido con su hermano y su novia durante el periodo que sus conversaciones estuvieron sometidas a vigilancia; dichas comunicaciones trataban de temas privados y algunas de ellas eran de carácter íntimo. La transcripción también contenía cinco mensajes breves que el demandante había intercambiado con su novia el 12 de julio de 2007 a través de una cuenta de Yahoo Messenger personal. Estos mensajes no revelaban información privada de ningún tipo.

22.- El mismo 13 de julio el demandante informó por escrito que consideraba a la empresa responsable de la comisión de un delito, es decir, la violación del secreto de correspondencia.

23.- El 1 de agosto de 2007 la empresa rescindió el contrato de trabajo del demandante.

24.- El demandante contestó la decisión de su despido ante el Tribunal del Condado de Bucarest (“el Tribunal del Condado”). Solicitó al tribunal en primer lugar la anulación de dicha decisión, en segundo lugar ordenar a la empresa empleadora pagarle las cantidades de sueldo y otros conceptos a las que consideraba tener derecho y la reincorporación a su puesto de trabajo, y en tercer lugar el pago de una indemnización por daños y perjuicios por un importe de 100.000 lei rumanos (alrededor de 30.000 euros) en concepto de daño moral que consideraba haber sufrido del hecho de su despido, y al pago de las costas.

25.- Sobre el fondo y en base a la sentencia Copland contra Reino Unido (TEDH 2007, 23) (núm. 62617/00, apds. 43-44, TEDH 2007-I), argumentó que las conversaciones telefónicas o por correo electrónico que un empleado realiza desde su puesto de trabajo están cubiertas por el

concepto de “vida privada” y “correspondencia”, y que por tanto gozan de la protección del artículo 8 del Convenio (RCL 1999, 1190, 1572). Asimismo mantenía la ilegalidad de la decisión de su despido y que al vigilar sus conversaciones y al acceder a su contenido, su empleador había infringido la legislación penal.

26.- Con respecto al daño moral que consideraba haber sufrido, el demandante recordaba el modo en que había sido despedido y alegaba haber sufrido un acoso que en su opinión se había visto materializado por la vigilancia de sus conversaciones y por la divulgación de su contenido entre “sus compañeros implicados de una u otra forma en el procedimiento de despido”.

27.- El demandante presentó al expediente a modo de prueba la copia integral de las transcripciones de sus conversaciones en Yahoo Messenger así como una copia de la nota informativa (ap. 15).

28.- En una sentencia de fecha 7 de diciembre de 2007, el Tribunal del Condado desestimó la queja del demandante y confirmó la legalidad de la decisión de despido. En sus partes aplicables, dicha sentencia establecía:

“El procedimiento sobre la conducta de la investigación disciplinaria se enmarca expresamente en las disposiciones del artículo 267 del Código del Trabajo.

En el presente asunto, ha quedado probado, por los documentos escritos presentados al expediente, que la empresa empleadora llevó a cabo la investigación disciplinaria contra el demandante convocándole en dos ocasiones por escrito y precisando el objeto, fecha, hora y lugar de la reunión, y que el demandante tuvo la posibilidad de presentar los argumentos en su defensa sobre los hechos que se le imputaban, como así lo demuestra la redacción de las dos notas explicativas aportadas al expediente (en copia en las páginas 89 y 91).

El tribunal estima que la validez del procedimiento disciplinario en el presente asunto no se ve menoscabada por el hecho de que las comunicaciones del [demandante] en Yahoo Messenger a través del ordenador de la empresa... durante horarios laborables fueran vigiladas - independientemente de la cuestión de saber si las acciones de la empresa empleadora pueden considerarse ilegales o no [desde el punto de vista del derecho] penal.

La redacción en términos imperativos de las disposiciones que imponen escuchar a una persona sospechosa de una falta y de examinar los argumentos que presenta en su defensa antes de decidir una sanción, demuestra que el legislador ha pretendido hacer del respeto a los derechos de la defensa una condición para la validez de la decisión de la sanción.

Sin embargo, puesto que el [demandante] alegó, durante el procedimiento disciplinario, que no utilizó Yahoo Messenger con fines personales sino para asesorar a los clientes en cuanto a los productos ofrecidos por su empresa, el tribunal estima que la única manera de comprobar la veracidad de la defensa del [demandante] era examinar el contenido de sus comunicaciones.

El derecho de la empresa empleadora de vigilar la manera en que los empleados usan los ordenadores de la empresa en el trabajo forma parte de su derecho más amplio de supervisar la forma en que efectúan sus tareas profesionales, regulado por las disposiciones del artículo 40d) del Código del Trabajo.

En la medida en la que la empresa recordó a los empleados, poco antes de que se impusiera una sanción disciplinaria al demandante que, otro empleado había sido despedido por haber hecho uso de internet, el teléfono y la fotocopiadora con fines personales, y les avisó de que serían

sometidos a medidas de vigilancia (véase la notificación núm. 2316 del 3 de julio de 2007, la cual comporta la firma del demandante, [tras haberla leído - en copia en la página 64], no se puede acusar a la empresa empleadora de haber obrado con falta de transparencia y de sinceridad en cuanto a su intención de vigilar el uso de los ordenadores por parte de sus empleados.

En el trabajo, los empleados deben poder tener acceso a internet. Es un instrumento que los gerentes proporcionan a los empleados con fines profesionales y no se puede negar que la empresa tiene derecho a mantener bajo control el uso de internet con fines personales, en virtud de su derecho a vigilar las actividades de los empleados.

Estos controles por parte de los gerentes son necesarios, inter alia, porque cabe la posibilidad de que, a través de su uso de internet, los empleados dañen los sistemas informáticos de la empresa, participen en actividades ilegales en nombre de la empresa, o divulguen secretos comerciales de la empresa.

El tribunal considera que los hechos cometidos por el demandante suponen una falta disciplinaria en el sentido de las disposiciones del artículo 263.2 del Código de Trabajo pues constituyen una violación de las disposiciones del artículo 50 del reglamento interno de S (...) que prohíbe el uso de los ordenadores por motivos personales.

Los hechos anteriormente mencionados son considerados, en virtud del reglamento interno, una falta grave sancionada conforme al artículo 73 del mismo reglamento con la rescisión del contrato por motivos disciplinarios.

Considerando los argumentos ya expuestos de hecho y de derecho, el tribunal concluye que la decisión impugnada está fundamentada y es legal, y desestima la acción del demandante como infundada.”

29.- El demandante interpuso recurso contra esta sentencia ante el Tribunal de Apelación de Bucarest (“el tribunal de apelación”). Repitió los mismos argumentos presentados ante el tribunal en primera instancia y mantuvo además que éste no había ponderado justamente los intereses en juego y había hecho prevalecer, de modo injusto, el interés del empleador de disponer discrecionalmente del tiempo y de los recursos de sus empleados. Alegaba asimismo, que ni el reglamento interno ni la nota informativa indicaban que el empleador pudiera vigilar las comunicaciones de sus empleados.

30.- El tribunal de apelación desestimó el recurso del demandante mediante sentencia de fecha 17 de junio de 2008. En sus partes aplicables la sentencia establecía:

“Es ajustado a derecho que la jurisdicción en primera instancia declarara que internet es un instrumento que el empleador pone a disposición del empleado para su utilización con fines profesionales y que el empleador está en su derecho de establecer las reglas de utilización de dicho instrumento, estableciendo prohibiciones y adoptando disposiciones que deben ser respetadas por los empleados en su lugar de trabajo; es evidente que la utilización por motivos personales debe ser rechazada, algo de lo que los empleados fueron debidamente informados mediante la nota emitida el día 26 de junio de 2007 en aplicación de las disposiciones del reglamento interno, instándoles a respetar los horarios de trabajo, permanecer en su lugar de trabajo durante estos horarios y utilizar eficazmente su tiempo de trabajo.

En conclusión, la empresa que ha realizado una inversión está en su derecho, en el marco del ejercicio de los derechos establecidos en el artículo 40.1 del Código de Trabajo, de vigilar ( monitoriza ) la utilización que se hace de internet desde el lugar de trabajo, y el empleado que

trasgreda las reglas del empleador sobre la utilización de internet con fines personales comete una falta disciplinaria que puede llevar consigo una sanción y en especial, la más grave de las sanciones.

Es cierto que existe un conflicto entre el derecho de la empresa a vigilar y el derecho de los empleados a la protección de su vida privada. Dicho conflicto se ha visto resuelto a nivel de la Unión Europea por la adopción de la Directiva 95/46/CE (LCEur 1995, 2977), que establece distintos niveles que regulan la vigilancia de la utilización de internet y del correo electrónico en los lugares de trabajo. Dichos principios son los siguientes:

- Principio de necesidad: la vigilancia (monitorizarea) debe ser necesaria para alcanzar un objetivo dado.
- Principio de finalidad: deben recogerse los datos con una finalidad específica, explícita y legítima.
- Principio de transparencia: el empleador debe proporcionar a los empleados todas las informaciones relativas a la vigilancia (monitorizare). - Principio de legitimidad: las operaciones de tratamiento de datos solo tendrán lugar con una finalidad legítima.
- Principio de proporcionalidad: los datos personales objeto de la vigilancia deben ser pertinentes y adecuados respecto a la finalidad indicada.
- Principio de seguridad: el empleador deberá tomar todas las medidas de seguridad al objeto de garantizar que los datos recogidos no sean accesibles a terceros.

Puesto que la dirección tenía el derecho y la obligación de garantizar el buen funcionamiento de la empresa y, a este efecto, [el derecho] de controlar la manera en que los empleados llevan a cabo sus tareas profesionales, y puesto que [la empresa] dispone de, y puede legítimamente ejercer el poder disciplinario que le [autoriza] a vigilar y transcribir las comunicaciones en Yahoo Messenger que su empleado negó haber intercambiado a fines personales, tras haber sido, junto con sus demás colegas, advertido de que estaba prohibido utilizar los recursos de la empresa para actividades personales, se puede considerar que la violación de la privacidad de la correspondencia era la única forma de alcanzar ese objetivo legítimo y que se mantuvo una ponderación adecuada entre la necesidad de proteger la vida privada del demandante y el derecho de la empresa de supervisar el buen funcionamiento de su negocio.

(...)

En consecuencia, dados los elementos presentados anteriormente, el tribunal declara que la decisión del tribunal de primera instancia es legal y fundamentada y que el recurso es infundado; conviene por tanto rechazarlo en aplicación de las disposiciones del artículo 312.1 del Código de Procesamiento Civil.”

31.- Entretanto, el 18 de septiembre de 2007, el demandante presentó una denuncia contra los representantes legales de S. por violación del secreto de correspondencia. El 9 de mayo de 2012 la Dirección de Investigaciones sobre la Delincuencia Organizada y el Terrorismo (DIICOT) del Ministerio Público del Alto Tribunal de casación y de justicia dictó una decisión de sobreseimiento debido a que la empresa era la propietaria del sistema informático y de la conexión a internet y que por tanto, podía controlar el tráfico de internet de sus empleados y utilizar las informaciones almacenadas en el servidor, considerando la prohibición de utilizar los sistemas informáticos con fines personales, prohibición que en su opinión, hacía posible la

vigilancia. El demandante no utilizó la posibilidad que le ofrecían las normas procedimentales vigentes de recurrir la decisión de la fiscalía ante los tribunales internos.

## **II. Legislación interna aplicable**

### **A. La Constitución**

32.- En sus partes aplicables, la Constitución rumana establece:

#### **Artículo 26**

“1. Las autoridades públicas respetan y protegen la vida íntima, familiar y privada.”

#### **Artículo 28**

“El secreto de cartas, telegramas y otros envíos postales, conversaciones telefónicas y otros medios legales de comunicación es inviolable.”

### **B. El Código Penal**

33.- En sus partes aplicables, el Código Penal en vigor en el momento en causa disponía lo siguiente:

#### **Artículo 195 - Violación del secreto de correspondencia**

“1. Todo individuo que abra ilegítimamente la correspondencia de otra persona o intercepte sus conversaciones o comunicaciones por teléfono, telégrafo u otro medio de transmisión a larga distancia podrá ser sometido a una pena de prisión de entre seis meses y tres años.”

### **C. El Código Civil**

34.- Las disposiciones aplicables del código civil en vigor en el momento en causa, disponían:

#### **Artículo 998**

“Cualquiera que cause a otro un daño por una falta, está obligado a repararle.”

#### **Artículo 999**

“Cualquiera es responsable del daño causado no solo por el hecho, sino por su negligencia o imprudencia.”

### **D. El Código del Trabajo**

35.- En su redacción en el momento de los hechos el Código del Trabajo disponía:

#### **Artículo 40**

“1. La dirección de la empresa tiene en principio los derechos siguientes:

(...)

d) controlar la manera en la que los empleados llevan a cabo sus tareas profesionales;

(...)

2. Corresponde a la empresa en principio las obligaciones siguientes:

(...)

i) garantizar la confidencialidad de los datos personales de sus empleados.”

### **E. La Ley núm. 677/2001 sobre la protección de individuos con respecto al tratamiento y a la libre circulación de datos personales**

36.- En sus parte aplicables, la Ley núm. 677/2001 sobre la protección de individuos con respecto al tratamiento y a la libre circulación de datos personales (“Ley núm. 677/2001”) que incorpora al ordenamiento jurídico rumano las disposiciones de la Directiva Núm. 95/46/EC de 24 de octubre de 1995 (LCEur 1995, 2977) del Parlamento Europeo y del Consejo de la Unión Europea, sobre la protección de individuos con respecto al tratamiento y a la libre circulación de datos personales (ap. 45), dispone:

#### **Artículo 3 – Definiciones**

“A los efectos de la presente ley se entiende por:

a) datos de carácter personal - cualquier información relativa a una persona física identificada o identificable ; una persona identificable es una persona que puede ser identificada directa o indirectamente, en especial por referencia a un número de identificación o a uno o varios elementos específicos, propios de su identidad física, psicológica, psíquica, económica, cultural o social; (...)”

#### **Artículo 5 - Condiciones de legitimidad del tratamiento de datos**

“1. Los datos de carácter personal (...) solo pueden ser objeto de algún tratamiento si la persona en cuestión lo ha consentido de manera expresa e inequívoca.

2. No es necesario el consentimiento de la persona en cuestión en los siguientes casos:

a) cuando se hace necesario el tratamiento para la ejecución de un contrato en el que el individuo en cuestión es parte o para la ejecución de medidas precontractuales tomadas a demanda de éste;

(...)

e) Cuando el tratamiento sea necesario para obtener el interés legítimo perseguido por el responsable del tratamiento o por los terceros a los que se comunican los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales de la persona en cuestión;

(...)

3. Las disposiciones del apartado 2 lo son sin perjuicio de las disposiciones legales relativas a la obligación de las autoridades públicas de respetar y de proteger la vida íntima, familiar y privada.”

#### **Artículo 18- Derecho de acudir a los tribunales**

“1. Las personas interesadas tienen el derecho, sin perjuicio de la posibilidad de presentar una denuncia a la autoridad de vigilancia, de acudir a los tribunales ante la vulneración de sus derechos, para obtener la protección de los derechos garantizados por la presente ley.

2. Toda persona objeto de un daño debido al uso ilícito de sus datos personales podrá acudir ante el tribunal competente para obtener una reparación (de su daño)

(...)”

### **III. Legislación y jurisprudencia internacional**

#### **A. Normas de Naciones Unidas**

37.- Los principios rectores para la reglamentación de los ficheros informatizados de datos personales adoptados por la Asamblea General el 14 de diciembre de 1990 en su resolución 45/95 (A/RES/45/95) plantean las garantías mínimas que deberían preverse en la legislación nacional. Disponen:

##### **“1. Principio de la licitud y lealtad**

Las informaciones relativas a las personas no se deberían recoger ni elaborar con procedimientos desleales o ilícitos, ni utilizarse con fines contrarios a los propósitos y principios de la Carta de las Naciones Unidas.

##### **2. Principio de exactitud**

Las personas encargadas de la creación de un fichero o de su funcionamiento deberían tener la obligación de verificar la exactitud y pertinencia de los datos registrados y cerciorarse de que siguen siendo lo más completos posibles a fin de evitar los errores por omisión y de que se actualicen, periódicamente o cuando se utilicen las informaciones contenidas en un expediente, mientras se estén procesando.

##### **3. Principio de finalidad**

La finalidad de un fichero y su utilización en función de esta finalidad deberían especificarse y justificarse y, en el momento de su creación, ser objeto de una medida de publicidad o ponerse en conocimiento de la persona interesada a fin de que ulteriormente sea posible asegurarse de que: a) Todos los datos personales reunidos y registrados siguen siendo pertinentes a la finalidad perseguida; b) Ninguno de esos datos personales es utilizado o revelado sin el consentimiento de la persona interesada, con un propósito incompatible con el que se haya especificado; c) El período de conservación de los datos personales no excede del necesario para alcanzar la finalidad con que se han registrado.

##### **4. Principio de acceso de la persona interesada**

Toda persona que demuestre su identidad tiene derecho a saber si se está procesando información que le concierne, a conseguir una comunicación inteligible de ella sin demoras o gastos excesivos, a obtener las rectificaciones o supresiones adecuadas cuando los registros sean ilícitos, injustificados o inexactos y, cuando esta información sea comunicada, a conocer los destinatarios. Debería preverse una vía de recurso, en su caso, ante la autoridad encargada del control de conformidad con el principio 8 infra. En caso de rectificación, el costo debería sufragarlo el responsable del fichero. Es conveniente que las disposiciones de este principio se apliquen a todas las personas, cualquiera que sea su nacionalidad o su residencia.

(...)

##### **6. Facultad de establecer excepciones**

Sólo pueden autorizarse excepciones a los principios 1 a 4 si son necesarias para proteger la seguridad nacional, el orden público, la salud o la moral pública y, en particular, los derechos y libertades de los demás, especialmente de personas perseguidas (cláusula humanitaria), a reserva de que estas excepciones se hayan previsto expresamente por la ley o por una

reglamentación equivalente, adoptada de conformidad con el sistema jurídico nacional, en que se definan expresamente los límites y se establezcan las garantías apropiadas.

(...)"

38.- La Oficina Internacional del Trabajo (OIT) elaboró en 1997 un repertorio de recomendaciones prácticas sobre la protección de datos personales de los trabajadores (repertorio de recomendaciones prácticas de la OIT") donde se enuncian los siguientes principios:

#### **"5. Principios generales**

5.1. El tratamiento de datos personales de los trabajadores debería efectuarse de manera ecuánime y lícita y limitarse exclusivamente a asuntos directamente pertinentes para la relación de empleo del trabajador.

5.2. En principio, los datos personales deberían utilizarse únicamente con el fin para el cual hayan sido acopiados.

5.3. Cuando los datos personales se exploten con fines distintos de aquéllos para los que fueron recabados, el empleador debería cerciorarse de que no se utilizan de un modo que sea incompatible con esa finalidad inicial y adoptar las medidas necesarias para evitar toda interpretación errada por causa de su aplicación en otro contexto.

5.4. Los datos personales reunidos en función de disposiciones técnicas o de organización que tengan por objeto garantizar la seguridad y el buen funcionamiento de los sistemas automatizados de información no deberían servir para controlar el comportamiento de los trabajadores.

5.5. Las decisiones relativas a un trabajador no deberían basarse exclusivamente en un tratamiento informático de los datos personales que a él se refieran.

5.6. Los datos personales obtenidos por medios de vigilancia electrónica no deberían ser los únicos factores de evaluación profesional del trabajador.

5.7. Los empleadores deberían evaluar periódicamente sus métodos de tratamiento de datos, con el objeto de: a) reducir lo más posible el tipo y el volumen de datos personales acopiados; y b) mejorar el modo de proteger la vida privada de los trabajadores.

5.8. Los trabajadores y sus representantes deberían ser informados de toda actividad de acopio de datos, de las reglas que la gobiernan y de sus derechos.

(...)

5.13. Los trabajadores no pueden renunciar a su derecho a proteger su vida privada."

39.- Con respecto a la vigilancia de los empleados, el repertorio de recomendaciones prácticas de la OIT prevé lo siguiente:

#### **"6. Acopio de datos personales**

6.1. En principio, el trabajador debería ser quien proporcione todos los datos personales.

(...)

6.14. (1) Cuando los trabajadores sean objeto de medidas de vigilancia, éstos deberían ser informados de antemano de las razones que las motivan, de las horas en que se aplican, de los métodos y técnicas utilizados y de los datos que serán acopiados, y el empleador deberá reducir al mínimo su injerencia en la vida privada de aquéllos.

(2) El secreto en materia de vigilancia sólo debería permitirse cuando:

a) se realice de conformidad con la legislación nacional;

o b) existan sospechas suficientes de actividad delictiva u otras infracciones graves.

(3) La vigilancia continua debería permitirse solamente si lo requieren la salud, la seguridad y la protección de los bienes.”

40.- Asimismo, el repertorio establece un inventario de derechos individuales de los trabajadores, especialmente en lo relativo a la información en cuanto al tratamiento de datos personales, al acceso a dichos datos y al control de estas medidas. Las partes aplicables disponen:

### **“11. Derechos individuales**

11.1. Los trabajadores deberían tener el derecho a ser informados con regularidad sobre los datos personales que les conciernen y sobre el tratamiento de éstos.

11.2. Los trabajadores deberían tener acceso a todos sus datos personales, independientemente de que sean objeto de un tratamiento automático o de que se conserven en un expediente manual o en cualquier otro fichero que comprenda datos personales suyos.

11.3. El derecho del trabajador a saber cómo se tratan sus datos personales debería comprender el de examinar y obtener copia de todos los expedientes, en la medida en que sus datos le conciernen.

(...)

11.8. En el caso de una investigación de seguridad, los empleadores deberían tener derecho a negar al trabajador el acceso a sus datos personales hasta el término de la misma y en la medida en que pueda menoscabar su objetivo. Con todo, no se debería tomar ninguna decisión sobre la relación de empleo antes de que el trabajador haya tenido acceso a todos sus datos personales.

11.9. Los trabajadores deberían tener derecho a exigir que se supriman o rectifiquen los datos personales inexactos o incompletos, así como los sometidos a una forma de tratamiento que vulnere lo estipulado en el presente repertorio.

(...)

11.13. Toda ley, reglamento, convenio colectivo, directiva laboral o política elaborada de conformidad con las disposiciones de este repertorio debería contemplar un procedimiento para que los trabajadores puedan poner en tela de juicio su observancia por parte del empleador. Deberían establecerse procedimientos para recibir y atender las quejas presentadas por los trabajadores. Estos procedimientos deberían ser sencillos y de fácil acceso para los trabajadores.”

41.- Asimismo, la Asamblea General de Naciones Unidas adoptó el 18 de diciembre de 2013 la Resolución núm. 68/167 sobre el derecho a la vida privada en la era digital (A/RES/68/167), donde exhorta a los Estados a que:

“a) Respeten y protejan el derecho a la privacidad, incluso en el contexto de las comunicaciones digitales;

b) Adopten medidas para poner fin a las violaciones de esos derechos y creen las condiciones necesarias para impedirlos, como cerciorarse de que la legislación nacional pertinente se ajuste a sus obligaciones en virtud del derecho internacional de los derechos humanos;

c) Examinen sus procedimientos, prácticas y legislación relativos a la vigilancia y la interceptación de las comunicaciones y la recopilación de datos personales, incluidas la vigilancia, interceptación y recopilación a gran escala, con miras a afianzar el derecho a la privacidad, velando por que se dé cumplimiento pleno y efectivo de todas sus obligaciones en virtud del derecho internacional de los derechos humanos;

d) Establezcan o mantengan mecanismos nacionales de supervisión independientes y efectivos capaces de asegurar la transparencia, cuando proceda, y la rendición de cuentas por las actividades de vigilancia de las comunicaciones y la interceptación y recopilación de datos personales que realice el Estado; [.]”

## **B. Normas del Consejo de Europa**

42.- El Convenio del Consejo de Europa para la protección de las personas respecto al tratamiento automatizado de los datos de carácter personal (RCL 1985, 2704) (1981, STE núm. 108) que entró en vigor para Rumanía el 1 de junio de 2002 prevé en particular lo siguiente:

### **Artículo 2 – Definiciones**

“A los efectos del presente Convenio:

a) “Datos de carácter personal” significa cualquier información relativa a una persona física identificada o identificable (“persona concernida”);

(...)

c) por “tratamiento automatizado” se entiende las operaciones que a continuación se indican efectuadas en su totalidad o en parte con ayuda de procedimientos automatizados: Registro de datos, aplicación a esos datos de operaciones lógicas aritméticas, su modificación, borrado, extracción o difusión;

(...)

### **”Artículo 3 - Ámbito de aplicación**

“1. Las Partes se comprometen a aplicar el presente Convenio a los ficheros y a los tratamientos automatizados de datos de carácter personal en los sectores público y privado. (...)

### **“Artículo 5 - Calidad de los datos**

Los datos de carácter personal que sean objeto de un tratamiento automatizado:

a) Se obtendrán y tratarán leal y legítimamente;

b) se registrarán para finalidades determinadas y legítimas, y no se utilizarán de una forma incompatible con dichas finalidades;

c) serán adecuados, pertinentes y no excesivos en relación con las finalidades para las cuales se hayan registrado;

- d) serán exactos y si fuera necesario puestos al día;
- e) se conservarán bajo una forma que permita la identificación de las personas concernidas durante un período de tiempo que no exceda del necesario para las finalidades para las cuales se hayan registrado.”

#### **Artículo 8 - Garantías complementarias para la persona concernida**

“Cualquier persona deberá poder:

a) Conocer la existencia de un fichero automatizado de datos de carácter personal, sus finalidades principales, así como la identidad y la residencia habitual o el establecimiento principal de la autoridad controladora del fichero;

b) obtener a intervalos razonables y sin demora o gastos excesivos la confirmación de la existencia o no en el fichero automatizado de datos de carácter personal que conciernan a dicha persona, así como la comunicación de dichos datos en forma inteligible;

(...)

d) disponer de un recurso si no se ha atendido a una petición de confirmación o, si así fuere el caso, de comunicación, de ratificación o de borrado, a que se refieren los párrafos b) y c) del presente artículo.”

#### **Artículo 9 - Excepciones y restricciones**

“(…)

2. Será posible una excepción en las disposiciones de los artículos 5, 6 y 8 del presente Convenio cuando tal excepción, prevista por la ley de la Parte, constituya una medida necesaria en una sociedad democrática:

a) Para la protección de la seguridad del Estado, de la seguridad pública, para los intereses monetarios del Estado o para la represión de infracciones penales;

b) para la protección de la persona concernida y de los derechos y libertades de los demás.. (…)”

#### **Artículo 10 - Sanciones y recursos**

“Cada Parte se compromete a establecer sanciones y recursos convenientes contra las infracciones de las disposiciones de derecho interno que hagan efectivos los principios básicos para la protección de datos enunciados en el presente capítulo.”

43.- La Recomendación CM/Rec (2015)5 del Comité de Ministros a los Estados miembros sobre el tratamiento de datos de carácter personal en el ámbito del trabajo, adoptada el 1 de abril de 2015, dispone lo siguiente:

4. Aplicación de los principios del tratamiento de datos

4.1. Los empleadores deberán vigilar que el tratamiento de datos de carácter personal se refiera únicamente a aquellos que sean estrictamente necesarios para alcanzar el objetivo determinado en los casos individuales.

(...)

6. Utilización interna de los datos

6.1. Los datos de carácter personal recogidos con fines de empleo solo podrán ser a tal fin.

6.2. Los empleadores deberán adoptar políticas de protección de datos, reglas y/o otros instrumentos relativos al uso interno de los datos de carácter personal conforme a los principios de la presente Recomendación.

(...)

## **10. Transparencia del tratamiento**

10.1. Las informaciones relativas a los datos de carácter personal obtenidas por los empleadores deben ser puestas a disposición del empleado afectado, bien directamente o por la intermediación de sus representantes, o bien ser puestas en su conocimiento por otros medios.

10.2. Los empleadores deben proporcionar a sus empleados las informaciones siguientes:

- las categorías de datos que serán tratados y una descripción de las finalidades del tratamiento;
- los destinatarios o categorías de destinatarios de dichos datos; - los medios de ejercer los derechos enunciados en el principio 11 de la presente Recomendación, sin desestimar medios menos favorables previstos en la legislación interna o en el sistema legislativo; - cualquier otra información necesaria para garantizar un tratamiento leal y lícito de los datos.

10.3. Debería proporcionarse una descripción especialmente clara y completa de las categorías de datos de carácter personal que pueden ser recogidas por medio del TIC, tales como la vigilancia, y su utilización potencial. Dicho principio vale para todas las formas particulares del tratamiento de datos de carácter personal previsto en la parte II del anexo de la presente Recomendación.

10.4. Deberán presentarse las informaciones de forma accesible y actualizada. Estas informaciones en cualquier caso, deben ser suministradas antes de que el empleado ejerza efectivamente la actividad o la acción prevista, y ser puesta a su disposición mediante los sistemas de información habitualmente empleados por el empleado.

(...)

## **14. Utilización de internet y de las comunicaciones electrónicas en el lugar de trabajo**

14.1. Los empleadores deben evitar la vulneración injustificada e irracional del derecho al respeto de la privacidad de los empleados. Este principio se aplica a todos los dispositivos técnicos y las TIC utilizadas por un empleado. Los interesados deberán ser correctamente y regularmente informados en virtud de una política clara en el respeto a la vida privada, de conformidad con el principio 10 de la presente Recomendación. La información proporcionada debe estar actualizada e incluir la finalidad del tratamiento, la duración de la retención de los datos recogidos, la copia de seguridad de los datos de inicio de sesión y el archivo de los mensajes electrónicos profesionales.

14.2. En lo referido en particular al posible tratamiento de datos personales en internet de páginas o de la intranet consultadas por el empleado, convendría preferentemente adoptar medidas preventivas, tales como la configuración de sistemas o la utilización de filtros que pueden impedir ciertas operaciones, y, por otra parte establecer eventualmente el control de los datos personales, preferentemente, de manera gradual y mediante sondeos no individualizados, mediante el uso de datos anónimos o, de alguna manera, agregados.

14.3. En cualquier caso, el acceso de los empleadores a las comunicaciones electrónicas profesionales de sus empleados, que habrán sido previamente informados de esta posibilidad, solo podrá suceder en caso de necesidad por razones de seguridad o por otros motivos legítimos. En ausencia de un empleado, los empleadores deberán tomar las medidas necesarias y establecer los procedimientos adecuados para permitir el acceso a las comunicaciones electrónicas profesionales, únicamente cuando dicho acceso sea necesario desde un punto de vista profesional. El acceso deberá producirse de la manera menos intrusiva posible y sólo después de informar a los empleados en cuestión.

14.4. En ningún caso deberán ser objeto de vigilancia el contenido, envío y recepción las comunicaciones electrónicas privadas en el marco del trabajo. 14.5. Cuando un empleado deja su trabajo, el empleador debería tomar las medidas necesarias técnicas y organizativas para que su mensajería electrónica se desactive automáticamente. Si fuera necesario recuperar el contenido de la mensajería para la buena marcha de la organización, el empleador debería tomar las medidas oportunas para recuperar su contenido antes de la marcha del empleado, y si fuera posible, en su presencia.

#### **IV. Legislación de la unión europea**

44.- Las disposiciones aplicables de la Carta de derechos fundamentales de la Unión europea (LCEur 2007, 2329) (2007/C 364/01) disponen:

##### **Artículo 7- Respeto de la vida privada y familiar**

“Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones.”

##### **Artículo 8 -Protección de datos de carácter personal**

“1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.

2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a su rectificación.

3. El respeto de estas normas quedará sujeto al control de una autoridad independiente

45.- La directiva 95/46/CE (LCEur 1995, 2977) de 24 de octubre de 1995 del Parlamento europeo y del Consejo de la Unión europea sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (“la Directiva 95/46/CE”), afirma que el objeto de las legislaciones nacionales relativas al tratamiento de datos de carácter personal es principalmente el de garantizar el respeto del derecho a la vida privada reconocido por el artículo 8 del Convenio (RCL 1999, 1190, 1572) y en los principios generales del derecho comunitario. Sus disposiciones aplicables disponen:

##### **Artículo 2 – Definiciones**

“A efectos de la presente Directiva, se entenderá por:

a) “datos personales “: toda información sobre una persona física identificada o identificable (el “interesado”); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios

elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social;

(...)

**“Artículo 6 1. Los Estados miembros dispondrán que los datos personales sean:**

- a) tratados de manera leal y lícita;
- b) recogidos con fines determinados, explícitos y legítimos, y no sean tratados posteriormente de manera incompatible con dichos fines; no se considerará incompatible el tratamiento posterior de datos con fines históricos, estadísticos o científicos, siempre y cuando los Estados miembros establezcan las garantías oportunas;
- c) adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente;
- d) exactos y, cuando sea necesario, actualizados; deberán tomarse todas las medidas razonables para que los datos inexactos o incompletos, con respecto a los fines para los que fueron recogidos o para los que fueron tratados posteriormente, sean suprimidos o rectificadas;
- e) conservados de una forma que permita la identificación de los interesados durante un período no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente. Los Estados miembros establecerán las garantías apropiadas para los datos personales archivados por un período más largo del mencionado, con fines históricos, estadísticos o científicos.

2. Corresponderá a los responsables del tratamiento garantizar el cumplimiento de lo dispuesto en el apartado 1.

**“Artículo 7 “Los Estados miembros dispondrán que el tratamiento de datos personales sólo pueda efectuarse si:**

- a) el interesado ha dado su consentimiento de forma inequívoca, o
- b) es necesario para la ejecución de un contrato en el que el interesado sea parte o para la aplicación de medidas precontractuales adoptadas a petición del interesado, o
- c) es necesario para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento, o
- d) es necesario para proteger el interés vital del interesado, o
- e) es necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero a quien se comuniquen los datos, o
- f) es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 del artículo 1 de la presente Directiva.

**“Artículo 8 - Tratamiento de categorías especiales de datos“**

1. Los Estados miembros prohibirán el tratamiento de datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad.

2. Lo dispuesto en el apartado 1 no se aplicará cuando:

a) el interesado haya dado su consentimiento explícito a dicho tratamiento, salvo en los casos en los que la legislación del Estado miembro disponga que la prohibición establecida en el apartado 1 no pueda levantarse con el consentimiento del interesado, o

b) el tratamiento sea necesario para respetar las obligaciones y derechos específicos del responsable del tratamiento en materia de Derecho laboral en la medida en que esté autorizado por la legislación y ésta prevea garantías adecuadas, o

c) el tratamiento sea necesario para salvaguardar el interés vital del interesado o de otra persona, en el supuesto de que el interesado esté física o jurídicamente incapacitado para dar su consentimiento, o

(...)

e) el tratamiento se refiera a datos que el interesado haya hecho manifiestamente públicos o sea necesario para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial.

(...)

4. Siempre que dispongan las garantías adecuadas, los Estados miembros podrán, por motivos de interés público importantes, establecer otras excepciones, además de las previstas en el apartado 2, bien mediante su legislación nacional, bien por decisión de la autoridad de control.”

46.- Se creó un grupo de trabajo sobre la protección de los datos (“el grupo de trabajo”) en virtud del artículo 29 de la directiva (LCEur 1995, 2977). Según el artículo 30 su misión será:

“a) estudiar toda cuestión relativa a la aplicación de las disposiciones nacionales tomadas para la aplicación de la presente Directiva con vistas a contribuir a su aplicación homogénea;

b) emitir un dictamen destinado a la Comisión sobre el nivel de protección existente dentro de la Comunidad y en los países terceros;

c) asesorar a la Comisión sobre cualquier proyecto de modificación de la presente Directiva, cualquier proyecto de medidas adicionales o específicas que deban adoptarse para salvaguardar los derechos y libertades de las personas físicas en lo que respecta al tratamiento de datos personales, así como sobre cualquier otro proyecto de medidas comunitarias que afecte a dichos derechos y libertades;

d) emitir un dictamen sobre los códigos de conducta elaborados a escala comunitaria.”

Este grupo es un órgano consultivo de la Unión europea y es independiente. En septiembre de 2001 presentó un informe sobre el tratamiento de los datos de carácter personal en el ámbito profesional (informe 8/2001) donde se resumen los principios fundamentales en el ámbito de la protección de datos: finalidad, transparencia, legitimidad, proporcionalidad, exactitud, seguridad e información del personal. En dicho informe, adoptado conforme a su mandato (contribuir a la aplicación homogénea de medidas nacionales tomadas en aplicación de la directiva 95/46/CE), precisó que la vigilancia de los correos electrónicos implicaba un

tratamiento de los datos de carácter personal, y consideró que la vigilancia de los trabajadores debía ser “una respuesta proporcionada del empleador a los riesgos que supone atentar contra la vida privada legítima y otros intereses de los asalariados”

47.- En mayo de 2002, el grupo de trabajo elaboró un documento de trabajo sobre la vigilancia de las comunicaciones electrónicas en el lugar de trabajo (en adelante “el documento de trabajo”) en el que se consideran expresamente las disposiciones de la directiva 95/46/CE (LCEur 1995, 2977) leídas al amparo de las disposiciones del artículo 8 del Convenio (RCL 1999, 1190, 1572)

En virtud de dicho documento, el simple hecho de que una actividad de control o de vigilancia sea considerada útil para el interés del empleador no justifica en sí misma la intrusión en la vida privada del trabajador, y toda medida de vigilancia debe responder a cuatro criterios: transparencia, necesidad, equidad y proporcionalidad.

48.- Con respecto al aspecto técnico, el documento de trabajo indica lo siguiente:

“Información rápida fácilmente publicable por un programa informático, por ejemplo, ventanas de advertencia que adviertan al empleado que el sistema ha detectado y tomado medidas para evitar una utilización ilícita de la red.”

49.- Más específicamente, con respecto a la cuestión del acceso a los e-mails de los empleados, el documento contiene el siguiente párrafo:

“La vigilancia del correo electrónico o de la utilización de internet de un empleado solo podría ser considerada necesaria en circunstancias excepcionales. Por ejemplo, la vigilancia del correo electrónico de un empleado puede considerarse necesaria para obtener la confirmación o la prueba de algunas de sus actuaciones. Dichas actuaciones debieran tener un carácter penal del empleado para que fuera necesario que el empleador defendiera sus propios intereses, por ejemplo, cuando es responsable de las acciones del empleado. Dichas actividades incluirían asimismo la detección de virus y, por regla general, cualquier actividad efectuada por el empleador para garantizar la seguridad del sistema. Conviene mencionar que la apertura de un correo electrónico de un trabajador puede considerarse igualmente necesaria por otras razones distintas que el control o la vigilancia, por ejemplo, para garantizar la correspondencia cuando se ausente el trabajador (por ejemplo, por enfermedad o en vacaciones) y que la correspondencia no puede garantizarse de otra forma (por ejemplo mediante las funciones de respuesta o de desvío automático).”

50.- El Tribunal de Justicia de la Unión Europea interpretó las disposiciones de la directiva 95/46/CE (LCEur 1995, 2977) a la luz del derecho al respeto de la vida privada tal como lo garantiza el artículo 8 del Convenio (RCL 1999, 1190, 1572) en el asunto *Österreichischer Rundfunk* y otros (TJCE 2003, 148) (C-465/00, C-138/01 y C-139/01, sentencia de 20 de mayo de 2003, ECLI:EU:C:2003:294, puntos 71 y siguientes).

51.- El Reglamento (UE) 2016/679 del Parlamento europeo y del Consejo de 27 de abril de 2016 (LCEur 2016, 605) relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la directiva 95/46/CE (LCEur 1995, 2977) (Reglamento general de protección de datos), publicado en el BO 2016 L 119/1, entró en vigor el 24 de mayo de 2016. Deroga la directiva 95/46/CE desde el 25 de mayo de 2018 (artículo 99).

Sus disposiciones aplicables disponen:

### **Artículo 30 - Registro de las actividades de tratamiento**

“1. Cada responsable y, en su caso, su representante llevarán un registro de las actividades de tratamiento efectuadas bajo su responsabilidad. Dicho registro deberá contener toda la información indicada a continuación:

- a) el nombre y los datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable, y del delegado de protección de datos;
- b) los fines del tratamiento;
- c) una descripción de las categorías de interesados y de las categorías de datos personales;
- d) las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales;
- e) en su caso, las transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49, apartado 1, párrafo segundo, la documentación de garantías adecuadas;
- f) cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos;
- g) cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 32, apartado 1.

2. Cada encargado y, en su caso, el representante del encargado, llevará un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de un responsable que contenga:

- a) el nombre y los datos de contacto del encargado o encargados y de cada responsable por cuenta del cual actúe el encargado, y, en su caso, del representante del responsable o del encargado, y del delegado de protección de datos;
- b) las categorías de tratamientos efectuados por cuenta de cada responsable;
- c) en su caso, las transferencias de datos personales a un tercer país u organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49, apartado 1, párrafo segundo, la documentación de garantías adecuadas;
- d) cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 30, apartado 1.

3. Los registros a que se refieren los apartados 1 y 2 constarán por escrito, inclusive en formato electrónico.

4. El responsable o el encargado del tratamiento y, en su caso, el representante del responsable o del encargado pondrán el registro a disposición de la autoridad de control que lo solicite.

5. Las obligaciones indicadas en los apartados 1 y 2 no se aplicarán a ninguna empresa ni organización que emplee a menos de 250 personas, a menos que el tratamiento que realice pueda entrañar un riesgo para los derechos y libertades de los interesados, no sea ocasional, o incluya categorías especiales de datos personales indicadas en el artículo 9, apartado 1, o datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10.

## **“Artículo 47 - Normas corporativas vinculantes”**

1. La autoridad de control competente aprobará normas corporativas vinculantes de conformidad con el mecanismo de coherencia establecido en el artículo 63, siempre que estas:

a) sean jurídicamente vinculantes y se apliquen y sean cumplidas por todos los miembros correspondientes del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, incluidos sus empleados;

b) confieran expresamente a los interesados derechos exigibles en relación con el tratamiento de sus datos personales, y

c) cumplan los requisitos establecidos en el apartado 2.

2. Las normas corporativas vinculantes mencionadas en el apartado 1 especificarán, como mínimo, los siguientes elementos:

a) la estructura y los datos de contacto del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta y de cada uno de sus miembros;

b) las transferencias o conjuntos de transferencias de datos, incluidas las categorías de datos personales, el tipo de tratamientos y sus fines, el tipo de interesados afectados y el nombre del tercer o los terceros países en cuestión;

c) su carácter jurídicamente vinculante, tanto a nivel interno como externo;

d) la aplicación de los principios generales en materia de protección de datos, en particular la limitación de la finalidad, la minimización de los datos, los periodos de conservación limitados, la calidad de los datos, la protección de los datos desde el diseño y por defecto, la base del tratamiento, el tratamiento de categorías especiales de datos personales, las medidas encaminadas a garantizar la seguridad de los datos y los requisitos con respecto a las transferencias ulteriores a organismos no vinculados por las normas corporativas vinculantes;

e) los derechos de los interesados en relación con el tratamiento y los medios para ejercerlos, en particular el derecho a no ser objeto de decisiones basadas exclusivamente en un tratamiento automatizado, incluida la elaboración de perfiles de conformidad con lo dispuesto en el artículo 22, el derecho a presentar una reclamación ante la autoridad de control competente y ante los tribunales competentes de los Estados miembros de conformidad con el artículo 79, y el derecho a obtener una reparación, y, cuando proceda, una indemnización por violación de las normas corporativas vinculantes;

f) la aceptación por parte del responsable o del encargado del tratamiento establecidos en el territorio de un Estado miembro de la responsabilidad por cualquier violación de las normas corporativas vinculantes por parte de cualquier miembro de que se trate no establecido en la Unión; el responsable o el encargado solo será exonerado, total o parcialmente, de dicha responsabilidad si demuestra que el acto que originó los daños y perjuicios no es imputable a dicho miembro;

g) la forma en que se facilita a los interesados la información sobre las normas corporativas vinculantes, en particular en lo que respecta a las disposiciones contempladas en las letras d), e) y f) del presente apartado, además de los artículos 13 y 14;

h) las funciones de todo delegado de protección de datos designado de conformidad con el artículo 37, o de cualquier otra persona o entidad encargada de la supervisión del cumplimiento

de las normas corporativas vinculantes dentro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, así como de la supervisión de la formación y de la tramitación de las reclamaciones;

i) los procedimientos de reclamación;

j) los mecanismos establecidos dentro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta para garantizar la verificación del cumplimiento de las normas corporativas vinculantes. Dichos mecanismos incluirán auditorías de protección de datos y métodos para garantizar acciones correctivas para proteger los derechos del interesado. Los resultados de dicha verificación deberían comunicarse a la persona o entidad a que se refiere la letra h) y al consejo de administración de la empresa que controla un grupo empresarial, o de la unión de empresas dedicadas a una actividad económica conjunta, y ponerse a disposición de la autoridad de control competente que lo solicite;

k) los mecanismos establecidos para comunicar y registrar las modificaciones introducidas en las normas y para notificar esas modificaciones a la autoridad de control;

l) el mecanismo de cooperación con la autoridad de control para garantizar el cumplimiento por parte de cualquier miembro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, en particular poniendo a disposición de la autoridad de control los resultados de las verificaciones de las medidas contempladas en la letra j);

m) los mecanismos para informar a la autoridad de control competente de cualquier requisito jurídico de aplicación en un país tercero a un miembro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, que probablemente tengan un efecto adverso sobre las garantías establecidas en las normas corporativas vinculantes, y.

n) la formación en protección de datos pertinente para el personal que tenga acceso permanente o habitual a datos personales.

3. La Comisión podrá especificar el formato y los procedimientos para el intercambio de información entre los responsables, los encargados y las autoridades de control en relación con las normas corporativas vinculantes a tenor de lo dispuesto en el presente artículo. Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen a que se refiere el artículo 93, apartado 2.

### **“Artículo 88 - Tratamiento en el ámbito laboral“**

1. Los Estados miembros podrán, a través de disposiciones legislativas o de convenios colectivos, establecer normas más específicas para garantizar la protección de los derechos y libertades en relación con el tratamiento de datos personales de los trabajadores en el ámbito laboral, en particular a efectos de contratación de personal, ejecución del contrato laboral, incluido el cumplimiento de las obligaciones establecidas por la ley o por el convenio colectivo, gestión, planificación y organización del trabajo, igualdad y diversidad en el lugar de trabajo, salud y seguridad en el trabajo, protección de los bienes de empleados o clientes, así como a efectos del ejercicio y disfrute, individual o colectivo, de los derechos y prestaciones relacionados con el empleo y a efectos de la extinción de la relación laboral.

2. Dichas normas incluirán medidas adecuadas y específicas para preservar la dignidad humana de los interesados así como sus intereses legítimos y sus derechos fundamentales, prestando especial atención a la transparencia del tratamiento, a la transferencia de los datos personales

dentro de un grupo empresarial o de una unión de empresas dedicadas a una actividad económica conjunta y a los sistemas de supervisión en el lugar de trabajo.

3. Cada Estado miembro notificará a la Comisión las disposiciones legales que adopte de conformidad con el apartado 1 a más tardar el 25 de mayo de 2018 y, sin dilación, cualquier modificación posterior de las mismas.”

## **V. Legislación comparada**

52.- Resulta de los documentos que dispone el Tribunal sobre el derecho de los Estados miembros del Consejo de Europa, en especial de un estudio de treinta y cuatro Estados miembros, que el conjunto de estos Estados reconocen con carácter general, a nivel constitucional o legislativo, el derecho al respeto de la privacidad y el secreto de la correspondencia. Sin embargo, únicamente Austria, Finlandia, Luxemburgo, Portugal, Reino Unido y Eslovaquia tratan la cuestión del ejercicio de la vida privada en el lugar de trabajo de una manera explícita, ya sea como parte de la legislación laboral, ya sea mediante leyes especiales.

53.- Con respecto a las prerrogativas de la vigilancia, treinta y cuatro Estados miembros del Consejo de Europa exigen al empleador que informe previamente al empleado de la vigilancia. Esta advertencia puede tomar varias formas, tales como la notificación a las autoridades encargadas de la protección de los datos personales o a los representantes de los empleados. Las leyes vigentes en Austria, Estonia, Finlandia, Grecia, Lituania, Luxemburgo, en la antigua República Yugoslava de Macedonia, Noruega, Polonia y Eslovaquia exigen que el empleador advierta directamente al empleado antes de iniciar la vigilancia.

54.- En Alemania, Austria, Dinamarca, Finlandia, Francia, Grecia, Italia, Portugal y Suecia, los empleadores pueden vigilar los correos electrónicos marcados por los empleados como “privados”, sin poder acceder a su contenido. En Luxemburgo, el empleador no puede abrir los correos electrónicos marcados como “privados” ni los que lo son obviamente. Italia, República Checa y Eslovenia, así como, en cierta medida, la República de Moldavia también imponen limitaciones al control que el empleador puede ejercer sobre las comunicaciones de sus empleados, dependiendo de la naturaleza personal o profesional de dichas comunicaciones. En Alemania y Portugal, una vez establecido el carácter privado de una comunicación, el empleador debe dejar de leerla.

## **Fundamentos de derecho**

### **I. Sobre la violación del artículo 8 del Convenio (RCL 1999, 1190, 1572)**

55.- El demandante sostiene que la decisión de su empresa de despedirle se tomó basándose en una vulneración de su derecho al respeto de la vida privada y la correspondencia, y los tribunales nacionales no protegieron ese derecho. Invoca el artículo 8 del Convenio (RCL 1999, 1190, 1572), el cual, dispone lo siguiente:

“1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.

2. No puede haber injerencia de la autoridad pública en el ejercicio de este derecho salvo 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.”

#### **A. Las conclusiones de la sala**

56.- En su sentencia de 12 de enero de 2016 (TEDH 2016, 1), la sala declaró, en primer lugar, que el artículo 8 del Convenio (RCL 1999, 1190, 1572) era aplicable en el presente asunto. Se fundamentó en la expectativa razonable respecto al concepto de vida privada, el Tribunal consideró que el presente caso se distinguía de los de Copland (TEDH 2007, 23) (sentencia citada, ap. 41) y Halford contra Reino Unido (TEDH 1997, 37) (25 de junio de 1997, ap. 45, Recopilación de las sentencias y decisiones 1997-III), ya que, en el presente caso, las normas internas de la empresa prohibían estrictamente a los empleados utilizar ordenadores y recursos de la empresa con fines personales. La sala tuvo en cuenta la naturaleza de las comunicaciones del demandante y el hecho de que su transcripción había sido utilizada como prueba en los procedimientos ante los tribunales nacionales y concluyó que el derecho del demandante al respeto de su “vida privada” y su “correspondencia” estaba en juego.

57.- A continuación, la sala situó su análisis sobre el terreno de las obligaciones positivas del Estado, ya que la decisión de despedir al demandante había sido adoptada por una persona privada. Por consiguiente, la sala tuvo que examinar si las autoridades nacionales habían ponderado un justo equilibrio entre los derechos del demandante del respeto de su vida privada y de su correspondencia y los intereses de la empresa empleadora.

58.- La sala observó que el demandante tuvo la oportunidad de acudir ante los tribunales laborales y exponer ante ellos sus alegaciones. Señaló también que los tribunales habían constatado que el demandante había cometido una infracción disciplinaria utilizando Internet para fines personales durante las horas de trabajo, y los tribunales habían constatado, en el curso del procedimiento disciplinario, que la empresa empleadora no había tenido acceso al contenido de las comunicaciones del demandante hasta que éste declaró que había utilizado Yahoo Messenger para fines profesionales.

59.- Por tanto, la sala constató que los tribunales internos no se habían basado en el contenido de las comunicaciones del demandante y que la vigilancia de la empresa empleadora se había limitado al uso que el demandante había hecho de Yahoo Messenger . 60 En consecuencia, la sala concluyó que no ha habido violación del artículo 8 del Convenio (RCL 1999, 1190, 1572) .

#### **B. El alcance del asunto ante la Gran Sala**

61.- El Tribunal constata que ante la sala el demandante alegó que la decisión de su empleador de rescindir su contrato de trabajo se basaba en una violación de su derecho al respeto de la vida privada y de la correspondencia protegida por el artículo 8 del Convenio (RCL 1999, 1190, 1572) y que, como los órganos jurisdiccionales internos no habían anulado esta decisión, éstos no habían cumplido su obligación de proteger ese derecho. La sala admitió a trámite la demanda el 12 de enero de 2016 (TEDH 2016, 1).

62.- El Tribunal reitera que el caso remitido ante la Gran Sala es la demanda admitida a trámite por la sala ( K. y T. contra Finlandia (TEDH 2001, 467) [GS], núm. 25702/94, ap. 140-141, TEDH 2001-VII, D.H. y otros contra República Checa (PROV 2007, 329300) [GS], núm. 57325/00, ap. 109, TEDH 2007-IV y Blokhin contra Rusia (PROV 2016, 63806) [GS], núm. 47152/06, ap. 91 TEDH 2016).

63.- En sus alegaciones ante la Gran Sala, el demandante manifestó por primera vez que en 2012 no se admitió una denuncia penal que había presentado por la violación del secreto de la correspondencia (véase apartado 90 más adelante).

64.- Esta nueva queja no fue mencionada en la resolución de admisibilidad del 12 de enero de 2016 (TEDH 2016, 1), en la que se establece el alcance del examen de la demanda. En consecuencia, está fuera del ámbito del procedimiento, aunque fue referida ante la Gran Sala. Por lo tanto, ésta no es competente para conocer del asunto y limitará su examen a la demanda declarada admisible por la sala.

### **C. Sobre la aplicación del artículo 8 del Convenio (RCL 1999, 1190, 1572)**

#### **1. Tesis de las partes**

##### **A) El Gobierno**

65.- El Gobierno sostiene que el demandante no podía alegar que creía que las comunicaciones que intercambiaba en una cuenta de mensajería instantánea creadas para fines profesionales, tenían carácter “privado”. Se fundamenta en la jurisprudencia de los tribunales franceses y chipriotas, sosteniendo que las comunicaciones enviadas por un empleado con medios técnicos puestos a su disposición por su empleador deben considerarse de carácter profesional, a menos que el trabajador declare expresamente su carácter privado. Afirma que Yahoo Messenger no ofrece la posibilidad técnica de marcar una comunicación como privada, pero el demandante tuvo la oportunidad idónea, en la primera fase del procedimiento disciplinario, de declarar que sus comunicaciones eran privadas y él sin embargo manifestó que eran profesionales. Añade que el demandante había sido informado no sólo de las normas internas de su empresa empleadora, que prohibían el uso personal de los recursos de la empresa, sino también que su empleador había establecido una vigilancia en sus comunicaciones.

66.- El Gobierno se basa también en un triple argumento para sostener que el artículo 8 del Convenio (RCL 1999, 1190, 1572) no es aplicable en el presente caso. Primero, no hay pruebas en el expediente de que la transcripción de las comunicaciones del demandante fueran reveladas a sus compañeros de trabajo; el propio demandante había reproducido la transcripción completa de esas comunicaciones ante los órganos jurisdiccionales internos sin que se le hubiera restringido el acceso a dichos documentos. En segundo lugar, los juzgados nacionales utilizaron la transcripción de las comunicaciones como prueba porque el demandante lo había solicitado y los juzgados penales ya habían resuelto que la vigilancia de las comunicaciones era lícita. En tercer lugar, la nota informativa había proporcionado información suficiente para permitir al demandante comprender que su empleador podía controlar sus comunicaciones, privándolas de su carácter privado.

##### **B) El demandante**

67.- El demandante no formula alegaciones sobre la aplicación del artículo 8 del Convenio (RCL 1999, 1190, 1572), pero sostiene sistemáticamente que sus comunicaciones eran de carácter privado.

68.- También argumenta que, al haber creado él mismo la cuenta de Yahoo Messenger y ser solo él el conocedor de la contraseña, podía razonablemente creer que sus comunicaciones eran privadas. También afirma que no había recibido de su empleador la notificación del establecimiento de vigilancia en sus comunicaciones.

## 2. Valoración del Tribunal

69.- El Tribunal observa que en el presente caso se plantea la cuestión de si los hechos denunciados por el demandante están comprendidos en el ámbito de aplicación del artículo 8 del Convenio (RCL 1999, 1190, 1572).

70.- En esta fase de su examen, el Tribunal considera útil recordar que la noción de “vida privada” es un concepto amplio que no se presta a una definición exhaustiva (Sidabras y Džiautas contra Lituania (TEDH 2004, 55), núms. 55480/00 y 59330/00, ap. 43, TEDH 2004-VIII). El artículo 8 del Convenio (RCL 1999, 1190, 1572) protege el enriquecimiento personal ( KA y AD contra Bélgica (TEDH 2005, 15) , núms. 42758/98 y 45558/99, ap. 83, 17 de febrero de 2005), ya sea en forma de desarrollo personal Christine Goodwin contra Reino Unido (PROV 2002, 181176) [GS], núm. 28957/95, ap. 90, TEDH 2002-VI) o de autonomía personal, que refleja un importante principio subyacente en la interpretación de las garantías del artículo 8 (Pretty contra Reino Unido (TEDH 2002, 23), núm. 2346/02, ap. 61, TEDH 2002-III).

El Tribunal reconoce que toda persona tiene derecho a una vida privada, lejos de la injerencia no deseada de otros ( Smirnova contra Rusia (PROV 2003, 162895) , núms 46133/99 y 48183/99, ap. 95, TEDH 2003-IX (extractos)). También considera que sería demasiado restrictivo limitar la noción de “vida privada” a un “círculo íntimo” en el que cada uno pueda vivir su vida personal como quiera y excluir completamente al mundo exterior de este círculo (Niemiets contra Alemania (TEDH 1992, 77), 16 de diciembre de 1992, ap. 29, Serie A núm. 251-B).

Así, el artículo 8 garantiza un derecho a la “vida privada” en sentido amplio, que incluye el derecho a realizar una “vida privada social”, es decir, la posibilidad de que el individuo desarrolle su identidad social. A este respecto, el mencionado derecho consagra la posibilidad de comunicarse con otros para establecer y desarrollar relaciones con sus semejantes (Bigaeva contra Grecia (TEDH 2009, 61), núm. 26713/05, ap. 22, 28 de mayo de 2009, y Özpinar contra Turquía (TEDH 2010, 103) , núm. 20999/04, artículo 45 in fine, 19 de octubre de 2010).

71.- El Tribunal considera que el concepto de “vida privada” puede incluir actividades profesionales (Fernández Martínez contra España (TEDH 2014, 35) [ G ], núm. 56030/07, ap. 110, TEDH 2014 (extractos), y Oleksandr Volkov contra Ucrania (TEDH 2013, 79) núm. 21722/11, apartados 165-166, TEDH 2013) o actividades que tengan lugar en un contexto público ( Von Hannover contra Alemania (TEDH 2012, 10) (núm. 2) [GS], núms. 40660/08 y 60641/08, ap. 95, TEDH 2012). Las restricciones establecidas en la vida laboral pueden incluirse en el artículo 8 cuando repercuten en la forma en que el individuo forja su identidad social a través del desarrollo de relaciones con otros. Cabe señalar en este punto, que es en el marco de la vida laboral donde la mayoría de la gente tiene muchas, si no la mayoría, de las oportunidades para fortalecer sus lazos con el mundo exterior Niemiets , precitado, ap. 29).

72.- Por otra parte, con respecto a la noción de “correspondencia”, cabe señalar que, en la redacción del artículo 8 del Convenio (RCL 1999, 1190, 1572 , la palabra no iba acompañada de ningún adjetivo, al contrario que el término “vida”. El Tribunal ya ha declarado que no es necesario clasificar este concepto en el caso de la correspondencia telefónica. En varios casos relativos a la correspondencia con un abogado, el Tribunal ni siquiera ha considerado la posibilidad de que el artículo 8 no sea aplicable por el carácter profesional de la correspondencia (véase, en este sentido, la sentencia Niemiets , precitada, ap. 32, con las referencias citadas).

También concluyó que las comunicaciones telefónicas abarcaban los conceptos de “vida privada” y “correspondencia” en el sentido del artículo 8 (Roman Zakharov contra Rusia (PROV

2015, 292490) [GS], núm. 47143/06, ap. 173, TEDH 2015). En principio, esto es igualmente aplicable cuando tales comunicaciones se originan o se reciben en los puestos de trabajo (Halford (TEDH 1997, 37), citada ap. 44, y Amann contra Suiza (TEDH 2000, 87) [GS], no 27798/95, ap. 44, TEDH 2000-II).

Lo mismo se aplica a los correos electrónicos enviados desde el lugar de trabajo: también están amparados por la protección del artículo 8, al igual que la información recogida mediante el seguimiento del uso que hace una persona de internet, (Copland (TEDH 2007, 23), antes citada, ap. 41 in fine).

73.- De la jurisprudencia del Tribunal se desprende que las comunicaciones que se emiten desde el puesto de trabajo, así como las del domicilio, pueden incluirse en las nociones de “vida privada” y de “correspondencia” a que se refiere el artículo 8 del Convenio (RCL 1999, 1190, 1572) (Halford (TEDH 1997, 37), antes citada, ap. 44 y Copland (TEDH 2007, 23), antes citada, ap. 41). Para determinar si los conceptos de “vida privada” y “correspondencia” son aplicables, el Tribunal ha intentado en varias ocasiones determinar si un individuo podía razonablemente suponer que su privacidad estaba protegida y era respetada (ibidem que se refiere a la “vida privada” véase Köpke contra Alemania (dec.), núm. 420/07, de 5 de octubre de 2010).

En este contexto, el Tribunal declaró que la expectativa razonable de protección y respeto de la vida privada era un criterio importante pero no necesariamente decisivo (Köpke, sentencia citada).

74.- Aplicando estos principios en el presente asunto, el Tribunal señala, en primer lugar, que el tipo de mensajería instantánea en Internet no es otra cosa que una forma de comunicación que forma parte del ejercicio de la intimidad social. Además, la noción de “correspondencia” se aplica al envío y recepción de mensajes, incluso desde el ordenador de la empresa empleadora. Sin embargo, el Tribunal observa que el empleador esperaba que él y los otros empleados se abstuvieran de cualquier actividad personal en su lugar de trabajo. Este requisito del empleador incluía de forma particular, la prohibición del uso de los recursos de la empresa para fines personales (véase el apartado 12).

75.- El Tribunal observa entonces que, para garantizar el cumplimiento de este requisito, el empleador estableció un sistema de control de la utilización de Internet por sus empleados (véanse los apartados 17 y 18 supra). De los documentos presentados en el expediente, en particular los relativos al procedimiento disciplinario contra el demandante, se desprende que durante dicha actividad de vigilancia se registraron y salvaguardaron tanto los flujos como el contenido de las comunicaciones del demandante (apartados 18 y 20).

76.- El Tribunal observa también que, a pesar de la prohibición de la empresa empleadora, el demandante intercambiaba comunicaciones de carácter personal con su novia y su hermano (véase apartado 21 supra). Algunas de estas comunicaciones eran íntimas (ibidem).

77.- El Tribunal considera que de los autos se desprende que el demandante había sido informado de la prohibición del uso de Internet para fines personales establecida en las normas internas de la empresa empleadora (apartado 14). Sin embargo, no está tan claro que se le informara de que sus comunicaciones estaban siendo supervisadas antes de que se pusiera en marcha la actividad de vigilancia. Por lo tanto, el Gobierno sostiene que el demandante tuvo de la nota informativa del empleador en una fecha no especificada entre el 3 y el 13 de julio de 2007 (apartado 16).

Sin embargo, los órganos judiciales nacionales no determinaron si el demandante había sido informado de la actividad de supervisión en una fecha anterior a la fecha de su realización, ya que la empresa empleadora registró las comunicaciones en tiempo real entre los días 5 a 13 de julio de 2007 (apartado 17).

78.- En cualquier caso, no parece que el demandante hubiera sido informado con antelación del alcance y la naturaleza de la supervisión efectuada por su empleador o de la posibilidad de acceder al contenido de sus comunicaciones.

79.- El Tribunal observa también la alegación del demandante según la cual él mismo había creado la cuenta de Yahoo Messenger y era el único que conocía la contraseña (apartado 68). Además, señala que, de las pruebas del expediente, se desprende que la empresa empleadora también tuvo acceso a la cuenta personal de Yahoo Messenger del demandante (apartado 21 supra). Por lo tanto, el demandante había establecido la cuenta de Yahoo Messenger en cuestión, siguiendo instrucciones de la empresa empleadora para responder a las preguntas de los clientes (apartado 11 supra), y el empleador tenía acceso a ellas.

80.- No está claro que las normas restrictivas de la empresa empleadora dejaran al demandante con la expectativa razonable de privacidad - una expectativa que queda por determinar. Sin embargo, las instrucciones de una empresa no pueden anular el ejercicio de la privacidad social en el puesto de trabajo. El respeto a la privacidad y confidencialidad de las comunicaciones sigue siendo necesario, aunque pueden limitarse dentro de las medidas de necesidad.

81.- Habida cuenta de todas estas consideraciones, el Tribunal concluye que las comunicaciones que el demandante realizó desde su lugar de trabajo estaban comprendidas en los conceptos de "vida privada" y "correspondencia". De ello se deduce que, dadas las circunstancias, el artículo 8 del Convenio (RCL 1999, 1190, 1572) es aplicable en el presente asunto.

#### **D. Sobre el cumplimiento del artículo 8 del Convenio (RCL 1999, 1190, 1572)**

##### **1. Tesis de las partes y observaciones de terceros intervinientes**

###### **A) El demandante**

82.- En las alegaciones presentadas ante la Gran Sala, el demandante sostiene que la sala no tuvo suficientemente en cuenta determinados elementos fácticos del asunto. En primer lugar, insiste en las especificidades de Yahoo Messenger, herramienta que está diseñada para uso personal. Considera que la elección hecha por la empresa empleadora de utilizar esta herramienta en el contexto profesional no puede cambiar el hecho de que está fundamentalmente destinada a fines personales. Él se considera el único propietario de la cuenta de Yahoo Messenger que abrió a petición de su empleador.

83.- En segundo lugar, el demandante alega que la empresa empleadora no tenía una política sobre el uso de Internet. Alega que no se le informó de la posibilidad de que sus comunicaciones pudieran ser vigiladas o leídas. También afirma que no había dado su consentimiento para ese fin. Dijo que si tal política hubiera estado en vigor y se le hubiera informado, se habría abstenido de exponer ciertos aspectos de su vida privada en Yahoo Messenger .

84.- En tercer lugar, el demandante considera que debe hacerse una distinción entre el uso de Internet para fines personales para obtener beneficios materiales y "una simple conversación corta e inofensiva", que no tenía por objeto obtener beneficios y que en ningún caso, causó

perjuicio al empresario - a este respecto, el demandante manifiesta que el empleador no alegó en el procedimiento disciplinario que se le hubiera causado un perjuicio a la empresa.

El demandante hace hincapié en el desarrollo de las tecnologías de la información y la comunicación y sobre las costumbres sociales a este respecto. Considera que las circunstancias actuales en el mundo del trabajo no permiten establecer una línea divisoria clara entre la vida laboral y la vida privada y considera ilegítima cualquier política de gestión que prohíba el uso de internet y dispositivos relacionados para fines personales en la vida laboral de un trabajador.

85.- Desde el punto de vista jurídico, el demandante considera que el Estado rumano no ha cumplido las obligaciones positivas que le impone el artículo 8 del Convenio (RCL 1999, 1190, 1572). En concreto, alega que los tribunales internos no revocaron su despido, aunque en su opinión se había violado su derecho al respeto de las comunicaciones privadas.

86.- Sostiene, en primer lugar, que la sala había cometido un error al distinguir el presente asunto de la sentencia Copland (TEDH 2007, 23) (antes citada, ap. 42). Según él, el factor determinante para el análisis, no es si la empresa empleadora toleraba el uso de Internet para fines personales, sino el hecho de que no notificó al empleado que sus comunicaciones pudieran ser monitorizadas.

A este respecto, alega que su empleador lo puso inicialmente bajo vigilancia y no le dio la oportunidad de aclarar si sus comunicaciones eran privadas o profesionales. Sostiene que es necesario analizar, por una parte, si el hecho de haber prohibido totalmente el uso de internet para fines personales, da a la empresa empleadora el derecho a controlar a sus empleados y por otra, si la empresa empleadora debe justificar esa vigilancia.

87.- En segundo lugar, el demandante considera que el análisis realizado por la sala con arreglo al párrafo segundo del artículo 8 no es conforme con la jurisprudencia del Tribunal: no se habría preguntado si la injerencia en su derecho al respeto de su vida privada y de su correspondencia estaba prevista por la ley, si perseguía un objetivo legítimo y si era necesaria en una sociedad democrática.

88.- En lo que respecta a la competencia de los tribunales laborales, el demandante afirma que ellos pueden ejercer un control total sobre la legalidad y el fundamento de la medida sometida a su examen. Según lo cual, corresponde al juez solicitar la presentación de las pruebas necesarias y plantear las cuestiones de hecho o de derecho pertinentes, incluso si las partes no las mencionan. Por lo tanto, los tribunales del trabajo tendrían una competencia amplia para poder examinar todas las cuestiones relativas a los conflictos laborales, incluidas las cuestiones relacionadas con el respeto de la vida privada y de la correspondencia de los empleados.

89.- Sin embargo, el enfoque de los tribunales nacionales en este caso fue restrictivo y sirvió sólo para confirmar la decisión de la empresa empleadora. Los jueces rumanos analizaron erróneamente los hechos del caso y no tuvieron en cuenta las especificidades de las comunicaciones en el mundo virtual. Así, la violación del derecho del demandante al respeto de su vida privada y de su correspondencia fue intencional e ilícita y tuvo por objeto presentar los medios de prueba que permitieran a la empresa empleadora rescindir el contrato de trabajo.

90.- Por último, el demandante aporta por primera vez en el procedimiento ante la Gran Sala la resolución de la denuncia penal que presentó en 2007: en 2012, la Dirección de Investigaciones sobre la Delincuencia Organizada y el Terrorismo (DIICOT) del Ministerio Público rechazó la denuncia sin haber establecido debidamente los hechos del asunto.

91.- En la audiencia ante la Gran Sala, el demandante declaró, en respuesta a una pregunta de los magistrados, que puesto que la empresa empleadora ponía a disposición de los trabajadores una sola impresora, todos sus colegas podrían haber accedido al contenido de las cuarenta y cinco páginas de transcripciones de sus mensajes en Yahoo Messenger.

92.- El demandante invita a la Gran Sala a concluir que se violó el artículo 8 del Convenio (RCL 1999, 1190, 1572) y a confirmar que en esa ocasión, el control de la correspondencia de los trabajadores sólo podía realizarse de conformidad con la legislación vigente, de manera transparente y por las razones previstas por la ley, y que la empresa empleadora no tenía facultades discrecionales para controlar la correspondencia de sus empleados.

## **B) El Gobierno**

93.- El Gobierno indica que la empresa empleadora registró las comunicaciones del demandante del 5 al 13 de julio de 2007 y luego le dio la oportunidad de explicar su uso de Internet, que había sido más abundante que el de sus colegas. Explica que, dado que el demandante alegó que el contenido de sus comunicaciones era profesional, el empleador verificó sus explicaciones.

94.- Sostiene que el demandante no ha impugnado, en su recurso contra la resolución del tribunal de primera instancia, la conclusión según la cual se le había informado de que su empleador supervisaba el uso de Internet. A este respecto, consta en el procedimiento una copia de la nota informativa de la empresa empleadora firmada por el demandante. En base al registro de asistencia de la empresa, sostiene que el demandante firmó la nota entre el 3 y el 13 de julio de 2007.

95.- El Gobierno también sostiene que el empleador había registrado las comunicaciones del demandante en tiempo real. Considera que del procedimiento no se desprende que la empresa tuviera acceso a comunicaciones anteriores o al correo electrónico privado del demandante.

96.- El Gobierno respalda las conclusiones de la sala y sostiene que el Estado rumano había cumplido sus obligaciones positivas en virtud del artículo 8 del Convenio (RCL 1999, 1190, 1572).

97.- De entrada, señala que el demandante optó por presentar su demanda ante los órganos jurisdiccionales nacionales en el marco de un procedimiento de Derecho laboral. Sostiene que los tribunales han examinado todas estas demandas y han sopesado los diversos intereses en juego, pero que el principal objetivo de su análisis era la conformidad de la legislación interna del procedimiento disciplinario contra el demandante.

Tuvo la posibilidad de interponer un recurso ante los órganos jurisdiccionales nacionales en relación con su demanda concreta basada en la vulneración de su derecho al respeto de su vida privada, en particular en el marco de una acción basada en las disposiciones de la Ley núm. 677/2001 o en una acción de responsabilidad civil por agravio, pero él escogió no hacerlo. También presentó una denuncia penal, en la que la Fiscalía decidió que no había motivo para que la vigilancia efectuada por la empresa empleadora de las comunicaciones de sus empleados fuera considerada ilegal.

98.- Con respecto a las obligaciones positivas del Estado en particular, el Gobierno declara que existe una amplia variedad de enfoques entre los Estados miembros del Consejo de Europa con respecto a la regulación sobre la supervisión que los empleadores pueden ejercer sobre sus empleados. Algunos Estados incluyen esta cuestión en un ámbito más amplio de tratamiento de datos personales, mientras que otros han adoptado una legislación específica al respecto. Incluso dentro de este segundo grupo de Estados, las soluciones adoptadas no son uniformes

en cuanto a la extensión y el propósito de la supervisión del empleador, la advertencia previa a los empleados o el uso de Internet para fines personales.

99.- En base a la mencionada sentencia Köpke, el Gobierno alega que los órganos jurisdiccionales nacionales han ponderado correctamente el derecho del demandante respecto de su vida privada y de su correspondencia, así como el de su empresa empleadora para organizar y supervisar el trabajo en su empresa. En su opinión, cuando la vigilancia de las comunicaciones es llevada a cabo por una persona privada, un control adecuado por parte de las autoridades nacionales es suficiente a los efectos del artículo 8 y no es necesario un sistema legislativo específico de protección.

100.- El Gobierno argumenta entonces que los tribunales nacionales habían examinado la legalidad y la necesidad de la decisión de la empresa empleadora y habían llegado a la conclusión de que el procedimiento disciplinario se había llevado a cabo de conformidad con la legislación vigente. Considera especialmente importante la forma en que se llevó a cabo este procedimiento, en particular por lo que respecta a la posibilidad ofrecida al demandante de indicar si las comunicaciones en cuestión tenían un carácter privado. En su opinión, si el demandante hubiera hecho uso de esta posibilidad, los tribunales habrían equilibrado los intereses en cuestión de manera diferente.

101.- A este respecto, el Gobierno subraya que, en el procedimiento ante las autoridades nacionales, fue el propio demandante quien aportó la copia completa de las transcripciones de sus comunicaciones sin tomar precauciones; alega que el demandante pudo indicar sólo los nombres de las cuentas de que se trataba o haber presentado extractos de sus comunicaciones, en particular las que no contenían información de índole privada. También afirma que, respecto a las alegaciones del demandante de que sus comunicaciones, fueron reveladas a sus colegas, precisa que sólo el comité disciplinario formado por tres personas tuvo acceso a ellas.

102.- El Gobierno considera además que la decisión de la empresa empleadora era necesaria: ésta debía haber comprobado los argumentos presentados por el demandante en el procedimiento disciplinario para determinar si el demandante había cumplido las normas internas.

103.- Por último, el Gobierno opina que debe distinguirse entre la naturaleza de las comunicaciones y su contenido. Al igual que la sala, observa que los órganos jurisdiccionales nacionales no tuvieron en cuenta el contenido de las comunicaciones del demandante, sino que examinaron su naturaleza y concluyeron que eran personales.

104.- Por consiguiente, el Gobierno concluye que la demanda presentada por el demandante basada en el artículo 8 del Convenio (RCL 1999, 1190, 1572) carecía de fundamento.

## **C) Los terceros intervinientes**

### **I. El gobierno francés**

105.- El Gobierno francés expone, en particular, su opinión sobre el alcance de la obligación positiva de las autoridades nacionales de velar por el respeto de la vida privada y la correspondencia de los trabajadores. Hace una exposición exhaustiva de las disposiciones aplicables del derecho civil, laboral y penal francés. A su juicio, el artículo 8 del Convenio (RCL 1999, 1190, 1572) se aplica únicamente a los datos, la correspondencia y las actividades electrónicas estrictamente personales. A este respecto, se basa en la jurisprudencia reiterada del Tribunal de Casación francés, según el cual, los datos tratados, enviados y recibidos por

medio de equipos electrónicos profesionales, se presume que tienen carácter profesional, a menos que el trabajador los designe, clara y precisamente, como personales.

106.- El Gobierno francés considera que el margen de apreciación de que gozan los Estados en este ámbito debe ser amplio, ya que es necesario encontrar un equilibrio entre los intereses privados concurrentes. Considera que el empresario puede ejercer una supervisión razonable de los datos y la correspondencia profesional de los empleados siempre que persiga un objetivo legítimo y utilice el resultado de dicha supervisión en el marco de un procedimiento disciplinario.

Destaca que la supervisión debe ir acompañada de una información previa a los empleados sobre este respecto. Por último, señala que cuando los datos son claramente identificados por el empleado como personales, el empresario puede llevar el asunto ante los tribunales para que ordenen medidas de investigación y nombren a un agente judicial para acceder a los datos en cuestión y grabar sus contenidos.

La Confederación europea de los sindicatos Tras recordar los principios aplicables del derecho internacional y europeo, declara que el acceso a Internet debería considerarse como un derecho y debería reforzarse el derecho a respetar la correspondencia. En su opinión, el consentimiento de los empleados o, al menos, su información previa, así como la información de sus representantes, es necesaria para que el empresario acceda a sus datos personales. La confederación europea de sindicatos considera crucial proteger el derecho al respeto de la vida privada en el contexto de las relaciones laborales, en particular en vista de la dependencia estructural de los empleados respecto a sus empleadores.

## **2. Valoración del Tribunal**

### **A) Sobre si el asunto se refiere a una obligación negativa o una obligación positiva**

107.- El Tribunal debe considerar si el presente asunto debe examinarse en términos de obligaciones negativas u obligaciones positivas del Estado. Recuerda que, de conformidad con el artículo 1 del Convenio (RCL 1999, 1190, 1572), los Estados miembros “reconocen a toda persona que esté dentro de su jurisdicción los derechos y libertades definidos (...) [en] el (...) Convenio”.

Si bien el objetivo principal del artículo 8 del Convenio es proteger al individuo de la injerencia arbitraria de las autoridades públicas, también puede imponer al Estado obligaciones positivas inherentes a la efectiva observancia de los derechos que garantiza (véase, en este sentido, entre otros, X y Y contra los Países Bajos (TEDH 1985, 4) , el 26 de marzo de 1985, ap. 23, la serie A núm. 91, Von Hannover (TEDH 2012, 10) (núm. 2), ap. 98, y Hämäläinen contra Finlandia (TEDH 2014, 50) [GS] núm. 37359/09, ap. 62, TEDH 2014).

108 En el caso de autos, el Tribunal señala que la medida impugnada por el demandante, a saber, el control de las comunicaciones realizadas en Yahoo Messenger por una autoridad del Estado, quien inició la apertura de un procedimiento disciplinario contra él y posterior despido por incumplimiento de las normas internas que prohibían el uso de los recursos de la empresa para fines personales, no fue tomada por una autoridad estatal sino por una empresa privada. El control de las comunicaciones del demandante por parte del empresario y la consulta de su contenido con vistas a justificar su despido no pueden, por lo tanto, considerarse una “injerencia” en el derecho del demandante.

109.- Sin embargo, el Tribunal observa que la medida adoptada por el empresario ha sido validada por los órganos jurisdiccionales nacionales. Es cierto que el control de las

comunicaciones del demandante no fue el resultado de una intervención directa de las autoridades nacionales, pero, sin embargo, la responsabilidad de dichas autoridades se vería afectada si los hechos de autos resultaran de un incumplimiento que garantizara al demandante el disfrute de un derecho consagrado en el artículo 8 del Convenio (RCL 1999, 1190, 1572) (véase, mutatis mutandis, Obst contra Alemania (PROV 2010, 325444), núm. 425/03, apartados 40 y 43, 23 de septiembre de 2010 y Schüth contra Alemania (PROV 2010, 325463), núm. 1620/03, apartados 54 y 57, TEDH 2010).

110.- Habida cuenta de las circunstancias particulares del caso, tal como se describe en el apartado 109 supra, el Tribunal considera que, a la luz de su conclusión sobre la aplicabilidad del artículo 8 del Convenio (RCL 1999, 1190, 1572) (véase el apartado 81 supra) y habida cuenta de que la violación del derecho del demandante al respeto de su vida privada y de su correspondencia fue por parte de una empresa privada, la demanda debía analizarse desde el punto de vista de las obligaciones positivas del Estado.

111.- Si bien la frontera entre las obligaciones positivas y negativas del Estado en virtud del Convenio (RCL 1999, 1190, 1572) no se presta a una definición precisa, los principios aplicables son, sin embargo, comparables. En particular, en ambos casos debe tenerse en cuenta el justo equilibrio entre el interés general y los intereses del individuo, ya que en cualquier caso el Estado goza de un margen de apreciación (Palomo Sánchez y otros contra España (TEDH 2011, 68) [GS], núms. 28955/06 y 3 otros 3, ap. 62, TEDH 2011).

#### **B) Los principios generales aplicables a la valoración de la obligación positiva del Gobierno de velar por el respeto a la vida privada y a la correspondencia en el contexto de las relaciones laborales**

112.- El Tribunal reitera que la elección de las medidas para asegurar el cumplimiento del artículo 8 en las relaciones interindividuales está en principio dentro del margen de valoración de los Estados miembros. Existen diferentes maneras de garantizar el respeto a la vida privada, y el tipo de obligación del Estado depende del aspecto de la vida privada que se esté cuestionando (Söderman contra Suecia (TEDH 2013, 84) [GS], núm. 5786/08, ap. 79, TEDH 2013, con las referencias citadas).

113.- En el presente asunto corresponde, por lo tanto, al Tribunal precisar la naturaleza y el alcance de las obligaciones positivas del Estado demandado, que tenía el deber de proteger el derecho del demandante respeto de su vida privada y de su correspondencia en el marco de sus relaciones laborales

114.- El Tribunal reitera su conclusión de que, en determinadas circunstancias, el Estado no cumple adecuadamente sus obligaciones positivas en virtud del artículo 8 del Convenio (RCL 1999, 1190, 1572), a menos que garantice el respeto de las relaciones entre los individuos mediante el establecimiento de un marco normativo que tenga en cuenta los diversos intereses que han de protegerse en un contexto determinado (X y Y contra los Países Bajos (TEDH 1985, 4), precitada, apds. 23, 24 y 27 y MC contra Bulgaria (PROV 2003, 253041), núm. 39272/98, ap. 150, TEDH 2003-XII, ambos relativos a las agresiones sexuales a menores, véase también KU contra Finlandia (TEDH 2008, 95), núm. 2872/02, apds. 43 y 49, TEDH 2008, caso relativo a un anuncio de naturaleza sexual publicado en nombre de un menor en un sitio de citas por Internet, Söderman (TEDH 2013, 84), antes citado, ap. 85, sobre la eficacia de los recursos respecto de una demanda por atentar contra la integridad personal infligida por un pariente cercano, y Codarcea contra Rumania (PROV 2009, 253903), núm. 31675/04, apartados 102-104 2 de junio de 2009, relativa a negligencias médicas).

115.- El Tribunal admite que las medidas de protección pueden estar previstas tanto en el derecho laboral como en el derecho civil y penal. Por lo que se refiere al derecho laboral, debe comprobar si, en el caso de autos, el Estado demandado hubiera tenido que adoptar un marco legislativo para proteger el derecho del demandante respeto de su vida privada y de su correspondencia en el contexto de sus relaciones de trabajo con la empresa empleadora.

116.- A este respecto, señala que el derecho laboral tiene características específicas que deben tenerse en cuenta. La relación entre una empresa y su empleado es una relación contractual, acompañada de derechos y obligaciones especiales, y caracterizada por una relación legal de subordinación. Se rige por su propio sistema jurídico, que es claramente distinto del sistema general de relaciones entre individuos (Saumier contra Francia (TEDH 2017, 4), núm. 74734/14, ap. 60, 12 de enero de 2017).

117.- Desde un punto de vista normativo, la legislación laboral proporciona un margen de negociación para las partes en el contrato de trabajo. Por lo tanto, corresponde generalmente a los propios contratantes determinar una parte importante del contenido de sus relaciones (véanse, mutatis mutandis, Wretlund contra Suecia (dec.), núm. 46210/99, 9 de marzo de 2004, asunto relativo al artículo 8 del Convenio (RCL 1999, 1190, 1572), sobre la obligación del demandante, empleado de una central nuclear, de someterse a pruebas de detección de drogas; en relación a la acción sindical desde la perspectiva del artículo 11, véase Gustafsson contra Suecia (TEDH 1996, 4) , 25 de abril de 1996, ap. 45, Informes 1996-II y, mutatis mutandis, Demir y Baykara contra Turquía (PROV 2008, 350504) [GS], núm. 34503/97, apartados 140-146, TEDH 2008, para el caso particular de los funcionarios).

i) De la jurisprudencia comparada del Tribunal se desprende, además, que no existe un consenso europeo al respecto. De hecho, pocos Estados miembros se han manifestado explícitamente sobre la cuestión de ejercer por parte de los trabajadores su derecho al respeto de su vida privada y de su correspondencia en su puesto de trabajo (apartado 52 supra).

118.- A la luz de estas consideraciones, el Tribunal considera que se debe otorgar a los Estados miembros un amplio margen de discrecionalidad para valorar la necesidad de adoptar un marco jurídico que establezca las condiciones en las que una empresa puede adoptar una política que regule las comunicaciones no profesionales, electrónicas u otro, de sus empleados en su lugar de trabajo.

119.- Sin embargo, la capacidad de que gozan los Estados en este campo no puede ser ilimitada. Los tribunales nacionales deben velar porque el establecimiento por una empresa de medidas para vigilar la correspondencia y otras comunicaciones, sea cual sea su alcance y duración, vaya acompañado de garantías adecuadas y suficientes contra los abusos (véase, mutatis mutandis, Klass y otros contra Alemania, 6 de septiembre de 1978 (TEDH 1978, 1), ap. 50, serie A, núm. 28, y Roman Zakharov (PROV 2015, 292490) , precitada, apds. 232-234).

120.- El Tribunal es consciente de que la situación está cambiando rápidamente en este ámbito. Sin embargo, considera que la proporcionalidad y las garantías procesales contra el carácter arbitrario son elementos esenciales. En este contexto, las autoridades nacionales deberían tener en cuenta los siguientes factores: i)

¿El empleado ha sido informado de la posibilidad de que el empleador tome medidas para supervisar su correspondencia y otras comunicaciones, así como la aplicación de tales medidas?

Si bien en la práctica esta información puede ser comunicada efectivamente al personal de diversas maneras, según las especificidades fácticas de cada caso, el Tribunal considera que, para que las medidas puedan ser consideradas conforme a los requisitos del artículo 8 del Convenio (RCL 1999, 1190, 1572), la advertencia debe ser, en principio, clara en cuanto a la naturaleza de la supervisión y antes del establecimiento de la misma.

ii) ¿Cuál fue el alcance de la supervisión realizada del empleador y el grado de intrusión en la vida privada del empleado? A este respecto, debe hacerse una distinción entre el control del flujo de comunicaciones y el de su contenido. También se debería tener en cuenta si la supervisión de las comunicaciones se ha realizado sobre la totalidad o sólo una parte de ellas y si ha sido o no limitado en el tiempo y el número de personas que han tenido acceso a sus resultados (véase, en este sentido, la sentencia Köpke, precitada). Lo mismo se aplica a los límites espaciales de la vigilancia.

iii) ¿El empleador ha presentado argumentos legítimos para justificar la vigilancia de las comunicaciones y el acceso a su contenido (véase, en los apartados 38, 43 y 45 supra, el estado del derecho internacional y europeo en la materia)? Dado que la vigilancia del contenido de las comunicaciones es por su naturaleza un método mucho más invasivo, requiere justificaciones más fundamentadas.

iv) ¿Habría sido posible establecer un sistema de vigilancia basado en medios y medidas menos intrusivos que el acceso directo al contenido de comunicaciones del empleado? A este respecto, es necesario evaluar, en función de las circunstancias particulares de cada caso, si el objetivo perseguido por el empresario puede alcanzarse sin que éste tenga pleno y directo acceso al contenido de las comunicaciones del empleado.

v) ¿Cuáles fueron las consecuencias de la supervisión para el empleado afectado (véase, mutatis mutandis, el criterio similar aplicado al examen de la proporcionalidad de una injerencia en el ejercicio de la libertad de expresión protegida por el artículo 10 del Convenio (RCL 1999, 1190, 1572) en Axel Springer AG contra Alemania (PROV 2012, 46200) [GS], núm. 39954/08, ap. 95, 7 de febrero de 2012, con las referencias citadas)? ¿De qué modo utilizó el empresario los resultados de la medida de vigilancia, concretamente si los resultados se utilizaron para alcanzar el objetivo declarado de la medida (véase, en este sentido, la sentencia Köpke, precitada)?

vi) ¿Al empleado se le ofrecieron garantías adecuadas, particularmente cuando las medidas de supervisión del empleador tenían carácter intrusivo? En particular, estas garantías debían impedir que el empleador tuviera acceso al contenido de las comunicaciones en cuestión sin que el empleado hubiera sido previamente notificado de tal eventualidad. En este contexto, debe recordarse que, para poder prosperar, las relaciones laborales deben basarse en la confianza entre las personas (sentencia Palomo Sánchez y otros (TEDH 2011, 68), precitada, ap. 76).

121.- Por último, las autoridades internas deben velar para que los empleados, cuyas comunicaciones hayan sido objeto de seguimiento, puedan presentar un recurso ante un órgano judicial que tenga competencia para pronunciarse, al menos en esencia, sobre el cumplimiento de los criterios antes expuestos y la legalidad de las medidas impugnadas (sentencia Obst , ap. 45; y Köpke , precitada).

122.- En el presente caso, el Tribunal examinará la forma en que los tribunales nacionales requeridos por el demandante examinaron la demanda que se basaba en la supuesta infracción del empleador sobre su derecho al respeto de su vida privada y de su correspondencia en el marco de las relaciones laborales.

### **C) Aplicación de los principios generales al presente asunto**

123.- El Tribunal señala que los órganos jurisdiccionales nacionales determinaron que, en este caso, habían entrado en juego, de un lado, el derecho del demandante al respeto de su vida privada y, por otro, el derecho de controlar y cumplir con las prerrogativas del empresario, para garantizar el buen funcionamiento de la empresa (véanse los apartados 28 y 30 supra). Considera que, de conformidad con las obligaciones positivas del Estado en virtud del artículo 8 del Convenio (RCL 1999, 1190, 1572), las autoridades nacionales debían sopesar estos intereses divergentes.

124.- El Tribunal reitera que el objeto específico de la demanda que se ha presentado es el supuesto incumplimiento por parte de los órganos jurisdiccionales nacionales, requeridos en el marco de un procedimiento de derecho laboral, de proteger, de conformidad con el artículo 8 del Convenio (RCL 1999, 1190, 1572), al demandante al respeto de su vida privada y de su correspondencia como parte de la relación laboral. Durante todo el procedimiento, el demandante denunció, tanto ante los tribunales nacionales como ante el Tribunal, la supervisión realizada por su empleador de sus comunicaciones sobre las cuentas de Yahoo Messenger en cuestión y del uso del contenido de estas comunicaciones en el contexto del procedimiento disciplinario en su contra.

125.- En cuanto a la cuestión de saber si el empresario reveló el contenido de estas comunicaciones a los compañeros del demandante (apartado 26 supra), el Tribunal observa que este argumento no está suficientemente corroborado por las pruebas que obran en el expediente y que, el demandante no presentó pruebas adicionales en la vista ante la Sala (apartado 91 supra).

126.- Por lo tanto, considera que la demanda está basada en el despido del demandante como consecuencia de la supervisión ejercida por el empresario. Más concretamente, debe averiguarse en el caso de autos si, de conformidad con los requisitos del artículo 8 del Convenio (RCL 1999, 1190, 1572), las autoridades nacionales han sopesado el derecho del demandante del respeto de su vida privada y de su correspondencia, y los intereses del empleador.

Por lo tanto, incumbe al Tribunal determinar si, a la luz de todo el asunto, las autoridades nacionales competentes han logrado un justo equilibrio entre los intereses divergentes en juego cuando evaluaron las medidas de control impuestas al demandante, (véase *mutatis mutandis*, Palomo Sánchez y otros (TEDH 2011, 68), antes citada, ap. 62). Reconoce que la empresa empleadora tiene un interés legítimo en garantizar el buen funcionamiento de la empresa, lo que puede hacer mediante la creación de mecanismos que garanticen que sus empleados desempeñen sus funciones profesionales de manera adecuada y con la celeridad requerida.

127.- A la luz de estas consideraciones, examinará en primer lugar la forma en que los tribunales nacionales han establecido los hechos pertinentes en el presente caso -tanto el Tribunal del Condado como el Tribunal de Apelación sostuvieron que el demandante había recibido una advertencia previa del empleador (apartados 28 y 30 supra) - y analizará si los tribunales nacionales han respetado los requisitos del Convenio (RCL 1999, 1190, 1572) en su examen del caso.

128.- En esta fase, el Tribunal considera útil recordar que, cuando se trata de establecer los hechos, consciente del carácter subsidiario de su objetivo, no puede asumir sin razón el papel de juez en primera instancia, a menos que ello se haga inevitable por las circunstancias del caso

de que conoce. (Mustafa Tunç y Fecire Tunç contra Turquía (PROV 2015, 102681) [GS], núm. 24014/05, ap. 182, 14 de abril de 2015).

Cuando se han llevado a cabo los procedimientos internos, no tiene que sustituir su propia versión de los hechos por la de los órganos jurisdiccionales nacionales, que deben establecer los hechos sobre la base de las pruebas recopiladas por ellos (véase, *Edwards contra Reino Unido* (TEDH 1992, 81), 16 de diciembre de 1992, ap. 34, Serie A, núm. 247-B).

Si las conclusiones de aquellos no vinculan al Tribunal, que es libre de efectuar su propia valoración a la luz de todas las informaciones que dispone, normalmente no se apartará de las conclusiones sobre los hechos de los órganos jurisdiccionales nacionales salvo que disponga de datos convincentes a tal efecto ( *Giuliani y Gaggio contra Italia* (PROV 2011, 85805) [GS], núm. 23458/02, ap. 180, TEDH 2011 (extractos), y *Aydan contra Turquía* (PROV 2013, 86068) , núm. 16281/10, ap. 69, 12 de marzo de 2013)

129.-De las pruebas aportadas ante el Tribunal se desprende que el demandante había sido informado del reglamento interno de la empresa empleadora, que prohibía el uso de los recursos de la empresa para fines personales (ap. 12). Conocía el contenido de este documento y lo había firmado el 20 de diciembre de 2006 (ap. 14). Además, la empresa empleadora distribuyó una nota informativa de fecha 26 de junio de 2007 entre todos los empleados, en la que recordaba la prohibición de uso de los recursos de la empresa para uso personal y precisó que una empleada había sido despedida por violar tal prohibición (apartado 15).

El demandante tenía conocimiento de esa nota y la firmó en una fecha que no se especifica, pero que fue entre el 3 y el 13 de julio de 2007 (apartado 16 supra). Por último, el Tribunal recuerda que el 13 de julio de 2007 el demandante fue citado dos veces por su empleador para explicar su uso personal de Internet (apartados 18 y 20). Inicialmente, cuando le mostraron los gráficos que describían su tráfico de Internet y el de sus colegas, afirmó que había utilizado su cuenta de Yahoo Messenger sólo con fines profesionales (apartados 18 y 19).

Después, cincuenta minutos más tarde, cuando se le presentó una transcripción de 45 páginas que contenían sus comunicaciones con su hermano y su novia, el demandante informó a su empleador que éste era responsable de la una infracción penal, a saber, la violación del secreto de la correspondencia (apartado 22 supra).

130.- El Tribunal observa que los tribunales nacionales habían identificado correctamente los intereses en juego, haciendo referencia explícita al derecho del demandante del respeto de su vida privada, así como a los principios jurídicos aplicables (apartados 28 y 30 supra). En particular, el Tribunal de Apelación se refirió expresamente a los principios de necesidad, finalidad, transparencia, legitimidad, proporcionalidad y seguridad establecidos en la directiva 95/46/CE (LCEur 1995, 2977) y recordó que el control del uso de Internet y las comunicaciones electrónicas en el lugar de trabajo se rige por estos principios (apartado 30 supra). Los tribunales nacionales también preguntaron si los procedimientos disciplinarios se habían llevado a cabo de conformidad con el principio de contradicción y si se había dado al demandante la oportunidad de presentar sus alegaciones.

131.- Queda por verificar cómo las autoridades nacionales tuvieron en cuenta en su razonamiento los criterios ya expuestos (apartado 121), cuando ponderaron el derecho del demandante sobre el respeto de su vida privada y su correspondencia y el derecho de control ejercido por el empresario para garantizar el correcto funcionamiento de la empresa, incluidas las normativas disciplinarias correspondientes.

132.- Por lo que respecta a la cuestión de saber si el demandante había recibido una advertencia previa por parte de su empresa empleadora, el Tribunal reitera que ha llegado a la conclusión de que no parecía que el demandante hubiera sido informado con antelación del alcance y de la naturaleza del control efectuado por la empresa o de la posibilidad de que la empresa tuviera acceso al contenido de sus comunicaciones (apartado 78 supra).

En cuanto a la posibilidad de supervisión, señala que el Tribunal del Condado se limitó a constatar que “se había indicado a los trabajadores que, poco antes de que el demandante fuera objeto de una sanción disciplinaria, otro empleado había sido despedido” (apartado 28) y el Tribunal de Apelación consideró que el demandante había sido advertido que no debía utilizar recursos de la empresa para fines personales (apartado 30). Por consiguiente, los órganos jurisdiccionales nacionales no determinaron si el demandante había sido previamente notificado de la posibilidad de que el empresario pudiera establecer medidas de vigilancia y del alcance y la naturaleza de dichas medidas.

El Tribunal entiende que, para ser considerada como previa, la advertencia del empleador debe darse antes de que comience la actividad de supervisión, y con mayor motivo, cuando la supervisión implica también el acceso al contenido de las comunicaciones de los empleados. Las normas internacionales y europeas van en esta dirección y exigen que la información se comunique al interesado antes de que sea objeto control (apartados 38 y 43; véase también en su perspectiva de derecho comparado, apartado 53). 133 En cuanto al alcance de la supervisión realizada y el grado de intrusión en la vida privada del demandante, el Tribunal observa que esta cuestión no fue examinada por el Tribunal del Condado o el Tribunal de Apelación (apartados 28 y 30), mientras que parece que el empleador registró en tiempo real todas las comunicaciones hechas por el demandante durante el período de vigilancia, que tuvo acceso a ellas y que imprimió el contenido (apartados 17 y 21 supra).

134.- No parece que los órganos jurisdiccionales nacionales hayan comprobado suficientemente la existencia de razones legítimas que justificaran el establecimiento de un control de las comunicaciones del demandante. El Tribunal no puede sino constatar que el Tribunal de Apelación no determinó qué era concretamente, en el presente asunto, el objetivo que pudo justificar una supervisión tan estricta.

Es cierto que esta cuestión había sido planteada por el Tribunal del Condado, que había mencionado la necesidad de evitar una vulneración en los sistemas informáticos de la empresa, el cuestionamiento de la responsabilidad de la empresa en caso de actividad ilegal en el espacio virtual, así como la divulgación de sus secretos comerciales (apartado 28 supra). Sin embargo, a juicio del Tribunal, estos ejemplos sólo pueden ser indicaciones teóricas, ya que no se acusó concretamente al demandante de exponer a la empresa a ninguno de esos riesgos. Además, el Tribunal de Apelación no se pronunció sobre esta cuestión.

135.- Por otra parte, ni el Tribunal del Condado ni el Tribunal de Apelación examinaron suficientemente si el objetivo perseguido por el empleador podía haberse logrado mediante métodos menos intrusivos que el acceso al contenido mismo de las comunicaciones del demandante.

136.- Además, ninguno de los dos examinó la gravedad de las consecuencias de la medida de control y del procedimiento disciplinario que se siguió. A este respecto, el Tribunal señala que el demandante había sido sometido a la medida disciplinaria más grave, a saber, el despido.

137.- Por último, el Tribunal observa que los órganos jurisdiccionales nacionales no comprobaron si, cuando compareció el demandante para que explicara el uso que había hecho de los recursos de la empresa, (apartados 18 y 20), el empresario había tenido ya acceso al contenido de las comunicaciones en cuestión. Observa que las autoridades nacionales no determinaron en qué momento del procedimiento disciplinario el empresario tuvo acceso a dicho contenido. Considera que admitir que el acceso al contenido de las comunicaciones pudo tener lugar en cualquier momento durante el procedimiento disciplinario, va en contra del principio de transparencia (véase, en este sentido la Recomendación CM/Rec (2015) 5 en el apartado 43 supra; para una perspectiva de derecho comparado, véase el apartado 54 supra).

138.- A este respecto, el Tribunal considera dudosa la conclusión del Tribunal de Apelación según la cual el justo equilibrio entre los intereses en juego debió haber sido sopesado (apartado 30). Esta observación parece bastante formal y teórica. De hecho, el Tribunal de Apelación no explicó cuáles eran las razones específicas, que se derivaban de la situación específica del demandante y de su empleador, que le permitieron llegar a esa conclusión.

139.- En estas circunstancias, parece que los órganos jurisdiccionales nacionales no consiguieron, por un lado, comprobar, concretamente, si el empleador había notificado previamente al demandante la posibilidad de que sus comunicaciones en Yahoo Messenger iban a ser controladas y, por otro, tener en cuenta que no se le había informado de la naturaleza y alcance de la vigilancia a que iba a ser sometido, así como del grado de intrusión en su vida privada y en su correspondencia. Por otra parte, no determinaron, en primer lugar, qué motivos concretos justificaban la introducción de las medidas de control, en segundo lugar, si el empresario pudo haber utilizado medidas menos intrusivas para la vida privada y la correspondencia del demandante y, en tercer lugar, si el acceso al contenido de las comunicaciones hubiera sido posible sin su conocimiento (apartados 120 y 121).

140.- A la luz de todas las consideraciones anteriores y sin perjuicio del margen de apreciación del Estado demandado, el Tribunal considera que las autoridades nacionales no protegieron adecuadamente el derecho del demandante respeto de su vida privada y su correspondencia y que, por lo tanto, no valoraron el justo equilibrio entre los intereses en juego. En consecuencia, se había producido una violación del artículo 8 del Convenio (RCL 1999, 1190, 1572).

II. Sobre la aplicación del artículo 41 del Convenio (RCL 1999, 1190, 1572)

141.- En virtud con el artículo 41 del Convenio (RCL 1999, 1190, 1572) “Si el Tribunal declara que ha habido violación del Convenio o de sus protocolos y si el derecho interno del Estado contratante sólo permite de manera imperfecta reparar las consecuencias de dicha violación, el Tribunal concederá a la parte perjudicada, si así procede, una satisfacción equitativa.”

## **A. Daños y perjuicios**

### **1. Perjuicio material**

142.- Ante la sala, el demandante solicitó un importe de 59.976,12 € (cincuenta y nueve mil novecientos setenta y seis euros con doce céntimos) en concepto del perjuicio material que consideraba haber sufrido. Explicó que esta suma representaba el valor actual de los salarios a los que hubiera tenido derecho si no hubiera sido despedido. Durante la audiencia ante la Gran Sala, los representantes del demandante declararon que mantenían su reclamación por ser satisfacción justa.

143.- En sus observaciones ante la sala, el Gobierno indicó que se oponía a la concesión de cualquier suma por el perjuicio material supuestamente sufrido. A su juicio, el importe reclamado era especulativo y no existía vínculo de causalidad entre el despido del demandante y el perjuicio alegado.

144.- El Tribunal reitera su constatación de que se ha violado el artículo 8 del Convenio (RCL 1999, 1190, 1572), ya que los órganos jurisdiccionales nacionales no establecieron los hechos pertinentes y no ponderaron el derecho del demandante al respeto de su vida privada y su correspondencia y los intereses de la empresa empleadora. El Tribunal no aprecia un vínculo de causalidad entre la violación constatada y el supuesto daño material y, por tanto, rechaza esa reclamación.

## **2. Daño moral**

145.- Ante la sala, el demandante también reclamó 200.000€ (doscientos mil euros) en concepto de daño moral sufrido como consecuencia de su despido. Afirma que, debido al motivo disciplinario del despido, no había podido encontrar otro empleo, su nivel de vida se había deteriorado, había perdido su condición social y, en consecuencia, su novia decidió en 2010 para poner fin a su relación.

146.- El Gobierno respondió que cualquier constatación de violación podría constituir en sí misma una satisfacción suficientemente justa. En cualquier caso, considera que la suma reclamada por el demandante era exorbitada en relación con la jurisprudencia del Tribunal de Justicia en esta materia.

147.- El Tribunal considera que la constatación de una violación constituye una satisfacción suficiente y justa por cualquier daño moral sufrido por el demandante.

## **B. Costas y gastos**

148.- Ante la sala, el demandante también reclamó 3.310 lei rumanos (RON) (aproximadamente 750€), en concepto de costas y gastos satisfechos ante los tribunales nacionales, y 500 RON (aproximadamente 115€) por los honorarios del abogado que lo había representado ante los tribunales nacionales. También reclamó 500€ (quinientos euros) por los honorarios de los abogados que lo habían representado ante el Tribunal. Él justificó la reclamación de su demanda con: - copias del contrato de asistencia letrada y recibo del pago de la suma de 500 RON, correspondiente a los honorarios del abogado que le representó ante los tribunales nacionales; - documentos que acreditan haber pagado a su empresario las sumas de 2700 RON y 610,30 RON en concepto de costas y gastos; - copia del recibo del pago de 2218,64 RON correspondiente a los honorarios de uno de los abogados que lo representó ante el Tribunal. El demandante no solicita el reembolso de las costas ocasionadas del procedimiento ante la Gran Sala.

149.- En sus observaciones ante la sala, el Gobierno solicita al Tribunal que atribuya al demandante únicamente las cantidades requeridas y correspondientes a las reclamaciones debidamente justificadas. A este respecto, declara que el demandante no había demostrado que había pagado 500€ (quinientos euros) de honorarios a los abogados que lo habían representado ante el Tribunal y que la recepción del pago de 500 RON de honorarios al abogado que lo representaba ante los tribunales nacionales no estaba acompañado de las horas de trabajo.

150.- Según la jurisprudencia del Tribunal, un demandante solo puede obtener el reembolso de los gastos y las costas en la medida en que se establezca su realidad, su necesidad y el carácter razonable de su cuantía (véase, en este sentido, la parroquia greco-católica Lupeni y otros contra Rumania (PROV 2015, 132474) [GS], núm. 76943/11, ap. 187, TEDH 2016 (extractos)). En el caso de autos, habida cuenta de los documentos de que se disponen y de su jurisprudencia, el Tribunal considera razonable la suma de 1.365€ (mil trescientos sesenta y cinco euros) por todos los gastos y lo acuerda a favor del demandante.

### **C. Intereses de demora**

151.- El Tribunal considera apropiado fijar el tipo de los intereses de demora en el tipo de interés de la facilidad marginal de los préstamos del Banco central europeo incrementado en tres puntos.

#### **POR ESTOS MOTIVOS, EL TRIBUNAL**

1 Declara por once votos contra seis que se ha violado el artículo 8 del Convenio (RCL 1999, 1190, 1572);

2 Declara por dieciséis votos contra uno que la constatación de una violación constituye una satisfacción justa suficiente por el daño moral sufrido por el demandante;

3 Declara, por catorce votos contra tres,

a) que el Estado demandado pague al demandante, en un plazo de tres meses, la suma de 1.365 € (mil trescientos sesenta y cinco euros), convertida en la moneda del Estado demandado, al tipo aplicable en el momento del pago, más las cargas fiscales correspondientes, en concepto de costas y gastos;

b) Que estas sumas se verán incrementadas por un interés simple anual equivalente al tipo de interés de la facilidad marginal de los préstamos del Banco central europeo incrementado en tres puntos a partir de la expiración del antedicho plazo y hasta el pago;

4 Rechaza, por unanimidad, el resto de la solicitud como satisfacción suficiente. Hecha en inglés y en francés, y leída en audiencia pública en el Palacio de Derechos Humanos, en Estrasburgo el 5 de septiembre 2017. Firmado: Søren Prebensen, Secretario adjunto, Guido Raimondi, Presidente.

Se adjunta a la presente sentencia, de conformidad con el artículo 45 ap. 2 del Convenio (RCL 1999, 1190, 1572) y 74 ap. 2 del Reglamento, la exposición de las siguientes opiniones separadas: - opinión parcialmente disidente de la jueza Karakaş;

- opinión disidente conjunta de los jueces Raimondi, Dedov, Kjølbros, Mits, Mourou-Vikström y Eicke.