Los datos de ubicación de telefonía móvil también son datos personales, aunque la línea sea propiedad de la empresa.

Pilar Rivas Vallejo
Catedrática de Derecho del Trabajo y de la Seguridad Social. Universidad de Barcelona

Resumen: *El derecho a privacidad, intimidad y protección de datos personales incluye los datos relativos a ubicación procedentes de la información sobre el uso de medios de comunicación de telefonía (proporcionada por la compañía operadora), aunque esta sea propiedad de la empresa, pues permiten identificar distintos elementos que afectan a la privacidad. No considerarlos datos personales implica una omisión de tutela por los tribunales nacionales que juzgaron la reclamación del trabajador.*

Palabras clave: *Derecho a la intimidad. Monitorización del trabajo. Datos de ubicación. Protección de datos personales.*

Abstract: *The right to privacy and protection of personal data includes location data derived from the mobile phone operator, even if the company is the owner of this phone line, as it allows for the identification of various elements that affect privacy. Failure to consider this data as personal data is considered a denial of State protection before a judicial body.*

Keywords: *Right to privacy. Worker´s monitoring. Location data. Data protection.*

DOI: *https://doi.org/10.55104/RJL_00691*

I. Introducción

Se estima la demanda presentada por el Sr. Petro Dmytrovych Guyvan contra Ucrania por la vulneración del art. 8.1 del CEDH en fecha de 26/9/2016, como consecuencia de la injerencia de su vida privada o en su correspondencia, por falta de tutela del Estado resultante de la desestimación de su demanda sobre incumplimiento empresarial en materia de tratamiento de datos personales, siendo estos los procedentes de la línea telefónica titularidad de la empresa, en el marco de una investigación disciplinaria interna, que incluía el seguimiento de las comunicaciones del trabajador reclamante.

II. Identificación de la resolución judicial comentada

Tipo de resolución judicial: Sentencia

Órgano judicial: Tribunal Europeo de Derechos Humanos (sección quinta)

Número de resolución judicial y fecha: 6 de noviembre de 2025, Caso Guyvan c. Ucrania

Tipo y número recurso o procedimiento: demanda núm. 46704/2016

ECLI:ES:TS:2025:3826

Ponente: Katerina Simachkova (presidenta), Georgios A. Serghides, Gilberto Felici, Andreas Zünd, Mykola Gnatovskyy, Vahe Grigoryan, Sébastien Biancheri, y Victor Soloveytchik (secretario)

III. Problema suscitado. Hechos y antecedentes

El empleador efectuó un seguimiento de las comunicaciones del trabajador reclamante en el marco de una investigación interna, para el cual solicitó a la operadora de telefonía móvil contratada información detallada sobre determinadas llamadas realizadas con el terminal puesto a disposición del trabajador, información que la empresa se negó a compartir con el primero y que sirvió para adoptar decisiones disciplinarias, contra las que este demandó, siendo desestimada su demanda. En su sentencia, el Tribunal Supremo consideró que dicha información no tenía el carácter de datos personales. Frente a dicha resolución, el demandante solicita que el TEDH valore tal actuación como injerencia en su privacidad y tratamiento de datos personales, que no fue protegida por los tribunales ucranianos conforme establece el art. 8 del CEDH, puesto que el terminal en cuestión se usaba indistintamente para llamadas profesionales y personales, habiendo sido con anterioridad (desde 2002) una línea personal, que se tornó dual, asumiendo su coste su empleador, en 7/11/2003. Siete años después, la empresa emitió una orden expresa sobre aplicación de límites al uso de servicios de telefonía por los trabajadores (unos treinta euros mensuales), indicando los usos laborales admitidos a cargo de la empresa, que incluían tarifas en itinerancia internacional cuando se tratara de viajes de trabajo, y, asimismo, que el exceso de este tope sería descontado del salario. La investigación de la empresa del uso del teléfono por el demandante en 2015 fue motivada por uso de itinerancia internacional en fechas en las que aquel estaba en su lugar de trabajo. Por tal motivo solicitó a la operadora de telefonía móvil información detallada sobre las llamadas realizadas en itinerancia desde la línea del demandante y los países a los que se habían realizado estas en cierto periodo de tiempo. La información facilitada por la citada compañía incluía duración, fecha, hora y país de la comunicación, carácter de entrante o saliente y la identificación del número de teléfono comunicante, compañía extranjera prestadora del servicio de itinerancia, y tipología de comunicación (llamada/mensaje de texto). La investigación dio lugar a denuncia ante la policía de la ciudad de residencia del trabajador en 2015, de la que el reclamante tuvo conocimiento en junio de 2023.

El demandante alegó en su demanda contra la empresa la recopilación de información personal sobre él y la denegación de acceso a los datos recopilados por parte de la empresa, vulneradora de la normativa de protección de datos personales. El mes siguiente a dicha demanda fue despedido por ausencias injustificadas. La sentencia (de 16/12/2015) desestimó su demanda sobre acceso a datos personales, en virtud de la titularidad empresarial de la línea telefónica, considerando que no se había hecho un uso indebido de dichos datos ni se habían registrado datos personales del trabajador.

IV. Posición de las partes y planteamiento judicial

La sentencia que resuelve el recurso de apelación contra la mencionada resolución, dictada en 26/1/2016, confirma tal decisión, y entiende que la información sobre los servicios telefónicos de itinerancia fue explorada por la empresa solo con la finalidad de comprobar si había estado o no presente en su puesto de trabajo durante el horario laboral en los días de las llamadas analizadas, no con ulteriores fines como saber dónde había estado, con quién se había comunicado o incluso calcular el coste del reembolso del consumo telefónico. Dicha sentencia también fue confirmada por la del Tribunal Supremo de 14/4/2016, por negar este la naturaleza de datos personales a la información en cuestión. Por tal motivo, el demandante considera que los tribunales ucranianos no han amparado el derecho que le garantiza el art. 8 CEDH.

Por su parte, el Gobierno ucraniano se opone por razones formales, por no haber agotado los recursos internos, al no haber reclamado contra la operadora de telefonía móvil por compartir los datos descritos, y por razones sustantivas, por no tratarse de información confidencial ni de acceso al contenido de sus comunicaciones, sino a aspectos técnicos. El TEDH descarta la relevancia de la reclamación a la operadora de telefonía, y, por tanto, desestima dicha alegación, al considerar agotados los recursos nacionales contra la decisión impugnada, centrándose en la cuestión sustantiva, que requiere examinar el fondo del asunto, concluyendo que la demanda debe admitirse por no ser infundada.

Por otra parte, el Gobierno ucraniano, aunque niega la implicación del Estado, pues se trata de una disputa entre dos partes privadas, se ampara en que los tribunales que analizaron el caso aplicaron la jurisprudencia sentada en el asunto Bărbulescu c. Rumanía (núm. 61496/08, de 5/9/2017), y que la actuación empresarial se ajustaba a los requisitos exigibles por dicha doctrina para autorizar la monitorización de las comunicaciones en el ámbito del trabajo, pues la información recopilada, puramente técnica, se hallaba dentro de un rango de previsibilidad, si se considera que las órdenes empresariales respecto al uso de dispositivos móviles de empresa eran precisas y conocidas, por lo que recopilar tal información no puede ser constitutiva de injerencia en el derecho al respeto de la vida privada. Asimismo, afirma que no se recopilaron datos personales y que estos no eran confidenciales, así como que no se accedió, ni pudo hacerse, al contenido real de las comunicaciones.

V. Normativa aplicable al caso

Arts. 2, 5 y 8 del Convenio Europeo de Derechos Humanos (CEDH).

VI. Doctrina básica

1. Concepto de vida privada

La vida privada protegida por el art. 8 CEDH no se limita a la esfera más íntima del individuo, sino que abarca a otras manifestaciones de su esfera privada en las que puedan estar implicados terceros en ámbitos profesionales y públicos, como se afirmó en el caso López Ribalda (nos. 1874/13 y 8567/13, de 17/10/2019).

Respecto a su contenido, integra también la información relativa a la ubicación de una persona en un momento concreto (Uzun c. Alemania, núm. 35623/05, CEDH 2010, y Florindo de Almeida Vasconcelos Gramaxo c. Portugal, núm. 26968/16, de 13/12/2022). Por tal razón, los servicios de itinerancia de una línea de teléfono móvil, que incluyen la ubicación de su usuario, forman parte de tal derecho.

Así, en tanto que la empresa permitió al trabajador utilizar la línea telefónica profesional con fines privados, incluso desde el extranjero, con la condición de reembolsar su coste, se concluye que su uso estaba autorizado por la misma, pero ello no priva a la información referida de su carácter personal, como es la ubicación en un lugar y fecha concretas o las personas con las que podía haber interactuado el afectado. Por tales motivos, el art. 8 es aplicable al caso.

2. Concepto de datos privados y deberes activos y pasivos de tutela

El tribunal sostiene que el objeto del artículo 8 es esencialmente proteger al individuo contra la injerencia arbitraria de las autoridades públicas, desde una perspectiva pasiva -debe de abstenerse de tal injerencia- y activa -la obligación de procurar el respeto efectivo de la vida privada o familiar-, que implica la adopción de medidas destinadas a garantizar el respeto de la vida privada incluso en el ámbito de las relaciones entre individuos, y cuyo incumplimiento deriva en responsabilidad del Estado por omisión de tutela, como ya se indicó en el asunto López Ribalda y otros.

Para la correcta aplicación del art. 8 CEDH es necesario determinar con precisión los límites entre los deberes positivos y negativos que marca dicho precepto, si bien estos no se encuentran definidos con absoluta claridad. Pero lo que el TJUE considera

que sí resulta palmario es la necesidad de equilibrar los intereses privados y públicos en lid, en el marco del margen de apreciación del Estado (y con los medios que estime adecuados para garantizar el cumplimiento del art. 8), que el TEDH debe revisar para determinar si tal actuación (v.gr., crear legislación específica, a su discreción, para dar efectividad al derecho, en este caso en el ámbito laboral, o que los recursos existentes proporcionen protección suficiente al derecho afectado) fue compatible con las disposiciones del convenio invocadas.

En el ámbito laboral y respecto de la monitorización de las comunicaciones, los criterios delimitadores aludidos se encuentran fijados en la sentencia Bărbulescu: a) si el empleado ha sido informado de la posibilidad de que el empleador pudiera tomar medidas para monitorizar las comunicaciones y de la implementación de dichas medidas, b) el alcance de dicha monitorización y el grado de su intrusión en la privacidad del empleado, c) si el empleador ha proporcionado razones legítimas para justificar la monitorización, d) si habría sido posible implementar métodos y medidas menos intrusivos, e) las consecuencias de la monitorización para el empleado sometido a ella, y si este ha contado con garantías adecuadas contra la arbitrariedad; y f) garantizarle el acceso a un recurso ante el órgano judicial competente para valorar los anteriores criterios. En todo caso, y dentro del margen de apreciación de los tribunales nacionales, ignorar dicha ponderación de los intereses en conflicto y la protección de datos constituiría un incumplimiento del art. 8 (STEDH Liebscher c. Austria, núm. 5434/17, de 6/4/2021).

En este caso, el contrato de telefonía móvil suscrito por la empresa le facultaba para recibir información acerca de las llamadas y mensajes emitidos y recibidos a fin de valorar cuáles eran de índole laboral, al objeto de determinar el coste a repercutir en el trabajador. Sin embargo, la finalidad de la solicitud del empleador (cursada en distintos días de 2015) fue otra muy distinta: recopilar y procesar datos para constatar la ubicación concreta del trabajador en determinadas fechas. Tales datos se encontraban enriquecidos con información adicional, innecesaria incluso para saber si el trabajador había estado en su lugar de trabajo en las fechas indicadas, como los números de teléfono con los que había interactuado el demandante y los países en los que se habían usado servicios en itinerancia. Tal exceso de información, no precisa para los fines legítimos autorizados por su recopilación, deviene invasión de la intimidad del empleado, cuya justificación había de evaluarse por los tribunales nacionales, pero, al no realizarse dicha valoración en su integridad, fallaron en la tutela que debían dispensarle con arreglo al art. 8 CEDH, al negarle a la información comprometida el carácter de dato personal. Por tal razón, el Estado incumplió sus obligaciones positivas en virtud del artículo 8 del Convenio.

VII. Parte dispositiva

La sentencia estima la demanda respecto de la vulneración del art. 8.1 del CEDH, y desestima el resto de las pretensiones accesorias de la misma.

VIII. Comentario

1. Los datos de ubicación son datos personales. La vida privada también puede desarrollarse en ámbitos laborales

Las previas SSTEDH (Gran Sala) de 5/9/2017 (asunto Bărbulescu c. Rumanía) y de 17/10/2019 (asunto López Ribalda y otros c. España) ya habían resuelto casos similares. La primera de ellas (Bărbulescu), la monitorización de una aplicación de mensajería instantánea -Yahoo Messenger-, usada con fines disciplinarios, y la segunda (asunto López Ribalda) la colocación de cámaras ocultas para la comprobación de irregularidades cometidas por trabajadores, también con fines disciplinarios. Ambas afirman que la vida privada (derecho a la intimidad personal en el derecho español, ex art. 18.1 CE, SSTC, Pleno, núm. 119/2022, de 29/9, y 66/2022, de 2/6), es un concepto que puede integrar también actividades profesionales, y que debe quedar protegida en el ámbito del trabajo, pese al reconocimiento de las facultades empresariales de vigilancia y control de la actividad laboral (en cuyo marco los

derechos fundamentales conservan igualmente su eficacia, SSTC núms. 88/1985, 6/1988, 129/1989, 126/1990, 99/1994, 106/1996, 186/1996, 90/1997, entre otras), porque en esta también existe vida privada, en la que quedan incluidas las comunicaciones, que, aun siendo laborales, constituyen correspondencia a los efectos protegidos por el CEDH.

Por otra parte, en el marco europeo y conforme al art. 4.1 RGPD, constituyen datos personales los datos de localización o ubicación (física o digital, a través de la identificación de la IP, SSTJUE de 24/11/2011, asunto Scarlet Extended, C-70/10, y de 19/10/2016, asunto B., C-582/14, respecto de las direcciones IP dinámicas si estas se acompañan de datos adicionales que permitan identificar al usuario, y STEDH de 24/4/2018 -rec. núm. 62357/2014-, asunto B. contra República de Eslovenia), mientras que el art. 2 del Convenio 108+ para la protección de las personas respecto al tratamiento automatizado de datos de carácter personal (2018, modernización del Convenio 108 de 1981), del Consejo de Europa, no efectúa tal concreción y los define como *cualquier información con respecto a un individuo identificado o identificable*. También el Tribunal Constitucional español (STC núm. 292/2000) ha afirmado que el derecho reconocido en el art. 18.4 CE incluye, más allá de los datos íntimos, cualquier tipo de dato personal, y protege tanto la utilización de los datos como su propia adquisición (SSTS de 21/9/2015 -rec. núm. 259/2014- y de 7/2/2018 -rec. núm. 78/2017). El TJUE relaciona la vida privada y la correspondencia con la expectativa razonable de respeto a la propia intimidad (SSTJUE B. contra Rumania, núm. 61496/08, y C. contra el Reino Unido, núm. 62617/00), sin ser dicha expectativa, no obstante, necesariamente concluyente, pero sí sujeta a una interpretación amplia, en aplicación del Convenio 108 del Consejo de Europa (STJUE A. contra Suiza, núm. 27798/95). Asimismo, considera que el art. 8 del CEDH ampara toda la información personal ligada a comunicaciones, así los datos de medición en los números de teléfono marcados (STJUE M. contra el Reino Unido, de 2/8/1984), y datos referentes al teléfono, correo electrónico y uso de Internet (sentencia C. contra Reino Unido).

En España, la STS núm. 163/2021, de 8/2, invocaba las razones de mercado para tolerar la geolocalización de los trabajadores durante la ejecución de su trabajo al valorar el llamado «proyecto Telepizza»[1]. Con ocasión de aquella sentencia, ya se apeló a la posibilidad de que el uso de medios de propiedad empresarial no impedía la captación de datos igualmente personales. El TEDH viene con la sentencia de 6 de noviembre de 2025 a confirmar que los datos de ubicación son datos personales a los efectos del CEDH y de su protección por el art. 8 como manifestación del derecho a la vida privada, sea cual sea la forma en que sean captados u obtenidos tales datos y sin perjuicio de que dicho tratamiento sea admitido como medio de control de la actividad laboral por un empleador. Es decir, la premisa que con esta resolución resulta indiscutible es que los datos de ubicación procedentes de un dispositivo puesto a disposición por la empresa para la ejecución del trabajo, es decir, propiedad de la empresa (en este caso, no el propio dispositivo, pero sí la línea que permite su operatividad), son datos personales y que la propiedad de los medios de trabajo (la línea telefónica en este caso) no es óbice para descartar que un dato concreto, como es la ubicación (*a priori* caracterizada como dato personal en el marco del art. 4.1 RGPD), tenga dicha naturaleza, como el resto de los que acompañan a la identificación del uso de la línea telefónica.

Caba apuntar que, a efectos de calibrar el alcance de la invasión de una intromisión en el uso de un teléfono inteligente, aunque no se explicita en la resolución comentada, un dispositivo inteligente como el que debemos suponer empleaba el demandante puede operar sin necesidad de compañía de telefonía de soporte, a través de conexión libre a cualquier wifi externa, y que, en el caso enjuiciado, la consulta a la operadora contratada por la empresa solo le permitía conocer la operatividad del terminal usando los servicios de dicha compañía. En consecuencia, que los datos facilitados abarcaban únicamente a los que fueron operados por la empresa de telefonía contratada, lo cual incluye no solo llamadas, sino también tráfico de internet en itinerancia y mensajería instantánea (short message service, SMS) si esta opera con servicio de datos (y no conexión a wifi), con exclusión de otro tipo de

mensajería distinta a la corta de telefonía (SMS), v.gr. WhatsApp, o, como en la sentencia Bărbulescu, Yahoo Messenger u otro similar.

Pues bien, los datos de ubicación, por más que se correspondan con tiempo y/o lugar de trabajo, pueden ser depositarios de otra información sensible que defina a la persona en rasgos, ideología o costumbres, incluida cualquier acción que, llevada a cabo en contextos laborales, pudiera ser usada por la empresa con distintos fines, entre ellos los disciplinarios, al revelar la presencia de un trabajador en determinados lugares identificados con características, inclinaciones o ideología personales (v.gr. lugares de culto, consumo de determinados productos o servicios, afiliación o asociación concretas…) o simplemente gustos o hábitos, de los que inferir rasgos de personalidad, ideología, tendencias … que sirvan a su empleador para adoptar ciertas decisiones desfavorables, especialmente si tales datos son tratados por un sistema de inteligencia artificial (IA) que extraiga de su explotación conclusiones o recomendaciones de utilidad para la empresa. Y es que un dato aislado como el de una ubicación en un momento concreto quizás otrora pudiera calificarse de insuficiente relevancia, como de hecho parece traslucir la STS núm. 766/2020, de 15/9 -rec. núm. 528/2018-, cuando alude a que los datos de posicionamiento obtenidos del GPS «no permiten captar circunstancia alguna de sus ocupantes ni su utilización refleja -ni tiene capacidad para ello- ninguna circunstancia personal (que le lleva a descartar la invasión de la esfera de privacidad, como consecuencia de limitarse a la ubicación y movimiento del vehículo)», pero no sucede lo mismo en la era de la inteligencia artificial, que permite exprimir cualquier tipo de dato para obtener una información final enriquecida por las inferencias producidas por la conjunción de datos manejados por el sistema de IA.

En consecuencia, admitido su carácter personal, que trasciende más allá de la mera ubicación de una persona en un momento concreto, ocurra esto o no en tiempo de trabajo, acceder o conocer los datos de ubicación y de geolocalización constituyen vulnerabilidades de protección de la intimidad de una persona, que permitan acceder intrusivamente a ella, y que exceden, por tal razón, de las expectativas de intimidad de cualquier persona (como afirma la STS núm. 766/2020, de 15/9 -rec. núm. 528/2018-, basada en la existencia de disposiciones o reglas expresas o en un uso social de tolerancia), como la del demandante en este caso, al no esperar que la empresa solicitara tales datos a la operadora de telefonía (aun cuando tenga el legítimo derecho que le confiere ser el titular de la línea). Por ello su conocimiento y, en su caso, uso empresarial con fines laborales no puede considerarse meramente accesorio e instrumental de sus facultades de dirección y control cuando se utilizan herramientas de trabajo propiedad de la empresa, en este caso, la línea telefónica móvil, aun en el contexto puramente laboral, como pueda ser en tiempo de trabajo (v.gr, dónde se realiza una parada para desayunar o comer o para atender a un asunto personal durante la jornada de trabajo, que los sistemas digitales que incorporan métodos reputacionales incluso permiten compartir con usuarios y clientes del servicio prestado). Por el contrario, en tanto que se conceptúen como datos personales, aun dentro de este marco estrictamente laboral, cualquier tipo de injerencia debe someterse a los requisitos fijados por la sentencia Bărbulescu para la admisión de intrusiones empresariales calificables como legítimas. En suma, el uso de medios de titularidad empresarial no excluye la necesidad del análisis de proporcionalidad, idoneidad y legitimidad en su control por el empleador.

2. La admisión del control de la ubicación y la geolocalización por la empresa

El respeto a la privacidad o intimidad se reconoce en el art. 8 CEDH, como en el art. 7 de la Carta de derechos fundamentales de la Unión Europea (que integra en tal derecho el respeto a sus comunicaciones), así como en el art. 8 de la misma carta (derecho a la protección de datos de carácter personal, desarrollado en el RGPD de 2016), o en el art. 18 de la Constitución Española (CE).

Según la doctrina constitucional española, el derecho fundamental a la intimidad personal otorga una facultad negativa o de exclusión, «que impone a terceros el deber de abstención de intromisiones salvo que estén fundadas en una previsión legal que

tenga justificación constitucional y que sea proporcionada» (SSTC núms. 85/2003, de 8/5, y 66/2022, de 2/6) y que permite decidir qué datos se comparten o proporcionan a un tercero (STJUE de 4/5/2023, C-487/21) y, asimismo, oponerse a su posesión o uso por un tercero (STC núm. 39/2016, de 3/3), para lo cual constituye presupuesto necesario el conocimiento de cuál es la finalidad perseguida por su captación o recopilación.

La jurisprudencia del TEDH -Sentencia 2/9/2010, caso Uzun v. Alemania- entiende que el art. 8.1 del CEDH abarca el derecho de todo ciudadano a desarrollar relaciones personales sin ser sometido a innecesarias injerencias en su vida privada, y, en dicho contexto, escala el grado de interferencia en la intimidad para situar en un nivel subordinado o menos intrusivo la geolocalización (STEDH de 8/2/2018, asunto Ben Faiza c. Francia, núm. 31446/12) respecto de la vigilancia de las telecomunicaciones telefónicas (SSTEDH de 2/12/2010, Uzun c. Alemania, y de 27/10/2015, R.E. c. Reino Unido), si bien refiere esta graduación a contextos de vigilancia pública (STJUE de 16/3/2023, C-351/2021, asunto Beobank) o policial, que comprometen no solo los parámetros delimitadores de las comunicaciones telefónicas, sino también su propio contenido. En contextos privados como las relaciones de trabajo, estos límites son de igual aplicación y, por ende, los datos de ubicación obtenidos a partir de una operadora de telefonía serían una clara intrusión en la vida privada, o en la intimidad personal.

La sujeción al círculo organizativo empresarial legitima la supervisión de la correcta ejecución del trabajo, que se extiende al uso de medios y herramientas de trabajo, incluidos los de comunicación, facilitados por la empresa (y que en España tiene su fundamento en el art. 20.3 ET, conforme a la interpretación de las SSTC núms. 186/2000, de 10/7, y 170/2013, de 7/10, entre otras). La propiedad y control de dichos medios y el fin perseguido con ello establece una nítida separación con los contextos públicos de vigilancia y seguimiento, que faculta al empleador para ejercer por sí mismo dicha vigilancia, y a usar los datos así obtenidos con fines disciplinarios. Fin legítimo (STEDH Bărbulescu) que, en tanto que supone un límite al pleno ejercicio de un derecho fundamental, se encuentra sometido al cumplimiento de los principios de idoneidad, necesidad y proporcionalidad (STC núm. 119/2022, de 29/9, Pleno -rec. núm. 7211/2021-), bajo la autoadministración del propio empleador (que justifica el tratamiento de datos según el art. 8.1 de la Carta europea de derechos humanos), en el marco del derecho interno de los Estados miembros del Convenio, bien sea a través de legislación específica (compatible con el estado de derecho, STJUE L. y otros contra Reino Unido, núm. 58243/00, de 1/7/2008, y S. y otros contra Finlandia, 58243/00, de 27/9/2005), si esta resulta necesaria, a juicio de tal Estado, cuando se trata de relaciones entre particulares, bien a través de garantías procesales (que incluyen el control judicial posterior, pues su control previo no puede ser fiscalizado, como en el ámbito penal, por órganos judiciales mediante autorizaciones de seguimiento, pese a su menor entidad, por no utilizar medios especialmente invasivos con carácter previo como serían los dispositivos de geolocalización, sino de control ex *post* a través del auxilio de la compañía de telefonía -STS, Sala II, núm. 824/2022, de 19/10 -rec. núm. 10094/2022-).

Dicha legislación debe garantizar, asimismo, que los datos personales conservados estén protegidos eficazmente contra el mal uso y el abuso conforme al art. 7 del Convenio 108 (STEDH de 30/1/2020 -rec. núm. 50001/2012-, asunto Breyer contra Alemania). En cuanto respecta a la monitorización de las comunicaciones en el ámbito del trabajo, los criterios que permiten su admisión se basan en cinco condiciones: notificación previa a los interesados (sobre adopción de la medida y forma de implementarla), alcance limitado de la monitorización y grado de intrusión exclusivamente necesario en la privacidad del empleado, concurrencia de razones legítimas para justificar la monitorización, inexistencia de alternativas menos intrusivas, información sobre las consecuencias de la monitorización para el empleado sometido a ella, y existencia de garantías adecuadas contra la arbitrariedad de la medida. Mientras la última resulta exigible a la legislación interna del Estado en cuestión, el

resto son directamente aplicables a la actuación empresarial (y, por tanto, fiscalizables por los órganos judiciales nacionales).

No es menos cierto que estamos ante un caso de desvinculación entre la titularidad empresarial y el uso privativo de la línea telefónica por el trabajador, como demuestra no solo que esté adscrita a su propio terminal, sino también el pacto de uso privado con asunción empresarial del coste, que convirtió a la línea sufragada por la empresa en una línea mixta, laboral y privada a la vez. Circunstancia que cobra especial relevancia en cuanto resulta extrapolable a situaciones similares, con idénticos pactos entre las partes o usos internos de empresa, por los cuales la parte trabajadora comparte una misma línea para asuntos privados y para fines profesionales.

En tales contextos, cualquier acción indagatoria desplegada por la empleadora (por sí misma o con el auxilio de un tercero, como, en este caso, la operadora de telefonía) sobre la línea telefónica (aun en su calidad de titular de aquella) y los detalles de su uso puede suponer una intromisión en la privacidad de la parte trabajadora, al convivir datos personales y profesionales, sin perjuicio de considerar que los de índole profesional puedan igualmente reunir el carácter de personales, como ya se ha analizado anteriormente.

Por tanto, conforme a las sentencias del TEDH Bărbulescu y López Ribalda, el correcto equilibrio entre los respectivos bienes jurídicos protegidos exige sujeción del control empresarial a los parámetros indicados, especialmente los de orden informativo y los relativos a la calibración de la idoneidad y proporcionalidad de la medida, si bien cabe matizar que la información previa a los sujetos objeto de vigilancia no ampara cualquier medida de control si la prueba de proporcionalidad no resulta positiva, y que tal información debe ser exhaustiva, comprendiendo no solo la forma de aplicar la medida, sino también la finalidad de esta y sus ulteriores consecuencias (v.gr., disciplinarias). También es doctrina de nuestro Tribunal Supremo que el control de los medios de trabajo facilitados por la empresa, incluidos los de comunicación, requiere haber establecido previamente las bases para el uso y haber informado a los trabajadores sobre dicho «control de los medios a aplicar en orden a comprobar su correcto uso, así como las medidas a adoptar para garantizar la efectividad laboral del medio informático cuando fuere preciso» (STS de 8/3/2011 -rcud. núm. 1826/2010- y del Pleno de 6/10/2011 -rcud. núm. 4053/2010-), que permitan soslayar la expectativa razonable de intimidad generada en los trabajadores a partir del uso social permitido o tolerado por la empresa.

En el caso analizado, se han incumplido ambas condiciones. La primera -deber informativo previo- porque los empleados podían tener conocimiento implícito de la posible vigilancia del uso de los medios de comunicación facilitados por la empresa, restringidos a finalidades puramente laborales, pero no del recurso al auxilio de terceros (la operadora de telefonía móvil) para completar la indagación sobre tal uso, ni del grado de intrusión permitido por la información recabada por la empresa, que abarcó no solo su ubicación en determinados días, sino las personas con las que estableció comunicación, como tampoco de la finalidad que se daría a los datos obtenidos (la ubicación del trabajador), distinta de la que resulta coherente con los términos del pacto entre ambos: la asunción personal del coste que superara un límite mensual (para cuya determinación, pese a que el TEDH parece admitir como plausible que la solicitud de información a la operadora de telefonía móvil se destinara a discriminar las llamadas laborales de las privadas, no parece necesario conocer la ubicación del trabajador ni tampoco los contactos establecidos), mientras que el propio contenido de la actuación empresarial revela, *per se*, ulteriores intenciones de índole disciplinaria (que se tradujeron en el inmediato despido disciplinario). De igual modo, tiene especial relevancia en la graduación de la intrusión la existencia de uso social o tolerancia por parte de la empresa en la utilización de la línea telefónica para finalidades profesionales y personales indistintas, que conllevan una legítima expectativa de privacidad para el trabajador implicado. La segunda condición tampoco se ha cumplido, porque los medios empleados para el fin buscado no se ajustan al requisito de la necesidad, ya que los datos de ubicación no resultaban precisos para

comprobar si el trabajador se encontraba o no en su puesto de trabajo en determinadas fechas (para tal comprobación existen otros medios adecuados y menos invasivos). Las medidas restrictivas de derechos fundamentales en el contexto laboral deben superar el juicio de proporcionalidad para ser admitidas (esto es, juicio de idoneidad -si la medida es susceptible de alcanzar el objetivo propuesto-, juicio de necesidad -si no existe otra alternativa menos invasiva de igual eficacia-, y juicio de proporcionalidad -si es equilibrada, en tanto no resulta más perjudicial que el interés protegido para otros valores en conflicto-), sin que baste, por tanto, cumplir con la notificación de la aplicación de la medida de vigilancia (al respecto, vid. STS núm. 766/2020, de 15/9/2020 -rec. núm. 528/2018-, sobre geolocalización de trabajadora a través de dispositivos de geoposicionamiento en vehículo de empresa fuera de la jornada laboral, conociendo la misma la prohibición empresarial de uso del vehículo para fines personales), y descartando toda equivalencia entre consentimiento -implícito- y conocimiento.

La sentencia deja apuntado, finalmente, que el uso de datos de ubicación con fines disciplinarios no supera la prueba de necesidad, además de ser divergente con la utilidad legítima de recabar los datos proporcionados por la compañía telefónica -discriminar las llamadas de índole personal de las de carácter profesional para dar cumplimiento al pacto sobre asunción de los costes de la línea-, por ser otra la finalidad real que persiguió la inmisión -determinar la localización exacta del trabajador en ciertas fechas-. En definitiva, la comprobación del debido cumplimiento de los deberes laborales no ampara medidas de índole policial como los datos de ubicación en fechas concretas, puesto que existen otros medios menos invasivos a disposición de cualquier empresa para realizar tal comprobación.

IX. Apunte final

En todo caso, lo que se enjuicia en este caso y la importancia de la resolución no es en sí la aplicación de los criterios sentados en la sentencia Bărbulescu y López Ribalda (reiterados en esta decisión judicial), sino la naturaleza de los datos analizados, los datos de ubicación vinculados a una línea telefónica, calificados como datos personales, la consideración como tales de ciertos datos unidos al uso de medios empresariales, y, en último término, la necesidad de valorar como hipotéticos datos personales todos aquellos que permitan aproximar una identificación personal como presupuesto para decidir acerca de la legitimidad de decisiones empresariales, aun dentro de sus facultades organizativas y disciplinarias, cuya omisión puede devenir en una falta de tutela por órganos jurisdiccionales.

NO SE HA UTILIZADO NINGUNA IAG PARA REDACTAR ESTE ARTÍCULO

Referencias:

1. ^ *Comentada en un número anterior de esta revista (3/2021), Rivas Vallejo, Pilar: «Geolocalizar a los trabajadores no es invasión de su intimidad si el dispositivo utilizado para ello es propiedad de la empresa», https://doi.org/10.55104/RJL_00226.*