Política de uso de dispositivos digitales y control empresarial: los metadatos también son datos personales.

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

Resumen: *La resolución comentada legitima la política empresarial de uso de dispositivos digitales porque entiende cumplido el test de proporcionalidad, necesidad e idoneidad, y afecta principalmente a metadatos y solo subsidiariamente a contenido de las comunicaciones, aunque no se haya negociado con la RLT. Sin embargo, en tanto que los metadatos también pueden permitir inferir datos personales, precisarían de mayor concreción sobre el alcance y finalidad de su tratamiento.*

Palabras clave: *Intimidad. Secreto de las comunicaciones. BYOD. Aplicaciones corporativas. Control empresarial.*

Abstract: *This resolution upholds the company´s digital device policy, finding the proportionality, necessity, and suitability tests satisfied, and considering that it primarily affects metadata rather than content, despite the absence of negotiation with Workers´ Representatives. However, as metadata may enable the inference of personal data, clearer limits on its scope and purpose are required.*

Keywords: *Privacy. Confidentiality of communications. BYOD. Corporate applications. Corporate control.*

DOI: *https://doi.org/10.55104/RJL_00730*

ECLIS: *ECLI:ES:AN:2026:594*

I. Introducción

La sentencia comentada analiza la política de uso de dispositivos digitales de la empresa en aplicación del artículo 87 Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD), para determinar cuál es el sentido del derecho de participación de la representación legal de los trabajadores (RLT) y si dicha política vulnera los derechos fundamentales de intimidad y secreto de las comunicaciones.

II. Identificación de la resolución judicial comentada

Tipo de resolución judicial: sentencia.

Órgano judicial: Audiencia Nacional (Sala Social).

Número de resolución judicial y fecha: 31/2026, de 18 de febrero.

Tipo y número procedimiento: procedimientos acumulados núms. 301/2025 y 328/2025.

ECLI:ES:AN:2026:594

Fuente: CENDOJ

Ponente: Ilmo. Sr. D. Juan Gil Plana.

Votos particulares: carece.

III. Problema suscitado. Hechos y antecedentes

La cuestión analizada en la sentencia comentada conecta con un documento elaborado por la empresa Nestlé sobre política de uso de dispositivos digitales en aplicación del artículo 87 LOPDGDD, impugnado por los sindicatos UGT-FICA, CSI-F, CGT, y FI-USO, en demanda de conflicto colectivo y por Comisiones Obreras, en sendas demandas acumuladas contra Nestlé España S.A. y Nestlé Purina Petcare España S.A.U. Ambas solicitan la nulidad de dicha política por incumplir con el derecho de participación de la representación legal del personal y por vulnerar los derechos de intimidad y de secreto de las comunicaciones, al implicar control sobre tráfico y contenido de dispositivos, correo electrónico e incluso aplicaciones instaladas y usadas en los dispositivos privados.

IV. Posición de las partes y planteamiento judicial

Los demandantes, con argumentario parcialmente divergente en cada caso, instan la nulidad del anexo a la política global de seguridad del usuario final (e indemnización accesoria) por dos motivos: a) no haberse dado participación y consulta a la RLT, constituyendo una vulneración de los artículos 64 ET y 87 LOPDGDD, y b) la vulneración de los artículos 18 CE y 87 LOPDGDD consecuencia del sistema empresarial de control aleatorio de cuentas personales y de su contenido, así como monitorización, supervisión y registro de los recursos y contratación interna de la política empresarial de «bring your own device».

La demandada sostiene que sus políticas de uso de medios tecnológicos, que prohíben el uso personal de ciertas herramientas TICs, se remontan al año 2003 (y versión posterior de 2018), y por ello nunca existió expectativa de privacidad plena, por ser conocida la prohibición de almacenar información personal en equipos corporativos y del uso personal del correo electrónico, así como la política de seguridad del usuario final vinculada con el principio de minimización de datos, a la que se une en 2023 la regulación del «bring your own device», y en 2025, una nueva política de seguridad adaptada al artículo 87.3 que flexibiliza para conceder usos privados ocasionales y justificados. Aclara que el control, legitimado por el artículo 87.1 y dirigido solo al tráfico de correos desde las cuentas corporativas hacia cuentas personales y no a su contenido, obedece a dos tipologías: uno aleatorio, preventivo y no intrusivo, referido al tráfico de mensajes, observando patrones de comportamiento sobre tráfico, consumo anómalo de datos, conexiones sospechosas, tráfico de actividad y metadatos, y otro concreto, motivado por la existencia de indicios concretos de comportamientos anómalos. Afirma que la participación exigida por el artículo 87 no se concreta en una negociación ni exige acuerdo, ni tampoco lo precisa el artículo 64 ET, pero que se respetó el derecho, al haberse concedido distintos periodos de alegaciones, que fueron consideradas por la empresa.

Por su parte, el M.º Fiscal interesa la desestimación de la demanda por haber existido participación de la RLT y no incurrir el anexo en las vulneraciones alegadas, al ser el ámbito del trabajo ajeno al desarrollo de la vida privada, y regular el protocolo solo las medidas de seguridad sobre los medios tecnológicos digitales corporativos.

V. Normativa aplicable al caso

Artículo 18 de la Constitución Española (CE), artículo 87.3 de la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD), y artículo 64 ET.

VI. Doctrina básica

En la sentencia analizada se abordan dos derechos: a) el de intimidad y secreto de las comunicaciones en el contexto del uso de dispositivos digitales conforme a la política de uso adaptada al artículo 87 LOPDGDD, y b) el de participación de la representación legal de los trabajadores en la elaboración de dicha política.

Por lo que respecta al primer aspecto, se sintetiza toda la evolución jurisprudencial europea y española en la materia, para concluir que esta consiente la supervisión de dispositivos titularidad de la empresa, así como los particulares dentro del sistema «BYOD», si dicho control forma parte de la política empresarial de uso de dispositivos digitales y se acomoda al artículo 87 LOPDGDD, excluyendo así la expectativa de privacidad derivada de la autorización, excepcional y restrictiva, del uso de los medios empresariales para fines personales, por cuanto dicha política informa a los usuarios de que la información que pueda verterse al dispositivo se encuentra expuesta a conocimiento empresarial.

En suma, la doctrina de la prolija sentencia que se glosa se condensa en las siguientes ideas (desarrolladas a partir de su página quince):

- El derecho fundamental a la intimidad y al secreto de las comunicaciones subsiste aun cuando exista un control empresarial legítimo y conocido del uso de dispositivos digitales. La ausencia de expectativa de privacidad a efectos de control no elimina la vigencia del derecho fundamental, que exige en todo caso el respeto del test de proporcionalidad, la delimitación de los usos autorizados y la previsión de garantías adecuadas (FD 5.º, *in fine*), pues «el reconocimiento de un uso personal no impide, ni anula, la facultad empresarial de control del dispositivo respecto a ese uso personal» (FD 7.º, 3.1 a), aunque deba someterse a los términos dispuestos en el propio anexo (garantía del respeto y cumplimiento del canon de constitucionalidad que supone la aplicación previa del test de proporcionalidad).
- El artículo 87 LOPDGDD (cuyo apartado tercero ordena a los empleadores establecer los criterios de uso de los dispositivos digitales puestos a disposición para desarrollar la prestación laboral) condiciona la expectativa de intimidad a la existencia de información previa y de otros presupuestos (indicación de las finalidades y alcance del control, su metodología y tipología, posibles actuaciones, y garantías previstas).
- Tal facultad empresarial, tal como se describe en el documento litigioso, se extiende a los dispositivos propiedad de la empresa cuando en ellos se actúe en un entorno puramente corporativo, a las cuentas de correo electrónico personal cuando se accede a ellas desde un dispositivo empresarial, y a las aplicaciones empresariales usadas en dispositivos personales. La sentencia valida el control sobre todos ellos, al considerar que la política empresarial se ajusta al canon constitucional de proporcionalidad. Al mismo tiempo entiende coherente explicitar que los instrumentos de trabajo «va(n) a ser objeto de control su uso, sin que dicha previsión suponga per se una lesión del derecho de intimidad», así como la

prohibición de alojar en los dispositivos digitales corporativos información intima o privada (que no se entiende invasiva del derecho de intimidad), o la inspección de mensajes de correo salientes dentro del método aleatorio de control.

- Se considera que el legítimo control admitido por el artículo 87.2 LOPDGDD también alcanza a su *contenido* (de los dispositivos, los mensajes enviados, su extensión y contenido, así como los historiales de navegación o el acceso remoto o forzado) y su *regularidad* (monitorización regular, preventiva aleatoria y generalizada). Respecto a la primera cuestión, se concluye que el artículo 87.2 LOPDGDD admite dos finalidades: el cumplimiento de las obligaciones laborales y garantizar la integridad de los dispositivos, y estas se cumplen en el documento litigioso, pues, aunque se prevé tanto respecto al flujo de actividad como al contenido, ambos casos están amparados por el precepto, que admite el acceso al contenido, siempre que se cumplan las finalidades autorizadas y se apliquen las garantías del artículo 87.3. Se argumenta que incluso la empresa opta por un método menos invasivo, como es el filtrado de metadatos, frente al control del contenido (previsto como alternativa subsidiaria), aunque el artículo 87.2 habilita el acceso al contenido. El tribunal también avala la naturaleza del control, por ajustarse a una justificación objetiva, conectada con el tamaño de la organización y el grado de sensibilidad de la información que gestiona, que legitima la necesidad de verificar el uso adecuado del canal corporativo y prevenir posibles riesgos legales o reputacionales dentro de su programa de compliance. Y lo entiende tolerable porque se concibe sin carácter exhaustivo, masivo, permanente, continuo ni intrusivo, sino referido solo a muestras representativas, conforme a criterios técnicos de proporcionalidad y pertinencia, reservando el acceso al contenido al cumplimiento de los principios de proporcionalidad, necesidad y minimización de datos.
- Se admite, igualmente, la monitorización y supervisión, porque se somete al test de proporcionalidad, acomodándose así a las exigencias del artículo 87.3 LOPDGDD y a la interpretación constitucional relativa a la valoración del equilibrio entre la vigencia de los derechos fundamentales y el control empresarial.
- Por lo que respecta a la política de *bring your own device*, se descarta cualquier vulneración, al entender que el pleito se ciñe a la configuración de los criterios contenidos en dicha política BYOD (apartado quinto del anexo) y no a futuras interpretaciones en su aplicación práctica, que precisará un control judicial *ad hoc* una vez tuviera lugar la hipotética vulneración. Por ello excluye la aplicación de la doctrina del TEDH, que «nace del enjuiciamiento de prácticas de control empresarial realizadas, no del establecimiento de criterios de uso de los dispositivos digitales», aunque lo que cuestionara el sindicato Comisiones Obreras era la necesidad de limitar la extensión del control más allá de las aplicaciones y datos estrictamente corporativos alojados en dispositivos personales.
- Subraya la resolución que la utilización de los medios personales para el desarrollo de la prestación laboral se concibe como algo excepcional y siempre previa solicitud del empleado, por lo que «parece lógico que la empresa aclare… que dichas aplicaciones permitirán controlar el adecuado uso que se realice de dichas aplicaciones corporativas» y atenerse a la inexistencia de expectativa de privacidad en el manejo de dichas aplicaciones.

- En el supuesto concreto de incidentes de seguridad también regulado, el tribunal reputa legítima la finalidad de salvaguardar la seguridad de las aplicaciones corporativas instaladas, la información en ellas contenida, y la información descargada en el dispositivo, ya que la intrusión en este caso se limita al bloqueo remoto del «acceso a las aplicaciones o utilidades corporativas que se hallasen almacenadas en el dispositivo o eliminarlas, junto con los archivos adjuntos» descargados, sin afectar a otros contenidos del dispositivo personal, y que «dicha facultad de bloqueo o eliminación no se configura de forma general, ni permanente, ni aleatoria, sino solo cuando se aprecie unas circunstancias concretas que supongan un incidente de seguridad».
- Se descarta igualmente la vulneración del derecho al secreto a las comunicaciones, al no ser los controles aleatorios exhaustivos, masivos, permanentes, continuos, ni intrusivos, y limitarse su ejecución a muestras representativas, siempre conforme a criterios técnicos de proporcionalidad y pertinencia, pues «la facultad de control empresarial por definición tiene que ser regular en el sentido de que el empresario puede desarrollarla en cualquier momento, puede tener carácter preventivo para vigilar tanto el cumplimiento de las obligaciones laborales como evitar posibles incumplimientos, puede ser generalizado y aleatorio en el sentido que puede dirigirse respecto de cualquier faceta del ciclo productivo y respecto de cualquier persona». En la obtención de información relativa al tráfico de datos desde o hacia los recursos TIC de la empresa, «parece razonable que el control consista en recabar información de datos de tráfico, sin que ello suponga, en principio una afectación del derecho al secreto de las comunicaciones». Sentencia, así, que eliminar funciones o utilidades del dispositivo en nada afecta al secreto de las comunicaciones, sino solo a contenido profesional.
- Aunque se descarta la aplicabilidad de la doctrina del TEDH, se sostiene que se cumplirían igualmente su parámetros, al constar la previa información de la política de control empresarial a los trabajadores (STEDH de 5/9/2017), el alcance de tal supervisión, grados de intrusión en la vida privada, sujetos con acceso a los resultados de control (apdo. 5.5), intereses legítimos y alcance del control (determinando el carácter subsidiario del acceso al contenido), garantía general de que cualquier medida de control deberá pasar previamente el filtro del triple juicio de idoneidad, necesidad, proporcionalidad y justificación de las medidas, así como proporcionalidad, monitorización no indiscriminada, minimización o eliminación inmediata de los datos, y ausencia de intromisión o afectación a la esfera íntima. Refuerzan tales garantías que la adopción de una medida de control no corresponderá únicamente al departamento de recursos humanos y que cualquier sanción se someterá a procedimiento contradictorio, o que se prevean las consecuencias del control. Se considera, asimismo, que, aunque no estamos ante prácticas concretas, el anexo también prevé la necesidad de utilizar medios menos intrusivos si ello es posible (juicios de idoneidad y necesidad integrados en el canon constitucional de proporcionalidad).

La segunda cuestión planteada, la vulneración del derecho de participación de la RLT, obtiene el mismo resultado desestimatorio en ambas demandas. La Sala excluye la vulneración alegada y, con ello, la nulidad del anexo controvertido, por no admitir que el documento se adoptara sin previa consulta, sino teniendo en cuenta la opinión de dichos representantes en dos ocasiones, suspendiendo su aplicación hasta considerar e incluso incorporar algunas de sus recomendaciones. Se identifica la solicitud de informes previos como forma de participación subsumible en la exigencia

del artículo 87.3 LOPDGDD, que van más allá del precepto (STS de 13/9/2016 –rec. núm. 206/2015–), por cuanto este no exige dar aplicación a las sugerencias de la RLT ni tampoco la emisión de informes previos comporta exigencia de modificación de la propuesta empresarial. Se rechaza, asimismo, la aplicabilidad de la STS de 6/2/2024 (rec. núm. 263/2022) porque en este supuesto sí se ha cumplido con el deber de conceder participación. Del mismo modo, concluye que no se ha vulnerado el derecho a la negociación colectiva planteado por UGT, CSIF, CGT y USO.

VII. Parte dispositiva

La sentencia desestima íntegramente la demanda por descartar la vulneración de derechos fundamentales, tanto del derecho a la negociación colectiva en su vertiente sindical, como de los derechos a la intimidad y al secreto de las comunicaciones, así como el derecho de participación en la elaboración de las normas de uso de dispositivos digitales en la empresa.

VIII. Pasajes decisivos

Se contienen en los fundamentos de derecho quinto a octavo.

IX. Comentario

1. Derechos de participación de la RLT en la política de uso de dispositivos digitales

El artículo 87.3 LOPDGDD regula, por una parte, el deber empresarial de reglar los criterios de utilización de los dispositivos digitales con la participación de la RLT en su elaboración, junto con la información a los trabajadores afectados, y, por otra, las condiciones para el ejercicio de la facultad de control empresarial cuando se conceda uso con fines privados en dispositivos corporativos, consistentes en la especificación precisa de los usos autorizados y el establecimiento de garantías para preservar el derecho a la intimidad (a título de ejemplo, se cita como garantía «la determinación de los períodos en que los dispositivos podrán utilizarse para fines privados»).

Respecto del derecho de participación, la sentencia identifica esta, en términos generales, con diversas acepciones: información, audiencia, emisión de informes, negociación… Sostiene que, en ciertos contextos, este derecho podría satisfacerse con la transmisión de información, entendiendo que esta es una forma de «participación», aunque parece incurrirse en cierta confusión entre los modos del propio verbo participar, que, acompañado de la preposición «a» implica, efectivamente, informar o comunicar (derecho pasivo en lo que respecta a la RLT), pero, cuando se trata de la preposición «de» o «en», cobra sentido el derecho al que se refiere el artículo 87.3 citado, que tiene una clara acepción pasiva que implica *tomar parte en* el proceso de elaboración de tales criterios. Lo cierto es que, a través de un camino argumental distinto, la resolución comentada acaba confluyendo en la identificación del derecho previsto en el artículo 87.3, y, con claridad, afirma, en relación con los criterios de utilización de los dispositivos digitales, que «en su elaboración deberán participar los representantes de los trabajadores», lo que significa que el derecho no consiste en la mera emisión de un informe previo, sino en una actuación real en su proceso de génesis, esto es, un derecho activo a ser parte en su elaboración, aunque no se requiera expresamente el concurso de su voto para obtener su aprobación.

Sin embargo, la resolución analizada rechaza dicha interpretación acogiendo una interpretación histórico-sistemática, a tenor de la cual la eliminación de la referencia explícita a la *obligación de acordar con la representación de los trabajadores un protocolo de utilización de los dispositivos digitales* facilitados por la empresa, que preveía el artículo 86.3 en su tramitación legislativa, pasando a convertirse en la versión aprobada –vigente art. 87.3– en el *derecho a participar en su elaboración*. De ello colige que la opción legislativa fue la de rebajar el grado de participación de la RLT desde la obligación de «acordar» a la de «participar en su elaboración», lo que se identifica con la inexistencia de previsión que «obligue a la empresa a negociar los

criterios», por lo que, en este caso, no ha existido lesión alguna de derechos colectivos.

No obstante, es factible sostener una tesis alternativa, derivada de idénticos argumentos, para afirmar que la norma niega la obligación de contar con la *anuencia o voto* de la RLT para aprobar tales criterios, *mas no para su elaboración.* Distinta cuestión es que dicha participación pueda entenderse cumplida por el trámite de alegaciones y por la consideración efectiva, en un grado que se desconoce, de algunas sugerencias efectuadas por la RLT. Por lo que cabría entender si esta participación en la elaboración de criterios se considera cumplida cuando no se abre un proceso de negociación, sino solo de participación a través del trámite de alegaciones, como sucede en procesos participativos públicos, proceso participativo en el que la empresa se reserva el derecho a incorporar, o no, las sugerencias de la RLT. No parece ser este el sentido de la dicción literal del artículo 87.3 LOPDGDD, como tampoco se puede desprender del artículo 64.5 f) ET, que, de hecho, se invoca como lesionado por los demandantes.

Al respecto, la Sala considera que del artículo 64.5 ET «no se deriva un derecho de consulta en materia de implementación o revisión de sistemas de control, sino únicamente un derecho de emisión de informe previo», y distingue entre el derecho de consulta y el de emitir informe previo, previsto el primero en el segundo párrafo para «las decisiones de la empresa que pudieran provocar cambios relevantes en cuanto a la organización del trabajo» y el segundo en el apartado f) en caso de «implantación y revisión de sistemas de organización y control del trabajo», interpretación avalada por la STS de 13/9/2016 (rec. núm. 206/2015), que considera que la consulta debe entenderse como «intercambio de opiniones y la apertura de un diálogo... con espíritu de cooperación», coligiendo que el artículo 64.5 f) ET solo reconoce el derecho a emisión de informe previo en las materias en él citadas, que no obliga a acoger las sugerencias emitidas en el mismo. Resulta asimismo reseñable que la sentencia equipara informe previo con alegaciones, porque los términos en los que se redacta el artículo 64.5 ET determinan la confluencia entre uno y otro modo de participación, ya que en ambos casos se conciben como participación *antes de la ejecución de medidas ya adoptadas* por la empresa, como reza literalmente dicho precepto. Lo que es evidente es que este no es el sentido del artículo 87.3 LOPDGDD cuando ordena participar en su elaboración, que no parece equivaler al trámite de audiencia al que se refiere el artículo 64.5 ET cuando alude a medidas empresariales ya decididas antes de su ejecución. Por el contrario, el artículo 87.3 parece estar acotando un momento participativo diferente, coincidente con el propio proceso de diseño o elaboración de los criterios. En consecuencia, no parece que pueda considerarse satisfecho el derecho colectivo con la mera consideración de las alegaciones emitidas por la RLT, sin que haya mediado un diálogo síncrono en lugar de dos actuaciones unilaterales, separadas y desconectadas entre sí, por parte de la empresa en un caso (redactando el protocolo y examinando las alegaciones de la RLT después) y por la RLT en el otro (redactando sus alegaciones frente al protocolo elaborado por la empresa), pues queda totalmente al albur de la empresa la decisión sobre la orientación de tales criterios y sobre la posible incorporación de alguna de las sugerencias de la RLT, sin que tampoco se acote con claridad en el caso analizado cuál es el grado de aceptación de estas.

El control que se proyecta realizar mediante la aplicación de los criterios puede tener lugar mediante sistemas de inteligencia artificial, por lo que, además, resultaría de aplicación un ulterior derecho informativo previsto en el artículo 64.4 d) ET, que sí tendría un indubitado carácter meramente informativo.

2. Incidencia de la política de uso de dispositivos digitales sobre el derecho a la intimidad y al secreto de las comunicaciones

La resolución que se reseña aborda el alcance de la expectativa de privacidad en el uso de medios físicos, o en el programario propiedad de la empresa cuando se instala en dispositivos digitales personales. Y concluye que el cumplimiento de las prevenciones o garantías descritas anteriormente satisface debidamente la protección

del derecho de los trabajadores, aun cuando entre las finalidades empresariales se encuentre la de control o verificación del cumplimiento de las obligaciones laborales, en el marco del artículo 87.3 LOPDGDD, esto es, en la definición de los criterios de utilización de los dispositivos digitales. Ello porque se ha informado a los trabajadores de tales criterios, se han precisado los límites del uso con fines privados, se ha advertido de la exposición de la privacidad en tales usos y se han dispuesto las necesarias garantías.

Pues bien, se entiende que los principios indicados resultan de igual aplicación al acceso tanto a la información «periférica» de los dispositivos objeto de control como a su propio contenido, aunque este segundo acceso sea subsidiario del primero, y por ello, entiende que especialmente garantista con la configuración del derecho, que no llega a exigir tal limitación. Sin embargo, cuando se aborda la naturaleza de la información distinta al propio contenido, se sostiene que esta no es susceptible de invadir la intimidad de los trabajadores no obstante incluir la revisión del tráfico de datos, los tipos de archivos circulantes, los volúmenes de información compartida o los accesos a páginas y cuentas externas. Se considera que, puesto que «se analizan solo los metadatos» de forma prioritaria, no hay riesgo para la intimidad, pero se olvida que precisamente este tipo de análisis, efectuado por sistemas de inteligencia artificial (IA), cuenta con potencial para extraer un volumen exhaustivo de información sobre la persona vigilada que afecta a su intimidad y comunicaciones. Tales sistemas tienen capacidad para interrelacionar la información proveniente de los metadatos para explotarla de modo que su explotación permita el acceso a valiosos datos con los que reconstruir un perfil concreto de comportamiento personal, que podría extenderse a los terceros con los que se realiza la comunicación. Lo que implica que si tradicionalmente esta información podía tener un alcance limitado que no entrañara riesgos para el derecho a la intimidad, no cabe ya sostener su inocuidad en la actualidad, cuando la empresa los explore dentro de un sistema de IA que seguramente vaya a efectuar ulteriores correlaciones con otros datos de los que disponga, extrayendo así valiosos datos (mediante minería de datos) de manera inadvertida para los afectados. Este acceso excedería la irrelevancia que se le predica en la resolución estudiada, porque, en el contexto del RGPD, los metadatos también son datos personales, y, además, permiten una explotación específica de la que obtener otros datos personales. Por el contrario, permitirían a la empresa establecer un patrón de conducta de los trabajadores e incluso derivar de ello consecuencias negativas en términos disciplinarios. Admitir esta política sin consentir tampoco su negociación con la RLT y extenderla incluso a dispositivos personales, por más que el acceso a estos se afirme limitado a bloquear la aplicación corporativa, tampoco es irrelevante. Por ello, ante tal riesgo potencial, la empresa debe igualmente cumplir con el deber de transparencia algorítmica, indicando en el protocolo si se empleará IA para realizar tal control e informar de que no existirá reutilización de datos para fines ulteriores, así como con el de evaluación de impacto (Guía de la AEPD *La protección de datos en las relaciones laborales* -2025-).

Por lo que respecta a la política BYOD, admitiendo que precisa del previo consentimiento de los trabajadores afectados, y que incluso tiene lugar a petición de los propios interesados, no es menos cierto que la autorización, como cualquiera que afecte a la instalación de aplicaciones en dispositivos digitales, comporta cierta cesión de datos, en la que la entidad propietaria de la aplicación obtiene acceso a datos personales alojados en el propio dispositivo. Que solo se tenga acceso a la aplicación en sí y a su bloqueo no parece ser coherente ni con el funcionamiento habitual de esta tecnología ni tampoco con los criterios que se correlacionan, y es que se permite el bloqueo de la aplicación ante la sospecha de irregularidades, pero tener conocimiento de estas cuando el tráfico de datos depende del dispositivo privativo ha de sostenerse necesariamente en un presupuesto, que es el previo acceso a tal flujo para identificar la existencia de sospechas. Aunque este pueda haberse detectado remotamente, en igual sentido ha de entenderse que el acceso remoto ha sido justamente a ese dispositivo particular. En definitiva, bajo estas premisas los datos y la intimidad no están tan a salvo como pareciera indicar el protocolo y su análisis judicial.

Y ello porque la aplicación de minería de datos sobre metadatos presentes en mensajes de correo electrónico puede inferir, incluso con cifrado de mensaje, detalles profundos sobre la vida privada, hábitos y círculos sociales de una persona. Se trata de datos invisibles desprotegidos a través de los cuales cabe construir el perfil detallado de un usuario, incluido su círculo social (red de contactos), hábitos, ubicación, interacciones (fecha de envío y recepción, momento y veces de apertura), ID del dispositivo, ... intervalos de tiempo, duración de la conexión o registros de flujo, y, como se ha indicado, otros datos obtenidos por inferencia que detectan, en suma, patrones de comunicación y, al mismo tiempo, permiten realizar perfilación de personas. Bien es cierto que se indica que la expectativa de privacidad es muy limitada, pero, al mismo tiempo, se afirma que tal acceso no será esporádico, sino sistemático, lo que expone a los trabajadores a un tratamiento permanente de datos que facilite la perfilación, así como la identificación de personas externas con las que realizar inferencias reveladoras de categorías especiales de datos conectadas con posible discriminación por asociación.

De singular importancia es la información transmitida en el protocolo litigioso, donde se indica que «estos procedimientos estarán documentados, se aplicarán de forma transparente y con acceso limitado solo a la información necesaria», fórmula que, por estándar, permite extrapolar reflexiones comunes a supuestos similares. Pues bien, al efectuarse remisión a unos supuestos procedimientos documentados a los que, *a priori,* la RLT no tiene acceso en su proceso de elaboración, resulta difícilmente entendible que esta pueda formular oposición informada al alcance de los mecanismos de supervisión, que es donde subyace, en realidad, el núcleo de la cuestión, con igual desconocimiento por parte de los propios trabajadores de la plantilla. Con semejante información es difícil reconocer el alcance real del binomio conformado entre expectativa de privacidad y uso razonable con fines privados, máxime si se deriva a una concreción posterior indeterminada temporalmente el plazo del que van a disponer los trabajadores para revisar los dispositivos antes de ser objeto de supervisión empresarial («plazo que se comunicará próximamente»). Tampoco es óbice al «rascado de datos» su eliminación previa por el usuario, ya que estos pueden rastrearse con posterioridad en el soporte donde se hubieran alojado anteriormente.

En definitiva, las garantías adecuadas y suficientes contra los abusos a las que se refiere la doctrina Barbulescu (STEDH de 5/9/2017) y Guyvan (STEDH de 6/11/2025) no pueden entenderse plenamente satisfechas, en cuanto el alcance de la supervisión y grado de intrusión en la vida privada, relativos a flujo de comunicaciones y a su contenido, no queda suficientemente delimitado, además de dejarse espacio a la obtención de información sensible mediante tratamiento de los metadatos de los que obtener inferencias e incluso realizar perfiles mediante sistemas de IA. Desconociéndose qué medios utilizará la empresa para realizar dicha supervisión, pues estos no se concretan, si se emplearán sistemas de IA interconectados u otros, y con qué finalidades, lo cierto es que el control pretendido no parece adecuadamente descrito, ni se ha permitido a la RLT incidir en ello ni, por supuesto, prestar su anuencia a su aprobación, que, por el contrario, se rechaza explícitamente a través del conflicto colectivo del que trae causa el pleito.

Otro tanto cabe predicar de las aplicaciones corporativas instaladas en los dispositivos personales (política BYOD). No se indica en este protocolo, y debería, qué tipos de datos pueden captar y si su instalación en dispositivos personales permite rechazar «cookies», información que ha de incorporarse a la política de privacidad, a integrar en este protocolo general, pues debería detallar qué datos se recogen y para qué se usarán. Ha de tenerse en cuenta que las aplicaciones corporativas pueden captar datos que no son estrictamente necesarios para su funcionamiento básico, información que debiera constar y compartirse igualmente con la RLT, además de contar con el consentimiento informado de los usuarios, así como recopilar únicamente los datos «adecuados, pertinentes y limitados» para el estricto funcionamiento de la misma, comenzando por el número de teléfono o correo privados (o, lo que es peor, la identificación digital que podría emplearse como método de registro –v.gr. identidad en Google–), aunque la aplicación habría de permitir un registro con dirección de correo

corporativa, pero también la dirección IP o la ubicación (que podría extenderse más allá del horario de trabajo). En cualquier caso, habría de precisar su desconexión automática fuera del horario de trabajo y toda esta información haber sido incluida en el anexo impugnado.

Es asimismo de difícil comprensión el desajuste entre el uso razonable de dispositivos corporativos con fines particulares, *de acuerdo con los usos sociales*, y la nula expectativa de intimidad anunciada por la empresa (contraria a los usos sociales admitidos por el artículo 87.3), por lo que la única interpretación posible es la admisión del –moderado– uso en sí durante la jornada de trabajo, que no se acompaña de garantía alguna de la intimidad (*ex* STS de 26/9/2007 –rec. núm. 966/2006–), pese a tratarse de hábitos conformes con los usos sociales. Pero, en todo caso, sería precisa una mayor concreción sobre cuál sea la «causa justificada» que habilitaría el acceso al contenido, pues esta no se especifica con claridad, concediendo así una especie de «carta blanca» al control empresarial que dificultaría sobremanera la protección de la privacidad en los usos concretos, en el sentido apuntado por la sentencia, que, si bien salva dicha interpretación, la condena en cierta medida al fracaso cuando admite la legitimidad del control así descrito y su aplicación general –que ha ganado legitimidad con una resolución judicial favorable–, sin perjuicio de se produzca una oposición concreta a un acto empresarial específico y mientras ello no tenga lugar.

En suma, el contenido del protocolo de uso debería ser mucho más detallado y ser conocido por la RLT, lo que en este caso no se ha producido.

X. Apunte final

En definitiva, el propósito del artículo 87.3 LO es definir el uso de dispositivos corporativos por los trabajadores durante la jornada de trabajo, para clarificar el margen de utilización privada de estos (partiendo de que ha de tolerarse cierta práctica, cuando esta sea razonable, de acuerdo con los usos sociales imperantes –aunque estos sean los de vivir pegado a un móvil–) y la expectativa de privacidad protegida en dichos usos, limitando el acceso empresarial a ellos, pero en el caso analizado el protocolo dictado en aplicación de dicho precepto parece más orientado a definir el alcance del control empresarial sobre tales dispositivos. Dada la normalización del uso de IA en la gestión de las relaciones laborales, sin duda la política de uso referida en el artículo 87 habría de especificar el posible tratamiento mediante esta tecnología, al facilitarse con ella las inferencias de datos y una explotación de información sensible en términos de intimidad incluso solo analizando metadatos.