ANÁLISIS Y CONTEXTOS

Dispositivos digitales, vigilancia y derecho a la intimidad

Comentarios jurídicos a la STS 225/2024, de 6 de febrero

Recomendaciones para la Negociación Colectiva

Marzo 2024

(Nº 63)

SERVICIO DE ESTUDIOS UGT

CONTENIDO

Resumen

El Tribunal Supremo ha dictado sentencia en la que considera que cualquier cambio en la política de uso de dispositivos digitales que afecte en la intimidad debe contar con la participación de los representantes de las personas trabajadoras.

Conforme a dicha sentencia, el procedimiento que debe seguirse para modificar, actualizar o especificar cualquier aspecto de la política de uso de los equipos informáticos propiedad de la empresa y puestos a disposición de las personas trabajadoras, así como el acceso a Internet, debe negociarse de forma colectiva con los representantes de las personas trabajadoras.

La Sentencia comentada supone un claro punto de inflexión en el papel que los Sindicatos debemos desempeñar a la hora de poner coto a comportamientos empresariales desmesurados y extramuros, contraponiendo a estos abusos los límites que impone la legislación y recalcando el papel fundamental que tiene la Negociación Colectiva.

Para cumplir con este objetivo, se realiza un breve recopilatorio de cómo debe articularse y negociarse el uso de las herramientas tecnológicas en el trabajo, bajo una visión jurídica y social.

Sentencia del Tribunal Supremo nº 225/2024, de 6 de febrero.

El Tribunal Supremo dictó, el pasado 6 de febrero, Sentencia nº 225/2024[1] en la que declara la nulidad de la comunicación efectuada por la empresa, relativa al uso de los equipos informáticos propiedad de la misma y puestos a disposición de las personas trabajadoras, así como al acceso a Internet a través de los mismos. El motivo por el que se declara la nulidad consiste en que la mencionada comunicación se elaboró por la empresa sin la participación de los representantes de las personas trabajadoras (RLT) en contra de lo establecido en el artículo 87.3 de la Ley Orgánica de protección de datos personales y de garantía de los derechos digitales (LOPD).

Antecedentes

- Se interpuso demanda de conflicto colectivo, de la que conoció la Sala de lo Social de la Audiencia Nacional, en la que se solicita "*Revocar íntegramente la nueva política sobre el uso del correo electrónico, Internet y almacenamiento de información en los discos duros de los equipos puestos a disposición de la plantilla en la empresa, así como la conexión a ordenadores de la oficina cuando se teletrabaja para poder vigilar en tiempo real qué se hace en cada momento, por ser una política en contra de las normas que hasta ese momento estaban vigentes para la plantilla y no haber sido negociada con la RLT, procediendo a declarar la necesidad de que se inicie periodo de negociación con la RLT para cumplir con el art. 87.3 LOPD, y así consensuar criterios que respeten, en todo caso, los estándares mínimos de protección de la intimidad de acuerdo con los usos sociales y los derechos reconocidos constitucional y legalmente".*

- Con fecha 22 de julio de 2022, la Sala de lo Social de la Audiencia Nacional dictó sentencia en la que estimó parcialmente la demanda y declaró la nulidad de la comunicación efectuada a la plantilla en los términos que más adelante se mostraran.

- Contra dicha resolución se interpuso recurso de casación por la representación de la empresa entendiendo que se había vulnerado el art. 20.3 ET. Concretamente, consideró que, según los hechos probados, ya existía una prohibición previa de uso personal de los medios informáticos facilitados por la empresa a los empleados y que la citada comunicación era un mero recordatorio y no la implantación de una nueva política de uso de los medios informáticos.

Análisis

Con carácter previo al análisis, debemos reseñar que la empresa estaba adscrita:

Código de Ética Profesional en el que, entre otras cosas, se refiere lo siguiente: "Los sistemas de comunicación incluyendo los sistemas telefónicos, de correo electrónico e Internet, se le proporcionan con fines profesionales, para permitirle hacer su trabajo (…). Aunque entendemos la necesidad del uso limitado, ocasional o infrecuente de los sistemas de comunicación para propósitos personales, usted debe conocer que los mensajes enviados y recibidos en nuestros sistemas de comunicación podrán ser monitoreados, inspeccionados y almacenados. Usted no debe tener ninguna expectativa de privacidad en relación con dichas comunicaciones. Usted es responsable por entender nuestras políticas distintas y más detalladas referentes al uso de nuestros sistemas de información tecnológica y el acceso al software y a Internet que se pone a su disposición para que lleve a cabo sus funciones de negocio".

Código de conducta en el que se detalla que la empresa es responsable en última instancia de todo el material enviado vía correo electrónico e Internet a través de los sistemas propiedad de la empresa, y podría ser objeto de acciones judiciales por el contenido ilegal, ofensivo o difamatorio de esos correos electrónicos o enviado a través de Internet.

Por tanto, aunque la empresa permita un uso personal limitado de Internet de la empresa (por ejemplo, el acceso a redes sociales) y de los servicios de correo electrónico, se espera que los usuarios actúen de forma sensata y responsable y se les aconseja que no envíen aquellos correos electrónicos o accedan a aquellas páginas de Internet que no quieran que vean otros miembros de la empresa.

Normalmente no se monitoriza el uso individual del correo electrónico e Internet, sin embargo, la empresa se reserva el derecho a hacerlo cuando se estime que dicho uso pueda perjudicar a la misma. La monitorización de la cuenta de un individuo solo se llevará a cabo cuando el Director de una Unidad de Negocio o País así lo solicite y siempre tras la aprobación del Director de Tecnologías de la Información del ámbito geográfico pertinente. La monitorización de la cuenta de un individuo, según lo expuesto en el presente código, se comunicará debidamente y con carácter previo a los representantes de los trabajadores en todos los casos que la ley así lo prevea, en la forma legalmente establecida (…).

Estamos ante un código de conducta que mezcla normas de uso obligatorio con otras de apreciación subjetiva causando desconcierto y confusión a las personas a las que va dirigido. De igual modo, en los casos en que la empresa decida una monitorización individual, debería concretar la forma de comunicación a la representación legal de las personas trabajadoras.

Posteriormente, la empresa notificó en papel a las personas trabajadoras que prestan servicios en forma presencial y por correo electrónico a las que trabajan a distancia lo siguiente:

"Por medio de la presente la empresa quiere recordar que tanto los equipos informáticos proporcionados por esta como los correos corporativos, tienen por única finalidad el desarrollo de la prestación de servicios contratada, estando prohibido su uso para fines particulares no relacionados con el desempeño de las funciones laborales encomendadas.

Con el objeto de impedir el uso indebido de los equipos informáticos propiedad de la empresa y puestos a disposición del trabajador, así como el acceso indebido a internet a través de estos, les informamos que en cumplimiento de la LO 3/2018 de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPD) que todos los ordenadores y todas las direcciones de correo electrónico corporativos facilitados por la EMPRESA al TRABAJADOR o utilizados por este con ocasión de su trabajo, serán accesibles por la EMPRESA, pudiendo ser los ordenadores, su contenido así como cualquier archivo guardado en los mismos por el TRABAJADOR en cualquier momento, analizados, examinados, formateados y/o reseteados mediante los oportunos medios informáticos al alcance de la empresa (auditoría informática, examen pericial informático, software de captura de pantallas etc.)".

El TS parte de la literalidad de los dos artículos objeto de debate (art. 20.3 ET y art. 87.3 LOPD) y lo hace para mantener que ambos preceptos obedecen a lógicas diferentes.

ARTÍCULO 20.3 ET	ARTÍCULO 87.3 LOPD
El empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad y teniendo en cuenta, en su caso, la capacidad real de los trabajadores con discapacidad	*Los empleadores deberán establecer criterios de utilización de los dispositivos digitales respetando en todo caso los estándares mínimos de protección de su intimidad de acuerdo con los usos sociales y los derechos reconocidos constitucional y legalmente. En su elaboración deberán participar los representantes de los trabajadores. El acceso por el empleador al contenido de dispositivos digitales respecto de los que haya admitido su uso con fines privados requerirá que se especifiquen de modo preciso los usos autorizados y se establezcan garantías para preservar la intimidad de los trabajadores, tales como, en su caso, la determinación de los períodos en que los dispositivos podrán utilizarse para fines privados. Los trabajadores deberán ser informados de los criterios de utilización a los que se refiere este apartado.*

Gráfico nº 1. Fuente: elaboración propia.

El art. 20.3 ET, precepto de carácter general aplicable a todo tipo de actividad, reconoce el poder de dirección del empresario en el ámbito de la relación laboral y, para verificar el cumplimiento por la persona trabajadora de sus obligaciones y deberes laborales, faculta al empresario para adoptar las medidas que estime más oportunas de vigilancia y control.

En cambio, el art. 87.3 LOPD se refiere, específicamente, a los criterios de utilización de los dispositivos digitales que el empresario pone a disposición de los empleados para la realización del trabajo y, al respecto, faculta al empresario para establecer normas y criterios para la utilización de los mismos, a la vez que establece limitaciones a ese poder de especificación empresarial vinculadas al derecho a la intimidad de las personas trabajadoras. Sobre estas cuestiones específicas, la norma ordena que la elaboración de los criterios de utilización de dichos medios se realice con la participación de los representantes de las personas trabajadoras.

La jurisprudencia considera que, dentro del genérico poder de dirección de la empresa del art. 20.3 ET, el art. 87.3 LOPD resulta una especificación para salvaguardar la intimidad de la persona trabajadora.

Gráfico nº 2. Fuente: elaboración propia.

Por otra parte, el Tribunal pone de relieve que el mandato del art. 87.3 LOPD tiene carácter imperativo en los supuestos en los que el trabajo se realice mediante dispositivos digitales ya que establece que "*los empresarios deberán establecer criterios de utilización*" y que tal establecimiento debe realizarse "*con la participación de los representantes de los trabajadores*".

Cualquier modificación de los criterios previamente establecidos a la entrada en vigor de la LOPD, o cualquier especificación de los mismos, ampliación o restricción debe seguir las normas establecidas en esta norma.

En consecuencia, la Sala entiende que lo que ha hecho la empresa no es un "*mero recordatorio*", sino que la instrucción de la empresa implica una modificación y, en todo caso, una actualización de los criterios que venían rigiendo en la empresa y que, consecuentemente, debieron ser elaborados cumpliendo la normativa vigente. En efecto, la circular o instrucción (…), tras recordar la prohibición del uso de los equipos informáticos para fines particulares no relacionados con el desempeño de las funciones laborales encomendadas, añade una serie de medidas dirigidas a *"impedir el uso indebido de los equipos informáticos»* así como *"el acceso indebido a internet*" estableciendo, al efecto la plena accesibilidad de la empresa a todos los ordenadores y a todos los correos electrónicos corporativos facilitados por la empresa a la persona trabajadora pudiendo ser analizados en cualquier momento, sin ninguna otra

precisión relativa a la información del interesado o a la participación o presencia del mismo o de sus representantes.

Comentarios jurídicos

La Sentencia del Tribunal Supremo, objeto de este comentario, es de especial importancia porque considera que cualquier modificación de los criterios (incluso los previamente establecidos a la entrada en vigor de la LOPD), o cualquier especificación de los mismos, ampliación o restricción, debe seguir las normas establecidas en el art. 87.3 LOPD y, por consiguiente, debe contar con la participación de los representantes de las personas trabajadoras.

La Sentencia pone de manifiesto el carácter imperativo del mandato del art. 87.3 LOPD en los supuestos en los que el trabajo se realice mediante dispositivos digitales. **Lo que supone que los empresarios deben establecer criterios de utilización de los dispositivos, y deben hacerlo con la participación de los representantes de las personas trabajadoras**. Este mandato supone que cualquier modificación, especificación, ampliación o restricción de los criterios, debe seguir las reglas de la LOPD.

En este supuesto, el TS ha considerado que la instrucción de la empresa implicaba una modificación de los criterios que venían rigiendo y por ello debieron ser elaborados cumpliendo la normativa vigente.

El poder de dirección del empresario en el ámbito de la relación laboral y la facultad para adoptar las medidas que estime más oportunas de vigilancia y control no pueden obviar al art. 87.3 LOPD que, específicamente, se refiere a los criterios de utilización de los dispositivos digitales que el empresario pone a disposición de los empleados para la realización del trabajo, y que establece limitaciones a ese poder de especificación empresarial vinculadas al derecho a la intimidad de las personas trabajadoras.

La Sala, reseña que ampliar **las posibilidades de acceso puede provocar una grave colisión con los derechos a la intimidad y dignidad de las personas trabajadoras, y por ello, los criterios debieron ser fijados con la participación de sus representantes**.

Conclusiones y recomendaciones para la negociación colectiva

Una de las mayores preocupaciones de las personas trabajadoras –y de sus representantes- es la referida al alcance del control empresarial de la actividad digital y si dicha monitorización cumple con los estándares de legalidad y legitimidad. No se trata de una sospecha ni baladí ni producto de una confabulación. La omnipresencia de las herramientas digitales en los puestos de trabajo es indiscutible: en 2023 dos de cada tres personas trabajadoras usan un ordenador para su desempeño profesional; a un 43% se le provee de dispositivos móviles de uso empresarial y a finales de 2023[1], las personas que trabajaban en remoto superaban los tres millones[2]. Que existe un interés de los empleadores en usar estas nuevas tecnologías para someter a sus empleados a una estrecha vigilancia es algo palmario: un 40% de las empresas españolas usa analítica de datos para monitorizar el desempeño de sus empleados (España es líder europeo en esta práctica[3]) y un tercio de las personas trabajadoras españolas son controladas por algoritmos (el doble que en Alemania[4]). La proliferación de empresas dedicadas a vender servicios de vigilancia digital para empleados es otra prueba irrefutable de esta realidad[5].

La Sentencia comentada supone un claro punto de inflexión en el papel que los Sindicatos debemos desempeñar a la hora de poner coto a comportamientos empresariales desmesurados y extramuros, contraponiendo a estos abusos los límites que impone la legislación y recalcando el papel fundamental que tiene la Negociación Colectiva. Por ello, vamos a hacer un breve recopilatorio de cómo debe articularse el uso de las herramientas tecnológicas en el trabajo bajo una visión socio-jurídica.

Las empresas pueden, al amparo del art. 20.3 ET, optar por medidas “de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales”, pero siempre teniendo la “consideración debida a su dignidad humana”. No obstante, como hemos visto en la sentencia comentada, este control del empleador (sea una empresa privada o una AAPP) no es absoluto.

---

[1] https://servicioestudiosugt.com/digitalizacion-de-la-empresa-espanola-2/

[2] https://www.ugt.es/la-negociacion-colectiva-logra-que-espana-supere-los-3-millones-de-personas-teletrabajando

[3] https://www.eurofound.europa.eu/en/publications/2020/employee-monitoring-and-surveillance-challenges-digitalisation

[4] https://publications.jrc.ec.europa.eu/repository/handle/JRC133016

[5] https://www.cnbc.com/2024/02/09/ai-might-be-reading-your-slack-teams-messages-using-tech-from-aware.html

Cuando hablamos del acceso a los dispositivos digitales que el empleador pone a disposición de los empleados para la realización del trabajo **existen limitaciones vinculadas con los derechos fundamentales.**

Así, la posibilidad de acceso por el empleador a los contenidos derivados del uso de los medios digitales solo está legitimada si atiende a estas dos finalidades[6]:

- Controlar el cumplimiento de las obligaciones laborales o estatutarias.
- Garantizar la integridad de los dispositivos.

Ambas finalidades no otorgan al empresario plenos poderes, sino que están condicionadas en varios aspectos.

La primera condición, tal y como acaba de ratificar el Tribunal Supremo, es la obligación de disponer de un protocolo o relación de criterios que expliquen e informen de cómo se pueden usar estas herramientas digitales, y, por tanto, de cómo se efectúa ese control de la actividad laboral. Dicho protocolo, **siempre debe ser negociado con la representación legal de las personas trabajadoras**, tal y como señala el art. 87.3 LOPD[7].

El segundo condicionante proviene de la necesidad de que **se haya informado previamente, y de forma clara, expresa y concisa**, a todas las personas trabajadoras y empleados públicos afectados del contenido y vigencia de citado protocolo.

El tercer condicionante reside en la dimensión de la vigilancia realizada. Para que dicha monitorización sea lícita debe cumplir con las siguientes condiciones:

- **Que sea proporcionada**, en el sentido de que la vigilancia resulta ponderada, equilibrada y no excesiva. Hablamos de derechos fundamentales (intimidad, privacidad) por lo que el control empresarial propuesto tiene que justificar un beneficio superior al perjuicio inherente a poner en riesgo dichos derechos fundamentales. Una monitorización desproporcionada de la actividad laboral no sólo es un abuso, es terminantemente ilegal.

- **Que sea idónea**, debe existir un vínculo lógico y directo entre el control y el objetivo perseguido. O, dicho de otro modo, que tal vigilancia no se haga por el

[6] GUÍA DEL TELETRABAJO, Servicio de Estudios de la Confederación. https://www.edicionescinca.com/producto/guia-del-teletrabajo/

[7] Artículo 87. Derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral (…). 3. Los empleadores deberán establecer criterios de utilización de los dispositivos digitales respetando en todo caso los estándares mínimos de protección de su intimidad de acuerdo con los usos sociales y los derechos reconocidos constitucional y legalmente. En su elaboración deberán participar los representantes de los trabajadores (…). Los trabajadores deberán ser informados de los criterios de utilización a los que se refiere este apartado.

mero hecho de poder hacerlo, sino que se produzca buscando un objetivo claro y conciso. Por ejemplo, los controles sorpresivos no son admisibles y las cláusulas que otorgan al empleador poderes omnímodos y permanentes sobre los dispositivos digitales, tampoco[8].

- **Que sea necesaria**, la vigilancia que pueda establecerse tiene que resolver un problema real, presente y crítico para el funcionamiento de la empresa o AAPP. No basta la mera conveniencia o rentabilidad como argumento para sustentar la vigilancia. Tiene que acreditarse un perjuicio que justifique esta necesidad de monitoreo laboral[9].

- Que respete todos los preceptos de **protección de datos personales**[10].

La cuarta condición está relacionada con la propiedad de los dispositivos: **las empresas no pueden obligar a usar ni los dispositivos personales de las personas trabajadoras ni sus herramientas informáticas privadas**.

No se puede exigir a un empleado que use su email particular con fines laborales, ni obligarle a que instale en su teléfono inteligente apps de la empresa; ni siquiera se puede exigir su uso para la recepción de SMS de acreditación de identidad (por ejemplo, en accesos de doble verificación) y mucho menos para recibir mensajes tipo WhatsApp con instrucciones relacionadas con la prestación laboral[11]. Las prácticas de algunas empresas instando, directamente o indirectamente, a instalar apps para registrar el inicio o final de jornada en los móviles particulares no tienen cabida en nuestro acervo legislativo.

Dos sentencias a seguir: STS 163/2021 y SAN 487/2024

En ambas sentencias se ponen límites al uso laboral de los dispositivos particulares de las personas trabajadoras. En ambos casos, se considera que no se puede imponer el uso de dispositivos personales para desarrollar una prestación laboral.

[8] Son nulas las cláusulas que reservan a la compañía la posibilidad de examinar el contenido de los dispositivos digitales, formatearlos o resetearlos sin la participación e información previa de la persona trabajadora y sus representantes legales.

[9] https://www.aepd.es/documento/orientaciones-evaluacion-impacto-desarrollo-normativo.pdf

[10] Como el principio de minimización o exactitud –que los datos recabados son adecuados, pertinentes y no excesivos en relación con la necesidad que justifica su recogida-, que cumpla con los plazos máximos de conservación que marca la ley o con los derechos los interesados (acceso, rectificación, oposición, etc). Para más información consultar el *Protocolo de actuación para la Negociación Colectiva de UGT*, https://www.ugt.es/sites/default/files/guia-proteccion_de_datos.pdf y el apartado 7.1. de la *GUÍA DEL TELETRABAJO* del Servicio de Estudios de la Confederación. https://www.edicionescinca.com/producto/guia-del-teletrabajo/

[11] https://servicioestudiosugt.com/el-uso-de-whatsapp-en-las-relaciones-laborales/

El quinto condicionante proviene de la **total prohibición de usar datos biométricos de las personas trabajadoras**. Las huellas digitales, el reconocimiento facial, la palma de la mano, el iris, etc. son datos especialmente protegidos, que suponen un alto riesgo[12] y no puede emplearse en los entornos laborales. La Agencia Española de Protección de Datos, en su momento, consintió el uso de huellas dactilares como método para el registro de jornada o para el control de accesos. No obstante, dicha permisividad ha quedado revocada por una directriz del Comité Europeo de Protección de Datos[13], obligando a la AEPD a rectificar su guía[14]. En la guía actualizada se indica que el *"registro de jornada y control de acceso* ***con fines laborales"*** **mediante biometría podría darse, únicamente, en el caso de existir un Convenio Colectivo que amparase tal práctica, un supuesto que debemos evitar a toda costa.**

Y finalmente, el sexto condicionante está íntimamente vinculado a los anteriores, en el sentido de que ninguno de los condicionantes antedichos puede revocarse usando el subterfugio de solicitar el consentimiento expreso de la persona trabajadora (por ejemplo, por medio de una adenda contractual).

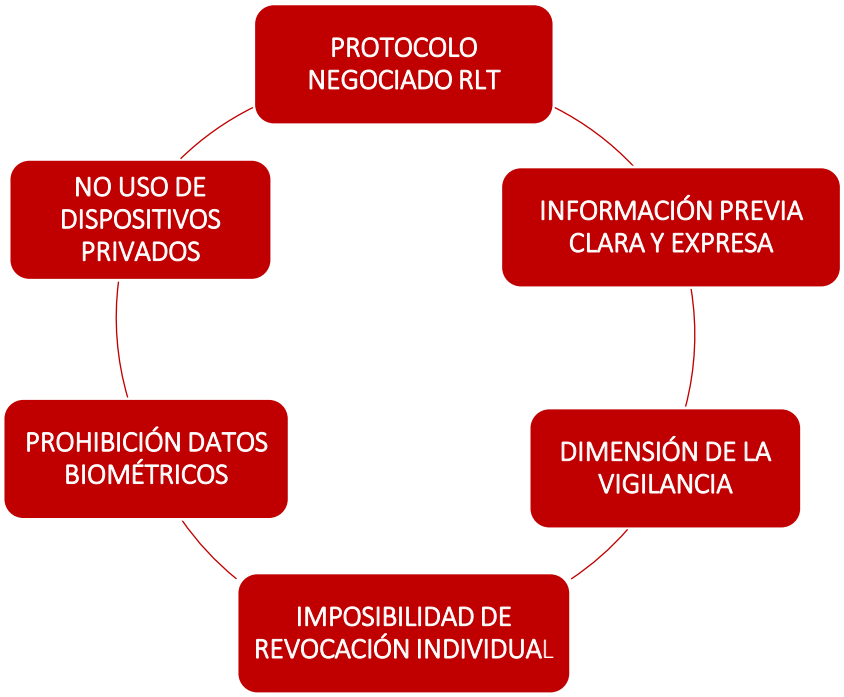

Gráfico nº 3. Fuente: elaboración propia.

[12] https://www.aepd.es/guias/guia-control-presencia-biometrico.pdf

[13] Directrices 05/2022 del Comité Europeo de Protección de Datos (CEPD), sobre el uso de reconocimiento facial en el ámbito de las fuerzas de orden público (Versión 2.0, de 26 de abril de 2023) https://edpb.europa.eu/system/files/2023-05/edpb_guidelines_202304_frtlawenforcement_v2_en.pdf

[14] https://www.aepd.es/prensa-y-comunicacion/notas-de-prensa/la-aepd-publica-una-guia-sobre-la-utilizacion-de-datos

Es muy importante tener en cuenta que **el consentimiento expreso de una persona trabajadora no es suficiente como base jurídica para el tratamiento de los datos personales ni para revocar las prerrogativas relacionadas con el uso de herramientas digitales**. En efecto, en una relación laboral empleador-empleado, se constata un evidente desequilibrio entre el interesado y el responsable del tratamiento, lo que invalida tal consentimiento[15].

Teniendo en cuenta todas las premisas enunciadas, se debe acometer la negociación colectiva del protocolo de uso, al objeto de clarificar como podrá el empleador controlar el cumplimiento de las obligaciones laborales/estatutarias y garantizar la integridad de los dispositivos puestos a disposición de sus empleadas y empleados.

Las recomendaciones de contenido de este protocolo son las siguientes:

- Debe abarcar y especificar todos los dispositivos digitales proporcionados por el empleador (ordenador de sobremensa, portátiles, telefónos móviles, pulseras, relojes, tabletas, etc), tanto en una prestación remota (teletrabajo) como en el centro de trabajo habitual.

- Debe incluir todas las herramientas digitales que se empleen durante la prestación laboral. A modo de recordatorio: el correo electrónico corporativo, las soluciones de mensajería corporativa (Microsoft TEAMS, WhatsApp/Instagram Business, Slack, Workplace de Meta/Facebook, etc.), el acceso a la web y la navegación por Internet y las aplicaciones de almacenamiento de datos, tipo Drive, OneDrive, Dropbox, etc.

- La vigilancia del contenido tanto de los dispositivos como de las herramientas digitales debe, además de garantizar que cumpla con los requisitos de necesidad, idoneidad y proporcionalidad, debe restringirse a un tiempo limitado y a unos supuestos específicos, evitando los controles aleatorios o sorpresivos. Además, se debe hacer constar las personas responsables que tendrán acceso a los resultados de esta vigilancia, que debe tener un volumen igualmente restringido.

[15] Dictamen 15/2011, cuando un interesado se encuentra en una situación de dependencia con respecto al responsable del tratamiento de los datos, ya sea debido a la naturaleza de su relación o a circunstancias particulares, puede haber una firme presunción de que la libertad para dar el consentimiento se ve limitada en dichos contextos (por ejemplo, en una relación laboral o en el caso de que sea una autoridad pública quien recoja los datos).

- El uso de los dispositivos y herramientas digitales debe contemplar un tratamiento social y extralaboral, que permita una cierta expectativa de confidencialidad; si es necesario, advirtiendo de que ese uso debe ser ocasional y no puede afectar a la prestación laboral. Cabe recordar que la misma Ley de protección de datos y garantía de derechos digitales hace una llamada a "la determinación de los períodos en que los dispositivos podrán utilizarse para fines privados". Del mismo modo, la política de almacenamiento de datos (documentos, imágenes, etc.), sean en remoto o en local, debe evitar una prohibición absoluta de almacenamiento de información personal, al objeto de dar un uso social y una expectativa de privacidad en estos dispositivos. Una buena práctica es permitir espacios privados bajo epígrafes del tipo "personal" o "privado".

- Para el acceso y navegación web se recomienda que, más que exponer una serie de webs con temáticas prohibidas o no recomendadas, la empleadora utilice herramientas de restricción de acceso a aquellos sitios que considere que están fuera del ámbito laboral y de negocio.

- En el caso de smartphones proporcionados por el empleador, se debe hacer constar claramente si existe una prohibición de instalar programas o apps fuera de las indicadas expresamente por la empleadora. Asimismo, es pertinente acotar los permisos y accesos de las app en los teléfonos inteligentes, puesto que un acceso ilimitado del empleador a imágenes tomadas con la cámara puede afectar a la intimidad de las personas trabajadoras.

- En el caso de emplear herramientas con videollamadas se debe especificar si es obligatorio permanecer con el video activado, teniendo en cuenta que la *webcam*/cámara debe ser proporcionada por el empleador y que no siempre es conveniente, técnicamente, tal práctica (muchas aplicaciones tienden a ralentizarse con muchos usuarios con video activado y las conexiones de Internet no siempre soportan *streaming* con la eficiencia debida). En este mismo apartado, la grabación de estas videollamadas deberá estar pormenorizadamente regulada, sometiéndose en todo caso a un estricto control sobre protección de datos (tiempo de almacenamiento, acceso, revocación, oposición, etc.), puesto que se estarán grabando datos biométricos de especial protección, como pueden ser la imagen facial o la voz.

- No se deben admitir controles basados en métricas de difícil conciliación con la valoración del rendimiento laboral. Por ejemplo, la medición de pulsaciones

en el teclado o clics en el ratón no es un parámetro que demuestre absolutamente nada. En este mismo sentido, debe limitarse la posibilidad de usar las cámaras para obtener fotografías/capturas del trabajador/a. Al realizarse una captura se está recogiendo un dato biométrico facial, un aspecto vedado por la norma, tal y como hemos explicado anteriormente. Además, en el caso de teletrabajar, se pueden obtener imágenes de la residencia, lo que puede interpretarse como una transgresión de la *inviolabilidad* de *domicilio*. En cuanto a la medición de actividad mediante temporizadores o cronómetros, se debe especificar qué actividades están sujetas a esta medición, cumpliendo siempre con los juicios de proporcionalidad y necesidad descritos anteriormente.

- Ineludiblemente, y con carácter previo a la puesta en marcha del protocolo, se deben especificar las políticas sancionadoras aplicables de forma clara, transparente y explícita, informando personalmente y con suficiencia a cada uno de los implicados. Se recomienda la incorporación de estas adendas al código disciplinario al cuerpo del Convenio Colectivo de referencia.

Este compendio de condicionantes y recomendaciones, nos permite acometer con garantías la necesaria negociación del protocolo de uso de herramientas y dispositivos digitales, una cuestión de gran importancia por sus repercusiones en los derechos de las personas trabajadoras y que debemos implementar en todas las empresas, empleadores públicos y sectores.

Esta colección nace con la voluntad, bien de aportar soluciones o herramientas útiles para el mundo del trabajo, o bien de efectuar un análisis de no excesiva enjundia, pero si con el rigor y claridad que precisa el objeto de estudio. *Análisis y Contextos* pretende atender las necesidades de muy diversa índole –jurídica, económica, social, etc.– que pueden surgir en el ámbito del mundo social, siempre desde una perspectiva práctica a fin de servir a la mayoría

UGT