DERECHOS DIGITALES

FUNDACIÓN PRIMERO DE MAYO

UCLM Universidad de Castilla-La Mancha

# DERECHOS DIGITALES

## GUÍA PARA SU APLICACIÓN EN EL ÁMBITO LABORAL EN EL SECTOR BANCARIO

Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

red.es

Plan de Recuperación, Transformación y Resiliencia

# Objetivo de la guía

Difundir los derechos digitales en el ámbito laboral, a partir de la Carta de Derechos Digitales y proporcionar herramientas de aplicación para la representación legal de las personas trabajadoras (RLPT) en el sector bancario y financiero.

**Elaboración**
Fundación 1° de Mayo

**Colaboración:**
Secretaría Confederal de Acción Sindical y Empleo de CCOO
Federación de Servicios de CCOO

**Edición:**
Fundación 1° de Mayo

**Maquetación:**
Pilixip

**Proyecto de implementación de la Carta de Derechos Digitales en el ámbito de los derechos digitales en el entorno laboral y empresarial Convenio Red.es y Universidad de Castilla La Mancha**

Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

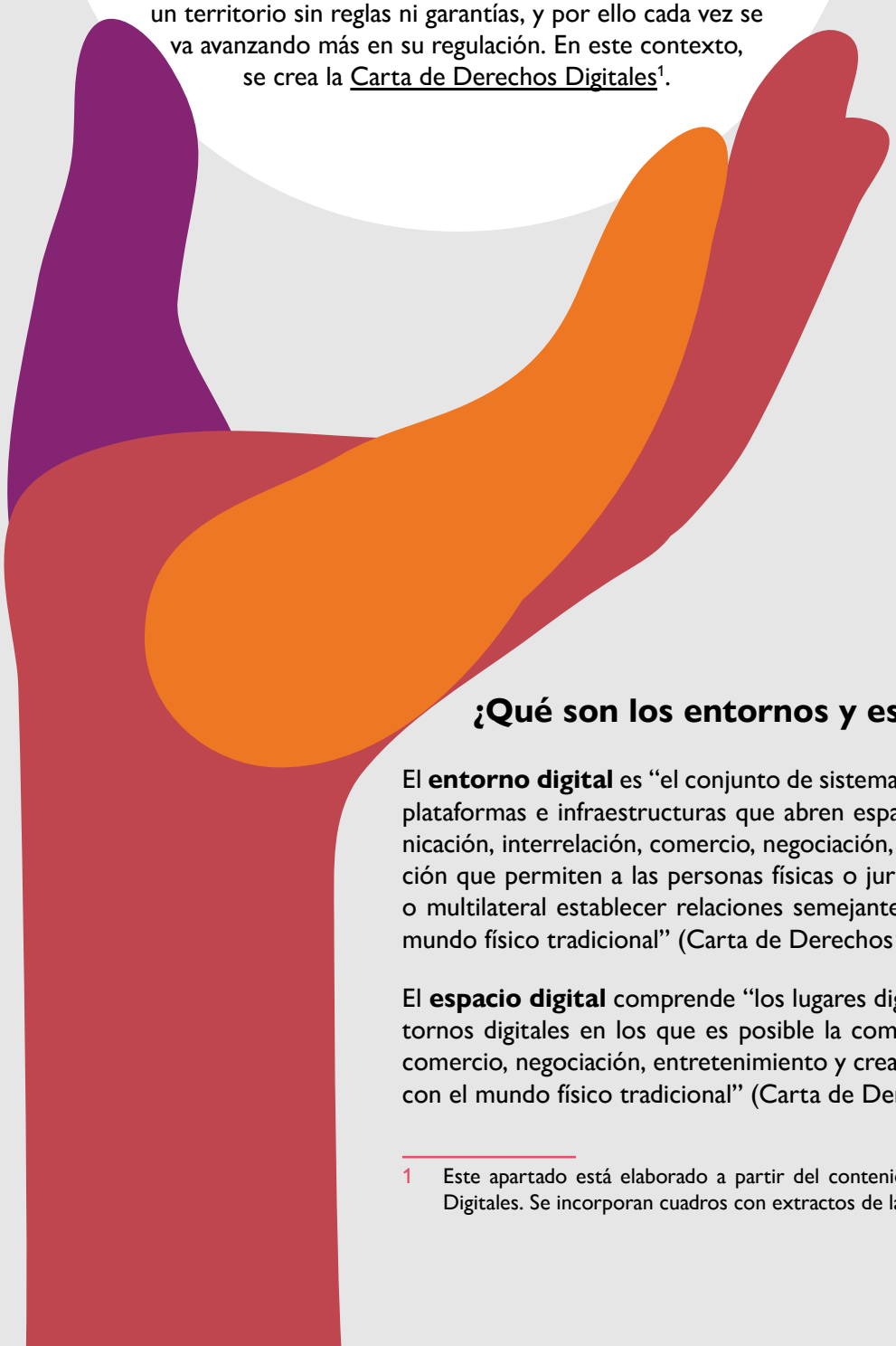
red.es

Plan de Recuperación, Transformación y Resiliencia

# Conoce tus derechos digitales: la Carta de Derechos Digitales

**Tus derechos no se apagan al entrar en el mundo digital**

Trabajamos, nos informamos y nos relacionamos a través de la tecnología, pero ¿sabemos realmente qué derechos nos protegen en estos entornos? El entorno digital no puede ser un territorio sin reglas ni garantías, y por ello cada vez se va avanzando más en su regulación. En este contexto, se crea la Carta de Derechos Digitales[1].



## ¿Qué son los entornos y espacios digitales?

El **entorno digital** es "el conjunto de sistemas, aparatos, dispositivos, plataformas e infraestructuras que abren espacios de relación, comunicación, interrelación, comercio, negociación, entretenimiento y creación que permiten a las personas físicas o jurídicas de forma bilateral o multilateral establecer relaciones semejantes a los existentes en el mundo físico tradicional" (Carta de Derechos Digitales).

El **espacio digital** comprende "los lugares digitales que abren los entornos digitales en los que es posible la comunicación, interrelación, comercio, negociación, entretenimiento y creación de forma especular con el mundo físico tradicional" (Carta de Derechos Digitales).

1 Este apartado está elaborado a partir del contenido de la Carta de Derechos Digitales. Se incorporan cuadros con extractos de la propia carta.

# ¿Qué es la Carta de Derechos Digitales?

Es un documento que recoge la batería de derechos que se extienden al entorno digital y que ya tenemos reconocidos en el entorno analógico. No es una ley, por lo tanto, sino un compendio de los principios y derechos fundamentales ya recogidos en otras leyes para proteger los derechos de la ciudadanía en el contexto de la implantación digital en cada vez más esferas de la vida cotidiana.

Con la Carta se pretende, por un lado, describir contextos y escenarios digitales en los que se pueden generar conflictos entre derechos, valores y bienes; por otro lado, intenta anticipar futuros escenarios en los que se pueden generar dichos conflictos. Y, por último, revalidar y legitimar los mecanismos para la aplicación de los derechos fundamentales en los entornos y espacios digitales.

La Carta se publicó en 2021 por el Gobierno de España, en el marco de la agenda España Digital 2025. Fue elaborada por un grupo de expertos, constituido por la Secretaría de Estado de Digitalización e Inteligencia Artificial del Ministerio de Asuntos Económicos y Transformación Digital. Contó, además, con la colaboración de representantes de otros Ministerios y Agencias.

La Carta, organiza la recopilación de **27 derechos** agrupados en **6 categorías**:

1. Derechos y libertades en el entorno digital
2. Derechos de igualdad
3. Derechos de participación y de conformación del espacio público
4. Derechos del entorno laboral y empresarial
5. Derechos digitales en entornos específicos
6. Garantías y eficacia

# 1. Derechos de libertad

### 1) Derechos fundamentales también en lo digital

- **Derechos y libertades en el entorno digital**: No solo en el trabajo. Se reconoce que los derechos fundamentales deben preservarse igualmente en espacios digitales, incluyendo libertad, dignidad, y no discriminación.

  *Los derechos y libertades reconocidos en la Declaración Universal de Derechos Humanos, la Constitución Española, el Convenio Europeo de Derechos Humanos, la Carta de los Derechos Fundamentales de la Unión Europea, y los tratados y acuerdos internacionales sobre las mismas materias ratificados por España son aplicables en los entornos digitales.*

### 2) Identidad, privacidad y control personal

- **Derecho a la identidad en el entorno digital**: Derecho a gestionar y acreditar tu identidad, además de no ser manipulada o controlada por terceros.
- **Derecho a la protección de datos**: Refuerza el control sobre los datos personales, incluyendo la rectificación, portabilidad o supresión de los mismos.
- **Derecho al pseudonimato**: Se garantiza la posibilidad de sustituir la identidad real, como forma de expresión o como protección de la identidad.
- **Derecho a no ser localizado y perfilado**: Permite a los ciudadanos decidir sobre el rastreo automatizado y el análisis de su comportamiento en línea.

### 3) Seguridad digital y herencia de derechos

- **Derecho a la ciberseguridad**: Asegura el establecimiento de mecanismos de protección frente a riesgos digitales, incluyendo la integridad de datos o la autenticidad de la información.
- **Derecho a la herencia digital**: Reconoce el derecho a decidir sobre el destino de datos y contenidos personales tras el fallecimiento.

  *Toda persona tiene derecho a que los sistemas digitales de información que utilice para su actividad personal, profesional o social, o que traten sus datos o le presten servicios, posean las medidas de seguridad adecuadas que permitan garantizar la integridad, confidencialidad, disponibilidad, resiliencia y autenticidad de la información tratada y la disponibilidad de los servicios prestados.*

# 2. Derechos de igualdad

### 1) Igualdad y justicia también en lo digital

- **Derecho a la igualdad y a la no discriminación en el entorno digital**: Asegura que ninguna persona sea excluida por razones de género, origen, edad, orientación sexual, o condición social.

### 2) Internet como derecho, no como privilegio

- **Derecho de acceso a Internet**: Garantiza el acceso universal, asequible y de calidad al entorno digital, una condición básica para ejercer otros derechos.

### 3) Protección de colectivos específicos hacia la ciudadanía digital plena

- **Protección de menores, personas mayores y con discapacidad**: Algunos colectivos tienen riesgos específicos, se promueve su plena inclusión digital.

# 3. Derechos de participación y de conformación del espacio público

### 1) Libertad de expresión y neutralidad de Internet: la base de un Internet libre e igualitario

- **Derecho a la neutralidad de Internet**: Asegura que los prestadores de servicios de gestión de la información den un trato igual, independientemente del emisor o el receptor: sin bloqueos, interferencias ni discriminación.
- **Libertad de expresión y libertad de información**: Reafirma el derecho a expresarse y difundir información sin censura arbitraria.
- **Derecho a recibir libremente información veraz**: Llama a blindar protocolos que aseguren la transparencia de la información de estos prestadores, incluyendo la obligación de informar sobre la mediación de procesos automatizados o publicidad.

### 2) Ciudadanía digital activa: participación, educación y derechos en la era digital

- **Participación ciudadana por medios digitales**: Fomenta el uso de tecnologías para intervenir en la vida democrática y tomar decisiones públicas.
- **Derecho a la educación digital**: Reconoce la necesidad de capacitar a todas las personas para que participen plenamente en la sociedad digital.
- **Relación digital con las Administraciones Públicas**: Asegura la participación ciudadana y el acceso a información y servicios públicos digitales sea equitativo y eficaz, sin brechas.

*Cualquier proceso de participación política, pública o privada, llevado a cabo por medios tecnológicos:*

*a) Deberá permitir el pleno y efectivo acceso a la información del proceso en cuestión.*

*b) Deberá permitir y garantizar la plena transparencia y rendición de cuentas de las personas implicadas, tanto si son Administraciones públicas en sus respectivos ámbitos competenciales, como otro tipo de entidades públicas o privadas.*

*c) Deberá garantizar las condiciones de igualdad y no discriminación participativa, lealtad institucional y justa y equilibrada competitividad.*

*d) Garantizará la accesibilidad de los sistemas digitales de participación pública.*

# 4. Derechos del entorno laboral y empresarial

### 1) Derechos fundamentales en el entorno digital laboral

- La dignidad y los derechos fundamentales de las personas trabajadoras se aplican plenamente en el ámbito digital. Esto implica el respeto a su integridad, privacidad y otros derechos inherentes a su condición laboral, adaptados al contexto de las nuevas tecnologías.

### 2) Derechos específicos en entornos digitales

- **Desconexión y conciliación:** Las personas trabajadoras tienen derecho al descanso y a la desconexión digital fuera de su horario laboral, así como a la conciliación de su vida personal y familiar, incluso en modalidades de teletrabajo.
- **Protección de la intimidad y datos:** Se garantiza la protección de su intimidad, honor, propia imagen, datos personales y secreto de comunicaciones frente al uso de dispositivos de vigilancia, grabación, herramientas de monitoreo y analítica.
- **Control empresarial lícito y transparente:** El uso de controles digitales por parte del empleador debe ser lícito, leal, proporcionado y transparente. Las personas trabajadoras tienen **derecho a ser informadas** sobre la política de uso de dispositivos digitales, incluyendo su posible uso privado.
- **Medios y protección frente al acoso:** Las personas empleadoras deben proporcionar los medios tecnológicos necesarios y no puede obligar al trabajador a usar sus propios dispositivos. Se garantiza la protección frente al acoso digital en el ámbito laboral.

### 3) Transformación digital y derechos de las personas trabajadoras

- **Formación y derecho a la información:** Las personas trabajadoras tienen derecho a una formación adecuada para adaptarse a los cambios tecnológicos. Su representación debe ser informada sobre los cambios tecnológicos que se implementen en la empresa.
- **Negociación colectiva y algoritmos:** La negociación colectiva puede establecer garantías adicionales sobre protección de datos y derechos digitales. El uso de algoritmos laborales requiere una evaluación de impacto en protección de datos, considerando principios éticos, perspectiva de género y no discriminación.
- **Seguridad y resiliencia de sistemas:** Las personas trabajadoras deben recibir información y formación sobre las condiciones de uso de los entornos digitales laborales, con especial atención a las obligaciones para garantizar la seguridad y resiliencia de los sistemas.

> *En los entornos digitales y el teletrabajo las personas trabajadoras del sector público o privado tienen derecho con arreglo a la normativa vigente, a [...] La protección de sus derechos a la intimidad personal y familiar, el honor, la propia imagen, la protección de datos y el secreto de las comunicaciones en el uso de dispositivos digitales, así como frente al uso de dispositivos de videovigilancia, de grabación de sonidos, así como en el caso de la utilización de herramientas de monitoreo, analítica y procesos de toma de decisión en materia de recursos humanos y relaciones laborales, y en particular, la analítica de redes sociales.*

### La empresa en el entorno digital: libertad, competencia y responsabilidad

Las empresas gozan de las libertades reconocidas en la Constitución Española, aplicable en los entornos digitales en el marco de la economía de mercado:

- Obligación de **respetar los derechos digitales de las personas en el desarrollo tecnológico y la transformación digital**.
- Reconocimiento del papel de los poderes públicos en la regulación, la transparencia, equidad y de reclamación de los usuarios y en la promoción de la investigación, desarrollo tecnológico e innovación.

# 5. Derechos digitales en entornos específicos

### 1) El bien de interés general en la digitalización

- **Derecho de acceso a datos con fines de interés público, cultural o científico**: Promueve el uso garantista y responsable de datos en investigaciones, archivos o políticas públicas. Se garantiza asimismo la producción y el acceso a contenido cultural y artístico.

### 2) Salud digital e inteligencia artificial: enfoques éticos y centrados en la persona

- **Derecho a la protección de la salud en el entorno digital**: Protege a las personas frente a usos tecnológicos que puedan afectar su bienestar físico o mental.
- **Derechos ante la inteligencia artificial**: Enfoque hacia la persona y su dignidad. Se garantiza transparencia, no discriminación y revisión humana de decisiones automatizadas.

  *En el desarrollo y ciclo de vida de los sistemas de inteligencia artificial:*

  *a) Se deberá garantizar el derecho a la no discriminación cualquiera que fuera su origen, causa o naturaleza, en relación con las decisiones y procesos basados en inteligencia artificial.*

  *b) Se establecerán condiciones de transparencia, auditabilidad, explicabilidad, trazabilidad, supervisión humana y gobernanza. En todo caso, la información facilitada deberá ser accesible y comprensible.*

  *c) Deberán garantizarse la accesibilidad, usabilidad y fiabilidad.*

### 3) Sostenibilidad

- **Derechos al entorno digital sostenible**: El desarrollo tecnológico debe ser sostenible, eficiente y respetuoso con el medioambiente, promoviendo dispositivos duraderos, energías limpias y políticas contra la obsolescencia programada.

### 4) Neurotecnologías

- **Derechos ante el uso de neurotecnologías**: Se reconocen los límites éticos y legales al uso de tecnologías que interactúan con la actividad cerebral, asegurando la autonomía y dignidad de la persona.

# 6. Garantías y eficacia

**Los derechos en entornos digitales deben ser plenamente garantizados mediante leyes, políticas públicas y mecanismos eficaces de control y supervisión**. La eficacia implica no solo su existencia legal, sino su aplicación práctica mediante recursos accesibles, protección judicial, y vigilancia ética del desarrollo tecnológico. Estas garantías son clave para que la digitalización respete el modelo democrático y los derechos fundamentales.

https://derechodigital.pre.red.es/

# Transformación digital en el sector de la banca: de los riesgos a los derechos

El sector bancario lleva años inmerso en un proceso de transformación digital que ha cambiado profundamente su composición y funcionamiento. Desde la implantación de plataformas digitales para la atención al cliente hasta el uso de sistemas automatizados de análisis y gestión financiera, la tecnología se ha convertido en una herramienta cotidiana, teniendo impactos sobre la organización del trabajo.

De acuerdo con la experiencia concreta de la representación legal de las personas trabajadoras en el sector, a pesar de la amplia variedad de condiciones de trabajo en las que se despliegan, los **principales riesgos** derivados de la digitalización se estructuran en torno a los siguientes ejes:

## 1. Desaparición de puestos de trabajo

En el contexto de un sector muy digitalizado, tras sucesivas reducciones de personal, la implementación de determinadas tecnologías como la inteligencia artificial produce temor a la eliminación de puestos de trabajo; por el riesgo a que todas las tareas que componen los mismos puedan ser automatizadas.

- Por ejemplo, la automatización de las tareas de atención al cliente ha desplazado a personas trabajadoras por simuladores informáticos de conversación (*chatbot*).

## 2. Falta de formación tecnológica

La falta de formación se identifica habitualmente como un riesgo. La obsolescencia formativa tiene varias implicaciones, desde la adaptación técnica (que aumenta el temor a ser desplazado/a por herramientas digitales) hasta la adaptación a los nuevos riesgos psicosociales derivados de la propia digitalización.

## 3. Impactos en la promoción y retribución

Como consecuencia del uso de nuevas tecnologías, crece la preocupación sobre el impacto en la promoción profesional y los sistemas de retribución como consecuencia de decisiones automatizadas: los sesgos proyectados en el algoritmo pueden generar situaciones discriminatorias.

Cabe resaltar el impacto sobre los expedientes sancionadores, especialmente en casos donde la evaluación de rendimiento se realiza mediante inteligencia artificial.

## 4. Uso de datos personales e intimidad

El uso de datos personales por parte de la empresa, como la geolocalización de dispositivos móviles, grabación y análisis de llamadas, control mediante tarjetas de acceso… es una preocupación creciente entre las personas trabajadoras del sector bancario. Si bien la vigilancia puede justificarse en términos de seguridad, estas formas de monitoreo pueden implicar un control desproporcionado contrario al derecho a la intimidad.

## 5. Acoso digital y deshumanización

La automatización del servicio y la exigencia de respuestas rápidas bajo supervisión constante, generan contextos que pueden facilitar situaciones de maltrato, desconsideración o acoso por parte de clientes, especialmente cuando el contacto es impersonal y mediado por herramientas digitales.

Las plantillas del sector bancario pueden ser víctimas de comportamientos violentos en redes sociales. La violencia se produce de diversas formas: comentarios sobre el servicio, descalificaciones sobre aspecto físico en redes sociales, críticas relacionadas con el servicio prestado, etc.

La implementación de herramientas digitales en el servicio puede producir una mayor desafección entre el personal y las personas usuarias, dando lugar a una creciente deshumanización que favorece la aparición de estos comportamientos.

## 6. Salud en el trabajo y riesgos psicosociales

La implantación de tecnologías de vigilancia y control puede dar lugar a diversos riesgos psicosociales (estrés, exceso de carga de trabajo, conflictividad interpersonal, falta de autonomía, inseguridad, interferencias entre la vida personal y laboral, etc.).

Aquí es altamente relevante la nueva relación digital establecida entre servicio y usuario/a, que puede derivar en trabajos más demandantes. Esto produce una mayor incidencia de los riesgos descritos, especialmente los relacionados con el exceso en la carga de trabajo y las exigencias emocionales (actitud positiva y disponibilidad constante en entornos digitales).

Cabría añadir un último aspecto relativo a los riesgos de la digitalización. La consideración empresarial de la tecnología como una "excepción" de los marcos regulatorios ha llevado a su implantación unilateral: **introducir la tecnología sin una gestión negociada con anticipación, y participación de las personas trabajadoras[2], produce indefensión**. Es necesario orientar hacia el entorno digital la capacidad de incidir en las condiciones de trabajo.

2 Tal y como se acordó entre los interlocutores sociales en el Acuerdo Marco Europeo sobre Digitalización.

# Los derechos digitales en el ámbito laboral

Ante la incorporación de cualquier tipo de tecnología en la empresa, existen una serie de derechos que pueden ser ejercidos por parte de las **personas trabajadoras**, así como de sus **representantes (RLPT)**. En este sentido, existen derechos que pueden ser ejercidos de forma individual y/o colectivamente.

Los derechos digitales individuales están orientados a proteger la dignidad, la privacidad, la autonomía y la salud de las personas trabajadoras frente al uso intensivo de tecnologías digitales. Estos derechos están reconocidos en diversas normativas, tanto europeas -los Reglamentos de Protección de Datos (RGPD) y de Inteligencia Artificial (RIA) y la Directiva relativa a la mejora de las condiciones laborales en el trabajo en plataformas-, como en el Estatuto de los Trabajadores (ET), la Ley Rider, la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD), la Ley de Prevención de Riesgos Laborales (LPRL) y la Ley Integral para la Igualdad de trato y no discriminación. Desde el punto de vista colectivo, se reconoce el derecho de la RLPT a participar activamente en las decisiones que afectan al empleo y las condiciones laborales de las personas trabajadoras.

Los principales derechos en el entorno laboral digital son:

| Derecho digital en el ámbito laboral | Derechos individuales | Derechos de la RLPT | Artículos legales de referencia |
|---|---|---|---|
| **Derecho a la intimidad** | Derecho a la protección de la intimidad en el uso de los dispositivos digitales puestos a su disposición.<br><br>El empleador sólo podrá acceder a los contenidos con el objetivo de controlar el cumplimiento de sus obligaciones y garantizar la integridad de los dispositivos. Este mecanismo de control debe estar justificado y sujeto a criterios de proporcionalidad.<br><br>Además, deberán establecer criterios de utilización de los dispositivos digitales, respetando los estándares mínimos de protección de derechos de intimidad y especificar las condiciones de su uso con fines privados e informar a la plantilla.<br><br>Este derecho es especialmente relevante en términos de videovigilancia y geolocalización. El uso de imágenes y datos obtenidos por sistemas de cámaras, videocámaras o sistemas de geolocalización debe estar supeditada al marco legal. Este uso debe ser informado previamente y estará orientado exclusivamente a fines legítimos como la seguridad o control de actividad. | La RLPT ostenta derechos de información y consulta. Además, puede participar en el establecimiento de los criterios de utilización de los dispositivos digitales en todo caso los estándares mínimos de protección de su intimidad de acuerdo con los usos sociales y los derechos reconocidos constitucional y legalmente. | LOPDGDD arts. 87, 89, 90 y 91.<br><br>ET arts. 20 bis. y 64. |

| Derecho digital en el ámbito laboral | Derechos individuales | Derechos de la RLPT | Artículos legales de referencia |
|---|---|---|---|
| **Desconexión digital** | Las personas trabajadoras tienen derecho a la desconexión digital para garantizar el respeto a su tiempo de descanso, permisos, vacaciones e intimidad personal y familiar, salvo situaciones de fuerza mayor.<br><br>Las modalidades de desconexión digital deben potenciar el derecho a la conciliación laboral, personal y familiar. | La RLPT debe ser consultada para la elaboración de "una política interna dirigida a trabajadores/as, incluidos los que ocupen puestos directivos, en la que definirán las modalidades de ejercicio del derecho a la desconexión y las acciones de formación y de sensibilización del personal sobre un uso razonable de las herramientas tecnológicas que evite el riesgo de fatiga informática". | LOPDGDD art. 88. |
| **Protección de datos personales** | El tratamiento de datos personales por parte del empleador debe cumplir con los principios de licitud, lealtad, transparencia, minimización, exactitud y limitación, es decir, solo deben recogerse los datos estrictamente necesarios, de forma clara y justificada. Para que este tratamiento sea lícito, debe basarse en una base jurídica válida, como el cumplimiento de una obligación legal o la ejecución del contrato laboral. Además, el empleador debe informar al trabajador de forma clara y accesible sobre el tratamiento de sus datos personales, especificando finalidades, responsables y derechos. Las personas trabajadoras, como titulares de sus datos, tienen derecho a acceder a ellos, rectificarlos, suprimirlos, oponerse a su tratamiento, limitarlo o solicitar su portabilidad, lo que les otorga un control efectivo sobre su información personal en el ámbito profesional. | Derechos de información y consulta de la RLPT. | RGPD arts. 5, 6, 13, 14, 15-22.<br><br>ET art. 64. |
| **Inteligencia artificial y decisiones algorítmicas** | Derecho a no ser objeto de decisiones basadas sólo en el tratamiento automatizado, incluida la elaboración de perfiles, que tenga efectos jurídicos en él o le afecte de modo similar. Aunque con consentimiento explícito o por necesidad para la celebración del contrato, la persona responsable del tratamiento ha de salvaguardar los derechos, libertades e intereses legítimos de la persona interesada. Esto implica, al menos, el derecho a la intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión.<br><br>Derecho a no ser discriminada por categorías personales o comportamientos en el uso de sistemas de IA categorizados como de alto riesgo: contratación, evaluación, promoción, despido, supervisión y asignación de tareas.<br><br>Derecho a recibir explicaciones claras y significativas del responsable del despliegue del sistema de IA, acerca del papel que ha tenido en el proceso de toma de decisiones que produzcan efectos jurídicos o que le afecten considerablemente sobre su salud, seguridad o derechos fundamentales.<br><br>Las personas que realizan trabajo en plataformas: derecho a ser informadas sobre la utilización de sistemas automatizados de seguimiento o de sistemas automatizados de toma de decisiones. | Derecho a ser informadas sobre el uso de algoritmos que afecten a condiciones laborales. La representación puede exigir transparencia sobre sistemas algorítmicos y su impacto laboral.<br><br>Derecho de información ante la introducción de sistemas de IA considerados de alto riesgo.<br><br>Derecho de información y consulta sobre la utilización de sistemas automatizados de seguimiento o de sistemas automatizados de toma de decisiones en el trabajo de plataformas. | RGPD art. 22.<br><br>ET art. 64.4.<br><br>Reglamento (UE) 2024/1689.<br><br>Directiva (UE) 2024/2831 (art.9 al art.15). |

| Derecho digital en el ámbito laboral | Derechos individuales | Derechos de la RLPT | Artículos legales de referencia |
|---|---|---|---|
| **Formación digital** | Derecho a formación continua ante cambios tecnológicos:<br>• Por adaptación de la actividad profesional.<br>• Por adaptación a nuevos riesgos laborales derivados.<br>Alfabetización en materia de IA: comprensión, uso, pensamiento crítico-ético y participación activa en el funcionamiento de IA. | Derecho a proponer medidas formativas colectivas.<br>Derecho a la consulta en relación al proyecto y la organización de la formación en materia preventiva. | Arts. 4.2.b y 23.1.d ET; 64.ET.<br>Art 19.1 LPRL; Art. 33.1.e LPRL.<br>Art. 4 Reglamento (UE) 2024/1689. |
| **Prevención de riesgos laborales** | El deber de protección empresarial es *ilimitado*, abarcando también el entorno digital. Este deber se expresa en:<br>• La **vigilancia de la salud** ante la implementación de nuevas tecnologías (sometida al consentimiento de la persona trabajadora, salvo excepciones legales o de seguridad).<br>• **Derecho a la formación e información específica** sobre riesgos del entorno digital, en lo relativo al uso de herramientas o la desconexión digital.<br>• **Derecho a la adaptación del trabajo**, un principio preventivo especial ante la "elección de los equipos y métodos de trabajo".<br>• El **derecho a la política de prevención de riesgos laborales** debe enfocarse sobre aspectos relacionados con el derecho al honor, incluyendo la **protección frente a humillaciones, ofensas, trato degradante o acoso**. | La dimensión colectiva es fundamental en términos preventivos: el deber de protección empresarial se realiza sobre los **derechos de información, consulta y participación** de las personas trabajadoras y la RLPT.<br>"No deberá utilizarse ningún dispositivo cuantitativo o cualitativo de control sin que los trabajadores hayan sido informados y previa consulta con sus representantes". | Arts. 14.2, 15.1, 19.1 y 22 LPRL.<br>Arts. 4.2.d) y e), 64 ET.<br>18 y 33 LPRL.<br>RD 488/1997 Anexo disposiciones mínimas 3b). |

En todo caso, en el marco de la transformación digital, las **personas trabajadoras y sus representantes tienen derecho a participar activamente** en las decisiones tecnológicas que afectan a su empleo y condiciones laborales.

En el ejercicio de este derecho se reconoce el principio transparencia, en el que la empresa dé cuenta con suficiente antelación de la información sobre la tecnología usada en la empresa y sus implicaciones en la gestión, monitorización y procesos de toma de decisión en materia de recursos humanos y relaciones laborales (LOPDGDD Art 87, ET 64.4). Además, requiere el establecimiento de evaluaciones de impacto en materia de protección de datos, que hagan posible el seguimiento de la implantación de la tecnología y los riesgos asociados (Reglamento UE 2024/1689, LOPDGDD), también en la directiva de plataformas. Y finalmente, se garantizan los derechos para el desarrollo de la acción sindical en los medios digitales, que hagan posible el ejercicio de representación, de forma accesible e inclusiva a todas las personas trabajadoras y (art. 79 y 91 LOPDGDD, art. 19 Ley 10/2021).

Finalmente, hay que remarcar el papel crucial que representan el diálogo social y la negociación colectiva en el avance de los derechos digitales. En los últimos años, han sido numerosos los acuerdos en este ámbito en diferentes niveles, tanto internacionales como en España. Entre los últimos acuerdos, cabe destacar el Acuerdo Social para la reducción de la Jornada Laboral, que incorpora algunas referencias a la desconexión digital[3].

3 El Gobierno ha aprobado en el Consejo de ministros una reducción de la jornada laboral, acordada con los sindicatos más representativos. En el que se regula el derecho a la desconexión: Artículo 18. Derecho a la desconexión digital. Las personas que trabajan a distancia tienen derecho a la desconexión en los términos establecidos en el artículo 20 bis del texto refundido de la Ley del Estatuto de los Trabajadores, aprobado por Real Decreto Legislativo 2/2015. En particular, se reconoce el derecho a la desconexión digital en los supuestos de realización total o parcial del trabajo a distancia, así como en el domicilio de la persona empleada vinculado al uso con fines laborales de herramientas tecnológicas, debiendo la empresa establecer los medios y medidas adecuadas para garantizar el ejercicio efectivo de tal derecho (…).

# ¿Cómo ejercer los derechos digitales en el ámbito laboral?

## Identificar los riesgos

El **primer paso** de la RLPT en el centro de trabajo es la **identificación de los riesgos asociados** a la transformación digital y su impacto en las condiciones de trabajo.

Es conveniente acudir a la negociación colectiva preestablecida, ya que probablemente las preocupaciones de las personas trabajadoras en el sector ya formen parte de su contenido. En el caso de que no sea así, se pueden utilizar diversos medios: a) el diálogo con las personas trabajadoras, bien de forma individual o colectiva (encuestas, entrevistas, reuniones, talleres y asambleas); b) la elaboración de un inventario de las tecnologías implementadas o previstas en el futuro cercano, para evaluar sus características y posibles impactos; c) la solicitud de información directamente a la empresa sobre la tecnología que incorporada o que se pretende utilizar; d) la utilización de las herramientas existentes (en materia de prevención de riesgos laborales, igualdad, etc.), ya disponibles al alcance de la RLPT.

En el caso del sector bancario, uno de los retos recientes más relevantes identificados por la RLPT es abordar **vulneraciones relativas al uso de datos personales**. Estas no solo se derivan del uso intensivo de datos y el **control a través de dispositivos tecnológicos por parte de la empresa**, también del modo en que estas herramientas alteran el entorno de trabajo y la **relación con las personas usuarias** por la digitalización de la atención al cliente.

A modo de ejemplo, a continuación, se presentan los **principales elementos** de actuación de la representación al respecto.

## Uso de datos personales y mecanismos de control digital

### Información, consulta, negociación y evaluación

#### a) Petición de información

Las y los representantes —ya sea a través del **comité de empresa** o la **sección sindical**— tienen el derecho a solicitar **por escrito** a la empresa una exposición detallada sobre la incorporación de tecnologías que puedan derivar en vulneraciones sobre el uso de datos personales o contra el derecho a la intimidad. La respuesta de la empresa debe recoger, en lenguaje no técnico y de forma concisa, los fundamentos para el uso de datos personales, así como las consecuencias que pueda tener sobre la privacidad y las condiciones laborales del personal. De este modo, la representación vela por que se respeten los principios de proporcionalidad y uso limitado conforme a la finalidad prevista

Es imprescindible que este requerimiento incluya un **compromiso por parte de la empresa de notificar por escrito y con la debida antelación cualquier modificación** futura que afecte al uso de datos personales de las personas trabajadoras, incluyendo los que afecten a las nuevas formas digitalizadas de atención al cliente.

Cabe resaltar que la solicitud se centra en obtener una descripción comprensible sobre la tecnología implantada, su propósito y los posibles efectos en el entorno de trabajo: no se trata de acceder a detalles técnicos delicados ni a elementos estratégicos de la empresa.

#### b) Modelos de solicitud de información

La Agencia Española de Protección de Datos (AEPD), ha realizado unos formularios para realizar solicitudes de petición de información, de rectificación, de oposición de tratamiento o de supresión de datos personales,

entre otros, con lo que las personas trabajadoras se pueden dirigir a sus empresas o a aquellas empresas que hayan publicado sus datos personales en internet para solicitar su modificación o supresión. En caso de que estas solicitudes no tengan el resultado deseado puede acudirse a la propia AEPD para solicitar el cumplimiento de esta acción.

| | |
|---|---|
| Solicitud información sobre datos personales **Derecho de acceso** | Solicitud rectificación de datos personales inexactos **Derecho de rectificación** |
| Solicitud de oposición al tratamiento de los datos **Derecho de oposición** | Solicitud de supresión de datos personales **Derecho al olvido** |

### c) Plazos de consulta

Se debe solicitar esta información con la **periodicidad adecuada**, preferiblemente establecida en los convenios colectivos durante su negociación. Es fundamental fijar un plazo máximo de entrega y asegurar el compromiso de la empresa para cumplirlo.

La empresa debe consultar, necesariamente, antes de implantar nuevas tecnologías que recojan o procesen datos del personal y antes de que se modifiquen sustancialmente los canales de atención al cliente que afecten al trabajo de personas. La consulta debe ser **previa a la implementación**. Aunque no existen plazos legales, si tampoco hay referencia en el convenio de aplicación, debe existir un **criterio de antelación debida**: debe ser un plazo razonable para que la representación legal de las personas trabajadoras pueda analizar la documentación, formular observaciones y, en su caso, proponer medidas alternativas o correctoras. Además, la consulta debe estar acompañada de la **documentación completa**, incluyendo un **análisis de impacto** (más adelante).

### d) Falta de información

De forma deliberada, por desconocimiento o negligencia, es habitual que las empresas no faciliten información ante la implementación de tecnologías de explotación de datos y nuevos mecanismos de control digital.

Esto se debe habitualmente a una mala praxis: la empresa no integra efectivamente a la RLPT en los procesos normales de actualización de la organización del trabajo, a menudo confundiendo la protección de datos con aspectos estratégicos legítimos de seguridad informática. El temor a que pueda cuestionarse o bloquearse el proyecto de digitalización no debería derivar en una **vulneración de los derechos de información y consulta**, es por ello que la petición de información es un derecho que puede y debe reclamarse.

La defensa de los derechos de información y consulta en estos casos no es una barrera al desarrollo tecnológico, sino una garantía imprescindible para el respeto a los derechos fundamentales en los centros de trabajo.

### e) Análisis de impacto

El análisis de impacto es una evaluación **obligatoria previa**, en caso de que las medidas impliquen vigilancia sistemática, uso de nuevas tecnologías, tratamiento de datos sensibles o simplemente pueda afectar a derechos fundamentales de las personas trabajadoras. El análisis debe detallar qué datos se tratan, qué riesgos existen y qué medidas han de tomarse.

La RLPT debe ser parte del proceso de consulta, que deberá velar por la aplicación de los **principios de minimización, necesidad y proporcionalidad**: no pueden recogerse más datos de los pertinentes para cumplir una finalidad laboral legítima, sólo cuando sea estrictamente necesario.

La actuación sindical al respecto debe seguir algunos pasos:

1. **Solicitar análisis de impacto** ante cualquier novedad tecnológica, tanto en la relación directa de la empresa con la plantilla como en los nuevos mecanismos de atención al cliente por parte de la plantilla.

2. Si no se facilita, exigir formalmente por **escrito**.

3. Si el contenido aportado por la empresa no es riguroso, pueden aportarse **informes propios** (con ayuda del servicio jurídico) para rebatirlo.

4. Denuncia si existe ausencia de:

    - Análisis de impacto.
    - Consulta a la RLPT.
    - Identificación de riesgos.

### f) Principales vulneraciones

La utilización de sistemas digitales de control y gestión virtual de la atención al cliente puede derivar en vulneraciones de diverso tipo.

- Falta de transparencia y consulta previa. Cuando se implementan sistemas digitales de seguimiento o evaluación sin haber informado ni consultado previamente a la representación de las personas trabajadoras, se está incumpliendo la obligación legal de garantizar su participación en decisiones que afectan a su uso (art. 64 ET). Esta omisión puede ser denunciada ante la Inspección de Trabajo o incluso ante la jurisdicción social, especialmente si afecta al ejercicio normal de la acción sindical.

- Intromisión en la vida privada: La monitorización de movimientos mediante geolocalización, el análisis de datos recogidos desde herramientas digitales de trabajo, como dispositivos móviles, puede constituir una invasión del derecho a la intimidad. En estos casos, corresponde exigir a la empresa documentación detallada, evaluaciones de impacto y la adopción de garantías específicas. Ante la ausencia de respuesta, se puede acudir a la Agencia Española de Protección de Datos o a la Inspección de Trabajo (LOPDGDD, RGPD y art. 20.bis ET).

- Vulneración al derecho al honor por parte de usuarios: La automatización parcial del servicio y la exigencia de respuestas rápidas bajo supervisión constante, generan contextos que pueden facilitar situaciones de maltrato, desconsideración o acoso por parte de clientes y usuarios. Se ha de exigir a la empresa el establecimiento de protocolos claros. Si no hubiese respuesta, debe demandarse ante Inspección de Trabajo y, en su caso, interponiendo demanda judicial contra el usuario o usuaria.

- Efectos negativos sobre la salud. La presión derivada del control digital continuo, el contacto deshumanizado con la clientela o la imposibilidad de desconexión real pueden deteriorar la salud mental y emocional de la plantilla. Cuando se detecten estos riesgos, debe exigirse una evaluación específica en materia de prevención de riesgos laborales, prestando especial atención a los factores psicosociales. Si la empresa no responde, se puede presentar denuncia ante la Inspección de Trabajo (LPRL y ET).

## Negociación colectiva: materias y proceso

Es relevante considerar el V Acuerdo para el Empleo y la Negociación Colectiva, que establece directrices para la negociación colectiva en el periodo 2023-2025, promoviendo un enfoque basado en el diálogo social y participación activa de la RLPT en la adaptación a los cambios tecnológicos. Entre otros aspectos, aborda la necesidad de incorporar cláusulas que regulen el uso de tecnologías digitales en el ámbito laboral, incluyendo la protección de datos, transparencia en la gestión del trabajo y el blindaje de los derechos de información a la RLPT.

La negociación colectiva debe partir del análisis de las exigencias legales en materia de protección de datos, derechos laborales y participación sindical, pero tiene además un papel central en la ampliación de garantías frente a los impactos de la digitalización en el empleo, la organización del trabajo y los derechos fundamentales.

Algunas materias que pueden tenerse en cuenta:

Por un lado, en lo relativo al **uso empresarial de datos personales y los mecanismos de control digital**, podemos destacar cláusulas relativas a:

- Políticas de privacidad y uso de datos.
  - **Definición clara y concisa** de las finalidades del tratamiento de datos personales de empleados y clientes.
  - Procedimientos para la **anonimización o seudonimización** de datos cuando sea posible.
- Transparencia y consentimiento.
  - **Información** detallada a los empleados sobre qué datos se recogen, cómo se utilizan y con qué fines.
  - **Garantías para la obtención del consentimiento** informado y explícito en situaciones que lo requieran.
- Mecanismos de control y supervisión digital:
  - Regulación del uso de herramientas de monitoreo y control digital (ej., software de seguimiento, teléfono móvil, cámaras, tarjetas de acceso).
  - Establecimiento de criterios claros y objetivos para su implementación, con justificación de los **principios de minimización, necesidad y proporcionalidad**.
  - **Procedimientos para la notificación y consulta** a la representación de las personas trabajadoras antes de implementar nuevas tecnologías de control.
- Formación y sensibilización:
  - Programas de formación obligatoria para todos los empleados sobre la normativa de protección de datos (RGPD, LOPDGDD), buenas prácticas y riesgos asociados.
  - **Formación específica** en prevención de riesgos psicosociales relativos a la implementación de nuevas tecnologías.
- Revisión y seguimiento:
  - Establecimiento de un **calendario regular de auditorías** internas y externas para verificar el cumplimiento de las políticas de protección de datos.
  - Definición de **mecanismos para la resolución** de incidencias, vulneraciones o brechas de seguridad, incluyendo la paralización cautelar.

- Creación de un **Comité de Protección de Datos** paritario para supervisar la aplicación del convenio en esta materia.

Algunas materias no quedarán extensamente reflejadas en la negociación, pero en su marco puede establecerse la creación de protocolos específicos que, con mayor detalle, complementen lo establecido convencionalmente (ej. protocolos de uso ético y transparente de datos).

En cuanto al acoso interno y externo mediante canales digitalizados de comunicación:

- Definición y tipificación del acoso:
  - Inclusión en el convenio de una **definición clara de acoso y comportamientos** inadecuados por parte de los clientes (ej., lenguaje ofensivo, amenazas, insinuaciones sexuales) en entornos digitales (chats, videollamadas, redes sociales).
    - Esto abarca tanto el acoso por parte de clientes (ej., lenguaje ofensivo, amenazas, insinuaciones sexuales en canales digitales como chats o videollamadas) como el acoso interno por parte del personal, incluido el dirigido específicamente a la representación de las personas trabajadoras en el ejercicio de sus funciones
  - **Tipificación** de las diferentes modalidades de acoso para facilitar su identificación y denuncia.
- Protocolos de actuación y denuncia:
  - Desarrollo de **protocolos claros y accesibles** para que los empleados puedan denunciar situaciones de acoso por parte de clientes.
  - Establecimiento de **canales de denuncia preferentes**, que puedan incluir la gestión por una entidad externa o un comité paritario con garantías.
  - Garantía de **anonimato** si el empleado lo desea, siempre que sea compatible con la investigación.
  - Procedimientos para la apertura de investigaciones inmediatas, rigurosas y objetivas ante cualquier denuncia de acoso.
- Medidas de apoyo y protección para los empleados:
  - **Apoyo psicológico y asesoramiento legal** para el personal afectado por situaciones de acoso.
  - **Medidas de protección** como el cambio de turno, la reasignación de tareas o la posibilidad de bloquear la comunicación con clientes acosadores, si es viable.
  - **Formación específica** para gestionar situaciones de conflicto y acoso en la atención digital.
- Medidas antiacoso:
  - Inclusión en las condiciones de uso de los servicios digitales bancarios de un **código de conducta** que sancione el acoso al personal.
  - Establecimiento de **mecanismos para la identificación y, si procede, el bloqueo o la restricción del acceso** a los servicios de clientes que incurran en acoso.
  - Establecimiento de un **régimen disciplinario claro y ejemplarizante** para las y los trabajadores, equipo directivo o cualquier miembro de la organización que incurra en acoso, con sanciones proporcionales a la gravedad.

La negociación colectiva se erige como la herramienta esencial para abordar estos desafíos, permitiendo construir un marco de derechos y deberes que garantice la protección de datos y un entorno laboral seguro.

La empresa debe reconocer la legitimidad del interlocutor en este cometido y, por otro lado, su responsabilidad en la protección de datos y la integridad moral y psicológica de sus trabajadores, que se materializa también mostrando el compromiso ineludible con la negociación.

## Algunos ejemplos:

### XXIII Convenio colectivo de las sociedades cooperativas de crédito (2024)

**Artículo 68. Transformación digital.**

La transformación digital es un factor intrínseco de la evolución de las estructuras empresariales, con potenciales efectos sobre el empleo y las características y condiciones de trabajo, por lo que resulta necesario que la representación de las empresas y las de los trabajadores colaboren proactivamente, anticipándose a estos cambios y a sus efectos sobre las condiciones de trabajo.

Por ello, las partes entienden que la negociación colectiva, por su naturaleza y funciones, es un instrumento para facilitar una adecuada y justa gobernanza del impacto de la transformación digital de las entidades sobre el empleo del sector.

A estos efectos, en los procesos de transformación digital, las Empresas informarán a la RLPT sobre los cambios tecnológicos que se vayan a implantar en las mismas cuando éstos sean relevantes y puedan tener consecuencias significativas sobre el empleo y/o cambios sustanciales en las condiciones laborales.

Fuente: BOE. 2025

### XXIII Convenio colectivo de las sociedades cooperativas de crédito (2024)

**Artículo 69. Derechos digitales**

[...]

2. Derecho a la intimidad y al uso de dispositivos digitales en el ámbito laboral.

Las Empresas, cuando carezcan de ellos, deberán elaborar con participación de la RLPT protocolos en los que se fijen los criterios de utilización de los dispositivos digitales que, en todo caso, deberán garantizar, en la medida legalmente exigible, la debida protección a la intimidad de las personas trabajadoras que hagan uso de los mismos, así como sus derechos establecidos constitucional y legalmente.

Los dispositivos digitales necesarios para el desempeño de la actividad laboral deberán ser facilitados a las personas trabajadoras por parte de las Empresas.

Por parte de la empresa, y en los términos dispuestos en el artículo 87 de la LOPD, se podrá acceder a los contenidos derivados del uso de medios digitales, a los solos efectos de controlar el cumplimiento de las obligaciones laborales o estatutarias y de garantizar la integridad de dichos dispositivos, estableciendo los criterios de utilización de los dispositivos digitales respetando en todo caso la protección de la intimidad de las personas trabajadoras.

En el supuesto de que se permita, por parte de las Empresas, el uso privado a través de los dispositivos digitales propiedad de las mismas, los protocolos deberán especificar, de modo preciso, qué tipos de usos son los autorizados, y establecerán garantías para preservar la intimidad de las personas trabajadoras tales como, en su caso, la determinación de los períodos en que los dispositivos podrán utilizarse para fines privados.

3. Derecho a la intimidad frente al uso de dispositivos de videovigilancia, grabación de sonidos y geolocalización en el ámbito laboral.

La implantación por parte de las Empresas de tecnologías de la información para el control de la prestación laboral, tales como videovigilancia, grabación de sonidos, controles biométricos, controles sobre el ordenador (monitorización remota, indexación de la navegación por internet, o la revisión o monitorización del correo electrónico y/o del uso de ordenadores) o controles sobre la ubicación física de la persona trabajadora mediante geolocalización, se realizará conforme a la legislación vigente. Además, dichas medidas deberán ser proporcionales a la finalidad de verificar el cumplimiento por parte de las personas trabajadoras de sus obligaciones y deberes laborales.

Para los casos de grabaciones de imágenes y sonidos, se procurarán establecer los medios necesarios para grabar aquellas imágenes y/o conversaciones consideradas como necesarias por la Empresa para garantizar la seguridad y/o la calidad de la actividad desarrollada en el centro de trabajo y/o la exigible cuando así sea requerido por la normativa legal en materia de protección de la clientela.

Fuente: BOE. 2025

## XXV Convenio colectivo del sector de la banca (2024)

**Artículo 80. Derechos digitales**

[...]

2. Derecho a la intimidad y al uso de dispositivos digitales en el ámbito laboral.

Las Empresas, cuando carezcan de ellos, deberán elaborar con participación de la RLPT protocolos en los que se fijen los criterios de utilización de los dispositivos digitales que, en todo caso, deberán garantizar, en la medida legalmente exigible, la debida protección a la intimidad de las personas trabajadoras que hagan uso de los mismos así como sus derechos establecidos constitucional y legalmente.

Los dispositivos digitales necesarios para el desempeño de la actividad laboral deberán ser facilitados a las personas trabajadoras por parte de las Empresas.

Por parte de la Empresa, en cumplimiento de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD), se podrá acceder a los contenidos derivados del uso de medios digitales facilitados a las personas trabajadoras a los solos efectos de controlar el cumplimiento de las obligaciones laborales o estatutarias y de garantizar la integridad de dichos dispositivos.

En el supuesto de que se permita, por parte de las Empresas, el uso privado a través de los dispositivos digitales propiedad de las mismas, los protocolos deberán especificar qué tipos de usos son los autorizados, y establecerán garantías para preservar la intimidad de las personas trabajadoras tales como, en su caso, la determinación de los períodos en que los dispositivos podrán utilizarse para fines privados. Las personas trabajadoras deberán ser informadas de los criterios de utilización.

[...]

5. Derecho ante la inteligencia artificial.

Las nuevas herramientas basadas en algoritmos pueden aportar valor hacia una gestión más eficiente de las Empresas, ofreciendo mejoras en sus sistemas de gestión. Sin embargo, el desarrollo creciente de la aportación de la tecnología requiere de una implantación cuidadosa cuando se aplica en el ámbito de las personas. Por ello, las personas trabajadoras tienen derecho a no ser objeto de decisiones basadas única y exclusivamente en variables automatizadas, salvo en aquellos supuestos previstos por la ley, así como derecho a la no discriminación en relación con las decisiones y procesos, cuando ambos estén basados únicamente en algoritmos, pudiendo solicitar, en estos supuestos, el concurso e intervención de las personas designadas a tal efecto por la Empresa, en caso de discrepancia.

Las Empresas informarán a la RLPT sobre el uso de la analítica de datos o los sistemas de inteligencia artificial cuando los procesos de toma de decisiones en materia de recursos humanos y relaciones laborales se basen, exclusivamente en modelos digitales sin intervención humana. Dicha información, como mínimo, abarcará los datos que nutren los algoritmos, la lógica de funcionamiento y la evaluación de los resultados

Fuente: BOE. 2025

# Anexo:

## Extracto del convenio colectivo para los establecimientos financieros de crédito sobre derechos digitales (2023).

### Artículo 35. Derechos digitales.

Las partes reconocen los siguientes derechos digitales que la plantilla tiene en el ámbito laboral:

**1. Derecho a la desconexión digital y laboral.**

Las partes firmantes consideran que la desconexión digital y laboral es un derecho cuya regulación contribuye a la salud de las personas trabajadoras disminuyendo, entre otras, la fatiga tecnológica o estrés, y mejorando, de esta manera, el clima laboral y la calidad del trabajo. La desconexión digital y laboral es además necesaria para hacer viable la conciliación de la vida personal y laboral, reforzando así las diferentes medidas reguladas en esta materia.

Por ello, conforme a lo regulado en el artículo 20 bis del ET, las partes acuerdan que las personas trabajadoras tienen derecho a la desconexión digital y laboral a fin de garantizar, fuera del tiempo de trabajo legal o convencionalmente establecido, el respeto de su tiempo de descanso, permisos y vacaciones o bajas por enfermedad, así como su intimidad personal y familiar.

A los efectos de la regulación de este derecho, se tendrán en cuenta todos los dispositivos y herramientas susceptibles de mantener la jornada laboral más allá de los límites de la legal o convencionalmente establecida: teléfonos móviles, tabletas, aplicaciones móviles propias de las Empresas, correos electrónicos y sistemas de mensajería, o cualquier otro que pueda utilizarse.

Con el fin de garantizar el cumplimiento de este derecho y regular las posibles excepciones, se acuerdan las siguientes medidas que tendrán el carácter de mínimas:

a) Se reconoce el derecho de las personas trabajadoras a no atender dispositivos digitales, fuera de su jornada de trabajo, ni durante los tiempos de descanso, permisos, licencias o vacaciones, salvo que se den las causas de urgencia justificada estipuladas en el punto c) siguiente.

b) Con carácter general, las comunicaciones sobre asuntos profesionales se realizarán dentro de la jornada de trabajo. En consecuencia, deberá evitarse, salvo que se den las situaciones de urgencia estipuladas en el punto c), la realización de llamadas telefónicas, el envío de correos electrónicos o de mensajería de cualquier tipo fuera de la jornada laboral. Las personas trabajadoras tienen derecho a no responder a ninguna comunicación una vez finalizada su jornada laboral diaria.

c) Se considerará que concurren circunstancias excepcionales muy justificadas cuando se trate de supuestos que puedan suponer un grave riesgo hacia las personas o un potencial perjuicio empresarial hacia el negocio, sus clientes y/o a sus accionistas, así como cualquier otro de carácter legal y/o regulatorio cuya urgencia requiera de la adopción de medidas especiales o respuestas inmediatas.

d) Asimismo, para una mejor gestión del tiempo de trabajo, se procurará la adopción de las siguientes medidas:

Programar respuestas automáticas, durante los periodos de ausencia, indicando las fechas en las que no se estará disponible, y designando el correo o los datos de contacto de la persona a quien se hayan asignado las tareas durante tal ausencia.

Evitar las convocatorias de formación, reuniones, videoconferencias, presentaciones, información, etcétera, fuera de la jornada laboral ordinaria diaria de cada persona trabajadora.

Convocar las sesiones indicadas en el párrafo anterior con la antelación suficiente para que las personas puedan planificar su jornada.

Incluir en las convocatorias la hora de inicio y finalización.

Con el fin de que el derecho a la desconexión digital y laboral sea efectivo, las empresas garantizarán que las personas que ejerzan ese derecho no se verán afectadas por ningún tipo de sanción, motivada por el ejercicio del mismo, ni se verán perjudicadas en sus evaluaciones de desempeño, ni en sus posibilidades de promoción.

Como complemento de estas medidas, en el ámbito de la Empresa se podrán establecer protocolos de actuación que amplíen, desarrollen y/o mejoren este derecho.

**2. Derecho a la intimidad y al uso de dispositivos digitales en el ámbito laboral.**

Las Empresas, cuando carezcan de ellos, deberán elaborar con participación de la RLT protocolos en los que se fijen los criterios de utilización de los dispositivos digitales que, en todo caso, deberán garantizar, en la medida legalmente exigible, la debida protección a la intimidad de las personas trabajadoras que hagan uso de los mismos, así como sus derechos establecidos constitucional y legalmente.

Los dispositivos digitales necesarios para el desempeño de la actividad laboral deberán ser facilitados a las personas trabajadoras por parte de las Empresas. Por parte de la Empresa, en cumplimiento de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD), se podrá acceder a los contenidos derivados del uso de medios digitales facilitados a las personas trabajadoras a los solos efectos de controlar el cumplimiento de las obligaciones laborales o estatutarias y de garantizar la integridad de dichos dispositivos.

Los medios tecnológicos y dispositivos digitales puestos a disposición del trabajador tendrán un uso exclusivamente profesional. En el supuesto de que se permita, por parte de las Empresas, el uso privado a través de los dispositivos digitales propiedad de las mismas, los protocolos deberán especificar qué tipos de usos son los autorizados, y establecerán garantías para preservar la intimidad de las personas trabajadoras tales como, en su caso, la determinación de los períodos en que los dispositivos podrán utilizarse para fines privados. Las personas trabajadoras deberán ser informadas de los criterios de utilización.

**3. Derecho a la intimidad frente al uso de dispositivos de videovigilancia, grabación de sonidos y geolocalización en el ámbito laboral.**

La implantación por parte de las Empresas de tecnologías de la información para el control de la prestación laboral, tales como videovigilancia, grabación de sonidos, controles biométricos, controles sobre el ordenador (monitorización remota, indexación de la navegación por internet, o la revisión o monitorización del correo electrónico y/o del uso de ordenadores) o controles sobre la ubicación física de la persona trabajadora mediante geolocalización, se realizará conforme a la legislación vigente.

Además, dichas medidas deberán ser proporcionales a la finalidad de verificar el cumplimiento por parte de las personas trabajadoras de sus obligaciones y deberes laborales.

Para los casos de grabaciones de imágenes y sonidos se procurarán establecer los medios necesarios para grabar aquellas imágenes y/o conversaciones consideradas como necesarias por la Empresa para garantizar la seguridad y/o la calidad de la actividad desarrollada en el centro de trabajo o teletrabajo y/o la exigible cuando así sea requerido por la normativa legal en materia de protección de la clientela.

**4. Derecho a la educación digital.**

Las Empresas facilitarán la formación de su personal en las competencias y habilidades digitales necesarias para afrontar la transformación digital y facilitar así su reconversión digital y la adaptación a las nuevas tareas que así lo requieran, así como para evitar y erradicar las brechas digitales y garantizar su empleabilidad. Por su parte, las personas trabajadoras deberán participar en este tipo de acciones formativas para su desarrollo y actualización permanente.

**5. Derechos ante la inteligencia artificial.**

Las nuevas herramientas basadas en algoritmos pueden aportar valor hacia una gestión más eficiente de las Empresas, ofreciendo mejoras en sus sistemas de gestión. Sin embargo, el desarrollo creciente de la aportación de la tecnología requiere de una implantación cuidadosa cuando se aplica en el ámbito de las personas. Por ello, las personas trabajadoras tienen derecho a no ser objeto de decisiones basadas única y exclusivamente en variables automatizadas[4], salvo en aquellos supuestos previstos por la Ley, así como derecho a la no discriminación en relación con las decisiones y procesos, cuando ambos estén basados únicamente en algoritmos, pudiendo solicitar, en estos supuestos, el concurso e intervención de las personas designadas a tal efecto por la Empresa, en caso de discrepancia.

Las Empresas informarán a la RLT sobre el uso de la analítica de datos o los sistemas de inteligencia artificial cuando los procesos de toma de decisiones en materia de recursos humanos y relaciones laborales se basen exclusivamente[5] en modelos digitales sin intervención humana.

Dicha información, como mínimo, abarcará los datos que nutren los algoritmos, la lógica de funcionamiento y la evaluación de los resultados.

4 Según la Reglamento (UE) 2024/1689 (IA Act), esto no sólo afecta a las decisiones automatizadas, también a aquellas semiautomatizadas o en las que no haya intervención humana significativa.

5 Según la Ley Rider, la información se debe dar siempre que se aplique un sistema algorítmico, independientemente de si hay, o no, intervención humana.