Estudios |
ISSN-e: 2792-8322

Ciberacoso laboral y digitalización del trabajo: análisis jurídico, riesgos psicosociales y tratamiento en la negociación colectiva

Carolina Claudia Bastante Velázquez
Investigadora Convenio Red.es-UCLM para la implementación de los derechos digitales en el entorno laboral y empresarial de la Carta de Derechos Digitales. Universidad de Castilla-La Mancha (España)
carolina.bastante@uclm.com | https://orcid.org/0009-0005-2491-2973

Extracto

Este artículo analiza el ciberacoso laboral como una manifestación emergente de violencia en el trabajo vinculada al uso de tecnologías digitales. Se contextualiza el fenómeno dentro de los riesgos psicosociales asociados a la digitalización del entorno laboral (como la hiperconexión, la tecnofatiga o la vigilancia intensiva), con especial atención a sus implicaciones para la salud mental y la organización del trabajo. A partir de fuentes normativas seleccionadas y contribuciones doctrinales recientes, se examina el debate sobre su eventual configuración como categoría jurídica autónoma, diferenciada del modelo tradicional de acoso laboral. El estudio incorpora, además, un análisis del tratamiento del ciberacoso en la negociación colectiva en España, a través de la revisión crítica de los convenios colectivos publicados en el Boletín Oficial del Estado entre 2023 y 2025. El trabajo subraya las especificidades del acoso digital en el contexto laboral y la necesidad de una respuesta jurídica y colectiva más coherente y adaptada a los nuevos entornos de trabajo digitalizados.

Palabras clave: digitalización; prevención de riesgos laborales; riesgos psicosociales; negociación colectiva; Convenio 190 OIT; conflicto colectivo; desconexión digital; violencia digital; ciberacoso en el trabajo.

Recibido: 19-09-2025 / Aceptado: 12-01-2026 / Publicado (en avance): 09-02-2026

Cómo citar: Bastante Velázquez, C. C. (2026). Ciberacoso laboral y digitalización del trabajo: análisis jurídico, riesgos psicosociales y tratamiento en la negociación colectiva. *Revista de Trabajo y Seguridad Social. CEF*, *491*. https://doi.org/10.51302/rtss.2026.24805

ISSN-e: 2792-8322

Cyberbullying in the workplace and the digitalization of work: legal analysis, psychosocial risks, and treatment in collective bargaining

Carolina Claudia Bastante Velázquez

Researcher (Red.es–UCLM Collaboration Agreement) for the implementation of the Digital Rights in the workplace and business environment under the Spanish Charter of Digital Rights. University of Castilla-La Mancha (Spain)

carolina.bastante@uclm.com | https://orcid.org/0009-0005-2491-2973

Abstract

This article analyzes workplace cyberbullying as an emerging form of violence at work linked to the use of digital technologies. The phenomenon is contextualized within the psychosocial risks associated with the digitalization of the workplace (such as hyperconnection, technofatigue, or intensive surveillance), with particular attention to its implications for mental health and work organization. Drawing on selected normative sources and recent doctrinal contributions, the article examines the debate on its possible recognition as an autonomous legal category, distinct from the traditional model of workplace harassment. The study also includes an analysis of how cyberbullying has been addressed in collective bargaining in Spain, through a critical review of collective agreements published in the *Official State Gazette* between 2023 and 2025. The article highlights the specific features of digital harassment in the workplace and the need for a more coherent and adapted legal and collective response to the new digitalized working environments.

Keywords: digitalization; occupational risk prevention; psychosocial risks; collective bargaining; ILO Convention 190; collective conflict; digital disconnection; digital violence; workplace cyberbullying.

Received: 19-09-2025 / Accepted: 12-01-2026 / Published (preview): 09-02-2026

Citation: Bastante Velázquez, C. C. (2026). Cyberbullying in the workplace and the digitalization of work: legal analysis, psychosocial risks, and treatment in collective bargaining. *Revista de Trabajo y Seguridad Social. CEF*, *491*. https://doi.org/10.51302/rtss.2026.24805

Sumario

Nota: Este artículo es fruto de la actividad investigadora desarrollada en el marco del Convenio de Colaboración C039-23OT entre Red.es y la UCLM para la implementación de los derechos digitales en el entorno laboral y empresarial de la Carta de Derechos Digitales, financiado con fondos *Next Generation*.

1. Transformación digital y riesgos psicosociales

La aceleración del proceso de digitalización está transformando todos los ámbitos de nuestra vida. En el contexto de las relaciones laborales –que es el que aquí nos ocupa–, esta transformación no solo ha reconfigurado los procesos productivos, sino que también ha alterado profundamente la forma en que se desarrollan dichas relaciones. Conceptos como el espacio y el tiempo, en ocasiones, se diluyen. Este nuevo escenario ha generado riesgos psicosociales emergentes que afectan directamente a la salud mental de las personas trabajadoras, así como cambios en la organización del trabajo y en el ejercicio de sus derechos fundamentales. Y, junto a estos cambios, han surgido también nuevos debates jurídicos vinculados a la desconexión digital, el uso de algoritmos y sistemas de inteligencia artificial, la vigilancia constante y la intensificación del trabajo (Rodríguez Fernández, 2024).

Esta transformación del tiempo y del espacio productivo tiene una doble vertiente: por un lado, ofrece posibilidades inéditas de conciliación, autonomía y flexibilidad; por otro, introduce factores de inseguridad, dependencia tecnológica y exposición constante a dinámicas laborales que escapan al control individual. El trabajo digitalizado genera una paradoja: se presenta como liberador, pero intensifica formas de subordinación y control que operan de manera más sutil.

El uso intensivo de tecnologías puede ocasionar problemas que afectan tanto a la salud física como mental, incluyendo la hiperconexión (Corrêa Gomes Cardim, 2023), el aislamiento, la difuminación del tiempo y lugar de trabajo, estrés, ansiedad, la sobrecarga mental e incluso posibles sesgos discriminatorios (Igartua Miró, 2023).

Estos problemas se agravan en sectores donde las tareas se gestionan mediante algoritmos o plataformas digitales. Conceptos como «tecnoansiedad», «tecnoadicción» o «tecnofatiga» –entendidos, respectivamente, como rechazo a las tecnologías por incapacidad para manejarlas; necesidad imperiosa de usarlas de forma continua, y agotamiento derivado de su utilización permanente– han sido reconocidos por la literatura especializada como efectos psicológicos vinculados a estas herramientas (Fernández-Costales Muñiz, 2024). Ello repercute no solo en el bienestar emocional, sino también en la motivación, la autoestima profesional y el sentido de pertenencia.

Para mitigar estos riesgos, la seguridad y salud laboral deben adaptarse al avance tecnológico, incorporando innovaciones que las fortalezcan y considerando nuevos empleos y

nuevas profesiones que requerirán identificar nuevos factores de riesgo (Fernández-Costales Muñiz, 2024). El avance digital ofrece oportunidades laborales, económicas y sociales, pero requiere capacitar a las personas trabajadoras para garantizar una gestión productiva y segura de la salud en el trabajo. La formación, por tanto, constituye un punto clave en la transición digital, ya que de ella depende la empleabilidad de las personas trabajadoras y su capacidad de adaptación a los cambios que se producen en los puestos de trabajo como consecuencia de la introducción de herramientas tecnológicas en los procesos productivos (Bastante Velázquez y Rodríguez Fernández, 2025).

Aunque España haya mejorado en competencias digitales, persisten importantes brechas formativas entre las personas trabajadoras que es necesario abordar. De acuerdo con los datos de Eurostat[1], en 2024 solo el 19,15 % de las empresas en nuestro país han provisto de formación en competencias digitales a su personal, lo que significa que la mayoría aún no lo han hecho. Esta formación no solo es una herramienta clave para la adaptación al cambio, sino también un pilar fundamental de la prevención en el entorno laboral digital.

Con el objetivo de orientar las políticas de prevención de riesgos laborales hacia los cambios que impone el nuevo entorno laboral, se ha desarrollado la Estrategia Española de Seguridad y Salud en el Trabajo para el periodo 2023-2027[2], que pone énfasis en adaptar la normativa preventiva a la digitalización y reconocer la centralidad de la salud mental y los factores psicosociales. En particular, esta estrategia identifica entre sus prioridades la necesidad de «anticipar y abordar los cambios derivados de las transiciones digital, ecológica y demográfica», lo que incluye de forma explícita los riesgos psicosociales relacionados con el uso de tecnologías. Asimismo, en el marco de su objetivo estratégico 1, destaca la importancia de fortalecer la prevención frente a estos riesgos mediante herramientas de diagnóstico, metodologías participativas y la integración de la perspectiva de género. También subraya la urgencia de actualizar los sistemas de vigilancia y formación, incorporando contenidos vinculados a los entornos virtuales, el trabajo a distancia, la desconexión digital y los efectos del uso de tecnologías de la información y la comunicación (TIC) en la salud mental, promoviendo con ello una cultura preventiva más inclusiva y eficaz.

Sin embargo, el tratamiento de estos riesgos sigue siendo limitado. La Ley 31/1995, de 8 de noviembre, de prevención de riesgos laborales (LPRL), establece la obligación empresarial de garantizar la salud y seguridad de las personas trabajadoras en todos los aspec-

1 https://ec.europa.eu/eurostat/databrowser/view/isoc_ske_ittn2/default/table?lang=en&category=isoc.isoc_sk.isoc_skt

2 Resolución de 20 de abril de 2023, de la Secretaría de Estado de Empleo y Economía Social, por la que se publica el Acuerdo del Consejo de Ministros de 14 de marzo de 2023, por el que se aprueba la Estrategia Española de Seguridad y Salud en el Trabajo 2023-2027 (BOE de 28 de abril de 2023).

tos relacionados con el trabajo. No obstante, no contempla de forma expresa los efectos derivados de la digitalización, como el uso intensivo de tecnologías, la hiperconectividad[3] o el ciberacoso.

En este contexto, el ciberacoso laboral se ha convertido en uno de los riesgos más graves asociados a la digitalización del trabajo. Es una consecuencia directa de cómo las nuevas tecnologías transforman la manera en que nos relacionamos en el entorno laboral. La Organización Internacional del Trabajo (OIT) lo define como «aquellas conductas violentas que se realizan mediante las nuevas tecnologías de comunicación y de información, pudiendo integrar imágenes, vídeos, mensajes, utilizar redes sociales, entre otros». Su gravedad reside tanto en el impacto que tiene sobre la salud mental y el bienestar de las personas trabajadoras como en las dificultades que plantea para su detección y regulación efectiva.

Un ejemplo que ayudó a poner el foco en este problema fue el caso IVECO[4] (2019), en el cual una trabajadora se suicidó tras la difusión por parte de sus compañeros de un vídeo de contenido sexual sin su consentimiento. Esto evidenció la necesidad de protocolos y reformas legales para prevenir y sancionar el ciberacoso laboral. Por ello es destacable el Convenio 190 de la OIT[5] sobre prevención y eliminación de la violencia y el acoso en el trabajo, ratificado por España en 2022 y en vigor desde el 25 de mayo de 2023, que sí pone el centro de atención en medidas como la evaluación de riesgos laborales, junto a la Recomendación 206, donde habla del ciberacoso como la forma más intensa de violencia en el ámbito digital en los entornos de trabajo y que busca facilitar una serie de pautas u orientaciones en relación con el contenido del Convenio (Megino Fernández, 2023).

Por ello, en los siguientes epígrafes, se desarrollará con mayor profundidad este fenómeno, analizando sus características jurídicas, sus elementos definitorios y los retos que implica su abordaje en un contexto laboral profundamente transformado por lo digital. Además, se abordará cómo lo ha afrontado y regulado la negociación colectiva española, destacando las medidas adoptadas y los retos que persisten en su implementación efectiva.

---

3 La hiperconectividad, entendida como factor de riesgo psicosocial derivado de la exposición constante a tecnologías digitales y la expectativa de disponibilidad permanente, puede generar efectos negativos en la salud física (fatiga, trastornos musculoesqueléticos, problemas cardiovasculares) y mental (estrés, ansiedad, depresión, insomnio, tecnoestrés), además de una difuminación de los límites entre vida laboral y personal que afecta a la intimidad y al bienestar de las personas trabajadoras (Benítez y Trillo Párraga, 2023). Esta situación, además, puede vincularse con el riesgo de ciberacoso, en la medida en que la disponibilidad permanente amplía los espacios y tiempos de exposición a interacciones potencialmente hostiles.

4 https://www.aepd.es/documento/e-06209-2020.pdf

5 Convenio sobre la violencia y el acoso, 2019 (núm. 190). https://normlex.ilo.org/dyn/nrmlx_es/f?p=NORMLEXPUB:12100:0::NO::P12100_INSTRUMENT_ID:3999810

2. Hacia el reconocimiento jurídico del ciberacoso laboral

2.1. Evolución del acoso laboral hacia su dimensión digital

En los últimos años, asistimos a una transformación progresiva del acoso laboral tradicional hacia nuevas formas de violencia mediadas por tecnologías digitales. La digitalización de las relaciones laborales, intensificada tras la pandemia de la COVID-19, ha configurado un nuevo ecosistema en el que las tecnologías ya no constituyen un mero soporte instrumental, sino un elemento estructural de la organización del trabajo, condicionando formas de interacción y de ejercicio de poder. Es decir, dicha evolución no implica una sustitución del acoso físico por el digital, sino más bien una coexistencia de ambas formas que, lejos de excluirse, se complementan y refuerzan mutuamente.

El proceso de digitalización del trabajo ha ampliado el espectro de escenarios donde puede producirse violencia, facilitando la aparición de nuevas modalidades de acoso, muchas de ellas con características específicas, que generan un impacto especialmente significativo en la salud mental de las personas trabajadoras. En este sentido, el uso generalizado de canales digitales de comunicación –como el correo electrónico, las aplicaciones de mensajería instantánea o las plataformas colaborativas– ha incrementado notablemente la probabilidad de que se generen comunicaciones inadecuadas, agresivas o invasivas que, en determinados contextos, pueden encuadrarse dentro de las conductas constitutivas de acoso laboral. Entre las prácticas concretas más comunes se encuentran la exclusión deliberada de reuniones telemáticas, el envío de correos con copia a superiores para desacreditar, la imposición de cargas burocráticas mediante plataformas, la difusión de rumores o mensajes vejatorios en canales de comunicación internos, y el hostigamiento a través de redes sociales en contextos extralaborales.

Por tanto, ningún sector está completamente a salvo de estas manifestaciones, aunque ciertos ámbitos de actividad, especialmente aquellos vinculados al teletrabajo o a entornos altamente digitalizados (Megino Fernández, 2023), presentan una mayor vulnerabilidad estructural frente a estos riesgos emergentes (Martínez Jiménez, 2024a).

2.2. Estándares internacionales: Convenio 190 OIT y Recomendación 206

Desde el ámbito normativo internacional, la respuesta al problema del acoso laboral –y en particular, a su expresión en entornos digitales– ha ganado protagonismo en los últimos años. La OIT ha incorporado de forma explícita el fenómeno de la violencia y el acoso en el trabajo dentro de sus instrumentos más recientes. Esta preocupación se refleja en el Convenio 190, donde no solo se redefine el concepto de acoso, sino que se reconoce abiertamente que estas conductas pueden producirse a través del uso de TIC, lo que amplía considerablemente el campo de protección para los trabajadores y trabajadoras.

Tradicionalmente, el acoso se entendía como una acción de carácter verbal o psicológico, sistemática, reiterada y persistente, con capacidad de generar un entorno hostil, humillante o degradante para quien lo sufre. Sin embargo, el Convenio 190 OIT introduce una definición más amplia y menos restrictiva del fenómeno, al eliminar dos elementos que durante años condicionaron su reconocimiento jurídico en diversas jurisdicciones, incluida la española: la reiteración de la conducta y la intención específica de causar daño (Moreno Solana, 2023). Esta flexibilización conceptual resulta especialmente pertinente en el caso del ciberacoso, donde las dinámicas propias de la comunicación digital dificultan a menudo la identificación de patrones reiterativos o la prueba de intencionalidad.

Además, el artículo 3 del convenio establece que la violencia y el acoso pueden producirse tanto en el lugar de trabajo como en otros espacios relacionados, incluyendo explícitamente el uso de TIC. No se especifica, sin embargo, si estas herramientas deben ser propiedad de la empresa o de la persona trabajadora, una ambigüedad que plantea importantes implicaciones prácticas[6]. En un entorno donde lo profesional y lo personal se entrelazan, la ausencia de esta distinción dificulta la determinación de responsabilidades y puede generar zonas grises en la aplicación del derecho.

El convenio impone a los Estados la obligación de exigir a los empleadores y empleadoras la adopción de medidas apropiadas para prevenir y abordar estos fenómenos (art. 9), lo que incluye la aprobación de una política específica en el lugar de trabajo, la integración de la violencia, el acoso y los riesgos psicosociales en la gestión de la seguridad y salud laboral, la identificación y evaluación participada de estos riesgos y la provisión de información y formación accesible a las personas trabajadoras. A ello se le suman la obligación de establecer procedimientos eficaces de denuncia e investigación (art. 10) y promover acciones de formación y sensibilización sostenidas en el tiempo (art. 11). Estas disposiciones se ven reforzadas por la Recomendación 206, que proporciona directrices prácticas sobre cómo articular marcos normativos y organizativos eficaces frente a la violencia laboral, incluyendo el ciberacoso como una de sus manifestaciones relevantes.

2.3. Marco español: legislación y jurisprudencia aplicables

En el contexto normativo español, si bien existen disposiciones que permiten abordar el acoso laboral en general, aún no se ha configurado un marco legal que reconozca de forma explícita el ciberacoso como una categoría diferenciada o que regule de manera específica

[6] Piénsese en un supuesto en el que una trabajadora sufre acoso mediante mensajes enviados a su cuenta personal de redes sociales, pero motivados por un conflicto estrictamente laboral. El hecho de que la herramienta no pertenezca a la empresa no elimina la conexión con el trabajo, pero sí complica la imputación de responsabilidades y la activación de protocolos preventivos.

sus manifestaciones. La LPRL, en su artículo 14, establece el derecho de las personas trabajadoras a una protección eficaz en materia de seguridad y salud en el trabajo y, con ello, el deber correlativo de la parte empleadora de proteger a las personas trabajadoras frente a los riesgos laborales[7], lo que incluye los riesgos de naturaleza psicosocial. Bajo esta formulación, cabría integrar el ciberacoso como una expresión emergente de riesgo laboral, especialmente en contextos de trabajo digitalizado, remoto o flexible. No obstante, esta integración se produce de forma implícita y requiere una interpretación extensiva de los principios generales de prevención.

En esta misma línea, la Ley orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales (LOPDPGDD), refuerza el marco preventivo mediante la incorporación de garantías específicas vinculadas al uso de tecnologías en el entorno laboral. Aunque su finalidad principal no es abordar directamente las situaciones de acoso, establece un conjunto de derechos que pueden contribuir a proteger la dignidad de las personas trabajadoras frente a posibles usos abusivos o invasivos de los entornos digitales. Así, el artículo 87[8] reconoce el derecho a la intimidad en el uso de dispositivos digitales facilitados por la empresa, y el artículo 88[9] regula el derecho a la desconexión digital, exigiendo la negociación de criterios que eviten la intromisión tecnológica fuera del horario

7 Este deber se despliega mediante obligaciones específicas: información y consulta/participación de las personas trabajadoras, formación en materia preventiva, medidas de emergencia y actuación ante riesgo grave e inminente, incluida la paralización de la actividad, y vigilancia de la salud. En el ámbito de los riesgos psicosociales –también cuando se manifiestan en entornos digitales– estos deberes implican, en particular, informar de reglas de uso de canales y TIC, garantizar la participación en la evaluación psicosocial y en la elaboración de protocolos de actuación, impartir formación específica, prever procedimientos de interrupción/alejamiento ante situaciones de hostigamiento que puedan valorarse como graves y asegurar una vigilancia de la salud tanto física como mental.

8 Artículo 87 de la LOPDPGDD:

> 1. Los trabajadores y los empleados públicos tendrán derecho a la protección de su intimidad en el uso de los dispositivos digitales puestos a su disposición por su empleador.
>
> 2. […]
>
> 3. Los empleadores deberán establecer criterios de utilización de los dispositivos digitales respetando en todo caso los estándares mínimos de protección de su intimidad […]. En su elaboración deberán participar los representantes de los trabajadores.
>
> […]

9 Artículo 88 de la LOPDPGDD:

> 1. Los trabajadores y los empleados públicos tendrán derecho a la desconexión digital a fin de garantizar, fuera del tiempo de trabajo legal o convencionalmente establecido, el respeto de su tiempo de descanso, permisos y vacaciones, así como de su intimidad personal y familiar.
>
> 2. […]
>
> 3. El empleador […] elaborará una política interna […] en la que definirá las modalidades de ejercicio del derecho a la desconexión y las acciones de formación y sensibilización del personal […].

laboral. Por su parte, los artículos 93[10] y 94[11], que desarrollan el derecho al olvido, permiten solicitar la eliminación de contenidos personales que puedan afectar a la reputación o el bienestar de la persona trabajadora. En su conjunto, estas disposiciones configuran un marco de actuación útil para guiar políticas empresariales respetuosas con los derechos fundamentales en entornos digitalizados, y pueden operar como referencia en la prevención de conflictos derivados del uso intensivo de las TIC en el trabajo.

Por su parte, la Ley orgánica 3/2007, de 22 de marzo, para la igualdad efectiva de mujeres y hombres, en su artículo 48, establece de forma expresa la obligación de las empresas de promover condiciones laborales que eviten la comisión de delitos y otras conductas contra la libertad sexual y la integridad moral, incluidos los cometidos en el ámbito digital. Esta previsión legal representa un avance normativo relevante, ya que reconoce la necesidad de actuar también frente a los riesgos asociados al uso de tecnologías en el trabajo. La norma contempla medidas como la elaboración de códigos de buenas prácticas, campañas informativas o acciones formativas, que deberán ser negociadas con la representación legal de las personas trabajadoras. Asimismo, impone un rol activo a la representación de las personas trabajadoras, a quienes se encomienda la tarea de contribuir a la prevención de estas conductas, tanto mediante la sensibilización del personal como a través de la comunicación a la dirección de aquellas situaciones que puedan propiciarlas. Esta formulación normativa reconoce explícitamente el carácter multidimensional y compartido de la prevención, lo que supone una base sólida para construir mecanismos eficaces frente al ciberacoso sexual y por razón de sexo.

En este sentido, la jurisprudencia también ha empezado a desempeñar un papel clave en la interpretación y aplicación de los principios constitucionales a las nuevas realidades laborales. La doctrina más reciente del Tribunal Constitucional aportada en la Sentencia 56/2019, de 6 de mayo, aunque referida a un caso de acoso en un entorno presencial, fija

[10] Artículo 93 de la LOPDPGDD:

> 1. Toda persona tiene derecho a que los motores de búsqueda en Internet eliminen de las listas de resultados [...] los enlaces publicados que contuvieran información relativa a esa persona cuando fuesen inadecuados, inexactos, no pertinentes, no actualizados o excesivos [...] teniendo en cuenta los fines para los que se recogieron o trataron, el tiempo transcurrido y la naturaleza e interés público de la información.
>
> […]

[11] Artículo 94 de la LOPDPGDD:

> 1. Toda persona tiene derecho a que sean suprimidos, a su simple solicitud, los datos personales que hubiese facilitado para su publicación por servicios de redes sociales y servicios de la sociedad de la información equivalentes.
>
> 2. […]
>
> 3. En caso de que el derecho se ejercitase [...] durante su minoría de edad, el prestador deberá proceder sin dilación a su supresión por su simple solicitud, sin necesidad de que concurran las circunstancias mencionadas en el apartado 2.

criterios que permiten extender su lógica al análisis del ciberacoso. El tribunal subraya la necesidad de valorar no solo la reiteración de la conducta, sino también la existencia de una intención lesiva (directa o indirecta), la generación de un perjuicio efectivo o potencial para la víctima y la capacidad objetiva del comportamiento para degradar, humillar o vejar a quien lo sufre. Estos tres elementos –intención, menoscabo y vejación– constituyen, en conjunto, el umbral mínimo para que una conducta sea calificada jurídicamente como acoso.

Lo interesante de esta doctrina es que permite una aplicación funcional a los contextos digitales, donde la reiteración puede adquirir formas distintas (por ejemplo, reenvíos masivos o permanencia indefinida del contenido en redes), y la intencionalidad puede no ser explícita, pero deducirse del resultado y del contexto. En este marco, resulta pertinente repensar los protocolos de prevención desde una lógica que incorpore tanto los elementos propios del entorno digital como los principios de protección de la salud laboral. Por otro lado, podrían destacarse al menos tres ejes claves de intervención para las organizaciones.

1. El fomento de la «tolerancia cero» frente al acoso, incorporando de forma clara el ciberacoso en los códigos internos de conducta.
2. La formación y sensibilización sobre esta problemática y sobre el uso responsable de canales digitales.
3. El impulso de la corresponsabilidad en el ámbito laboral, promoviendo que todos los actores involucrados –las empresas, las personas trabajadoras y autoridades competentes– trabajen conjuntamente para prevenir y abordar el ciberacoso de manera eficaz.

2.4. Debate y especificidades del ciberacoso: forma, significado y efecto multiplicador

Ahora bien, al margen de las respuestas organizativas, cabe plantearse una cuestión más estructural: ¿tiene sentido reconocer el ciberacoso como una categoría jurídica autónoma, diferenciada del acoso laboral tradicional? La doctrina no ofrece una respuesta unívoca. Una parte de la literatura considera que no existe un bien jurídico nuevo o diferente protegido por el ordenamiento (Álvarez del Cuvillo, 2021; Molina Navarrete, 2019), y que el acoso cometido mediante TIC no es sino una variante instrumental del acoso tradicional. Desde esta óptica, la distinción no sería necesaria, pues lo relevante es el contenido de la conducta, no el canal a través del cual se manifiesta (De Stefano *et al.*, 2020).

Sin embargo, otras voces sostienen que el medio digital introduce dinámicas propias que no pueden ser ignoradas: la posibilidad de anonimato, la difusión inmediata e incontrolada, la permanencia de los mensajes o imágenes en redes, la ambigüedad de los contextos comunicativos y la dificultad de delimitar lo laboral y lo personal. Estas especificidades gene-

ran una forma de violencia que, aunque conectada con el acoso tradicional, posee rasgos distintivos que justifican un tratamiento más preciso y, eventualmente, una categorización diferenciada (Álvarez del Cuvillo, 2021).

Además, esta discusión no es meramente técnica: tiene implicaciones políticas, jurídicas y organizativas. Reconocer el ciberacoso como una figura autónoma permitiría visibilizar su impacto, generar obligaciones normativas más claras y desarrollar políticas preventivas mejor adaptadas. Por el contrario, mantenerlo difuso dentro del acoso general puede diluir su relevancia, dificultar su prueba y limitar la intervención institucional o empresarial.

Para profundizar en la especificidad del ciberacoso laboral como fenómeno diferenciado, resulta útil recurrir al marco analítico propuesto por el profesor Álvarez del Cuvillo (2021), que distingue tres dimensiones clave desde las que examinar su impacto y su tratamiento jurídico: la forma de la conducta, la significación del comportamiento y su efecto multiplicador. Estas categorías permiten descomponer el fenómeno más allá de la superficie tecnológica y analizar cómo el entorno digital no solo modifica el canal de agresión, sino también sus consecuencias, sus implicaciones normativas y su potencial lesivo.

A) La forma de la conducta acosadora

El primer aspecto se refiere a cómo se configura y manifiesta la conducta en los entornos digitales. A diferencia del acoso físico o presencial, el ciberacoso se desarrolla en espacios no materiales, como correos electrónicos, chats corporativos, redes sociales u otras plataformas digitales. Esta desmaterialización del escenario no implica que el impacto sea menor; al contrario, en muchos casos el daño psicológico se intensifica por la continuidad, la permanencia o la difusión pública del contenido ofensivo.

La variedad de conductas susceptibles de ser consideradas ciberacoso es amplia: suplantaciones de identidad, envíos reiterados de mensajes hostiles o intimidatorios, aislamiento intencionado en canales de trabajo, difusión de rumores o descalificaciones, coacciones para mantenerse conectado fuera del horario laboral o violaciones del derecho a la desconexión digital. Algunas de estas prácticas, además, pueden contener una dimensión de acoso sexual o por razón de sexo, especialmente cuando implican contenido de carácter íntimo o invasivo (Cabeza Pereiro y Cardona Rubert, 2025).

La virtualidad del espacio de trabajo también afecta a las barreras éticas y emocionales de quien ejerce la violencia. La pantalla actúa como escudo, reduciendo la percepción de la otra persona como sujeto digno de respeto y facilitando formas de deshumanización que agravan la gravedad del comportamiento. En este sentido, el entorno digital no solo facilita la comisión de conductas abusivas, sino que amplifica su capacidad lesiva, especialmente en lo relativo a la dignidad de la persona trabajadora.

B) Las diferencias de significación de la conducta

El segundo factor alude a cómo se interpreta y valora la conducta en el contexto sociolaboral en que ocurre. En el análisis jurídico del acoso laboral, juega un papel central el concepto de «entorno laboral hostil, humillante o intimidatorio», una noción jurídicamente indeterminada que requiere aplicar criterios de razonabilidad y ponderación según las circunstancias del caso.

En entornos digitales, sin embargo, estas valoraciones se ven afectadas por una mayor ambigüedad comunicativa. La informalidad de ciertos canales (como WhatsApp), el carácter fragmentario de los mensajes o la falta de lenguaje no verbal dificultan la interpretación de las intenciones y pueden generar malentendidos. A ello se suma que las normas culturales sobre lo aceptable en el entorno digital no siempre coinciden con las del espacio físico, y varían entre generaciones, sectores y empresas.

Esta variabilidad hace que la frontera entre una conducta ilícita y un comportamiento socialmente inadecuado sea más difícil de trazar. No obstante, la mayor tolerancia que algunos contextos digitales parecen ofrecer a formas de interacción agresiva o invasiva no justifica su normalización jurídica. Todo lo contrario, obliga a extremar las precauciones y a adaptar los marcos de prevención y detección a las especificidades de la comunicación digital.

C) El posible efecto multiplicador del daño

Por último, el entorno digital potencia lo que podríamos denominar la capacidad expansiva del acoso. A diferencia del entorno presencial, donde la conducta puede quedar limitada a un espacio concreto y a un número determinado de personas, en el ciberacoso el daño puede replicarse y persistir en el tiempo. Un solo mensaje ofensivo o una imagen íntima compartida sin consentimiento pueden ser reenviados, comentados y archivados, afectando de forma continua la reputación, la salud y el bienestar de la persona acosada.

Este efecto multiplicador puede agravar la calificación jurídica de la conducta, incluso en ausencia de reiteración, ya que el daño acumulado puede ser equivalente (o superior) al generado por una conducta persistente en el espacio físico. Además, la participación activa o pasiva de terceras personas en la diseminación del contenido puede reforzar el aislamiento y la estigmatización de la víctima, profundizando el sufrimiento y dificultando su recuperación psicosocial (Cabeza Pereiro y Cardona Rubert, 2025).

En este punto, cobra especial importancia la difuminación de los límites espaciotemporales del trabajo en la era digital. Muchas de las conductas que deben ser prevenidas y sancionadas no ocurren dentro del horario laboral ni en los espacios físicos de la empresa, sino fuera de ellos, a través de medios particulares o en momentos de ocio. Esta ambigüedad dificulta la imputación directa al entorno laboral, lo que en ocasiones conduce a una inacción empresarial injustificada. Frente a ello, el Convenio 190 de la OIT, en su artículo 3, aclara que la

violencia y el acoso serán considerados laborales cuando: (1) ocurran durante la jornada, con independencia del lugar; (2) se produzcan con ocasión o en relación con el trabajo, y (3) constituyan una consecuencia directa del trabajo, incluso si se producen fuera del horario laboral.

Este análisis permite concluir que, aunque el ciberacoso no constituya aún una categoría jurídica autónoma –ni sea necesariamente imprescindible su reconocimiento inmediato–, sus particularidades exigen una atención diferenciada tanto en el plano normativo como organizativo. Aun así, no puede descartarse que, en el futuro, a medida que el fenómeno evolucione y se consoliden sus rasgos específicos, pueda resultar pertinente configurar una categoría jurídica propia. Las características propias del entorno digital –como la dificultad de delimitar el ámbito laboral, la velocidad de propagación de los contenidos o el acceso permanente a las víctimas– suponen retos importantes para las estrategias de prevención, detección y reparación del daño.

Por ello, es fundamental avanzar hacia una normativa más precisa que reconozca el impacto específico de estas conductas y articule mecanismos de tutela adecuados. Entre ellos, cabe mencionar la elaboración de protocolos internos que contemplen supuestos de violencia digital, la formación especializada de los equipos de recursos humanos, la incorporación de cláusulas específicas en los convenios colectivos y la cooperación activa con las autoridades laborales y judiciales para la identificación y sanción de estas prácticas.

Del mismo modo, las empresas deben asumir un compromiso firme con la erradicación del ciberacoso, no solo como una obligación legal, sino como parte de su responsabilidad social y de la construcción de entornos de trabajo seguros, saludables y respetuosos. Esto requiere políticas activas de prevención, sistemas accesibles de denuncia, medidas de protección para las personas afectadas y una cultura corporativa que rechace de manera clara toda forma de violencia, también en el espacio digital.

El desarrollo progresivo del derecho del trabajo frente a los desafíos tecnológicos deberá incorporar estas problemáticas en su agenda, garantizando que el proceso de digitalización no suponga una regresión en los derechos laborales ni en la protección de la dignidad en el trabajo. La negociación colectiva, como veremos en el siguiente epígrafe, se configura como un instrumento privilegiado para articular estas respuestas desde una lógica participativa y adaptada a las realidades concretas de cada sector o empresa.

3. Estrategias de prevención frente al ciberacoso laboral

3.1. Dimensión organizativa y preventiva

La gestión del ciberacoso exige llevar al plano operativo los mandatos preventivos, integrando en la evaluación y la planificación, con un enfoque anticipatorio y no meramen-

te reactivo, los factores psicosociales ligados al uso de TIC (intensidad y asincronía de las comunicaciones, trazabilidad y permanencia de los mensajes, y reglas de gobernanza de los canales corporativos) (Fernández-Costales Muñiz, 2024), lo que a su vez exige revisar periódicamente esos instrumentos y las reglas de uso conforme evolucionen la organización y las herramientas[12].

En términos organizativos, el deber de informar, formar y vigilar se concreta en reglas claras sobre uso de canales digitales, políticas antiacoso o antihostigamiento que contemplen su dimensión *online*, protocolos de actuación con plazos y responsables, participación efectiva de la representación de la plantilla en la evaluación psicosocial y en la revisión de normas de convivencia digital, vigilancia de la salud con dimensión psíquica e interrupción/alejamiento digital cuando sea necesario para proteger a la persona afectada (Gil Pérez, 2024).

En este marco, el derecho a la desconexión digital opera como una muy buena herramienta preventiva, ya que reduce la ventana temporal de exposición a interacciones potencialmente hostiles a la vez que delimita el perímetro de las comunicaciones laborales y evita la prolongación del hostigamiento fuera de la jornada. Su eficacia exige protocolos internos de desconexión con franjas horarias definidas, excepciones tasadas y mecanismos de seguimiento, diseñados con participación de la representación de las personas trabajadoras (Gil Pérez, 2024).

La formación es el otro pilar central. Según los datos del Eurostat, existe una brecha en educación digital por razón tanto de edad[13] como de género[14]. En este contexto, situar la capacitación como medida preventiva frente al ciberacoso es decisivo: cuando la plantilla recibe formación específica en funcionamiento y buen uso de las TIC –normas de comunicación, gestión de conflictos en entornos virtuales, detección temprana de conductas abusivas y vías de actuación (incluida la preservación de evidencias)– se estrecha el margen para comportamientos hostiles y se refuerza una cultura del respeto en el ámbito digital. Para que tenga eficacia real, esta formación debe acompañarse de protocolos de actuación y programas de uso responsable que definan canales, tiempos y límites coherentes con la desconexión digital, con seguimiento periódico y ajustes según la evolución tecnológica.

[12] El Convenio 190 y la Recomendación 206 instan a articular políticas específicas, integrar estos riesgos en los sistemas de seguridad y salud en el trabajo, identificarlos y evaluarlos con participación de la plantilla e informar/capacitar de forma continuada.

[13] Según los datos el 68,8 % de las personas de entre 15 y 34 años tienen educación/competencias digitales frente a 31,2 % de las mayores de 34. Por ello sería aconsejable adaptar la formación por grupos de edad. https://ec.europa.eu/eurostat/databrowser/view/isoc_ski_itage/default/table?lang=en&category=isoc.isoc_sk.isoc_skt.is oc_skt_

[14] El 83,7 % de hombres tienen educación digital frente al a 16,3 % de mujeres. https://ec.europa.eu/eurostat/databrowser/view/isoc_ski_itsex/default/table?lang=en&category=isoc.isoc_sk.isoc_skt.isoc_skt_

Por último, la arquitectura preventiva ha de alinearse con un marco sancionador que garantice su efectividad: tipificación expresa del ciberacoso y su gradación en los códigos disciplinarios para evitar zonas de impunidad, y coherencia entre prevención (políticas, formación, vigilancia) y respuesta (medidas cautelares y sanciones) a fin de asegurar intervenciones rápidas y proporcionadas (Megino Fernández, 2023).

3.2. El papel de la negociación colectiva frente al ciberacoso laboral

Tal como se ha anticipado, la negociación colectiva desempeña un papel esencial en la configuración de medidas eficaces frente al ciberacoso laboral. A continuación, se analiza cómo se ha plasmado –con avances y carencias– en los convenios colectivos publicados en el BOE entre julio de 2023 y junio de 2025, a la luz del V Acuerdo de Empleo y Negociación Colectiva[15] (V AENC) y del marco normativo vigente.

La negociación colectiva constituye un instrumento privilegiado para dar respuesta a los nuevos retos que plantea la digitalización en el ámbito de las relaciones laborales, al adaptarse a las necesidades propias de cada empresa o sector de actividad, a los mandatos legales y a cualquier otro tipo de protocolo o forma de actuación en materia de riesgos digitales (Fernández-Costales Muñiz, 2024). En este sentido, el V AENC, suscrito en 2023 por las principales organizaciones sindicales y empresariales de nuestro país, representa un hito relevante. Ya en su preámbulo recoge el compromiso de adaptar los contenidos de la negociación colectiva a los cambios tecnológicos y sociales, asumiendo de forma explícita la necesidad de «preservar la seguridad y salud de las personas trabajadoras». En línea con esta premisa, el V AENC incorpora en su capítulo VIII la recomendación de elaborar y hacer seguimiento de protocolos de gestión de conflictos psicosociales asociados a la violencia y el acoso en el trabajo, incluyendo expresamente el «ciberacoso, el *mobbing* y otras formas de violencia ejercidas a través de los medios digitales».

El V AENC supone que los agentes sociales de nuestro país toman bajo su responsabilidad la gestión del impacto de la transición digital sobre el empleo y el trabajo, por medio del diálogo social y apelando directamente a la negociación colectiva como vehículo más eficaz para abordar las oportunidades y desafíos del avance de la digitalización. En palabras de la profesora Rodríguez Fernández,

> la negociación colectiva es un instrumento normativo básico de las relaciones de trabajo, pero también, y sobre todo, una fuente de distribución de la riqueza, lo que

[15] Resolución de 19 de mayo de 2023, de la Dirección General de Trabajo, por la que se registra y publica el V Acuerdo para el Empleo y la Negociación Colectiva (BOE de 31 de mayo de 2023).

> la entronca directamente con la igualdad que haya en una sociedad, y un mecanismo de compartir el poder de la empresa por parte de los trabajadores, lo que la vincula a la idea misma de democracia (Rodríguez Fernández, 2016).

Esta afirmación adquiere aún más relevancia en un momento en el que la tecnología puede convertirse tanto en una herramienta de empoderamiento como en un medio de control.

Es bien sabido que el V AENC carece de eficacia normativa, lo que significa que no se impone jurídicamente sobre toda la negociación colectiva del país; ahora bien, su artículo 1 recoge el compromiso de las partes firmantes de

> ajustar [su] comportamiento y acciones a lo pactado [y de] intensificar los esfuerzos para establecer con [sus] respectivas organizaciones en los sectores o ramas de actividad […] los mecanismos y cauces más adecuados que les permitan asumir y ajustar sus comportamientos para aplicar los criterios, orientaciones y recomendaciones contenidas en este Acuerdo.

De este modo, los contenidos del V AENC, aun no siendo imperativos, se despliegan en cascada por todo el sistema de negociación colectiva español (Canalda Criado, 2023), ya que existe la necesidad de adoptar criterios comunes que sirvan de guía para la negociación de los más de cuatro mil convenios sectoriales y de empresa que se renegocian de forma periódica en nuestro país (Cavas Martínez, 2023).

No obstante, antes de profundizar en las cláusulas más recientes, conviene detenerse en la evolución del tratamiento de los riesgos psicosociales en el marco de la negociación colectiva. Esta evolución se ha materializado en tres instrumentos principales: los convenios colectivos, los planes de igualdad y los protocolos de actuación. Permitiendo estos dos últimos desarrollar clausulas más específicas, especialmente en relación con la violencia de género y, de forma incipiente, con el ciberacoso laboral (Martínez Jiménez, 2024b).

Pese a estos avances, el tratamiento del ciberacoso sigue siendo parcial, fragmentado y reactivo. En la mayoría de los casos, las menciones al ciberacoso aparecen integradas dentro de cláusulas generales sobre acoso o violencia, sin delimitar sus manifestaciones concretas ni desarrollar medidas preventivas adaptadas al entorno digital. Algunas excepciones, no obstante, reflejan buenas prácticas. Así, por ejemplo, el Convenio colectivo de Telefónica[16] dentro de su anexo V sobre «Las nuevas formas de trabajo en TdE, TME y TSOL» recoge en su apartado 2.18 el «Ciberacoso» y establece una «tolerancia cero en el ámbito laboral frente a cualquier tipo de acoso, incluido el "ciberacoso laboral" en sus diferentes mani-

[16] III Convenio colectivo de Telefónica de España, SAU, Telefónica Móviles España, SAU, y Telefónica Soluciones de Informática y Comunicaciones, SAU (BOE de 28 de febrero de 2024).

festaciones». Este convenio reconoce las particularidades del trabajo a distancia y el uso masivo de las TIC para configurar medidas contra el acoso, como complemento al procedimiento previsto en el plan de igualdad.

A su vez reconoce que «los avances tecnológicos y las TICs provocan que estemos ante una nueva realidad […] con unas relaciones laborales y personales más interconectadas, en las que se crean nuevos y mayores riesgos que necesariamente hay que prevenir». Entre estos riesgos destaca el «ciberacoso laboral», que debe ser combatido con «cuantas medidas sean necesarias en cuanto supone un comportamiento inaceptable y un claro incumplimiento del deber de buena fe contractual garantizando el debido respeto a la dignidad de todas las personas trabajadoras».

Respecto a su definición, se entiende como

> todo comportamiento de violencia psicológica, de comportamientos humillantes o vejatorios […] realizado a través de medios tecnológicos de amplio contenido […] de forma ocasional o recurrente y sistemática […] con el fin de destruir a la persona trabajadora acosada (en su salud, en su integridad física y psíquica).

Se enumeran conductas como distribuir imágenes delicadas, crear perfiles falsos, enviar mensajes hostigadores, usurpar identidad, difundir rumores falsos y uso persistente del teléfono móvil para acosar, entre otras.

Otros convenios, como el Convenio colectivo de Carburos Vía Augusta[17] o el de tejas, ladrillos y piezas especiales de arcilla cocida[18], incorporan también definiciones de este concepto y enumeran ejemplos concretos de conductas constitutivas de esta forma de violencia. Este enfoque, basado en catálogos abiertos resulta especialmente útil para identificar situaciones que, aunque novedosas o ambiguas, generan un impacto lesivo en la salud mental y la dignidad de las personas trabajadoras.

En términos cuantitativos, el número de convenios que abordan explícitamente el ciberacoso sigue siendo limitado. Quitando los ejemplos nombrados anteriormente, la mayoría de los que lo hacen, establecen mandatos genéricos para «promover condiciones de trabajo que eviten delitos y conductas contra la libertad sexual y la integridad moral, incluyendo el acoso cometido en el ámbito digital», como el artículo 89 del Convenio colectivo de empresas de mediación de seguros privados[19] o el artículo 56.6 del Convenio

[17] Convenio colectivo de Carburos Vía Augusta Logistics, SL (BOE de 3 de mayo de 2024).

[18] Convenio colectivo estatal de tejas, ladrillos y piezas especiales de arcilla cocida (BOE de 7 de diciembre de 2023).

[19] Convenio colectivo de empresas de mediación de seguros privados (BOE de 15 de noviembre de 2023).

colectivo de centros y servicios veterinarios[20]. Otros, como el Convenio colectivo de Severiano Servicio Movil[21], o el de Crit Interim España ETT[22] hacen únicamente referencia al ciberacoso dentro del protocolo de actuación para la atención del acoso y violencia contra las personas LGTBI+.

Un caso peculiar es el del Convenio colectivo del corcho[23] que incorpora una Comisión para la protección de los derechos digitales en su artículo 115, dotada de competencias en relación con el uso de dispositivos digitales, la protección de datos personales y la desconexión digital. Esta comisión paritaria tiene entre sus funciones la negociación de criterios de uso tecnológico durante la vigencia del convenio, la promoción de acciones formativas y de sensibilización para las personas trabajadoras, así como el seguimiento y control del cumplimiento de lo pactado en esta materia. No obstante, el convenio no le atribuye competencias expresas en relación con el acoso laboral ni con las manifestaciones digitales de violencia, lo que representa una limitación significativa si se aspira a una protección integral frente al ciberacoso en el entorno laboral. A pesar del valor institucional que supone su creación, este diseño confirma que los mecanismos de garantía de los derechos digitales no siempre incorporan una perspectiva preventiva suficiente respecto a las nuevas formas de violencia laboral mediada por tecnologías.

En consecuencia, la negociación colectiva aún no ha desplegado todo su potencial como herramienta preventiva frente al ciberacoso. Para que ese potencial se materialice, es imprescindible articular una estrategia compartida que combine tres planos de responsabilidad: (i) el impulso decidido de los agentes sociales en la mesa de negociación; (ii) la asunción de un papel proactivo por parte de los poderes públicos –encargados de dotar de mayor protagonismo al ámbito digital en la prevención del acoso y de fijar, cuando sea necesario, contenidos mínimos inderogables–, y (iii) la incorporación de sistemas de prevención de tres niveles correlativos: primario, orientado a eliminar factores de riesgo, secundario, dirigido a reducir el daño una vez manifestado, y terciario, centrado en la asistencia y reparación de la víctima (Molina Navarrete, 2019).

Este planteamiento entronca con el apartado 4 de la Recomendación 206 de la OIT, que exhorta a «fomentar el reconocimiento efectivo del derecho de negociación colectiva a todos los niveles como medio para prevenir y abordar la violencia y el acoso […] y apoyar dicha negociación mediante la recopilación y divulgación de buenas prácticas». Encargar a la negociación colectiva la regulación del ciberacoso –por su mayor flexibilidad y cercanía a las realidades concretas del trabajo– no significa que los poderes públi-

[20] II Convenio colectivo de centros y servicios veterinarios (BOE de 5 de octubre de 2023).

[21] Convenio colectivo de Severiano Servicio Móvil, SAU (BOE de 12 de marzo de 2025).

[22] Convenio colectivo de Crit Interim España ETT, SL (BOE de 12 de marzo de 2025).

[23] IX Convenio colectivo estatal del corcho (BOE de 7 de septiembre de 2023).

cos puedan desentenderse de su responsabilidad. Les corresponde fijar unas garantías mínimas comunes que aseguren una protección equitativa y eviten desigualdades entre sectores o territorios.

Solo a través de una combinación coherente entre un diálogo social sólido, estándares públicos bien definidos y una estrategia preventiva integral será posible convertir las directrices del V AENC en cláusulas eficaces. Estas deberán poner en primer plano la dignidad y la salud mental de las personas trabajadoras, afianzando entornos laborales seguros también frente a los riesgos derivados del uso de tecnologías.

4. Conclusiones y propuestas para una prevención integral del ciberacoso laboral

El análisis realizado en este trabajo confirma que el ciberacoso laboral, lejos de ser una cuestión marginal, constituye una de las manifestaciones más complejas y urgentes derivadas del cambio tecnológico en las relaciones laborales. La transformación digital del trabajo ha multiplicado las posibilidades de comunicación, pero también los riesgos de exposición a dinámicas de control, hostigamiento y violencia psicológica que operan en entornos virtuales y que, por tanto, escapan a los instrumentos tradicionales de prevención. La ausencia de una normativa específica, la dispersión de las respuestas en la negociación colectiva y la escasa atención en los convenios colectivos ponen de manifiesto que el derecho del trabajo aún no ha sido capaz de dar una respuesta eficaz a esta nueva realidad (González Vidales, 2024; Igartua Miró, 2023). A ello se une que la cultura preventiva sigue anclada en modelos presenciales, lo que dificulta la adaptación a los riesgos derivados del uso de las tecnologías en el trabajo, especialmente en modalidades como el teletrabajo o en contextos de hiperconectividad (Álvarez del Cuvillo, 2021).

En primer lugar, resulta imprescindible reforzar la prevención del ciberacoso desde una triple vía: normativa, organizativa y cultural. Desde el punto de vista normativo, urge definir con claridad el concepto de ciberacoso laboral, delimitando sus elementos esenciales y reconociendo su especificidad frente a otras formas de violencia en el trabajo. Como ha señalado la doctrina más reciente, no se trata de sustituir el marco vigente sobre acoso moral o sexual, sino de complementarlo con una categoría o subcategoría que visibilice nuevas manifestaciones, facilite su identificación y oriente las medidas de intervención (Martínez Jiménez, 2024b). Esta definición debe abarcar tanto conductas activas –hostigamiento, amenazas, suplantaciones de identidad, difusión de contenido íntimo o mensajes vejatorios– como conductas omisivas, especialmente las que se producen mediante aislamiento o invisibilización en espacios digitales, por ejemplo ignorar de forma reiterada correos o mensajes, excluir deliberadamente de grupos de mensajería o reuniones virtuales, o restringir el acceso a plataformas y canales de comunicación necesarios para el desempeño laboral.

En segundo lugar, se debe adoptar un enfoque preventivo que vaya más allá de los protocolos que se activan únicamente tras la denuncia. Tal y como señala la profesora Igartua Miró (2023), las herramientas jurídicas actuales siguen abordando el acoso (incluido el digital) desde una lógica reparadora o sancionadora, que actúa solo cuando el daño ya se ha producido. Esta aproximación resulta inadecuada frente a dinámicas cuya característica principal es la inmediatez y la capacidad multiplicadora. Por ello, deben integrarse medidas preventivas desde el diseño de los entornos laborales digitales, incorporando evaluaciones específicas de los riesgos psicosociales derivados de las tecnologías, limitaciones en el uso de los canales corporativos fuera del horario laboral, medidas de desconexión digital y controles éticos en la gestión algorítmica. La formación adquiere aquí un papel central, no solo como cumplimiento formal, sino como herramienta de concienciación y transformación cultural. El V AENC subraya la importancia de estas acciones formativas en competencias digitales y en el uso respetuoso de las TIC, aunque su desarrollo en la práctica es muy desigual (González Vidales, 2024). Es necesario garantizar que todas las personas trabajadoras, cualquiera que sea su puesto o función, reciban formación suficiente y periódica sobre acoso digital, derechos digitales y la adecuada utilización de los medios tecnológicos puestos a su disposición.

En tercer lugar, la negociación colectiva debe reforzar su papel como instrumento flexible, capaz de adaptarse a las realidades concretas de los sectores y empresas. Hasta ahora, la mayoría de los convenios colectivos no abordan el ciberacoso o lo hacen de manera marginal, como una nota añadida en cláusulas generales, sin desarrollar protocolos, canales de denuncia ni medidas cautelares. Algunos ejemplos avanzados, como los Convenios colectivos de Telefónica o Carburos Vía Augusta, han empezado a incluir definiciones operativas, catálogos abiertos de conductas prohibidas y referencias al uso seguro de las TIC, pero siguen siendo la excepción. La negociación colectiva debe incorporar de manera efectiva el tratamiento del ciberacoso como una manifestación diferenciada de violencia que exige medidas específicas y adaptadas. Esto implica dotar de competencias reales a las comisiones paritarias y garantizar el seguimiento efectivo de los acuerdos alcanzados. Asimismo, sería deseable incluir cláusulas sobre supervisión del uso de herramientas digitales, tiempos de exposición frente a pantallas y condiciones ergonómicas de los entornos virtuales, aspectos que inciden directamente en la salud mental y el bienestar emocional (Martínez Jiménez, 2024b).

En cuarto lugar, debe promoverse una cultura organizacional de «tolerancia cero» frente al ciberacoso, que trascienda las declaraciones de intenciones. La empresa debe asumir que su responsabilidad preventiva no se agota en disponer de un protocolo, sino que exige una vigilancia activa de los espacios virtuales de trabajo, la implicación real de los responsables jerárquicos y un compromiso sostenido en el tiempo. Los protocolos no pueden concebirse únicamente como una prueba de diligencia en un eventual proceso judicial, sino como una herramienta viva que genere confianza y permita actuar con rapidez y proporcionalidad (Megino Fernández, 2023). Esto supone que las actuaciones no dependan exclusivamente de la denuncia expresa de la víctima y que existan mecanismos efectivos de detección y freno

de las conductas prohibidas. Además, debe fomentarse la corresponsabilidad entre todos los actores del entorno laboral, tal y como recomienda el Convenio 190, desde una lógica participativa y no meramente jerárquica. En este sentido, resulta clave implicar a las personas trabajadoras en la construcción de entornos digitales seguros, reforzando el respeto mutuo y la empatía, especialmente en contextos en los que la comunicación pierde los códigos del lenguaje no verbal y las interacciones descontextualizan con facilidad.

En quinto lugar, resulta imprescindible reforzar el papel de los poderes públicos no solo como garantes del cumplimiento legal, sino como agentes activos en la configuración de un marco coherente y actualizado frente al ciberacoso laboral (Martínez Jiménez, 2024a). Aunque existen disposiciones legales que ofrecen puntos de partida relevantes, como la LOPDPGDD, su potencial no ha sido desarrollado plenamente en la práctica cotidiana. Instrumentos como el derecho a la intimidad en el uso de dispositivos digitales, la desconexión digital o el derecho al olvido se incorporan con frecuencia a los protocolos empresariales desde una lógica defensiva, pero no siempre se traducen en mecanismos de prevención eficaces ni en una acción institucional suficientemente coordinada.

Para que estas herramientas operen como auténticos instrumentos de protección, es necesario que las Administraciones públicas y, en particular, la Inspección de Trabajo, dispongan de medios técnicos, formación especializada y criterios homogéneos de actuación para así evitar incidentes como el citado caso IVECO. A menudo, las dificultades para acreditar el daño, identificar responsabilidades o intervenir en entornos virtuales deslocalizados impiden una respuesta eficaz. Esta falta de capacidad institucional refuerza el riesgo de impunidad y debilita la confianza en los canales formales de denuncia. De ahí que sea prioritario no solo adaptar el marco normativo, sino también articular estrategias públicas de acompañamiento, asesoramiento y seguimiento que faciliten la implementación de protocolos específicos, especialmente en pequeñas y medianas empresas.

La integración de estos derechos en actuaciones preventivas concretas sigue siendo desigual. Pensemos, por ejemplo, en un caso en que circula una imagen vejatoria por mensajería interna. Una respuesta adecuada requeriría detener su difusión, proteger la confidencialidad de la víctima, activar el protocolo, valorar medidas cautelares, ofrecer apoyo psicológico y documentar lo ocurrido para su posible traslado a la autoridad laboral.

En definitiva, el ciberacoso laboral no puede entenderse como un problema puntual del trabajo digital, sino como una manifestación estructural derivada de las nuevas formas de organización del entorno laboral en la era digital. Ignorar su especificidad supone dejar fuera del sistema de protección jurídica a un gran número de personas trabajadoras, especialmente vulnerables en contextos marcados por la precariedad, la fragmentación organizativa o el aislamiento tecnológico. Solo una acción integral –normativa, colectiva e institucional– permitirá avanzar hacia entornos laborales realmente seguros, inclusivos y sostenibles también en lo digital. En este reto, el derecho del trabajo debe mantener su función histórica de contrapeso frente al poder empresarial, asumiendo que hoy dicho poder también se ejerce

a través de medios tecnológicos. Por ello, una regulación clara y firme del ciberacoso laboral no constituye únicamente un paso necesario en la modernización del ordenamiento jurídico laboral, sino también un compromiso ético ineludible con las personas trabajadoras que enfrentan formas de violencia frecuentemente silenciadas o invisibilizadas en los entornos digitales.

Referencias bibliográficas

Álvarez del Cuvillo, A. (2021). El ciberacoso en el trabajo como categoría jurídica. *Temas Laborales: Revista Andaluza de Trabajo y Bienestar Social, 157,* 167-192.

Bastante Velázquez, C. C. y Rodríguez Fernández, M. L. (2025). Los derechos digitales y la inteligencia artificial en la negociación colectiva. *Temas Laborales: Revista Andaluza de Trabajo y Bienestar Social, 176*, 239-272.

Benítez, O. E. y Trillo Párraga, F. (2023). Conexión y desconexión digital: derechos de seguridad y salud de las personas trabajadoras. *Revista de Derecho Social, 106*, 37-54.

Cabeza Pereiro, J. y Cardona Rubert, B. (2025). Los *derechos digitales en el entorno laboral y empresarial de la Carta de Derechos Digitales desde la perspectiva de género* [Informe]. Red. es; Universidad de Castilla-La Mancha. https://ruidera.uclm.es/server/api/core/bitstreams/af180995-6ee9-4c23-b9f1-1e6511579602/content

Canalda Criado, S. (2023). Análisis del V AENC en la trayectoria de la negociación interconfederal. *Lan Harremanak - Revista de Relaciones Laborales, 50*, 40-71. https://doi.org/10.1387/lan-harremanak.25295

Cavas Martínez, F. (18 de mayo de 2023). El V Acuerdo para el Empleo y la Negociación Colectiva (V AENC). *Asociación Española de Derecho del Trabajo y de la Seguridad Social*. https://www.aedtss.com/el-v-acuerdo-para-el-empleo-y-la-negociacion-colectiva-v-aenc/

Corrêa Gomes Cardim, T. (2023). De la hiperconexión del trabajador a la esclavitud digital: riesgos psicosociales y desafíos de la conciliación entre tiempo de trabajo y vida privada. *Revista Internacional y Comparada de Relaciones Laborales y Derecho del Empleo, 11*(1), 417-437. https://ejcls.adapt.it/index.php/rlde_adapt/article/view/1252

De Stefano, V., Durri, I., Stylogiannis, C. y Wouters, M. (2020). *«Actualización de las necesidades del sistema»: Mejora de la protección frente al ciberacoso y a la violencia y el acoso en el mundo del trabajo posibilitados por las TIC*. Organización Internacional del Trabajo. https://webapps.ilo.org/static/spanish/intserv/working-papers/wp001/index.html

Fernández-Costales Muñiz, J. (2024). Salud laboral, digitalización, nuevas tecnologías y su reflejo en la negociación colectiva. *Revista Internacional y Comparada de Relaciones Laborales y Derecho del Empleo, 12*(1), 19-47. https://ejcls.adapt.it/index.php/rlde_adapt/article/view/1395

Gil Pérez, M. E. (2024). El derecho a la desconexión digital y su desarrollo legal. *Lan Harremanak - Revista de Relaciones Laborales, 52*, 390-416. https://doi.org/10.1387/lan-harremanak.27027

González Vidales, C. (2024). Tecnología y prevención de riesgos laborales en la negociación colectiva estatal. *Lex Social: Revista de los Derechos Sociales, 14*(2), 1-36. https://doi.org/10.46661/lexsocial.10823

Igartua Miró, M. T. (2023). Transición digital y seguridad y salud en el trabajo: El AENC 2023 y el futuro de la negociación colectiva. *Lan Harremanak - Revista de Relaciones Laborales*, *50*, 72-103. https://doi.org/10.1387/lan-harremanak.25249

Martínez Jiménez, M. M. (2024a). El ciberacoso en el trabajo como riesgo emergente: claves de su régimen jurídico preventivo en las leyes y convenios colectivos más recientes. *Revista de Estudios Jurídico Laborales y de Seguridad Social (REJLSS), 8,* 235-261. https://doi.org/10.24310/rejlss8202418760

Martínez Jiménez, M. M. (2024b). La negociación colectiva y los riesgos psicosociales asociados a la digitalización: en especial al ciberacoso en el trabajo. En J. L. Monereo Pérez (Coord.), *40 años de propuestas jurídicas sobre empleo, negociación colectiva y solución de conflictos laborales en Andalucía. XL Jornadas Universitarias Andaluzas de Derecho del Trabajo y Relaciones Laborales* (pp. 849–865). Junta de Andalucía, Consejo Andaluz de Relaciones Laborales. https://www.juntadeandalucia.es/sites/default/files/2024-06/MONOGRAF%C3%8DAS%2066.pdf

Megino Fernández, D. (2023). Violencia digital y ciberacoso: Reflexiones al calor del Convenio 190 de la OIT y de los actuales planteamientos en la negociación colectiva. *Estudios Latinoamericanos de Relaciones Laborales y Protección Social, 16,* 87-110.

Molina Navarrete, C. (2019). *El ciberacoso en el trabajo: Cómo identificarlo, prevenirlo y erradicarlo en las empresas*. La Ley-Wolters Kluwer.

Moreno Solana, A. (2023). El impacto de la normativa internacional y europea en la regulación actual y futura del acoso, en especial, el ciberacoso o acoso digital. En J. R. Mercader Uguina y A. de la Puebla Pinilla (Dirs.), *Cambio tecnológico y transformación de las fuentes laborales: Ley y convenio colectivo ante la disrupción digital* (pp. 273–310). Tirant lo Blanch.

OpenAI. (2025). *ChatGPT (GPT-5)* [Large language model]. *OpenAI*. https://chat.openai.com[24]

Rodríguez Fernández, M. L. (2016). *Negociación colectiva, igualdad y democracia.* Comares.

Rodríguez Fernández, M. L. (2024). Inteligencia artificial, género y trabajo. *Temas Laborales: Revista Andaluza de Trabajo y Bienestar Social, 171*, 11-39.

Carolina Claudia Bastante Velázquez. Investigadora en el convenio de colaboración entre la UCLM y Red.es para impulsar la implementación de la Carta de Derechos Digitales en el entorno laboral, financiado con fondos *Next Generation* EU. Doctoranda en la Universidad de Castilla-La Mancha (UCLM). https://orcid.org/0009-0005-2491-2973

[24] La autora de este trabajo ha utilizado herramientas basadas en inteligencia artificial (ChatGPT, desarrollada por OpenAI) limitándose a las funciones de apoyo a la redacción, concretamente para sintetizar información preliminar procedente de fuentes normativas y doctrinales y sugerir mejoras de estilo y organización de los apartados.