El Convenio 190 OIT y su trascendencia en la gestión preventiva de la violencia digital y ciberacoso en el trabajo

Fernando de Vicente Pachés

Profesor titular de Derecho del Trabajo y de la Seguridad Social.
Director académico del Espacio Jurídico de Estudios Laborales UJI.
Universidad Jaume I

Extracto

En la evolución de las relaciones laborales, el trabajo telemático y la utilización de los dispositivos tecnológicos se han incrementado de manera significativa. La violencia digital y ciberacoso en el trabajo surgen como consecuencia de una inadecuada utilización de las tecnologías de la información y comunicación, especialmente de internet, las redes sociales y la telefonía móvil, presentes de manera frecuente en el ámbito de las relaciones personales y cada vez en mayor medida en las relaciones del mundo del trabajo.

El objetivo de este estudio consiste en exponer una serie de ideas y reflexiones en relación con el fenómeno de la violencia digital y ciberacoso en el trabajo y la repercusión del Convenio OIT 190 en la prevención de estos riesgos psicosociales emergentes, desde el momento que esta norma internacional reconoce expresamente el derecho de toda persona a un entorno de trabajo libre de violencia y acoso.

La violencia y acoso digital que se produce en las organizaciones productivas es cada vez más un grave problema de salud laboral en el ambiente de trabajo. La incidencia de esta forma de acoso en la salud de las personas trabajadoras tiene la suficiente entidad como para exigir un tratamiento jurídico específico en la normativa preventiva de riesgos laborales, siendo la tutela preventiva el instrumento adecuado para evitar que la violencia digital y el ciberacoso en el trabajo se extiendan progresivamente.

Palabras clave: riesgo laboral psicosocial; prevención y salud; violencia digital y ciberacoso en el trabajo; política de uso de redes; Convenio 190 OIT.

Fecha de entrada: 11-05-2020 / Fecha de aceptación: 21-05-2020

Cómo citar: Vicente Pachés, F. de. (2020). El Convenio 190 OIT y su trascendencia en la gestión preventiva de la violencia digital y ciberacoso en el trabajo. *Revista de Trabajo y Seguridad Social. CEF*, *448*, 69-106.

ILO Convention 190 and its significance in the preventive management of digital violence and cyberbullying at work

Fernando de Vicente Pachés

Abstract

In the evolution of industrial relations, telematic work and the use of technological devices has increased significantly. Digital violence and cyberbullying at work arise as a result of inadequate use of information and communication technologies, especially internet, social network and mobile telephony, frequently present in the field of personal relations and increasingly in the relations of the world of work.

The objective of this study is to present a series of ideas and reflections on the phenomenon of digital violence and cyberbullying at work and the impact of ILO Convention 190 on the prevention of these emerging psychosocial risks, from the moment when this international norm expressly recognizes the right of every person to a working environment free from violence and harassment.

Violence and digital harassment in productive organizations is increasingly a serious occupational health problem in the workplace. The impact of this form of harassment on the health of working people has enough entity to require specific legal treatment in the preventive regulations of occupational risks, with preventive protection being the appropriate instrument to prevent digital violence and cyberbullying at work from spreading progressively.

Keywords: psychosocial work risk; prevention and health; digital violence and cyberbullying at work; political use of networks; ILO Convention 190.

Citation: Vicente Pachés, F. de. (2020). ILO Convention 190 and its significance in the preventive management of digital violence and cyberbullying at work. *Revista de Trabajo y Seguridad Social. CEF*, *448*, 69-106.

Sumario

Lo esencial en esta sociedad de conectividad
es la formación del sujeto moral y el respeto a la
dignidad humana.

Adela Cortina

1. Algunas cuestiones previas: la violencia digital y el ciberacoso en el trabajo como riesgos psicosociales expresamente reconocidos en el Convenio 190 OIT

Este estudio pretende exponer en qué consiste el fenómeno del ciberacoso en el trabajo en cuanto riesgo psicosocial emergente y cómo se ha convertido en una nueva forma de ejercer la violencia en el trabajo que debemos combatir y eliminar desde el ámbito de la tutela preventiva. Y más, desde el momento en que en la evolución de las relaciones laborales el peso del trabajo telemático –tanto dentro como fuera de las empresas– es cada vez mayor.

El ciberacoso o acoso digital en sus múltiples formas (laboral, moral, sexual, sexista, discriminatorio…) es un fenómeno que genera cada vez más alarma social y ha ampliado en mayor medida las formas de ejercer la violencia digital en las relaciones personales y profesionales. A ello hay que sumar la proliferación de las nuevas modalidades de trabajo, como el teletrabajo, que se ha visto incrementado exponencialmente como consecuencia de la situación excepcional generada en el mundo del trabajo por la epidemia de COVID-19.

El acoso digital que se produce en las organizaciones productivas es un grave problema de salud laboral en el ambiente de trabajo. De ahí la importancia de que a través de una norma internacional de tanta trascendencia como es el Convenio 190 de la Organización Internacional del Trabajo (OIT) y la Recomendación 206 OIT se reconozca el derecho de toda persona a un entorno de trabajo libre de violencia y acoso, quedando comprendidas las conductas de violencia y acoso realizadas por medio de las tecnologías de la información y comunicación (TIC)[1]. La obligación supondría liberar el entorno laboral de riesgos psicosociales tan nocivos y contaminantes como la violencia y el ciberacoso o acoso digital y afrontarlos desde dentro de un sistema de gestión preventiva eficaz de estos riesgos. El Convenio 190 OIT ha supuesto un hito normativo, una regulación pionera que supondrá

[1] En una reunión celebrada el 2 de marzo de 2020, España anunció su compromiso formal de ratificar este Convenio 190 OIT, por lo que una vez iniciado este proceso de ratificación sería el segundo país en dar el paso y, en consecuencia, el convenio empezaría a desplegar sus efectos.

un cambio de modelo en la lucha contra la violencia y acoso en el mundo del trabajo y una necesaria reforma de nuestra normativa de prevención[2].

La incidencia del acoso cibernético en la salud de las personas trabajadoras tiene la suficiente entidad como para exigir un tratamiento jurídico específico en la normativa preventiva de riesgos laborales, pues ha de ser la tutela preventiva el instrumento adecuado para evitar que el ciberacoso en el trabajo se extienda progresivamente, ya que la existencia de este riesgo laboral de naturaleza psicosocial implica que las organizaciones actúen para que este no se produzca, analizando y evaluando el riesgo y adoptando cuantas medidas se precisen en prevención del mismo –como tendremos ocasión de exponer más adelante–, a fin de evitar daños en la salud de las personas trabajadoras, garantizando así un ambiente de trabajo sano y seguro.

Con la aparición del Convenio 190 OIT, sería momento oportuno para que se recogieran de manera explícita los riesgos psicosociales en nuestra norma de prevención, en la Ley 31/1995, de 8 de noviembre, de prevención de riesgos laborales (LPRL), como norma marco y que, al mismo tiempo, se desarrollaran a través de una disposición reglamentaria las obligaciones concretas de las empresas con respecto a este tipo de riesgos (Velázquez, 2019). Abordar el ciberacoso en la normativa podría hacer que empleadores y trabajadores cobraran conciencia de su gravedad y también aportaría cierta claridad sobre cómo prevenir y combatir adecuadamente este fenómeno. Los tribunales también podrían interpretar de la manera adecuada la legislación contra el acoso cuando sucedan casos de ciberacoso.

La violencia en el trabajo, como es sabido, puede adoptar múltiples y variadas formas. Puede tratarse de agresiones físicas o de amenazas, o de violencia psicológica, manifestándose a través de intimidación, hostigamiento o acoso –moral, sexual, sexista– por diversos medios y formas. Actualmente, uno de estos medios son las TIC (o, en terminología más actual, las TRIC, en clara alusión a las nuevas tecnologías de relación, información y comunicación): internet, las redes sociales y, cada vez en mayor medida, la telefonía móvil.

Por eso podemos hablar de una nueva forma de acoso en el trabajo que va en aumento, el acoso a través de TRIC, que denominamos –de forma sintetizada– con variedad de términos y expresiones: acoso digital, acoso cibernético, acoso virtual, acoso en red, acoso *online*, acoso por medio de TRIC, o la más conocida o utilizada de «ciberacoso» en el trabajo (De Vicente, 2018; Molina, 2019a).

[2] La OIT publicó, en febrero de 2020, el primer documento de trabajo en relación con el ciberacoso con el título ««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» (<https://www.ilo.org/global/about-the-ilo/how-the-ilo-works/departments-and-offices/workquality/WCMS_736237/lang--es/index.htm>). Este estudio examina las fuentes legales en torno al ciberacoso en el mundo del trabajo, revisa las medidas adoptadas en los países para contrarrestar el acoso y analiza cómo podrían utilizarse para abordar también el ciberacoso. El estudio concluye con sugerencias preliminares sobre las posibles formas de contrarrestar el ciberacoso.

La realidad es que el acoso, en sus múltiples formas, ha existido desde siempre, si bien ahora con la aparición y el uso masivo de internet, las redes sociales y la telefonía móvil el acoso se introduce en una nueva dimensión, en un nuevo contexto, en un espacio virtual donde da la impresión de que no existen límites. Se ha producido como una mutación del acoso a otro espacio, que no es otro que el espacio virtual. Hemos pasado del acoso físico (*offline*) al acoso digital (*online*), dos formas de acoso que no se excluyen y que, lamentablemente, conviven en la actualidad en el ámbito de las relaciones de trabajo.

Lo rápido y lo ilimitado en cuanto a la difusión de una información o de unas imágenes (sean reales o falsas), la inmediatez e instantaneidad, la persistencia en los ataques por los acosadores, el aparente anonimato de estos dispositivos de comunicación, la aparente mayor facilidad de ocultación de las conductas delictivas… hacen que el fenómeno del ciberacoso sea un problema que está aumentando vertiginosamente y en constante evolución.

Por otra parte, ningún grupo de trabajadores, sector o industria está exento de sufrir esta nueva forma de acoso, esta violencia digital o virtual, aunque algunos grupos y sectores laborales, lógicamente, por su actividad en sí misma en el uso frecuente de estas tecnologías corren mayor riesgo de sufrirla que otros[3]. Es cierto que especialmente vulnerables son todas las personas que tienen la condición de empleados, si bien lo padecen en mayor medida las mujeres, colectivo al que el Convenio 190 OIT protege de manera especial –de ahí que se ha acuñado el término «ciberviolencia de género»–, los trabajadores jóvenes –por su condición de nativos digitales– y las personas que se encuentran en una situación social y laboral de por sí más vulnerable[4].

Las consecuencias del acoso digital pueden ser de distinta naturaleza y afectar a varios ámbitos. El ciberacoso laboral se ha convertido en un claro problema en las relaciones de trabajo, tanto para las entidades empresariales como para la salud de la persona trabajadora. No solamente afecta a los empleados y empleadores, sino también a los lugares de trabajo, los compañeros, las familias y, en definitiva, a la sociedad en general.

[3] Como quienes trabajan en plataformas que dependen de las calificaciones de su rendimiento por los clientes, ya que las plataformas asignan tareas y trabajos futuros en función de las calificaciones y también ponen fin a su relación de trabajo a aquellos cuyas calificaciones caen por debajo de determinado promedio. Los trabajadores en plataformas, por lo tanto, pueden sentirse obligados a aguantar los comportamientos abusivos de los clientes por temor a perder su empleo.

[4] El apartado 9 de la Recomendación 206 OIT, que complementa al Convenio 190 OIT, señala expresamente que:

> Los miembros deberían adoptar medidas apropiadas para los sectores o las ocupaciones y las modalidades de trabajo más expuestos a la violencia y el acoso, tales como el trabajo nocturno, el trabajo que se realiza de forma aislada, el trabajo en el sector de la salud, la hostelería, los servicios sociales, los servicios de emergencia, el trabajo doméstico, el transporte, la educación y el ocio.

Para la persona trabajadora afectada y víctima de esta modalidad de acoso, no tiene siempre las mismas consecuencias, ni provoca las mismas reacciones, debido fundamentalmente a que las diferencias entre las habilidades, capacidades y recursos para afrontar las situaciones de acoso virtual pueden ser muy distintas; no obstante, sus consecuencias en la salud son devastadoras en la mayor parte de los casos. La violencia digital en el trabajo puede ser gravemente perjudicial para el estado de salud de la persona trabajadora. Las víctimas de esta forma de acoso presentan cuadros más o menos severos de estrés, depresión, ansiedad, trastornos emocionales y de la conducta social, conflictos familiares, distorsiones cognitivas, trastornos psicosomáticos y otras afecciones que, en caso límite, pueden desembocar en el suicidio, como el de la mujer trabajadora de la empresa Iveco por la difusión de unos vídeos sexuales e íntimos en los que ella aparecía.

Por otra parte, para la empresa, los procesos de violencia y acoso por medios tecnológicos se traducen en un mayor absentismo laboral, en un deterioro de la productividad y de la calidad del servicio prestado, deterioro de las relaciones laborales y, en general, un clima laboral tóxico, irrespirable e inhumano. En ocasiones, se encuentran en la necesidad de contratar a trabajadores sustitutos de la persona trabajadora víctima de esa violencia virtual, en la obligación de pagar subsidios por incapacidad temporal y eventuales indemnizaciones a los trabajadores acosados en el caso de incurrir en responsabilidades. Asimismo, por no prevenir este tipo de conductas pueden producirse quejas, reivindicaciones y litigios contra la empresa que, entre otras consecuencias, pueden perjudicar su reputación e imagen corporativa y, por consiguiente, un impacto negativo en la productividad.

En definitiva, evidenciamos que la violencia laboral digital es, lamentablemente, un fenómeno cada vez más presente en nuestras organizaciones. La violencia laboral a través de dispositivos digitales de todo tipo y naturaleza está incrementándose. La realidad es que las tensiones, las agresiones, las diferentes formas de acoso forman ya parte de la vida laboral de muchos centros de trabajo. Estos comportamientos y agresiones se producen actualmente también a través de dispositivos digitales o tecnológicos que terminan por generar un mal clima laboral o ambiente de trabajo con importantes repercusiones en la salud y bienestar de los trabajadores, afectando a las relaciones de trabajo y a la propia productividad de la empresa. Y el Convenio 190 OIT es un nuevo instrumento normativo de utilidad para la prevención y protección frente a estas agresiones en un mundo del trabajo digitalizado.

2. Presupuestos que caracterizan a la violencia y el ciberacoso en el trabajo: configuración del ciberacoso en el trabajo tras el impacto del Convenio 190 OIT

La realidad es que no hay todavía una definición unánime o de consenso de ciberacoso o acoso cibernético en el trabajo, lo que induce a errores de regulación y gestión en el seno de las empresas (Molina, 2019a, p. 57), pero sí podemos describir las notas o elementos

que caracterizan al ciberacoso como tipo jurídico, para, de alguna manera, tratar de identificarlo o delimitarlo. No existe ninguna definición única de ciberacoso, o de acoso, que esté aceptada internacionalmente. Pero en cambio se sigue utilizando «ciberacoso» como término genérico para designar una serie de comportamientos agresivos que tienen lugar a través de las TIC (OIT, 2020, p. 7).

Por lo que respecta a la diferenciación entre los conceptos de violencia y (ciber)acoso, la OIT mantiene una definición unificada, dado que –como analizaremos– el artículo 1.1 del Convenio 190 OIT establece un concepto único de violencia y acoso en el trabajo, si bien recomienda a las legislaciones de cada país miembro que –si así es su deseo– diferencie ambos conceptos.

Es importante partir de la idea de que la violencia digital supone –tal y como se ha indicado– diversas acciones intimidatorias a través de internet o en la red, si bien ello no significa que todos los casos de intimidación y agresión a través de las redes supongan necesariamente que estemos siempre ante un supuesto claro y evidente de ciberacoso en el trabajo, dado que se tendrán que dar los elementos o presupuestos que lo sustentan o delimitan. Por ello, debemos distinguir entre situaciones de violencia o intimidación digital y las típicas de ciberacoso en el trabajo.

En una definición básica de ciberacoso, y de primera aproximación, quedarían comprendidos el conjunto de comportamientos mediante los cuales una o varias personas –o incluso una organización– usan las TRIC para hostigar a una o más personas. Dichos comportamientos incluyen, aunque no de forma excluyente, conductas, amenazas y falsas acusaciones, suplantación de la identidad, usurpación de datos personales, daños al ordenador de la víctima, vigilancia en red y por dispositivos tecnológicos de las actividades de la víctima, uso de información privada e imágenes para chantajear o extorsionar a la víctima, etc.

Con carácter genérico, el término «ciberacoso» se ha utilizado para describir conductas agresivas llevadas a cabo a través de las TIC, y puede incluir imágenes, vídeos, correos electrónicos o sitios de redes sociales, entre otros. El ciberacoso en el mundo del trabajo es un fenómeno relativamente reciente e inexplorado, a pesar del uso generalizado de las TRIC en los entornos y modalidades de trabajo actuales[5].

El profesor Molina Navarrete nos proporciona –siguiendo una evolución doctrinal, constitucional y normativa– una definición de «violencia cibernética en el trabajo» (2019a, p. 73) tomando como base jurídica la normativa –de futuro– ahora objeto de nuestro estudio, como es el Convenio 190 OIT, entendiendo por tal el:

[5] Royakkers (2000), en otra de las definiciones más referidas, mantiene –desde una perspectiva general y no laboral– que el ciberacoso es «una intromisión en la vida íntima de la persona utilizando los medios digitales, fundamentalmente las posibilidades que ofrece internet, las redes sociales y la telefonía móvil».

> […] conjunto de comportamientos y prácticas inaceptables [conductas actuales], o las amenazas de ellos [intimidación con conductas futuras], se manifiesten de una sola vez [agresión ocasional] o repetida [acoso], susceptibles de causar un daño [personal o económico] cualquiera que sea su motivación, incluida la razón de sexo, mediante las comunicaciones por medio de tecnología digital y relacionadas con el trabajo (art. 1 a) en relación con el art. 3 d) Convenio 190 OIT).

Por lo tanto, en esta definición extraída de la que se desprende del Convenio 190 OIT se introducen varios elementos –o presupuestos que caracterizan o configuran el acoso digital o ciberacoso en el mundo del trabajo– que deben ser tenidos en cuenta y debidamente clarificados para comprender nítidamente este fenómeno:

1.º Es una agresión/conducta violenta utilizando las TRIC –consistente en intimidar, atacar, humillar, difamar, vigilar, chantajear a la persona trabajadora–. Es la violencia ejercida por medio de dispositivos digitales o tecnológicos tan comunes en nuestras vidas como el WhatsApp, el correo electrónico, la mensajería instantánea (SMS), las páginas web, las tabletas, los blogs, los foros, las redes sociales –como Facebook, Instagram, Twitter…–, los chats internos de las empresas, YouTube, y tantos otros en una lista que sería casi interminable. Pues bien, a través de todos estos medios tecnológicos o digitales la persona trabajadora podría ser acosada y sufrir diversas conductas de ciberviolencia.

   Es intrascendente que los medios utilizados para la agresión sean de titularidad privada, esto es, es totalmente indiferente que los medios personales para cometer la conducta agresora sean de la persona trabajadora o sean medios de titularidad de la empresa, medios propios de la organización productiva.

   Los avances tecnológicos, indiscutiblemente, han revolucionado al mundo y el mundo del trabajo no podía ser la excepción. En las organizaciones productivas, dentro y fuera de ellas, son habituales espacios de trabajo donde se desarrollan actividades con un uso extendido de las redes sociales, de internet, del correo electrónico, del uso de la mensajería instantánea o del WhatsApp o cualquier otro medio o dispositivo digital: blogs, foros, chats… desde los que se pueden acometer acciones de violencia y acoso.

2.º La agresión por medio de estos dispositivos digitales suele realizarse de forma repetida (acto reiterado), o puede tratarse de un solo acto, una única agresión, una agresión ocasional o puntual (como los casos de ciberacoso sexual y sexista), donde una sola vez puede ser suficiente para estimar la conducta antijurídica y de gran intensidad dañosa, como el caso de publicar fotos o un vídeo íntimo o sexual que puede en un instante ser visto por numerosas personas y permanecer en el tiempo mientras no sea eliminado o borrado.

   En ocasiones, al igual que el acoso laboral presencial, se trata de comportamientos repetidos de manera sistemática y continua. La frecuencia de los comportamientos

lesivos –aunque también ha sido un presupuesto cuestionado– es una nota definitoria fundamental del acoso digital, esto es, la frecuencia de los ataques, en su repetición, la persistencia en el acto de acoso. Si bien, para ciertas formas de ciberacoso –como el ciberacoso sexual y el sexista–, no es siempre estrictamente necesaria esta reiteración o repetición para estimarla y calificarla como conducta acosadora, de manera que una única conducta ilícita sería suficiente para su consideración como conducta inaceptable y punible.

En el mismo Convenio 190 OIT sobre violencia y acoso en el mundo del trabajo se insiste en esta idea, señalando que la expresión «violencia y acoso» en el mundo del trabajo:

> […] designa un conjunto de comportamientos y prácticas inaceptables, o de amenazas de tales comportamientos y prácticas, ya sea que se manifiesten una sola vez (agresión ocasional) o de manera repetida (acoso), que tengan por objeto, que causen o sean susceptibles de causar, un daño físico, psicológico, sexual o económico.

En otras ocasiones, se está ante una conducta que, además de repetirse o reiterarse, se mantiene durante un cierto tiempo. La frecuencia y prolongación en el tiempo evidencian –en determinadas conductas ciberacosadoras– que se está ante un comportamiento unificado, planeado y programado que persigue un único objetivo: vejar, humillar, acechar, chantajear… sin importar la destrucción de la víctima. La duración de los ataques, la prolongación o persistencia en el tiempo –lo que viene a denominarse como «efecto acumulativo»– produce en la propia víctima la sensación de inseguridad, de indefensión y que su temor vaya en aumento.

También es necesario clarificar que cuando hacemos referencia a la reiteración en el tiempo de la agresión, este elemento debe ser matizado, dado que las conductas de ciberacoso normalmente y por su forma de ejecución (a través de la red) permanecen de por sí en el tiempo, esto es, tienen una mayor durabilidad temporal, sus efectos se prolongan en tanto no se borren o eliminen del espacio virtual o cibernético en el que «habitan» (si es que realmente desaparecen o se perpetúan en la red). Además de que la acción de acoso digital cuenta con una amplia difusión pública al llegar a un número indefinido de personas y en breve escaso tiempo, por la propia viralidad de su transmisión, lo que supone, asimismo, una mayor potencia lesiva de esta forma de acoso que la diferencia del acoso físico o presencial.

3.º La agresión puede provenir de sujetos internos o externos al ámbito de trabajo. El ciberacoso laboral se caracteriza por ser realizado –generalmente– por uno o varios compañeros de trabajo –caso más habitual– o por superiores –si bien, aunque se produce, es menos común–, e incluso por terceras personas ajenas o externas al propio lugar de trabajo (caso de clientes, usuarios, proveedores…), es decir, los ciberacosadores pueden provenir tanto del entorno laboral como del entorno

extralaboral, esto es, extramuros de la empresa. El Convenio 190 OIT hace referencia expresa en su artículo 4 a estas terceras personas ajenas al entorno laboral, al señalar que todo Estado deberá adoptar un enfoque inclusivo para prevenir y eliminar la violencia y el acoso en el mundo del trabajo y este enfoque debería tener en cuenta la violencia y el acoso que «impliquen a terceros».

Algunos tipos de violencia digital –tal y como se ha indicado– tienden a producirse más en sectores específicos. Los sectores como educación (profesorado), personal médico-sanitario, las actividades de contacto directo con el público (sector servicios y ocio), los medios de comunicación (cine, radio, televisión), el periodismo (presentadores de televisión), el mundo del espectáculo, la política, deportistas de élite, teleoperadoras o *telemarketing* son algunos de los sectores entre cuyo personal se registran casos frecuentes de violencia externa[6].

4.º Es indiferente que la agresión se realice dentro como fuera de la jornada y del tiempo de trabajo. Es suficiente constatar que la acción o conducta agresora tenga lugar «con ocasión de la prestación de trabajo», en definitiva, que existe algún vínculo o punto de conexión relevante con el trabajo. La agresión por dispositivos móviles puede hacerse desde cualquier lugar y en todo momento. Por consiguiente, puede realizarse tanto dentro como fuera de la jornada y del tiempo de trabajo, como establece expresamente el Convenio 190 OIT, siendo suficiente constatar que la acción tenga lugar «durante el trabajo, en relación con el trabajo o como resultado del trabajo».

Si algo caracteriza a esta forma de acoso son sus amplias posibilidades desde donde poder acometerlo o perpetrarlo, pues la acción o conducta agresora en red puede generarse en cualquier momento y desde cualquier lugar, carece de las limitaciones de espacio y tiempo, por lo que es indiferente si se realiza tanto dentro como fuera de la jornada y del tiempo de trabajo.

Por tanto, la noción de violencia y acoso en el «mundo del trabajo» abarca conductas relacionadas con el trabajo «en cualquier momento y lugar» sin límites espaciales y temporales para combatir el ciberacoso, fenómeno que pone de manifiesto cómo la tecnología puede desdibujar las fronteras entre la vida personal y laboral y cómo se pueden producir conductas agresivas mucho más allá de los límites del «lugar de trabajo». Para ello, hace falta entender de manera amplia el «mundo del trabajo» y las cuestiones relacionadas con el trabajo.

[6] El suicidio de la luchadora profesional Hana Kimura, de 22 años, gran promesa sobre el cuadrilátero y concursante del *reality Terrace House Tokyo*, un programa de Netflix que se convirtió en un éxito internacional y que tras la muerte de la joven ha sido cancelado. Hana Kimura sufría ciberacoso. El caso ha abierto un intenso debate en Japón sobre la necesidad de endurecer las medidas contra los abusos en las redes sociales.

5.º Las conductas agresivas son susceptibles de causar un grave daño a la víctima en su salud, su integridad física y psíquica, como indica el Convenio 190 OIT: «causen o sean susceptibles de causar un daño físico, psicológico, sexual, profesional o económico». En consecuencia, el daño (personal o económico) puede o no haberse materializado, no siendo, por tanto, necesario un resultado dañoso de la acción agresora. El ciberacoso produce daños físicos o psicológicos de gravedad. Es, tal y como se ha incidido, un grave problema de salud laboral, reconocido como nuevo riesgo psicosocial emergente. Las consecuencias son graves dado que pueden generar en la persona cuadros de ansiedad, estrés postraumático, depresión, incapacidad para el trabajo e incluso el suicidio (caso Iveco).

Debemos tener presente que se trata de una intromisión disruptiva, en el sentido de inapropiada o inaceptable (como dice el Convenio 190 OIT) y abrupta. Es decir, el acosador ejerce su poder sobre elementos que la víctima considera privados y personales (unas fotos o vídeos personales e íntimos, una información, su vida privada…). Con esta irrupción, de forma súbita, el ciberacosador trata de poner en evidencia aspectos de la vida personal de la víctima que esta desearía mantener en el ámbito de lo más estrictamente privado. El riesgo de que aspectos de la vida íntima como fotos, vídeos o datos privados de todo tipo sean distribuidos entre un número indeterminado de usuarios de internet es una poderosa herramienta de dominación y sumisión a la que se enfrenta la víctima. Se produce un «poder desigual» entre las víctimas y los perpetradores y una desconexión o desentendimiento emocional, ya que los agresores, a diferencia del acoso presencial, no se enfrentan directamente a las reacciones y emociones de sus víctimas.

6.º Otro elemento clave en determinadas formas de acoso digital o ciberacoso laboral es que este se produce tras la negativa de la víctima, en contra de la voluntad de la víctima, esto es, sin su consentimiento. El acosador persiste, así, en su comportamiento a pesar de que la persona acosada haya explicitado su negativa a continuar recibiendo mensajes, llamadas, comentarios o cualquier otra información procedente del ciberacosador.

Sin embargo, y a diferencia de la versión del acoso *offline* o presencial, en muchos casos la víctima no conoce quién es el ciberacosador o agresor, si bien, como suele ser común, se trata en muchas ocasiones de una persona de su ámbito o entorno cercano en un sentido amplio, estando también entre los posibles sospechosos los compañeros de trabajo, amigos, excompañeros, mandos directivos o supervisores. Las posibilidades que ofrece internet para la ocultación de la identidad, así como la distancia física entre la persona agresora y la víctima, implican la imposibilidad de manifestar dicha negativa. En muchos casos, los SMS, los correos electrónicos, los wasaps enviados por el acosador se realizan desde un número oculto, los comentarios en las redes sociales del acosado o acosada se realizan desde una cuenta con identidad falsa o no explícita, etc. Esto no solo implica que la víctima no puede mostrar su rechazo, sino que no sabe a quién mostrarlo. Esta indefensión es una fuente de incertidumbre con efectos muy negativos y perversos sobre el equilibrio psicológico de la víctima.

3. El Convenio 190 OIT: nueva norma jurídica internacional necesaria para la prevención de la violencia y el ciberacoso en el trabajo

La OIT, después de dos sesiones de discusión en la Conferencia Internacional del Trabajo (durante los años 2018 y 2019), va a aprobar finalmente en junio de 2019 el Convenio número 190 sobre la eliminación de la violencia y el acoso en el mundo del trabajo. Norma jurídica internacional a la que se acompaña, como viene haciéndose de forma habitual, de una recomendación, la Recomendación número 206, que complementa a este Convenio 190 OIT, con la finalidad de facilitar pautas interpretativas para su mejor puesta en práctica por parte de los Estados y de las empresas.

Este Convenio 190 OIT se convierte en el instrumento principal para poder abordar y gestionar eficazmente desde las organizaciones productivas la prevención de riesgos tan emergentes en el entorno laboral como la violencia y el acoso, también del acoso en su versión digital o virtual, al que denominamos, entre sus múltiples acepciones, «ciberacoso laboral» (acoso en red, acoso cibernético, acoso *online*, acoso por medio de TRIC, etc.). Y viene confirmado desde el momento en que el mismo convenio precisa que se aplica a la violencia y acoso en el marco de las comunicaciones que estén relacionadas con el trabajo y son realizadas por medio de TIC (art. 3 d). Es importante observar que no hay obstáculos físicos o temporales aplicables a esta disposición, que abarca comunicaciones en todas sus formas, siempre que estén relacionadas con el trabajo.

Con esta norma internacional se recuerda a los Estados y organizaciones productivas o empresas que tienen la importante responsabilidad de promover un entorno general de tolerancia cero frente a la violencia y el (ciber)acoso con el fin de facilitar la prevención de este tipo de comportamientos y prácticas, y que todos los actores del mundo del trabajo, en consecuencia, deben abstenerse de recurrir a la violencia y el acoso, prevenirlos y combatirlos.

Y en este mismo sentido, en este convenio se recoge el derecho de toda persona a un entorno de trabajo libre de violencia y acoso, reconociendo, asimismo, que la violencia y el acoso en el trabajo pueden constituir una violación o un abuso de los derechos humanos, que la violencia y el acoso son una amenaza para la igualdad de oportunidades, que son inaceptables e incompatibles con el trabajo decente y que en el mundo del trabajo afectan a la salud psicológica, física y sexual de las personas, a su dignidad, y a su entorno familiar y social.

Tanto el Convenio 190 como la Recomendación 206, partiendo de un enfoque global o integral, definen los contenidos básicos que debe incluir la legislación de los Estados sobre violencia y acoso en el trabajo, poniendo de relieve que la violencia y el acoso en el trabajo deben tener un tratamiento común y coherente dentro de cada legislación nacional, evitando un tratamiento parcial y disperso, y que las normas que lo regulen deben tener un alcance multidisciplinar, abarcando normas de diversa naturaleza (de trabajo, empleo, seguridad y salud en el trabajo, igualdad y no discriminación, derecho penal…).

En el apartado de definiciones, el artículo 1.1 del Convenio 190 OIT establece un concepto único de violencia y acoso en el trabajo, así se dispone que:

> La expresión «violencia y acoso» en el mundo del trabajo designa un conjunto de comportamientos y prácticas inaceptables, o de amenazas de tales comportamientos y prácticas, ya sea que se manifiesten una sola vez o de manera repetida, que tengan por objeto, que causen o sean susceptibles de causar, un daño físico, psicológico, sexual o económico, e incluye la violencia y el acoso por razón de género.

Si bien matiza, a continuación, que la definición de ambos términos podrá hacerse por separado en las legislaciones nacionales cuando desarrollen los compromisos adquiridos tras su oportuna ratificación, de manera que si es voluntad de los Estados: «[…] la violencia y el acoso pueden definirse en la legislación nacional como un concepto único o como conceptos separados».

Un primer aspecto importante de la definición de violencia y acoso sobre el que incide el Convenio 190 OIT es la reiteración o no de las conductas, cuando delimita que las conductas de violencia y acoso pueden ser un acto único o, en cambio, un acto reiterado y prolongado en el tiempo. El convenio 190 OIT –como terminamos de comprobar– insiste en este aspecto, pudiendo tratarse de una conducta repetida o de una sola vez y única. La agresión por medio de los dispositivos digitales –como hemos tenido ocasión de analizar– suele realizarse de forma repetida (acto reiterado y mantenido en el tiempo), pero también puede tratarse de un solo acto, una única agresión, una agresión aislada u ocasional (como los casos de ciberacoso sexual), donde una sola vez puede ser de gran intensidad dañosa, como el hecho de publicar fotos o vídeos íntimos o sexuales que en un instante pueden ser vistos por multitud de personas y permanecer en el tiempo mientras esas fotos o vídeos no se han borrado.

Otro aspecto interesante de esta definición que nos aporta el Convenio 190 OIT es que con ella se objetiviza el concepto de violencia y acoso en el trabajo, perdiendo trascendencia el elemento de la intencionalidad en la acción acosadora, no siendo requisito determinante o necesario la intencionalidad del sujeto de causar un daño o de destruir a la víctima como elemento constitutivo o requisito esencial para la calificación de este tipo de conductas. Este matiz es significativo dado que supone desviarse del criterio seguido hasta ahora por la doctrina judicial mayoritaria –que ha exigido la intencionalidad de causar un daño– adoptando un criterio más próximo al contemplado en la Sentencia del Tribunal Constitucional (STC) 56/2019, de 6 de mayo, en un caso de acoso moral que sufrió un empleado público, en la que respecto del requisito de la intencionalidad se señala claramente que:

> […] con carácter general, la protección constitucional de los derechos fundamentales no puede quedar supeditada a la indagación de factores psicológicos y

> subjetivos de arduo control, pudiendo bastar la presencia de un nexo de causalidad adecuado entre el comportamiento antijurídico y el resultado lesivo prohibido por la norma (FJ 5.º c).

Por otra parte, el daño, el resultado dañoso, tampoco es un elemento o requisito esencial del concepto de acoso en el trabajo, ya que es suficiente con que la conducta acosadora sea susceptible de producir el daño –sea este físico, psíquico, sexual o económico– sin necesidad de que se materialice o se actualice, siendo suficiente con constatar la existencia de un riesgo relevante de que la lesión pueda llegar a producirse. Y, en este sentido, la definición de violencia y acoso en el trabajo recogida en el Convenio 190 OIT es clara –como ya se expuso–, pues «designa un conjunto de comportamientos y prácticas inaceptables, o de amenazas de tales comportamientos y prácticas, que tengan por objeto, que causen o sean susceptibles de causar, un daño físico, psicológico, sexual o económico».

También, debemos subrayar de este Convenio 190 OIT, la importante perspectiva o dimensión de género que asume esta norma internacional, esto es, la especial atención hacia las cuestiones de género, incluyendo un concepto propio y diferenciado de «violencia y acoso por razón de género», consciente esta norma internacional de que el colectivo femenino sufre en mayor medida estas formas de violencia y acoso, teniendo en cuenta también los supuestos más numerosos de violencia y acoso que se producen a mujeres por medio de dispositivos tecnológicos o digitales. En este sentido, se indica que: la expresión «violencia y acoso por razón de género» designa la violencia y el acoso que van dirigidos contra las personas por razón de su sexo o género, o que afectan de manera desproporcionada a personas de un sexo o género determinado, e incluye el acoso sexual. Por tanto, quedarán perfectamente comprendidos los supuestos de ciberacoso sexual en el trabajo y los de ciberacoso en el trabajo por razón de sexo o género (Molina, 2019b), a los que habría que adicionar, y tener en cuenta, los relativos al acoso digital o cibernético en el trabajo por motivos de orientación sexual e identidad de género[7].

Por todo ello, se establece, igualmente, como principio fundamental, que todo Estado deberá adoptar un enfoque inclusivo, integrado y que tenga en cuenta las consideraciones de género para prevenir y eliminar la violencia y el acoso en el mundo del trabajo (art. 7). Este enfoque inclusivo debería tener en cuenta la violencia y el acoso que impliquen a terceros,

[7] Y, en este mismo sentido, de manera clarificadora se recoge en el preámbulo del Convenio 190 OIT el reconocimiento de que:

> […] la violencia y el acoso por razón de género afectan de manera desproporcionada a las mujeres y las niñas, y […] también que la adopción de un enfoque inclusivo e integrado que tenga en cuenta las consideraciones de género y aborde las causas subyacentes y los factores de riesgo, entre ellos los estereotipos de género, las formas múltiples e interseccionales de discriminación y el abuso de las relaciones de poder por razón de género, es indispensable para acabar con la violencia y el acoso en el mundo del trabajo.

cuando proceda, y consiste, en particular, en: a) prohibir legalmente la violencia y el acoso; b) velar por que las políticas pertinentes aborden la violencia y el acoso; c) adoptar una estrategia integral a fin de aplicar medidas para prevenir y combatir la violencia y el acoso; d) establecer mecanismos de control de la aplicación y de seguimiento o fortalecer los mecanismos existentes; e) velar por que las víctimas tengan acceso a vías de recurso y reparación y a medidas de apoyo; f) prever sanciones; g) desarrollar herramientas, orientaciones y actividades de educación y de formación, y actividades de sensibilización, en forma accesible, según proceda, y h) garantizar que existan medios de inspección e investigación efectivos de los casos de violencia y acoso, incluyendo a través de la Inspección de Trabajo o de otros organismos competentes (art. 7).

El acoso sexual en el ámbito laboral –tanto el de chantaje como el acoso sexual ambiental– también pueden materializarse, lógicamente, a través de dispositivos digitales o tecnológicos, al crear a través de estos instrumentos un entorno claramente intimidatorio, hostil, degradante u ofensivo. Estaríamos, en esencia, frente a lo que podríamos denominar «ciberacoso sexual en las relaciones de trabajo» (*cibersexual harassment*) e, incluso, «ciberacoso por razón de sexo o género» (*cibergender harassment*) (De Vicente, 2018, p. 117).

La referencia a los grupos vulnerables y a los grupos en situación de vulnerabilidad, como es el caso del colectivo de mujeres, nos dice la Recomendación 206 (art. 13) que «debería interpretarse de conformidad con las normas internacionales del trabajo y los instrumentos internacionales sobre derechos humanos aplicables»[8].

Las víctimas de ciberacoso son en buena medida personas de ambos sexos, si bien mayoritariamente lo padecen las mujeres en una proporción muy superior a la de los hombres. Mientras que los varones principalmente son insultados o sufren amenazas en la red, las

[8] Y en la misma Recomendación 206 OIT (art. 20) se constata igualmente la importancia de tener conocimientos y formación en cuestiones de género, al señalarse expresamente que:

> Los inspectores del trabajo y los agentes de otras autoridades competentes, según proceda, deberían recibir formación específica sobre las cuestiones de género para poder detectar y tratar la violencia y el acoso en el mundo del trabajo, incluidos los peligros y riesgos psicosociales, la violencia y el acoso por razón de género y la discriminación ejercida contra determinados grupos de trabajadores.

Y que –art. 23 b) y e)– los Estados miembros deberían financiar, elaborar, aplicar y difundir:

> […] directrices y programas de formación que integren las consideraciones de género para asistir a jueces, inspectores del trabajo, agentes de policía, fiscales y otros agentes públicos a cumplir su mandato en lo que respecta a la violencia y el acoso en el mundo del trabajo, así como para asistir a los empleadores y a los trabajadores de los sectores público y privado, y a sus organizaciones a prevenir y abordar la violencia y el acoso en el mundo del trabajo; [y] planes de estudios y materiales didácticos sobre violencia y acoso, con inclusión de la violencia y el acoso por razón de género, que tengan en cuenta la perspectiva de género, en todos los niveles de la educación y la formación profesional, de conformidad con la legislación y la situación nacional.

mujeres padecen agresiones de naturaleza sexual (ciberacoso sexual y ciberacoso por razón de sexo o sexista). Y hay más agresores hombres que mujeres, por las relaciones de poder y desigualitarias existentes y porque el acoso es una forma de generar dominación, sumisión y relaciones desiguales.

La Agencia de Derechos Fundamentales de la Unión Europea constató (encuesta de 2014) que el 23 % de las mujeres había manifestado sufrir «acoso o abuso en red» al menos una vez en su vida y que una de cada diez mujeres ha sido víctima de violencia en la red desde los 15 años. El estudio sobre «Ciberviolencia y discurso de odio *online* contra las mujeres», publicado en 2018 por el Parlamento Europeo, pone de relieve que «el 20 % de las mujeres jóvenes de la Unión Europea han sufrido ciberacoso sexual». Los estudios e informes en Europa demuestran claramente que el 90 % de las personas que sufren acoso sexual (presencial y en red) son mujeres. Y más del 65 % de las víctimas no se atreven a denunciar. Un gran número de casos de ciberacoso sexual o sexista no llega a denunciarse como consecuencia del miedo a represalias, a cambios de puesto, a ser despedidas, la dificultad para conseguir pruebas, unos insuficientes canales de denuncia, el deficiente seguimiento y protección de las víctimas. Dudas, culpa, malestar; dar el paso de denunciar supone, en la mayoría de los casos, una lucha interna. El temor a no ser creídas; de ahí la importancia de que en los protocolos preventivos de acoso de las organizaciones existan canales adecuados de denuncia, el dar curso a las quejas o denuncias… Por otra parte, hay una respuesta reducida desde el ámbito judicial y desde las organizaciones productivas. Las resoluciones judiciales de condena son escasas y la protección penal tiene lugar solo en casos muy graves de acoso sexual. El movimiento #MeToo expuso una situación endémica de acoso y abuso en los lugares de trabajo, y permitió que las mujeres –de todas las edades, nacionalidades y procedencias sociales y económicas– compartieran sus historias de abuso. Este movimiento ayudó a sacar a la luz los abusos constantes a las mujeres en el lugar de trabajo y evidenció que el sistema no puso freno a esa situación. Y ello, a pesar de los recientes casos de condena por agresiones sexuales como el del productor de cine estadounidense Harvey Weinstein.

El ámbito personal de aplicación y protección de este Convenio 190 OIT es la relación de trabajo. Este convenio protege a los trabajadores y a otras personas en el mundo del trabajo, con inclusión de los trabajadores asalariados, así como a las personas que trabajan, cualquiera que sea su situación contractual, las personas en formación (contratos para la formación y el aprendizaje, contratos en prácticas, personas becarias y estudiantes realizando prácticas externas –prácticas no laborales– de una determinada titulación o grado) incluidos los pasantes y los aprendices, los trabajadores despedidos, los voluntarios (regulado en la legislación española en la Ley 45/2015, de 14 de octubre), las personas en busca de empleo y los postulantes a un empleo (candidatos de empleo que carecen de la condición de trabajadores y, en consecuencia, de protección y están en situación de mayor vulnerabilidad), y los individuos que ejercen la autoridad, las funciones o las responsabilidades de un empleador, en clara referencia a los directivos e incluso extensivo a los trabajadores por cuenta propia o autónomos. Este convenio se aplica

a todos los sectores, público o privado, de la economía tanto formal como informal, en zonas urbanas o rurales (art. 2).

El ámbito subjetivo de protección de este convenio se extiende a las relaciones de empleo público, independientemente de cuál sea su naturaleza (contractual, estatutaria, eventual, administrativa…). En definitiva, se protege a todas las personas que entran en relación o contacto con la empresa o con las instituciones públicas. Se ha criticado su irrealismo por su pretensión de aplicación no solo a la economía formal, sino también a la economía informal, donde será difícil identificar claramente al empleador responsable en la vertiente preventiva e interna (Molina, 2019a, p. 416).

Por lo que respecta al ámbito espacial y funcional de la protección frente a la violencia y el acoso, el convenio se aplica a la violencia y el acoso en el mundo del trabajo que ocurre o acontece «durante el trabajo», esto es, en tiempo de trabajo y cualquiera que sea el lugar en el que se produzca –fuera o dentro de la empresa–, «en relación con el trabajo», con ocasión o en conexión con la actividad que se realiza, o «como resultado del mismo», esto es, cuando tiene su causa u origen en la actividad de trabajo prestada, sin necesidad de que se sufra la conducta violenta o (ciber)acosadora ni durante el trabajo ni en el lugar de trabajo. El convenio, en consecuencia, hace referencia a la responsabilidad de la empresa en lo relativo a las conductas que tengan lugar durante el trabajo, en relación con el trabajo o como resultado del mismo.

Y el convenio es explícito en cuanto a la determinación de estos espacios relacionados con el trabajo, dada la amplitud de los conceptos utilizados en la norma, señalando: a) en el lugar de trabajo, inclusive en los espacios públicos y privados cuando son un lugar de trabajo; b) en los lugares donde se paga al trabajador, donde este toma su descanso o donde come, o en los que utiliza instalaciones sanitarias o de aseo y en los vestuarios; c) en los desplazamientos, viajes, eventos o actividades sociales o de formación relacionados con el trabajo; d) en el marco de las comunicaciones que estén relacionadas con el trabajo, incluidas las realizadas por medio de TIC; e) en el alojamiento proporcionado por el empleador, y f) en los trayectos entre el domicilio y el lugar de trabajo (violencia o acoso *in itinere*).

Uno de los espacios de protección de la violencia y acoso es el que se produce en los desplazamientos, viajes, eventos o actividades sociales o de formación relacionados con el trabajo. Ello se debe a las cada vez más numerosas actividades recreativas entre las personas que trabajan en una empresa, se desarrollen estas dentro o fuera de la jornada o dentro y fuera de la misma empresa. En el precepto habría que entender englobados la organización de torneos deportivos, la promoción de asistencia a gimnasios financiados por la empresa o cualquier otro tipo de celebraciones con la finalidad de mejorar la comunicación, el «clima laboral» y bienestar de las personas trabajadoras de una empresa. Este aspecto pone en evidencia los contornos tan difusos existentes actualmente entre lo social y lo laboral, esto es, las dificultades de deslindar entre las relaciones laborales y sociales, entre lo que queda dentro del ámbito personal y el laboral (De Vicente, 2005).

Podemos observar –y este es un aspecto trascendental en nuestro objeto de análisis– cómo se reconoce y garantiza expresamente en la norma –dedicándole un apartado propio y específico– la protección frente a la violencia y acoso a través de las TIC, de manera que está protegiendo específicamente las formas de violencia y acoso por medio de dispositivos digitales o tecnológicos (art. 3 d). De conformidad con lo dispuesto en este precepto, la protección del convenio comprendería indiscutiblemente el ciberacoso en el trabajo, que puede ocurrir dentro o fuera del lugar de trabajo y que pudiera realizarse indistintamente con medios de titularidad o propiedad de la empresa o con medios individuales o de titularidad propia de la persona trabajadora. La redacción del supuesto es de una gran amplitud, literalmente «en el marco de las comunicaciones que estén relacionadas con el trabajo», siendo únicamente relevante que exista algún vínculo o punto de conexión significativo con el trabajo. En consecuencia, sería merecedora de protección cualquier forma de comunicación tecnológica que pudiera poner en peligro o riesgo la salud, la dignidad o integridad de las personas trabajadoras.

Y, en esta línea, finalmente, el convenio pone también de relieve que todo Estado que lo ratifique deberá respetar, promover y asegurar el disfrute del derecho de toda persona a un mundo del trabajo libre de violencia y acoso (art. 4) y deberá adoptar una legislación que defina y prohíba la violencia y el acoso en el mundo del trabajo, y con un enfoque inclusivo e integrado, primando la faceta o dimensión preventiva (de prevención de riesgos laborales), obligando a las empresas a poner en práctica las políticas oportunas de gestión eficaz frente a la violencia y acoso, comprendiendo, igualmente, también el ciberacoso o acoso por medio de dispositivos digitales. El reconocimiento y garantía de este derecho desde la dimensión preventiva pasamos a abordarlo de forma detallada en el epígrafe siguiente de este estudio.

4. La protección frente a la violencia y acoso digital desde la perspectiva de la prevención de riesgos laborales regulada en el Convenio 190 OIT

El Convenio 190 OIT dedica un capítulo específico (el IV) a la protección y prevención de la violencia y acoso. Por lo que respecta al disfrute del derecho a un entorno laboral libre de violencia y (ciber)acoso desde la perspectiva de la prevención de riesgos laborales, el precepto más relevante y regulador de esta materia es el artículo 9, que dispone expresamente que todo Estado deberá adoptar una legislación que exija a los empleadores tomar medidas apropiadas y acordes con su grado de control para prevenir la violencia y el acoso en el mundo del trabajo.

Y desde esta perspectiva preventiva para combatir la violencia y acoso, el convenio concreta –a modo de listado– que las empresas y organizaciones deberán: a) adoptar y aplicar una política del lugar de trabajo relativa a la violencia y el acoso; b) tener en cuenta la violencia y el acoso, así como los riesgos psicosociales asociados, en la gestión de la seguridad y

salud en el trabajo; c) identificar los peligros y evaluar los riesgos de violencia y acoso, con participación de los trabajadores y sus representantes, y adoptar medidas para prevenir y controlar dichos peligros y riesgos; y d) proporcionar a los trabajadores y otras personas concernidas, en forma accesible, según proceda, información y capacitación acerca de los peligros y riesgos de violencia y acoso identificados, y sobre las medidas de prevención y protección correspondientes.

Si observamos la redacción contenida en este precepto (art. 9) del convenio, podemos afirmar que, en realidad, no existen notables diferencias con lo que se contempla ya en nuestra normativa de prevención, principalmente como se regula en la LPRL. Sin embargo, ello no significa minusvalorar o menospreciar lo consagrado en el Convenio 190 OIT y concluir que esta norma aporte poco o nada a lo que ya viene regulado por nuestra normativa de prevención de riesgos laborales. Sino que, por el contrario, entendemos que el Convenio 190 OIT está incluyendo de forma expresa en la LPRL y reforzando la obligación de desarrollar una protección eficaz ante la violencia y acoso y, por supuesto, frente al ciberacoso en las relaciones de trabajo. Aspecto este que tiene su trascendencia en cuanto existiría en nuestra normativa, en la LPRL, un reconocimiento expreso de los factores y riesgos psicosociales como son la violencia y acoso. Si bien es cierto que un reconocimiento expreso por obra y gracia de esta norma internacional no va a suponer de inmediato garantizar de por sí su puesta en práctica en todas las organizaciones o en el mundo del trabajo en general. Creemos que para ello, esto es, para garantizar una protección eficaz y contar con una auténtica política de empresa en prevención de la violencia y (ciber)acoso, son necesarias acciones de mayor envergadura, de mayor compromiso y sensibilización por parte de todos los interlocutores sociales a la hora de afrontar estos factores de riesgo psicosocial.

Por consiguiente, el Convenio 190 OIT viene a reforzar la importancia de una gestión eficaz e integral en materia preventiva, de tener diseñadas unas políticas de empresa y adoptar medidas para prevenir y controlar tales riesgos (violencia y ciberacoso), puesto que la prevención, tal y como se expuso, debe ser el instrumento más adecuado para evitar que el ciberacoso prolifere en los centros de trabajo. La calificación del ciberacoso como riesgo psicosocial en el trabajo conlleva que los empresarios y las Administraciones públicas respecto del personal a su servicio, en cuanto «deudores de seguridad o de protección», deben actuar para que este riesgo no se produzca, analizando y evaluando el riesgo existente y adoptando cuantas medidas sean necesarias en prevención del mismo, contando con una política de empresa frente a la violencia y (ciber)acoso, con la participación de los trabajadores y sus representantes, a fin de evitar un daño –a la salud, a la dignidad, a la integridad– de las personas trabajadoras, garantizando así un ambiente de trabajo sano y seguro.

Así pues, el empleador –empresario o Administración pública– es responsable de garantizar a sus trabajadores un entorno laboral seguro y libre de riesgos, incluido también, tal y como reconoce el convenio, el «derecho a un entorno laboral libre de violencia y acoso». De esta forma, entre las obligaciones establecidas por nuestra LPRL –en total paralelismo con lo dispuesto en el convenio OIT– cabe entender comprendida la de prevenir la violencia

y el ciberacoso, dado que estos comportamientos representan un serio riesgo psicosocial profesional capaz de ocasionar graves daños sobre la salud de los trabajadores afectados.

De acuerdo con el artículo 14 de la LPRL, como es sabido, es obligación del empresario y de las Administraciones públicas la prevención de los riesgos laborales garantizando «una protección eficaz en materia de seguridad y salud en el trabajo», adoptando en el marco de sus responsabilidades «cuantas medidas sean necesarias» para tal fin, siguiendo un sistema de gestión y planificación de las actividades preventivas y valiéndose de una organización y los medios necesarios. Con estos mismos criterios, sin aportar novedades sustanciales, se manifiesta y reconoce igualmente el Convenio 190 OIT (arts. 4 y 9).

En la misma línea, la Recomendación 206 señala que los Estados deberían especificar en la legislación, según proceda, que los trabajadores y sus representantes deberían participar en la elaboración, la aplicación y el seguimiento de la política del lugar de trabajo mencionada en el artículo 9 a) del convenio, y dicha política debería: a) afirmar que la violencia y el acoso no serán tolerados; b) establecer programas de prevención de la violencia y el acoso, si procede, con objetivos medibles; c) definir los derechos y las obligaciones de los trabajadores y del empleador; d) contener información sobre los procedimientos de presentación de quejas e investigación; e) prever que todas las comunicaciones internas y externas relacionadas con incidentes de violencia y acoso se tengan debidamente en consideración y se adopten las medidas que correspondan; f) definir el derecho de las personas a la privacidad y la confidencialidad, como se establece en el artículo 10 c) del convenio, manteniendo un equilibrio con el derecho de los trabajadores a estar informados de todos los riesgos; y g) incluir medidas de protección de los denunciantes, las víctimas, los testigos y los informantes frente a la victimización y las represalias.

En este sentido, comprobamos que las organizaciones productivas –dentro del marco de la LPRL y de lo que se desprende del Convenio 190 OIT– continúan, en definitiva, teniendo fundamentalmente una doble obligación en materia preventiva:

- La obligación de identificar el riesgo y valorarlo.
- La obligación de adoptar las medidas procedentes para erradicarlo o minimizar este tipo de riesgos.

4.1. La obligación de identificar los peligros y evaluar (valorar) los riesgos de violencia y (ciber)acoso

Una vez que la dirección de la empresa u organización tiene conocimiento de conductas de violencia y acoso, estará obligada a intervenir, analizando la situación y adoptando las medidas correctoras procedentes. En esta valoración de las condiciones objetivas se debía entrar a considerar especialmente las cuestiones de orden o factor organizativo (relaciones

de poder, distribución de roles a mujeres y hombres, formas de organizar el trabajo, relaciones entre personas…) que son en esencia –según el parecer de expertos– las principales causantes de este tipo de conflictos y de agresiones ciberacosadoras.

Por ello, en este mismo sentido, en la evaluación de riesgos en el lugar de trabajo que menciona el artículo 9 c) del Convenio 190 OIT se señala que se deberían tener en cuenta los factores que aumentan las probabilidades de violencia y acoso, incluyendo los peligros y riesgos psicosociales. Y concretamente que debería prestarse especial atención a los peligros y riesgos que: a) se deriven de las condiciones y modalidades de trabajo, la organización del trabajo y de la gestión de los recursos humanos, según proceda; b) impliquen a terceros como clientes, proveedores de servicios, usuarios, pacientes y el público; y c) se deriven de la discriminación, el abuso de las relaciones de poder y las normas de género, culturales y sociales que fomentan la violencia y el acoso (art. 8 Recomendación 206 OIT).

Por otra parte, se hace hincapié en la necesidad de identificar riesgos y evaluarlos en sectores específicos o formas de ejercicio de la actividad laboral más expuestos a estos riesgos, exigiendo a los Estados la adopción de medidas apropiadas para los sectores o las ocupaciones y las modalidades de trabajo más expuestos a la violencia y el acoso, tales como «el trabajo nocturno, el trabajo que se realiza de forma aislada, el trabajo en el sector de la salud, la hostelería, los servicios sociales, los servicios de emergencia, el trabajo doméstico, el transporte, la educación y el ocio» (art. 9 Recomendación 206 OIT).

A estos sectores habría que adicionar los sectores profesionales específicos que sufren ciberacoso, entre los que se encuentran el profesorado, personal médico-sanitario, personal de medios de comunicación, personal político, teletrabajadores… y otros tantos a los que hemos hecho referencia anteriormente.

4.2. La obligación de adoptar las medidas de prevención y protección para erradicar o minimizar los riesgos de violencia y (ciber)acoso

Estas medidas pueden ser de diferentes modalidades y de mayor o menor calado, en correspondencia con las que se refieren en el propio Convenio 190 OIT. En el marco de la política de prevención de riesgos laborales, la dirección de la empresa, esencialmente, debe:

1.º Delimitar adecuadamente cuáles son las actitudes y situaciones consideradas como de violencia y acoso digital en el trabajo. Determinar a modo de catálogo o inventario cuáles son las conductas constitutivas de acoso cibernético. Definir qué se entiende por violencia digital y ciberacoso en el mundo del trabajo, considerándose para ello esencial por su utilidad la definición que nos proporciona el Convenio 190 OIT y la Ley orgánica 3/2007, de 22 de marzo, para la igualdad

efectiva entre mujeres y hombres (LOIMH). Asimismo, es trascendental impulsar una política educativa de concienciación y sensibilización frente a esta nueva forma de acoso. En esta misma línea de delimitación e identificación de conductas, el Convenio 190 OIT dispone la obligación de «proporcionar a los trabajadores y otras personas concernidas, en forma accesible, según proceda, información y capacitación acerca de los peligros y riesgos de violencia y acoso identificados».

2.º Prohibir de forma tajante y expresa dicho tipo de conductas, dejando constancia clara de que los comportamientos considerados como de violencia y (ciber) acoso no serán permitidos en el seno de la empresa y serán objeto de su oportuna atención y debida sanción. En definitiva, tolerancia cero frente a la violencia y las diferentes manifestaciones de ciberacoso en el entorno de trabajo. Si bien no podrán únicamente limitarse a la prohibición expresa de estas conductas de violencia y acoso digital, sino que será necesario incluir expresamente procedimientos o protocolos específicos para prevenirlas o, por lo menos, reducir los daños derivados de las agresiones (daños a la dignidad, integridad, intimidad, no discriminación y salud de las personas trabajadoras).

3.º Adoptar las medidas precisas para establecer canales y procedimientos adecuados de comunicación y denuncia. Esto significa que las personas trabajadoras puedan recibir y aportar la información necesaria (también de forma anónima) sobre la existencia de ciberacoso en la empresa, incluso dando facilidades de comunicación y manifestando que, si alguna persona trabajadora se cree víctima de esa situación, lo ponga de inmediato en conocimiento de la empresa. Investigar y tratar de eliminar o reducir el factor contaminante o tóxico del entorno laboral desde el primer momento (incluso en ausencia de denuncia) es una acción considerada fundamental para su erradicación o disminución. En este sentido, el Convenio 190 OIT incide en este aspecto al establecer la obligación de garantizar un fácil acceso a vías de recurso y reparación apropiadas y eficaces y a mecanismos y procedimientos de notificación y de solución de conflictos en los casos de violencia y (ciber)acoso en el mundo del trabajo, que sean seguros, equitativos y eficaces (art. 10 b). Y entre ellos menciona:

- Procedimientos de presentación de quejas e investigación y, si procede, mecanismos de solución de conflictos en el lugar de trabajo.
- Mecanismos de solución de conflictos externos al lugar de trabajo (en referencia a la tutela administrativa).
- Juzgados o tribunales (en referencia a la tutela judicial).
- Medidas de protección de los querellantes, las víctimas, los testigos y los informantes frente a la victimización y las represalias.
- Medidas de asistencia jurídica, social, médica y administrativa para los querellantes y las víctimas.

Y teniendo en especial consideración la dimensión de género, al indicar específicamente que se debe prever que las víctimas de violencia y acoso por razón de género en el mundo del trabajo tengan acceso efectivo a mecanismos de presentación de quejas y de solución de conflictos, asistencia, servicios y vías de recurso y reparación que tengan en cuenta las consideraciones de género y que sean seguros y eficaces; así como reconocer los efectos de la violencia doméstica (en clara referencia a lo que nosotros denominamos «violencia de género») y, en la medida en que sea razonable y factible, mitigar su impacto en el mundo del trabajo (art. 10 e) y f) Convenio 190 OIT).

Asimismo, el artículo 10 g) del Convenio 190 OIT reconoce el derecho de resistencia de los trabajadores (*ius resistentiae*) ante situaciones de riesgo grave e inminente por violencia y acoso (en correspondencia con lo preceptuado en nuestra norma preventiva en el art. 21 LPRL) al señalar que los Estados deberán:

> Garantizar que todo trabajador tenga el derecho de alejarse de una situación de trabajo sin sufrir represalias u otras consecuencias indebidas si tiene motivos razonables para considerar que esta presenta un peligro grave e inminente para su vida, su salud o su seguridad a consecuencia de actos de violencia y [ciber]acoso, así como el deber de informar de esta situación a la dirección.

Y en conexión con lo ordenado en este precepto (y con lo preceptuado en el art. 44 LPRL), se establece igualmente la obligación de velar por que la Inspección de Trabajo y otras autoridades pertinentes estén facultadas para actuar en caso de violencia y acoso en el mundo del trabajo, incluyendo el dictado de órdenes que requieran la adopción de medidas de aplicación inmediata, o que impongan la interrupción de la actividad laboral en caso de peligro inminente para la vida, la salud o la seguridad de los trabajadores, a reserva de cualquier recurso judicial o administrativo que pueda prescribir la legislación (art. 10 h) Convenio 190 OIT).

4.º Deberá informar y formar suficiente y adecuadamente a trabajadores, a directivos y mandos intermedios sobre violencia y acoso digital, para que sean capaces de detectarlo y, si se produce algún supuesto, actuar en consecuencia. La formación deberá estar adaptada al nivel de responsabilidad y competencias que se tengan en la empresa. En este sentido, el artículo 11 b) del Convenio 190 OIT señala expresamente que:

> Se proporcionen orientaciones, recursos, formación u otras herramientas sobre la violencia y el acoso en el mundo del trabajo, incluyendo la violencia y el [ciber]acoso por razón de género, a los empleadores y a

los trabajadores y a sus organizaciones respectivas, así como a las autoridades competentes, en forma accesible, según proceda[9].

Obligación de información y de formación que se refuerza incidiendo el convenio en la obligación de «proporcionar a los trabajadores y otras personas concernidas, en forma accesible, según proceda, información y capacitación acerca de los peligros y riesgos de violencia y acoso identificados».

5.º Todas estas obligaciones descritas se suelen condensar –en muchos casos– en los denominados «protocolos de actuación y prevención frente al acoso» (moral, sexual, sexista, discriminatorio) donde deberemos incluir de manera específica y concreta también la violencia y acoso digital laboral o ciberacoso (art. 48 LOIMH). En consecuencia, deben adecuarse las políticas internas de gestión de tales riesgos y de usos sociales razonables sobre los modos de conducta en redes sociales que tienen por finalidad fomentar un clima de respeto y tolerancia en el entorno laboral, garantizando la salud psicosocial de los riesgos asociados a las TRIC y, al mismo tiempo, cuidando la reputación social y productividad empresarial.

Aquí podemos traer a colación la protección a través de la Ley orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales (LOPDGDD), en desarrollo del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales (Preciado, 2019). En el artículo 88 de la LOPDGDD (en conexión con los arts. 20 bis Estatuto de los Trabajadores y 14 j) bis Estatuto Básico del Empleado Público) se indica claramente que los empleadores deberán establecer criterios de utilización de los dispositivos digitales, esto es, tener establecidas en la empresa políticas de uso razonable de las nuevas tecnologías de la información y de la comunicación (NTIC). Ello acorde con la obligación recién referenciada de educación-capacitación de sus empleados en el uso responsable de las NTIC, pues se debe «proporcionar a los trabajadores y otras personas concernidas, en forma accesible, según proceda, información y capacitación acerca de los peligros y riesgos de violencia y acoso identificados, y sobre las medidas de prevención y protección correspondientes […]» en relación con la aplicación de estas políticas empresariales.

Los protocolos está claro que no garantizan la prevención eficaz y en su totalidad del ciberacoso, pero es cierto que su inexistencia en las organizaciones productivas

[9] Y en la Recomendación 206 OIT (art. 23 d) se establece que los Estados deberán elaborar, aplicar y difundir:

> Campañas públicas de sensibilización […] que hagan hincapié en que la violencia y el acoso, en particular la violencia y el acoso por razón de género, son inaceptables, denuncien las actitudes discriminatorias y prevengan la estigmatización de las víctimas, los denunciantes, los testigos y los informantes.

aumenta el riesgo de sufrirlo y la gravedad de los daños (Sentencia del Tribunal Superior de Justicia –STSJ– del País Vasco 1809/2015, de 6 de octubre).

Y es que, actualmente, aunque existen por parte de las organizaciones productivas –públicas y privadas– numerosas actuaciones y protocolos de gestión de la prevención del acoso en general, debe instarse a los poderes públicos –al legislador, fundamentalmente– y a los agentes sociales negociadores e interlocutores de estos protocolos preventivos del acoso a que incorporen explícitamente el tratamiento de la violencia digital y el ciberacoso en el trabajo, con el fin de poder combatir el problema desde su origen como se merece y de la manera más eficaz posible. En este sentido, se ha demandado por parte de UGT una regulación específica para combatir el ciberacoso laboral y ha destacado el Protocolo general de actuación, firmado en septiembre de 2019 por el Ministerio de Trabajo y la Agencia Española de Protección de Datos, que insta a los agentes sociales a que, a través del diálogo social, acuerden un protocolo específico para actuar en el supuesto de acoso digital en el trabajo.

6.º Si se comprueba la existencia de violencia y acoso digital en la empresa, deberán aplicarse las medidas disciplinarias adecuadas en función de la gravedad del caso de que se trate, que podrá llegar a sancionarse con despido si la gravedad del acoso lo hiciera necesario, y todo ello de conformidad con lo dispuesto en el artículo 10 d) del Convenio 190 OIT, que establece la obligación de «prever sanciones, cuando proceda, para los casos de violencia y acoso en el mundo del trabajo».

El ordenamiento jurídico laboral contempla una doble responsabilidad del empresario respecto de las conductas de acoso digital o ciberacoso laboral. De un lado, existiría una responsabilidad por acción, como consecuencia de una conducta activa del propio empresario o de sus empleados; y de otro, una responsabilidad por omisión, resultante de la inactividad del empresario por consentir y no adoptar las medidas preventivas y protectoras necesarias para evitar conductas de acoso a través del uso de TRIC. Una política activa ejemplar y disuasoria contra el acoso denunciado tiene un efecto de exclusión o, al menos, de reducción de la responsabilidad empresarial (STC 250/2007).

Por otra parte, cada vez son más frecuentes los pronunciamientos judiciales que estiman la responsabilidad de las empresas por falta de medidas preventivas de los riesgos psicosociales o de total ausencia de gestión preventiva de entornos de naturaleza psicosocial tóxicos (STC 56/2019), e incluso en supuestos en los que exista o no una situación real de acoso.

Otro instrumento para prevenir y actuar frente al acoso por medios tecnológicos o digitales es la inclusión en la normativa interna de las organizaciones productivas, a modo de políticas internas de empresa, de normas éticas o códigos éticos o de conducta, esto es, de concretas obligaciones y compromisos, a modo de «buenas prácticas» o guías en relación con el proceder de la persona trabajadora en

el momento de emitir opiniones, comentarios o manifestaciones que se pudieran publicar en internet y en las redes sociales (fuera o dentro de la empresa). Según un estudio de Manpower, solo un 20 % de las empresas encuestadas a nivel mundial contaban con una política formal sobre el uso de internet y de redes sociales. En nuestro país, el porcentaje de empresas que contaban con un mecanismo de actuación frente al uso de redes sociales se reducía a un escaso 10 %.

La tecnología amplifica y potencia el daño, por ello la sugerencia o recomendación suele ser que cualquier empresa debe tener un protocolo, reglamento o documento de funcionamiento con respecto al uso de los canales corporativos sociales y también, y muy importante, respecto a lo que puede y debe hacer cada persona en su ejercicio libre de expresión con sus cuentas en redes sociales.

Dichos protocolos deben ser informados a cada persona y deben estar accesibles para ser consultados. Los códigos internos de usos de las redes sociales son protocolos de presencia en redes sociales con pautas de relación de los empleados con los canales corporativos e indicaciones sobre el uso de los canales personales fuera de un entorno laboral. Las empresas deberán tener un criterio claro definido sobre cómo actuar. Si bien es importante tener presente que se admite que el trabajador en redes pueda realizar comentarios, emitir opiniones, escribir textos o difundir imágenes en el ejercicio de su derecho a la libertad de expresión, siempre que no descalifiquen a la empresa o a personas vinculadas con esta. En consecuencia, no se puede prohibir genéricamente que se emitan declaraciones o comentarios por parte de los trabajadores en redes sociales ajenos a la empresa o sobre la realidad de sus condiciones de trabajo.

En este sentido, el artículo 87.3 de la LOPDGDD, en relación con el ejercicio del derecho a la intimidad y el uso de dispositivos digitales en el ámbito laboral (Orellana, 2019) –en clara referencia a instrumentos digitales propiedad de la empresa de uso privado por los trabajadores–, recoge expresamente que:

> Los empleadores deberán establecer criterios de utilización de los dispositivos digitales respetando en todo caso los estándares mínimos de protección de su intimidad de acuerdo con los usos sociales y los derechos reconocidos constitucional y legalmente y que en su elaboración deberán participar los representantes de los trabajadores.

Además, para reforzar el papel que desempeñan los representantes legales, incide en que «los convenios colectivos podrán establecer garantías adicionales de los derechos y libertades relacionados con el tratamiento de los datos personales de los trabajadores y la salvaguarda de derechos digitales en el ámbito laboral» (art. 91). Por consiguiente, por medio de la negociación colectiva podrán desarrollarse estas políticas de uso razonable de las TIC a los efectos de evitar agresiones en red.

Afortunadamente son cada vez más numerosos los convenios colectivos que recogen una perspectiva preventiva del acoso, promoviendo procedimientos específicos de gestión de los conflictos psicosociales. Ahora, el paso siguiente es que esos mismos convenios colectivos tengan en cuenta y regulen los supuestos de ciberacoso o acosos cibernéticos.

5. Conductas y prácticas comunes de violencia y acoso digital en el trabajo: doctrina judicial actual en materia de violencia y ciberacoso laboral

La violencia digital laboral es, lamentablemente, un fenómeno cada vez más presente en nuestras organizaciones. La violencia laboral a través de dispositivos digitales de todo tipo y naturaleza es hoy en día cada vez mayor y prueba de ello son los numerosos pronunciamientos judiciales. La realidad es que las tensiones, las agresiones, las diferentes formas de acoso (moral, sexual, sexista, discriminatorio…) forman ya parte de la vida laboral digital de muchos centros de trabajo y el Convenio 190 OIT, desde esta perspectiva preventiva, debe servir de instrumento firme para tratar de erradicarlas o reducirlas a la mínima expresión. Todos estos comportamientos y conductas que vamos a exponer se producen actualmente a través de dispositivos tecnológicos que generan indiscutiblemente un clima o ambiente tóxico de trabajo con importantes repercusiones en la dignidad, intimidad y salud de las personas trabajadoras, afectando a las relaciones de trabajo y a la propia productividad de la empresa.

Los supuestos existentes de violencia y ciberacoso son amplísimos. Y es difícil realizar un listado –cerrado y definitivo– de todas y cada una de las conductas o comportamientos de violencia digital y acoso cibernético que se producen. Además, el propio desarrollo de las TRIC, tan avanzado y tan rápido, conlleva necesariamente que cada poco tiempo los ciberacosadores encuentren nuevas formas de intimidar y hostigar a través de la red.

Los supuestos que se exponen a continuación están extraídos, en algunos casos, de pronunciamientos judiciales (en su mayoría de tribunales laborales y penales), pero también hay otros supuestos que se han producido y, a pesar de su existencia, no han llegado formalmente a los tribunales, entre otras razones, por ausencia o falta de denuncia.

Debemos partir de la idea de que hay conductas que, aunque tienen su trascendencia o dimensión laboral –en ocasiones, merecedoras de una sanción laboral como pudiera ser el despido–, no siempre debemos identificarlas o considerarlas a todas como auténticas conductas o situaciones de violencia digital y ciberacoso laboral. Entre otras razones porque en determinados casos y circunstancias se exigiría cierta reiteración en la conducta (así como otros elementos o presupuestos definitorios de este tipo de conductas) y una gravedad para afectar en cierta medida a la salud, la integridad y dignidad de las personas víctimas que han

sido hostigadas, ofendidas o injuriadas. A menudo detrás de muchos comportamientos en redes se evidencia la existencia de entornos laborales enrarecidos y de excesiva conflictividad laboral que, sin poder ser calificados de auténticos supuestos de acoso digital o cibernético, sí son situaciones que indiscutiblemente deberán ser tenidas en cuenta desde una protección integral y una gestión eficaz de los entornos laborales, tal y como promueve el Convenio 190 OIT.

Con estas advertencias, presentamos a continuación una muestra de las prácticas que podemos considerar más comunes de violencia digital y acoso en red que se han producido (o pudieran producirse) en las empresas y, en general y por extensión, en el ámbito de las relaciones de trabajo.

5.1. Difundir en internet imágenes o datos delicados de la víctima

La conducta ilícita consiste en distribuir o difundir en internet una imagen comprometida –que puede ser real o trucada– o datos susceptibles de perjudicar a la víctima. Se trata de subir a internet una imagen comprometida, así como otros datos personales delicados que pueden perjudicar o avergonzar a la víctima, y darlos a conocer en su entorno de relaciones personales o profesionales.

La manipulación de fotografías del acosado o acosada es otro medio o práctica bastante frecuente; el acosador puede retocar o modificar una imagen con el objetivo de subirla a diferentes espacios de internet con la finalidad de herir, asustar y menoscabar la dignidad de su víctima. En este sentido, hablamos de extorsión cuando las fotografías o vídeos (que pueden ser de contenido íntimo-sexual o no) en manos de la persona inadecuada pueden constituir un elemento para extorsionar o chantajear a la persona protagonista de esas imágenes. El chantaje consiste en la utilización de tales imágenes para obtener algo de la víctima amenazando con su publicación.

A esta modalidad de extorsión en red también se la conoce como «pornovenganza» (*revenge porn*) o venganza sentimental, consistente en la publicación –a través de la telefonía móvil o cualquier otro dispositivo de mensajería instantánea– de fotografías o vídeos íntimos de la expareja una vez terminada la relación afectiva o sentimental. Son los supuestos denominados o considerados como de *sexting* o de sextorsión.

Sexting es una palabra tomada del inglés que une «*sex*» (sexo) y «*texting*» (envío de mensajes de texto vía SMS desde teléfonos móviles). Aunque el sentido original se limitase al envío de textos, el desarrollo de los teléfonos móviles ha llevado a que actualmente este término se aplique al envío, especialmente a través del teléfono móvil, de fotografías y vídeos con contenido íntimo, tomadas o grabados en ocasiones por las propias personas protagonistas de los mismos.

Un caso conocido de pornovenganza en el ámbito laboral (Sentencia del Juzgado de lo Penal núm. 17 de Barcelona de 8 de enero de 2018, proc. abreviado 143/2012) fue el del subinspector de la Guardia Urbana de Barcelona, quien fue juzgado por haber difundido una foto de carácter sexual con su expareja, también agente de la Guardia Urbana, para vengarse de ella por haber puesto fin a su relación. La imagen fue enviada por el subinspector a todos los contactos de la agente compañera[10].

El *sexting* en sí mismo no es una figura delictiva, lo que se penaliza –y así se ha tipificado como delito en nuestro Código Penal– es la difusión de esas imágenes íntimas sin autorización de la persona afectada y cuando la divulgación menoscabe gravemente la intimidad de la persona que envió las fotografías o vídeos. El supuesto de *sexting* más estremecedor ocurrido en nuestro país fue el de la trabajadora de la empresa Iveco que se suicidó en su casa, tras llevar más de 1 mes bajo presión por estar circulando entre sus compañeros de trabajo unos vídeos sexuales en los que ella aparecía con su expareja, con la que tuvo una relación sentimental 5 años atrás. Durante más de 10 días, la trabajadora tuvo que soportar por los pasillos de su puesto de trabajo cómo resonaban las burlas, risas y comentarios de compañeros del centro y cómo se acercaban a su puesto de trabajo para cerciorarse de que era ella la que salía en las imágenes. El vídeo se difundió viralmente, circulaba de móvil a móvil a la velocidad de la luz y cada vez entre un mayor número de compañeros[11]. Un supuesto de *sexting* con uno de los finales más dramáticos posibles como es la muerte de la persona[12].

5.2. Dar de alta en espacios web para ridiculizar o estigmatizar a la víctima

Otra práctica ilícita frecuente consiste en dar de alta a la víctima en un sitio o espacio web de internet donde puede estigmatizarse y ridiculizarse a la víctima como persona. Puede

[10] Un caso reciente de sextorsión conocido y proveniente de personas ajenas y externas al entorno laboral ha sido el del entrenador del Málaga, CF, que, además de padecer la difusión de un vídeo íntimo personal, le causó, lamentablemente, el despido al trabajador por parte de la dirección del club.

[11] Tras cumplirse 1 año del suceso, el Juzgado de lo Penal número 5 de Alcalá de Henares ha sobreseído provisionalmente el caso por «falta de autor conocido» del delito de descubrimiento y revelación de secretos al no poderse identificar la primera persona responsable de divulgar el vídeo y porque no había denuncia en el delito de trato degradante por el que investigaba la jueza. Queda pendiente de resolverse la investigación que la Inspección de Trabajo abrió después de que CC. OO. Industria de Madrid presentara una denuncia contra Iveco España al considerar que no aplicó el protocolo de acoso ni cumplió con la LPRL, a pesar de tener conocimiento por la propia víctima de lo que estaba sucediendo.

[12] El *sexting* se ha tipificado como delito en nuestro actual Código Penal tras la reforma de 2015, concretamente en su artículo 197.7, castigando a quien, sin autorización de la persona afectada, difunda, revele o ceda a terceros imágenes o grabaciones audiovisuales de aquella que hubiera obtenido con su anuencia y cuando la divulgación menoscabe gravemente la intimidad personal de esa persona.

servir como ejemplo una web donde se escogen determinadas cualidades de la persona (inteligencia, atractivo, aspecto físico, etc.) presentando la posibilidad de cargarla del máximo número de votos o puntos por parte de los que visiten ese espacio web. También recibe el nombre de «web apaleador», esto es, web creada a propósito para agredir a la víctima, menospreciándola de manera pública y con el claro objetivo de ridiculizarla. De esta forma y desde este espacio en internet se anima a los participantes que acceden a que hostiguen e intimiden a la víctima[13].

5.3. Usurpar la identidad de la víctima y en su nombre realizar comentarios ofensivos

El comportamiento supone usurpar la identidad de la víctima y, en su nombre y desde el anonimato, hacer comentarios ofensivos o participaciones inoportunas en chats, en redes u otras plataformas digitales, de tal modo que despierte reacciones adversas hacia quien en verdad es la víctima. La identidad de la persona en estos casos queda totalmente en entredicho. La persona ciberacosadora emite opiniones o comentarios en red en nombre de la víctima con la finalidad de insultar o desprestigiar.

El procedimiento consiste en acceder de forma ilegal a la cuenta de correo electrónico, red social, chat o red de mensajería instantánea, suplantando la identidad de la víctima para los fines expuestos e incluso insultar a los contactos de la víctima misma.

En la Sentencia del Juzgado de lo Social número 1 de Cartagena (Murcia) 517/2011, de 6 de julio, se justificó el despido de un trabajador que procedió a crear un perfil en la red social Facebook a nombre de un superior jerárquico, sin su conocimiento ni consentimiento, utilizando sus datos personales y emitiendo en su nombre expresiones objetivamente injuriosas sobre la empresa en la que ambos prestaban sus servicios, con la intención de difundirlas.

En la STSJ de Galicia 977/2012, de 23 de febrero, un trabajador publicó un vídeo en un blog subtitulando la famosa escena de la película *El hundimiento*, identificando a Hitler con el administrador único de la compañía; en su discurso ficticio este administrador insultaba a los trabajadores de la empresa y admitía haber sobornado a algunos clientes.

[13] Estas prácticas recuerdan los orígenes de Facebook, pues siendo su fundador estudiante en Harvard creó una página web ilegal –denominada Facemash (germen del actual Facebook)– con el objetivo de comparar a mujeres en virtud de su atractivo físico, creando una competición donde había que votar a la más atractiva o sensual. Por estas prácticas fue acusado de violar la seguridad del campus, infringir derechos de autor por el uso de las fotos y lesionar la privacidad de los estudiantes.

5.4. Acceder a dispositivos tecnológicos y usurpar información personal de la víctima

Estaríamos ante la figura más cercana del denominado «*hacking*», en referencia a todos aquellos supuestos posibles de monitorización de los actos de la víctima, al objeto de robar datos y rastrear movimientos por la red o a través de programas espía para vigilar llamadas y, en general, para el control de todas y cada una de las actividades que realizan sus víctimas.

En ocasiones, la conducta consiste en entrar o asaltar el correo electrónico, el ordenador o cualquier otra herramienta o dispositivo tecnológico de la víctima e incluso de sus familiares (tableta, teléfono móvil, etc.) accediendo a todos sus mensajes, archivos y demás datos personales y colgar en la red sus documentos, audios e imágenes (vídeos, fotos) de carácter privado.

5.5. Realizar en redes sociales comentarios ofensivos, opiniones y declaraciones insultantes o amenazantes

Lamentablemente, es esta una de las prácticas más comunes en la red y que ha supuesto su aparición y tratamiento en numerosos pronunciamientos judiciales. Consiste, fundamentalmente, en enviar mensajes ofensivos y hostigadores a través de *e-mails*, SMS, tuits, wasaps, o redes sociales o espacios de internet, en general, que utilizan habitualmente la víctima y compañeros de trabajo e incluso terceras personas ajenas a la empresa u organización. Si hacemos un recorrido por los pronunciamientos de nuestros tribunales, nos encontramos en la actualidad con los casos siguientes:

En la STSJ de Castilla y León/Valladolid 435/2010, de 21 de abril, se calificó como procedente un despido por el hecho de proferir amenazas –bajo el seudónimo «la Cosa Nostra»– en un foro de internet a un directivo (jefe de personal) de la empresa en la que trabajaba. Como señala la mencionada sentencia: «no estamos propiamente ante una expresión de ideas u opiniones, legítimas o no, ni ante la transmisión de información, veraz o no, sino ante un llamamiento a la intimidación de un directivo de la empresa».

En la STSJ de Galicia 4798/2014, de 8 de octubre, se declara procedente el despido de un trabajador que presta servicios en la Casa Sacerdotal de la Diócesis de Ourense por publicar en Facebook expresiones que incluso «bien pudieran integrarse en la calumnia». Otros pronunciamientos de nuestros tribunales en los que el trabajador es despedido por comentarios en Facebook graves e injuriosos con insultos a superiores o responsables de la empresa los localizamos en las SSTSJ de Aragón 350/2016, de 18 de mayo, y de Cataluña 6585/2015, de 6 de noviembre. En esta última, se observa un caso típico de menosprecio y trato denigrante de la compañera de trabajo por su mera condición de mujer (la llama «sinvergüenza» y «zorra»), por lo que podríamos estar ante un supuesto, desgraciadamente bastante común en redes, que podríamos calificar o catalogar de ciberacoso laboral sexista o de violencia sexista.

En la STSJ de Murcia 278/2014, de 31 de marzo, se declaró procedente el despido de una persona trabajadora por injurias a la empresa a la que calificó de «tirana» y de acosar a trabajadores y robarles su prestación de incapacidad temporal. En otras ocasiones, los comentarios por red no tienen la entidad o gravedad suficiente para ser merecedores de despido, como el caso de la trabajadora que hizo comentarios burlones en su red de Facebook respecto a la pregunta de un cliente sobre si en la empresa retocaban fotos a fin de eliminar granos de la cara.

En la STSJ de Andalucía/Málaga 817/2014, de 22 de mayo, se declara procedente el despido de un trabajador por colgar en el muro de Facebook varios comentarios críticos, con expresiones injuriosas y amenazantes, dirigidos a la empresa en general y a una compañera de trabajo, tales como «esta hija de puta ha jugado con la comida de mis hijos siendo mentira todo lo que ha hecho […] es una rastrera de mierda».

En la STSJ de Cataluña 5613/2015, de 30 de septiembre, el tribunal declara igualmente procedente un despido porque una trabajadora envió expresiones vejatorias e insultos a una compañera vía telefónica y por WhatsApp, y a la hija de esta última a través de su cuenta en la red social Facebook; a lo que se añadieron ofensas verbales y escritas que dirigió a compañeros de trabajo.

En la STSJ de Murcia 448/2017, de 26 de abril, se declara la procedencia del despido al darse los requisitos de gravedad y culpabilidad necesarios, pues la trabajadora a través de Facebook y de una entrevista de radio profirió ofensas verbales al gerente de la empresa, extralimitándose en el ejercicio de su derecho a la libertad de expresión, siendo el motivo u origen de las descalificaciones el impago de los salarios de varios meses y el silencio de la empresa frente a las protestas de las trabajadoras.

Otro caso significativo es el de la STSJ de Cataluña 191/2016, de 3 de marzo, en donde un trabajador fue despedido por motivos disciplinarios. El trabajador, cantante del Gran Teatro del Liceo de Barcelona y encontrándose en situación de excedencia voluntaria, realizó desde su cuenta de Facebook distintas manifestaciones y comentarios contra la entidad y algunos trabajadores de la misma. El tribunal analiza las distintas manifestaciones vertidas por el actor y los términos usados para realizar las denuncias de determinadas actuaciones y maneras de proceder por parte del Gran Teatro del Liceo. A este respecto, la sala las califica de malsonantes y sacadas de contexto, desagradables y «sin duda reprochables moralmente», pero refiere a continuación que las mismas han de valorarse teniendo en cuenta la situación en la que se encontraba el actor, el momento y las circunstancias en que se llevaron a cabo, en definitiva, valorar si las mismas tenían o no un claro ánimo de injuriar o, por el contrario, se hicieron con el simple ánimo de crítica o denuncia.

Un tema relacionado con esto, y actualmente nada pacífico, es el relativo al control empresarial de las actuaciones y comportamientos del trabajador en las redes sociales y cómo afecta al ejercicio del derecho a la libertad de expresión del trabajador, esto es, si una empresa puede sancionar también por emitir el trabajador opiniones personales en redes sociales

que nada tienen que ver con la empresa o con la relación laboral, pues se han considerado ilegítimos los controles empresariales ilimitados de la actividad del trabajador en internet por el hecho de haber incluido una cláusula en el convenio colectivo, acuerdo o código de conducta que sanciona la realización de comentarios que puedan vulnerar la imagen o reputación de la empresa, y se ha llegado a estimar inadmisible un control injustificado de las publicaciones de los trabajadores en la red, sin que se limite, claramente, su libertad de expresión (Serrano, 2019).

En este sentido, se admite que el trabajador pueda realizar comentarios, emitir opiniones, escribir textos o difundir imágenes que no descalifiquen a la empresa o a personas vinculadas con esta, caso de compañeros, directivos o responsables. De esta forma, los trabajadores pueden revelar sus auténticas condiciones de trabajo en las redes sociales sin vulnerar la imagen, el honor o la reputación de la empresa y siempre que la crítica se haga sin que se propague al exterior y quede en el ámbito interno de la empresa, sin repercusión de terceros, tal y como entiende la STSJ de Madrid 883/2013, de 16 de diciembre. Por consiguiente, no se puede prohibir genéricamente que se emitan declaraciones o comentarios por parte de los trabajadores en redes sociales ajenos a la empresa o sobre la realidad de sus condiciones de trabajo.

Y así, en la STSJ de Navarra 45/2014, de 21 de febrero, el tribunal, aplicando la teoría gradualista, estima improcedente el despido por los comentarios en Twitter de un trabajador descalificantes sobre la forma de proceder de la empresa en situaciones de conflicto ante el agravamiento de las condiciones laborales, pues «no parece que dichos comentarios hayan llegado a tener la publicidad y extensión suficiente para haber llegado a ser conocidos por el gran público y llegar a dañar la imagen de la compañía ante proveedores y clientes».

En la STSJ de Andalucía/Málaga 86/2018, de 17 de enero, el tribunal admite la nulidad del despido de una trabajadora por vulneración de los derechos de libertad de expresión y de libertad sindical de la trabajadora. La trabajadora había sido despedida por comentarios en Facebook llamando al gerente de la empresa «dueño del cortijo» y a los trabajadores «palmeros». En otro supuesto, se condenó a un ayuntamiento por vulnerar la dignidad y libertad sindical de un delegado sindical por los comentarios proferidos por el jefe de personal en una red social criticando el uso que hacía del crédito horario, diciendo del delegado sindical que «[…] el liberado sindical conocido como el chicharra, es una pérdida de tiempo, es un caso perdido, un especialista en vivir del cuento y del chismorreo».

En la STSJ de Andalucía/Granada 1647/2016, de 30 de junio, la trabajadora de un ayuntamiento es despedida por manifestaciones en el perfil de Facebook contra el alcalde y el equipo de gobierno. El tribunal, en este caso, califica el despido de improcedente por considerar que existe falta de proporcionalidad en la sanción impuesta a la trabajadora al considerar que existe un derecho a criticar y escrutar las acciones y actitudes de esos funcionarios en lo que atañe a la función pública. La trabajadora se ha limitado a llevar a cabo una opinión personal y dichas expresiones ni son ofensivas ni merecen la sanción impuesta.

En la STSJ de Castilla-La Mancha 443/2016, de 8 de abril, el trabajador fue despedido por publicar comentarios ofensivos de claro contenido sexual y sexista respecto de otras compañeras en Facebook («y el resto del día, lo he dedicado a ver a Amparo y Felicidad […] y a pensar cositas guarras, hasta que me ha dicho el compañero que sudaba mucho y, claro, el mono cada vez más apretado […]») a sabiendas de que eran esposas de empleados de la empresa e incitando a que entrasen a leerlo en esta red social. De ahí la importancia que tiene la protección especial de la calidad de clima laboral en relación con las mujeres en el trabajo, como recoge la STSJ de Canarias/Las Palmas 246/2018, de 6 de marzo.

En la STSJ de Andalucía/Sevilla 932/2017, de 23 de marzo, un jefe de sección realiza un comentario y ofensas de contenido tan obsceno de una empleada en una foto del muro de Facebook que justifican el despido inmediato del mismo («joder… Ascensión q ganas d follarte bien y que chilles xq t estoy partiendo el coño en dos»). Las expresiones se consideran tan soeces y de tal envergadura que justifican la procedencia del despido y por crear un entorno claro y manifiestamente ofensivo para la trabajadora. En el derecho irlandés, sirva como ejemplo, un comentario en redes de naturaleza obscena –fuera del trabajo y en tiempo de ocio del trabajador– es considerado acoso sexual. Se trata del caso Teggart vs. TeleTech UK Limited[14], en el que un trabajador de un *call center* fue despedido después de hacer comentarios ofensivos sobre una compañera en Facebook. Los comentarios sugerían que la empleada había sido sexualmente promiscua con otros compañeros. Tras una investigación formal y exhaustiva por parte de la compañía, Teggart fue despedido por mala conducta, por perjudicar la reputación de la compañía –se calificó su conducta de un grave y culpable incumplimiento de la política de empresa– y por haber acosado en redes a su compañera de trabajo.

En la STSJ de Galicia de 29 de mayo de 2019 (rec. 682/2019), el trabajador, mientras recrimina a su responsable de personal por una encerrona que había sufrido en una reunión, graba con el móvil a su compañero de trabajo que estaba practicando marcha deportiva, quien no le autoriza la grabación solicitándole que deje de grabar y ante tal situación persecutoria y acosadora se ve obligado a marcharse cogiendo un taxi. El trabajador subió el contenido del vídeo a Facebook con la finalidad de hacerlo público, vídeo que circuló por diversos grupos de WhatsApp de trabajadores del centro de trabajo teniendo posteriormente el responsable de personal que someterse a burlas y comentarios jocosos del resto de compañeros.

Como podemos comprobar, los aspectos que se tienen en cuenta para justificar la procedencia o no del despido son: 1) si se han utilizado expresiones ofensivas o injuriosas; 2) cómo se han realizado, si son verbales o por escrito; 3) el lugar y contexto en el que los comentarios o expresiones se han hecho; y 4) el alcance y difusión de tales manifestaciones o comentarios.

[14] <http://www.xperthr.co.uk/editors-choice/call-centre-worker-fairly-dismissed-for-offensive-facebook-comments-about-colleague/112847/>.

En consecuencia, observamos que, con el tiempo, comienza a existir una doctrina judicial en nuestro país que, aplicando la teoría gradualista, trata de valorar diferentes elementos tales como la gravedad de la conducta, el tiempo y el lugar de la infracción, la publicación y el grado de difusión o extensión, entre otras circunstancias, a la hora de calificar la existencia o no de un incumplimiento laboral que pudiera acarrear la sanción de despido del trabajador.

5.6. Acciones de presión para actuar conforme a las solicitudes del acosador digital

Se trata de acciones de presión permanente a través de TRIC para actuar conforme a las solicitudes del agresor –compañero, jefe, cliente, tercera persona ajena a la organización productiva, etc.–. Sirva como ejemplo el hecho de «enviar más de 1.000 wasaps» pidiendo de manera insistente tener una relación o presiones para realizar actos de naturaleza sexual a cambio de obtener un determinado puesto de trabajo, tal y como se recoge en la STSJ del País Vasco 947/2014, de 13 de mayo:

> […] el demandado comenzó a coger más confianza con la demandante, a agarrarla, obligándola a agacharse para besarla, a darle palmadas en el culo, a contarle detalles de su relación íntima con su mujer, a decirle que se había enamorado de ella, a enviarle mensajes telefónicos con propuestas sexuales, llegando a enviar a la actora unos 1.000 mensajes entre el 9 de enero y el 24 de febrero de 2013.

Una de las más comunes y dañinas consiste en las críticas continuadas y la revelación de intimidades de la pareja tras extinguirse la relación afectiva a modo de venganza o revancha como consecuencia de la ruptura de la pareja o relación entre compañeros o excompañeros de trabajo. Una práctica que, desgraciadamente, va en continuo aumento. Cabe advertir que este tipo de conductas de ciberacoso –además de en personas jóvenes– se produce cada vez más sobre mujeres de edad adulta o mayores, que se ven controladas, acosadas, humilladas, amenazadas y sometidas mediante el uso de las TRIC por parte de quienes en algún momento mantuvieron o siguen manteniendo una relación de amistad o afectiva.

Es también una práctica frecuente acosar a través de llamadas telefónicas silenciosas, o con amenazas, insultos, con expresiones intimidatorias, colgando repetidamente la comunicación cuando contestan, llamar a horas inoportunas o intempestivas, como el caso de llamar a altas horas de la madrugada. Las amplias posibilidades que brinda la actual telefonía móvil han sabido ser empleadas perversamente por los ciberacosadores. La más tradicional es la de las llamadas ocultas realizadas a horarios inoportunos. Pueden ir desde llamadas silenciosas a amenazas graves que incluyen insultos, gritos o mensajes intimidatorios.

Un supuesto de acoso digital fuera del horario laboral o del lugar de trabajo lo ratifica la STSJ de La Rioja 14/2016, de 22 de enero. En este caso, el tribunal avala el despido disciplinario de una empleada que, con ocasión de la celebración del fin de año, envió más de 60 mensajes de WhatsApp a su compañero de trabajo a altas horas de la madrugada y en los días inmediatamente posteriores. El motivo principal era el deseo de la trabajadora de mantener una relación sentimental o afectiva con su compañero de trabajo, que este rechazaba por estar comprometido en una relación con otra mujer.

En la STSJ del País Vasco/Bilbao 1646/2017, de 18 de julio, se le aplica al trabajador la máxima sanción de suspensión de empleo y sueldo por una actuación de hostigamiento para con una compañera (referencia ruptura sentimental), donde se reconoce la autoría de mensajes, llamadas y wasaps, a través del teléfono empresarial, a determinadas horas desconsideradas. Incluso la trabajadora manifiesta haber recibido regalos y cartas en su lugar de trabajo.

Como hemos tenido ocasión de exponer, y así lo recoge el Convenio 190 OIT, el acosador puede perseguir a su víctima fuera de la jornada y más allá del horario laboral. Si la persona acosada tiene WhatsApp y el acosador tiene su número de móvil, algo normal y habitual, no existirá límite alguno para que invada su espacio y tiempo, como una obsesión o fijación del acosador con su víctima, en supuestos cercanos al denominado *cyberstalking* en el lugar de trabajo o persecución digital en el trabajo (*cyberstalking at work*, que pudiera traducirse como ciberacecho o ciberpersecución), como una comunicación hostigadora, repetida e insistente.

En la STSJ de Cataluña 5206/2018, de 5 de octubre, el trabajador (jefe de cocina) enviaba a su compañera de trabajo (camarera) mensajes de WhatsApp a última hora del día e incluso de madrugada, solicitándole que le enviara una foto de ella o que le dijera lo que estaba haciendo en ese preciso momento y cuánto la echaba de menos y la extrañaba esa noche. Ante la negativa por parte de la compañera de trabajo, el trabajador empezó a mantener una actitud más hostil de forma continuada, incluyendo comentarios sexistas.

En esta misma línea, de ciberacecho o ciberpersecución de la persona en el ejercicio de su actividad profesional, se sitúa el caso en el que un cliente acosó a una procuradora del turno de oficio con más de 20.000 mensajes, hechos por los que fue condenado a 4 años de cárcel por un delito continuado de acoso, amenazas graves y quebrantamiento de medidas cautelares. Además, se le prohibió acercarse a menos de 500 metros de la víctima y se determinó una indemnización de 12.000 euros por los perjuicios morales causados[15]. Curiosamente se ha producido un elevado número de casos de letrados –profesionales de la abogacía y procuradores de los tribunales– que son amenazados por sus clientes. Todo se inició cuando a este hombre le asignan en un proceso judicial a la procuradora con la

[15] <https://www.elconfidencialdigital.com/articulo/Judicial/anos-carcel-acosador-envio-mas-20000-mensajes-procuradora-turno-oficio/20200302192955139893.html>.

que él contacta. En este caso, estaríamos ante un claro supuesto de ciberacoso sexual en el trabajo (cercano al *cyberstalking*), en la actividad profesional de esta procuradora, acoso procedente de una tercera persona o cliente. A partir de este momento, la víctima comienza a vivir 1 año y medio de acoso mediante todo tipo de mensajes de WhatsApp, SMS, llamadas e, incluso, llegando a personarse en su casa. Los mensajes, de contenido claramente «ofensivo e intimidatorio» como «quiero hacerte el amor hoy por todo tu cuerpo», «no puedo hacer nada sin ti», «quiero verte», «solo me importas tú», etc., también quedan reflejados en el fallo. Estas comunicaciones, según la sentencia, provocaron en ella «una sensación de temor e intranquilidad con grave alteración del estado anímico de la vida personal y familiar de la trabajadora-procuradora». La letrada vio alterada su vida normal, teniendo que adoptar medidas preventivas inusuales en su actividad profesional.

Referencias bibliográficas

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

Molina Navarrete, C. (2019b). Redes sociales digitales y gestión de riesgos profesionales: prevenir el ciberacoso sexual en el trabajo, entre la obligación y el desafío. *Diario La Ley, 9452*.

OIT. (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. Recuperado de <https://www.ilo.org/global/about-the-ilo/how-the-ilo-works/departments-and-offices/workquality/WCMS_736237/lang--es/index.htm>.

Orellana Cano, A. M.ª (2019). *El derecho a la protección de datos personales como garantía de la privacidad de los trabajadores.* Pamplona: Thomson Reuters-Aranzadi.

Preciado Domènech, C. H. (2019). *Los derechos digitales de las personas trabajadoras. Aspectos laborales de la LO 3/2018, de 5 de diciembre, de protección de datos y garantía de los derechos digitales*. Pamplona: Thomson Reuters-Aranzadi.

Royakkers, L. (2000). The Dutch Approach to Stalking Laws. *California Criminal Law Rewiew*, *3*, 1-14.

Serrano García, J. M.ª (2019). El derecho a la libertad de expresión del trabajador a través de las nuevas tecnologías y el derecho a la reputación de la empresa. *Nueva Revista Española de Derecho del Trabajo*, *217*, 101-126.

Velázquez Fernández, M. P. (2019). El Convenio 190 de la OIT sobre violencia y acoso en el trabajo: principales novedades y expectativas. *Revista de Trabajo y Seguridad Social. CEF, 437-438*, 119-142.

Vicente Pachés, F. de. (2005). Las facultades empresariales de vigilancia y control en las relaciones de trabajo: concepto y fundamento. Una primera aproximación a las diversas formas de control empresarial. En I. García Ninet (Dir.) y F. de Vicente Pachés (Coord.), *El control empresarial en el ámbito laboral* (pp. 17-47). Valencia: CISS.

Vicente Pachés, F. de. (2018). *Ciberacoso en el trabajo*. Barcelona: Atelier.