FCT-P
2|03

Laboratorio-Observatorio de Riesgos Psicosociales de Andalucía

LARPSICO | Universidad de Jaén

FICHA CIENTÍFICO-TÉCNICA PREVENTIVA
Colección #02/2021
Digitalización de las organizaciones de trabajo y gestión de riesgos psicosociales: nuevos factores, riesgos emergentes

Violencia en línea y ciberacoso, riesgos psicosociales en entornos laborales digitalizados: cómo detectarlos, prevenirlos y/o erradicarlos

Online violence and cyberbullying, psychosocial risks in digitalized work environments: how to detect, prevent and/or eradicate them

Cristóbal Molina Navarrete
Catedrático de Derecho del Trabajo y de la Seguridad Social. Universidad de Jaén
Director académico del LARPSICO

Junta de Andalucía
Consejería de Empleo, Formación y Trabajo Autónomo
INSTITUTO ANDALUZ DE PREVENCIÓN DE RIESGOS LABORALES

LABORATORIO OBSERVATORIO del IAPRL

Universidad de Jaén

Violencia en línea y ciberacoso, riesgos psicosociales en entornos laborales digitalizados: cómo detectarlos, prevenirlos y/o erradicarlos

Online violence and cyberbullying, psychosocial risks in digitalized work environments: how to detect, prevent and/or eradicate them

SUMARIO

1. Introducción: la digitalización, caldo de cultivo para nuevas modalidades de violencia y acoso en el trabajo. 2. ¿Qué cabe entender por "violencia digital" y "ciberacoso" a efectos de las políticas de seguridad y salud en el trabajo? **3. ¿Qué consecuencias nocivas tiene la actualización del riesgo de violencia digital y ciberacoso en el mundo del trabajo?** 4. Fundamentos normativos de la obligación empresarial de prevenir el riesgo de violencia digital y ciberacoso laboral: un marco complejo (triple). **5. De las normas a las prácticas: cómo actualizar los protocolos preventivos del (ciber)acoso y las políticas internas de usos razonables de TIC.** 6. Para saber más.

Palabras clave: violencia digital, ciberacoso en el trabajo, Convenio 190 OIT, trabajo remoto, riesgos psicosociales
Keywords: digital violence, cyberbullying at work, ILO Convention 190, remote work, psychosocial risks

1. Introducción: la digitalización, caldo de cultivo para nuevas modalidades de violencia y acoso en el trabajo

Tal es la intensidad de penetración de las nuevas tecnologías de la información, comunicación y relación (NTICR) que nuestro modo de vida es inconcebible sin ellas. La era digital altera y/o modula profundamente nuestras formas de comunicación social, también de relacionarnos, incluido el entorno laboral. La epidemia y ciertas decisiones para abordarla reduciendo el riesgo biológico de contagio (ej. teletrabajo) aceleraron estos procesos transformadores. El retorno a una cierta "normalidad" lejos de frenarlos los alimenta, evolucionando a un mundo laboral híbrido (lo presencial convive con lo virtual). Asimismo, también en los centros de trabajo presenciales, el uso de dispositivos tecnológicos (ordenador), internet, la mensajería instantánea, etc., se hace cotidiano.

No hay duda de que esta transformación digital de nuestros mundos de vida, también en el trabajo, está llena de grandes ventajas o beneficios, para las empresas, y para las personas trabajadoras. El diálogo social multinivel (ej. **acuerdo marco sobre la digitalización**, junio 2020) así lo reconoce. En consecuencia, desarrollada bajo ciertas condiciones de usos razonables, la revolución tecnológica puede mejorar del bienestar de las personas empleadas. Pero también tiene riesgos sociales (ej. usos antisociales de las redes), y, claro, laborales. Su omnipresencia abre canales comunicativos no amables, sino, al contrario, incívicos, hostiles, difamatorios, permitiendo un elenco de conductas constitutivas de violencia psíquica, episódica (intimidación digital puntual) o reiterada (ciberacoso), por razones múltiples (genéricas, sexuales, discriminatorias).

A diferencia del "ciberacoso escolar" o "ciberbullyng" (muy estudiado y más conocido), incluso del "ciberacoso de pareja" (violencia y acoso digital de género, incluso se tipifica como delito en el art. 172 ter Código Penal)[1], la "violencia online" y el "ciberacoso laboral" son fenómenos relativamente recientes e inexplorados. Y ello a pesar del uso generalizado de las NTICR en los entornos de trabajo de nuestro tiempo. Conocidos con distintos nombres (violencia digital, acoso cibernético o violencia en red, etc.), las conductas que describen irán en aumento. En este escenario, una novedad tanto del art. 3 del **Convenio 190 OIT** (prevención y erradicación de la violencia y el acoso en el mundo del trabajo) cuanto del art. 4 de la **Ley 10/2021, 9 de julio, trabajo a distancia** es la tipificación normativa de dos riesgos psicosociales emergentes:

a) la "**violencia digital**" (forma o modalidad genérica de conducta inapropiada)
b) el "**ciberacoso en el trabajo**", acoso digital o en red (forma específica de aquélla).

[1] También hallamos formas de "ciberacoso social" sin mediar relación específica, laboral o no. Por ejemplo, recientemente conocíamos que la Audiencia Nacional ha acordado la entrega de un ciudadano belga que era reclamado por "acoso en red" a políticos y deportistas.
https://www.poderjudicial.es/cgpj/es/Poder-Judicial/Audiencia-Nacional/Noticias-Judiciales/La-Audiencia-Nacional-acuerda-la-entrega-de-un-ciudadano-belga-reclamado-en-su-pais-por-amenazas-y-acoso-por-Internet-a-politicos-y-deportistas

Violencia en línea y ciberacoso, riesgos psicosociales en entornos laborales digitalizados: cómo detectarlos, prevenirlos y/o erradicarlos

Online violence and cyberbullying, psychosocial risks in digitalized work environments: how to detect, prevent and/or eradicate them

2.

¿Qué cabe entender por "violencia digital" y "ciberacoso" a efectos de las políticas de seguridad y salud en el trabajo?

2.1. En busca de conceptos con fundamento normativo y consenso científico internacionales suficientes

Para un buen número de analistas, la "violencia en línea" y el "acoso digital" o "ciberacoso" no son nuevos tipos de violencia y acoso, sino tan solo los nuevos canales (tecnológicos) de expresión de estos (ej. **Nota Técnica Preventiva 854/209, del INSST**). Por lo tanto, no tendrían más novedad que (1) el medio (canal digital) de realización y (2) la mayor celeridad de difusión de sus efectos nocivos (rapidez de difusión, número potencialmente ilimitado de destinatarios, etc.). Según este prisma, la violencia online y el acoso digital no serían más que la violencia y el acoso ya conocidos en el mundo laboral (intimidaciones, agresiones, acoso sexual, acoso discriminatorio, acoso moral, etc.), pero realizados mediante diversas (nuevas o no —ej. teléfono—) tecnologías de la de información, comunicación y relación (TICR), esto es, usos comunicativos hostiles.

¿Qué significa, en la práctica, esta visión relativista —y medial— de la novedad de la violencia digital y el ciberacoso en el mundo del trabajo? Dos cosas, al menos. Primera, que los bienes jurídicos en juego serían, en última instancia, los mismos (ej. dignidad, intimidad, no discriminación, libertad sexual), incluidos, claro está, el riesgo para la salud y la integridad moral de las personas. Segundo que, en consecuencia, bastaría para su prevención integrar estas modalidades digitales en los instrumentos ya existentes para prevenir-erradicar la violencia y el acoso laborales (Políticas de prevención de riesgos —ej. protocolos— ex **art. 14 LPRL** y Planes de igualdad ex **art. 48 y 62 LOIEMH**).

Entonces **¿el ciberacoso (solo) sería el mismo fenómeno que el acoso, solo que replicado y trasladado al plano digital?** No. La especificidad del medio va más allá, p.ej.:

- En la delimitación del concepto de acoso en red. La reiteración, inherente al concepto de acoso moral, incluso del acoso sexista (no así al de acoso sexual), es menos significativa, o deban modularse, para el ciberacoso.
- En la identificación de los bienes jurídicos más afectados (ej. adquiere, o puede adquirir, singular importancia el derecho a la protección de datos y el derecho a la privacidad, como asume la **Agencia Española de Protección de Datos —AEPD—** en **su protocolo de gestión del ciberacoso**).
- En la mayor potencialidad de riesgos y daños (el efecto multiplicador que pueden tener los canales utilizados, aunque haya acoso en línea sin difusión pública, permiten su réplica entre un colectivo ilimitado y alta velocidad).
- En la eficacia preventiva (ej. **políticas internas de usos razonables de las TIC**, incluido internet y las redes, según el **art. 88 LOPDGDD**).

Aunque, la norma internacional universal (C190 OIT) debe permitir alcanzar un mayor consenso, no solo normativo-institucional, sino científico-social, no existe a día de hoy un concepto suficientemente aceptado de "ciberacoso en el trabajo". Por eso, se ha venido utilizando la genérica, empleada para el entorno escolar (convencionalmente se le llama "Ciberbullyng"). La **Guía de actuación contra el ciberacoso** (Instituto Nacional de Tecnologías de la Comunicación: INTECO) lo define como proceso de:

Violencia en línea y ciberacoso, riesgos psicosociales en entornos laborales digitalizados: cómo detectarlos, prevenirlos y/o erradicarlos

Online violence and cyberbullying, psychosocial risks in digitalized work environments: how to detect, prevent and/or eradicate them

> "amenazas, hostigamiento, humillación u otro tipo de molestias [insultos, robos de contraseña, amenazas, ridiculizaciones, vacío relacional, suplantaciones de identidad o provocaciones de todo tipo] realizadas por una persona [adulta o menor] contra otra [adulta o menor de edad] a través de tecnologías telemáticas [internet, telefonía móvil, correo electrónico, mensajería instantánea, videoconsolas, etc.], sea con mensajes de texto, de voz, imágenes o videos, a fin de provocar de provocarle un estado de victimización psíquica, estrés emocional y rechazo social" (2013, p. 12).

No obstante, el concepto de ciberacoso en el trabajo más aceptado, dentro y fuera de nuestras fronteras, lo identifica, siguiendo las pautas de la delimitación clásica de acoso moral en el trabajo, del siguiente modo:

> Toda conducta intimidatoria, **intencional y repetida**, realizada por una o varias personas, internas o externas a la empresa, dirigida contra otra u otras, también internas o externas, **para provocarles un daño** (personal y/o profesional) grave **mediante medios electrónicos** (NTIC, redes sociales), **a causa o con ocasión de una relación de trabajo.**

Esta delimitación es poco útil para el ámbito preventivo, pues no solo requiere intencionalidad sino un resultado dañoso, poniendo énfasis igualmente en la nota de gravedad. Por eso, creemos mucho más útil, cuando menos a los efectos de diseñar y poner en prácticas políticas preventivas, según la evolución —doctrinal, constitucional y normativa—, entender por «violencia cibernética en el trabajo» cualquier tipo de:

> **Comportamiento y/o práctica inaceptables** [*conductas actuales*], o las amenazas de ellos [*intimidación con conductas futuras*], se manifiesten una sola vez [agresiones ocasionales] o repetidas [*acoso*], **susceptibles de causar daño** (*personal —físico, psíquico, moral— o económico*), cualquiera que sea su motivación y el bien jurídico afectado de forma prevalente, incluida por razón de sexo [acoso sexual y/o sexista], **realizados mediante canales de comunicación digital**, siempre que estén **relacionadas con el trabajo o** se produzcan **con ocasión del mismo**, aun fuera del lugar y la jornada de trabajo [*art. 1 a) en relación con el art. 3 d) C 190 OIT*].

Debe advertirse, una vez más, que el origen de la violencia online y el ciberacoso no están en las tecnologías, sino en los usos humanos inapropiados de ellas. De ahí, la utilidad de las citadas políticas de usos razonables o adecuados de las TIC. También si se trata —como es frecuente— de ciberacosos híbridos (parte presencial, parte tecnológico).

2.2. Modalidades de "violencia digital" y "ciberacoso" en el trabajo: especial referencia al sexo, al género y a la protección de datos

Clasificación según los bienes jurídicos (derechos fundamentales) afectados

En esta delimitación conceptual unitaria, siguiendo la propuesta del C190 OIT (y adaptado a la doctrina constitucional: **STC 56/2019, 6 de mayo**), comprobamos que, al igual que sucede con la violencia y el acoso en el mundo del trabajo presenciales, las causas de estas formas de comunicación hostil pueden ser múltiples, como plurales son los bienes jurídicos afectados (dignidad, salud, integridad, no discriminación, intimidad, etc.). Ahora bien, como veremos en la selección de casos, una de las razones prevalentes en la violencia digital y el ciberacoso reside en el sexo (violencia o/y ciberacoso sexual), así como en el género (violencia o/y ciberacoso sexista). Precisamente, así sucede:

Violencia en línea y ciberacoso, riesgos psicosociales en entornos laborales digitalizados: cómo detectarlos, prevenirlos y/o erradicarlos

Online violence and cyberbullying, psychosocial risks in digitalized work environments: how to detect, prevent and/or eradicate them

a) En el ámbito escolar. Aquí, cuando la situación tiene un elemento sexual se denomina "grooming" o "child-grooming". Su especificidad da lugar a un delito informático autónomo (**art. 183 ter CP**), lesivo de la libertad sexual.
b) En el ámbito familiar. El género como factor de ciberacoso ofrece situaciones específicas, como el "**cyberstalking**" (forma de persecución mediante el uso de una TIC con el fin de asediar a alguien, mediante acciones reiteradas, persistentes e indeseables que perturban la vida de las víctimas). Aunque conoce otras razones, a menudo —lo muestra la jurisprudencia penal— es una forma de acoso ejercida por el hombre contra su expareja (**art. 172 ter CP**).

Esta especificidad debe reseñarse también en el ámbito laboral, tanto en el plano conceptual como en el de la intervención preventiva y/o correctora, como enfatiza el C190 OIT (y la citada ley 10/2021, de trabajo a distancia). Este reconoce la necesidad de atender de forma particular la prevención y erradicación de la violencia (digital) y el acoso (digital) por razón de sexo y de género. Por lo tanto:

a) Cuando en la conducta o práctica, actual o potencial, inapropiada medie un rasgo sexual —sin perjuicio de su carácter pluriofensivo— es "**ciberacoso sexual laboral**" («sextorsión», «pornovenganza», acoso sexual en línea, etc.).
b) Cuando la causa sea claramente sexista (estereotipos sociales y laborales) estaremos ante un tipo de violencia o/y "**ciberacoso por razón de género**".

Esta especial significación del sexo en la violencia y el acoso digitales en trabajo se reconoce normativamente (C190 y Ley 10/2021) y se verifica en la práctica (según la Agencia de Derechos Fundamentales de la UE el 23 % de las mujeres manifiesta haber sufrido acoso o abuso en línea al menos una vez en su vida). Se halla también en algunos de los —muy pocos— protocolos que mencionan el ciberacoso laboral. El **Protocolo del Hospital Universitario La Paz** (Madrid) lo incluye (solo) como acoso sexual no verbal.

En los supuestos en que la violencia digital o/y el ciberacoso en el mundo del trabajo tenga como causa prevalente cualquier otra causa discriminatoria (discapacidad, orientación sexual, edad, origen étnico, razones sindicales, etc.), estamos ante:

a) La modalidad de "violencia digital" y/o "**ciberacoso discriminatorio laboral**".
b) Mientras que cuando no hay causa específica prevalente, sino razón genérica, poniendo en riesgo la integridad, no solo la salud de las víctimas se tratará de "**violencia psíquica digital**" o/y "**ciberacoso moral en el trabajo**".

Hasta aquí la principal clave diferencial clasificatoria sigue residiendo en el medio (digital) de realización de la conducta de violencia o/y acoso en el mundo laboral, según el bien jurídico (derecho fundamental de las personas trabajadoras o relacionadas con la empresa de algún modo —ej. clientes—) típicamente afectado, en términos análogos a los tipos y modalidades de violencia y/o acoso de índole presencial. Ahora bien, es necesario reseñar una relevante especificidad de la violencia digital o/y el ciberacoso cuál es la **especial significación que adquiere**, al menos de forma potencial, superior a la que puede albergar el acoso presencial, **las nuevas situaciones de riesgo lesivo para derechos distintos** a la salud, la integridad o la no discriminación, como: la reputación personal y profesional (honor), la imagen, así como la intimidad y el secreto de comunicaciones (art. 18 CE) de las personas víctimas, por la ya referida mayor lesividad potencial derivada de la publicidad del medio digital (incluidas redes sociales en abierto: facilidad para viralizarse y perdurabilidad en el entorno en línea). También la empresa puede ver afectadas su imagen y reputación corporativas en algunas de estas conductas.

Violencia en línea y ciberacoso, riesgos psicosociales en entornos laborales digitalizados: cómo detectarlos, prevenirlos y/o erradicarlos

Online violence and cyberbullying, psychosocial risks in digitalized work environments: how to detect, prevent and/or eradicate them

Justamente, la AEPD es plenamente consciente de ello. De ahí que en sus útiles recomendaciones ponga énfasis en la **protección de datos como garantía de efectividad para las políticas de prevención del ciberacoso en el trabajo**. Las recomendaciones de la AEPD irían dirigidas al que podría considerarse como el auténtico "**acoso digital laboral**", esto es:

> los comportamientos inapropiados reiterados (en los términos vistos del art. 1 C190 OIT) producidos de forma preeminente en el ámbito de la comunicación digital y mediante usos particularmente relevantes de datos personales de las personas víctimas durante el trabajo, en relación o con ocasión del trabajo y su entorno relacional social (según los factores de riesgos psicosociales del art. 15 LPRL).

En suma, los derechos a la protección de datos y a la privacidad hallan un plus de riesgo en el ciberacoso. De lado contrario, otro derecho, la libertad de expresión crítica entra en juego del lado en estas situaciones de comunicación digital hostil, no siendo en todos los casos fácil diferenciar la hostilidad u ofensividad de la crítica agria y desabrida.

Clasificación de la violencia digital y el ciberacoso en el mundo del trabajo según el tipo de relación entre las personas víctimas y las victimarias (agresoras/acosadoras)

Clásicamente, la clasificación de la violencia y/o acoso en el mundo del trabajo no responde solo a los derechos afectados, sino también a la relación existente entre las personas implicadas en el proceso, víctimas y acosadoras. Al respecto, se distinguen dos tipologías diferenciadas. A saber:

1. Según el origen de la "ciber-violencia" (o/y ciberacoso), desde dentro o desde fuera de la organización de trabajo. En este caso se distingue:

   a) La **violencia digital y/o ciberacoso de origen interno** (entre personas que se relacionan laboralmente en la organización).
   b) La **violencia digital y/o ciberacoso de origen externo** (ej. clientela hacia las personas trabajadoras; estudiantado a profesorado, etc.)

Por ejemplo, **los protocolos de gestión de la violencia y el acoso del sistema de salud madrileño** diferencian claramente ambas tipologías.

2. Según el tipo de relación entre la persona víctima y la agresora, de modo que medie una relación de poder (jerárquico o no)

   a) Violencia digital y ciberacoso laboral **vertical descendente** (desde personas con poder jerárquico hacia personas empleadas)
   b) Violencia digital y ciberacoso **vertical ascendente** (desde personas sujetas al ejercicio del poder directivo hacia quienes lo ejercen o participan de él)
   c) Violencia digital o/y ciberacoso laboral **horizontal** (entre personas compañeras en la empresa)

De todas estas modalidades ofreceremos algún ejemplo en el estudio de casos. Se comprobará que, a diferencia del acoso laboral presencial, donde prevalecerá el acoso vertical descendente, en el ciberacoso laboral tiene prevalencia la modalidad horizontal.

Violencia en línea y ciberacoso, riesgos psicosociales en entornos laborales digitalizados: cómo detectarlos, prevenirlos y/o erradicarlos

Online violence and cyberbullying, psychosocial risks in digitalized work environments: how to detect, prevent and/or eradicate them

2.3. ¿Cómo diferenciar el "ciberacoso laboral" respecto de las demás formas de "violencia digital"? Elementos para su caracterización

Hasta aquí hemos analizado simultáneamente la violencia digital y el ciberacoso en el mundo del trabajo. **El C190 OIT reclama la necesidad de prevenir-erradicar todas las formas de violencia, al margen de sus características diferenciales y su gravedad**. Por lo general, y a ello sigue apuntando el C190 OIT, el acoso se entiende como una forma especialmente grave de violencia psíquica, caracterizada por su reiteración en el tiempo, de ahí su plus de peligrosidad y lesividad. El acoso constituiría un proceso creador de un entorno intimidatorio, ofensivo y degradante, mientras que la violencia se identifica con una conducta particular, no frecuente, aunque sea también grave ¿Puede diferenciarse, entonces, el ciberacoso laboral de la violencia digital en el trabajo por la reiteración de comportamientos en aquél frente al carácter puntual o episódico de ésta?

En otros términos ¿el ciberacoso laboral se integra con análogos elementos que el acoso presencial (conducta intimidatoria recurrente, grave, deliberada y resultado de daño a la persona víctima), añadiendo el canal digital de comisión? Ya anticipamos que no exactamente. Como el acoso presencial, las conductas constitutivas de ciberacoso en el trabajo pueden ser múltiples (ej. enviar mensajes ofensivos o insultantes por la red, difusión de rumores falsos o conductas socialmente reprochables, distribución de fotografías o vídeos privados de contenido personal, a menudo sexual, suplantación de identidad de la víctima para realizar actos que perjudiquen su nombre o reputación, creación de webs y perfiles falsos en redes en nombre de la víctima, frecuentemente con reclamos sexuales, etc.). Ahora bien, a diferencia del acoso presencial, que requiere de una cierta reiteración y frecuencia, aunque no venga predeterminada cuál (ej. puede ser inferior a una vez a la semana y una duración de 6 meses, como exigía Leymann, sin que sea aceptado jurisprudencialmente —ej. **STEDH 9 de noviembre de 2021**—), no para todos los supuestos de ciberacoso en el trabajo esa recurrencia/frecuencia adquiere el mismo sentido, precisamente por la especificidad del medio digital.

Desde esta perspectiva, las principales diferencias en los elementos típicos del ciberacoso en el trabajo respecto del acoso presencial serían (una síntesis en la tabla 2):

- **La reiteración puede equivaler a un efecto duradero por la difusión en la red**

Las Guías relativas al ciberacoso escolar exigen que la situación de acoso se dilate en el tiempo. Pero las TIC permiten un acceso repetido al contenido publicado en línea, por lo que un único acto puede tener el efecto duradero (documento de trabajo 1, 2020, de la OIT **"Actualización de las necesidades del Sistema: Mejora de la protección frente al ciberacoso...posibilitado por las TIC"**), aun si la persona ciberacosadora no pretende ese resultado (complicidad de terceras personas: accesos ilimitados, reenvíos, etc.). La recurrencia de la conducta, pues, o se relativiza en el ciberacoso, al difuminarse, o se redefine, en términos de perjuicio duradero (ej. permanencia en red, veces compartida).

- **El ciberacoso laboral puede realizarse fuera del lugar de trabajo y de la jornada**

El acoso presencial tiende a realizarse dentro de la jornada laboral y en el entorno de trabajo, aun de forma sutil, para que no deje una huella registrable fácilmente. Pero los canales digitales abren más posibilidades de comunicación hostil, que pueden llegar a ser más difíciles de registrar aún, en la medida en que se desenvuelven en espacios privados y tiempos de autodeterminación. En consecuencia, a efectos preventivos, las empresas hallarán más limitaciones para los

Violencia en línea y ciberacoso, riesgos psicosociales en entornos laborales digitalizados: cómo detectarlos, prevenirlos y/o erradicarlos

Online violence and cyberbullying, psychosocial risks in digitalized work environments: how to detect, prevent and/or eradicate them

debidos registros (ej. auditorías digitales o pruebas periciales tecnológicas) si los dispositivos y/o redes son de titularidad privada, también si se realizan las conductas extramuros del trabajo (**STSJ Cantabria 51/2019, de 21 de enero**). Por lo que podría llevar a requerir el auxilio de terceros con poder público (AEPD, autorizaciones judiciales, etc.).

- **La asimetría de posiciones no es una condición sine qua non: prevalencia del ciberacoso horizontal (entre personas compañeras)**

Normativa (ej. art. 173 CP) y técnicamente (**NTP 854 INSST**) se asume que el acoso (moral, sexual, sexista) presupone un desequilibrio de poder inherente ex art. 173 CP) también se difumina en el ciberacoso en el trabajo. De forma traslaticia, la propia AEPD requiere, en sus **recomendaciones**, esta asimetría de poder para el ciberacoso, aunque no se trate de una relación de jerarquía. Ahora bien, al margen del eventual dominio desigual de las TIC entre la persona acosadora y la persona víctima (asimetría cognitiva o competencial tecnológica) no será esta la principal característica del ciberacoso, sino la prevalencia de la modalidad horizontal (entre personas compañeras), incluso vertical, pero ascendente (a —no de— mandos, personas supervisoras, directivas, directivos), sobre la base del "poder difuso" que parece conceder la tecnología y el aparente "anonimato". No obstante, el pretendido "poder del anonimato digital" puede ser más aparente que real, pues los dispositivos tecnológicos, así como las redes en línea, suelen dejar "huella digital" siempre, aun recóndita, pudiéndose identificar la autoría mediante sofisticadas pruebas periciales. Si bien no siempre es posible, por supuesto (ej. trágico **caso IVECO** —suicidio de una mujer empleada en esta empresa a raíz de la divulgación de un video sexual entre sus colegas de la empresa: archivado por el juzgado penal por falta de autoría, y por la inspección de trabajo por relegarlo al ámbito privado, no laboral—).

- **El elemento subjetivo de la intencionalidad no es un elemento necesario**

La intencionalidad no es relevante ya ni como elemento típico del acoso presencial (STC 56/2019) ni del ciberacoso (art. 3 en relación con el art. C190 OIT), aunque esté normalizado. Del mismo modo, tampoco es significativo, a efectos preventivos, la usual menor conciencia moral sobre el sufrimiento (dolor) de las víctimas en el ciberacoso (por el anonimato y la distancia física del medio digital) que respecto del acoso presencial. Debería eliminarse de los protocolos de ciberacoso que lo exigen (ej. **Grupo Axa**).

- **Autoría más difusa por el potencial auditorio indeterminado (accesibilidad de la red), pero la conducta sigue siendo imputable a quien inicia la conducta**

Cuando la conducta de ciberacoso no se realiza por un canal exclusivo entre la persona víctima y la acosadora, sino abierto (ej. redes; grupo Whatsapp, etc.), el efecto, en duración e intensidad puede escapar al control (y a la voluntad) de la persona autora, ante el riesgo de difusión por un auditorio indeterminado. Pero no por ello resultará menos imputable. Por lo tanto, las personas en el seno de las organizaciones deben ser muy conscientes de ese riesgo de efecto multiplicador (del daño), educándolas en usos prudentes de las TIC y redes, a través de las políticas internas de usos razonables.

Violencia en línea y ciberacoso, riesgos psicosociales en entornos laborales digitalizados: cómo detectarlos, prevenirlos y/o erradicarlos

Online violence and cyberbullying, psychosocial risks in digitalized work environments: how to detect, prevent and/or eradicate them

Tabla 2. Enunciado de las notas caracterizadoras del ciberacoso en el trabajo en relación con el acoso presencial.

- La reiteración se identifica con el efecto duradero por la difusión en la red.
- El ciberacoso laboral puede realizarse fuera del lugar de trabajo y de la jornada: *"en cualquier momento, en cualquier lugar".*
- La asimetría de posiciones no es condición sine qua non: prevalece el horizontal.
- La intencionalidad no es un elemento necesario.
- La autoría puede ser más difusa por la participación de un auditorio incierto, pero no por ello dejará de ser imputable la conducta originaria.

En definitiva, a la luz de lo expuesto hasta ahora, por ciberacoso en el mundo del trabajo cabe entender toda conducta:

> Creadora, por personas internas o externas (violencia de terceros) en una empresa u organización (pública), de un entorno intimidatorio, degradante u ofensivo, mediante el uso inapropiado de tecnologías de la información, comunicación y relación digitales (incluso redes), aun de titularidad privada y fuera de la jornada y tiempo de trabajo, susceptible de causar un grave daño (personal y/o profesional) a una o varias personas trabajadoras (o externas, pero relacionadas con la empresa —ej. clientela; alumnado—). Y ello cualquiera que sea la causa (ciberacoso moral), sin perjuicio de atender de forma particular a los generados por razones discriminatorias, de sexo-género (ciberacoso sexual y/o sexista) o por cualquier otra (orientación sexual, etnia, etc.).

Violencia en línea y ciberacoso, riesgos psicosociales en entornos laborales digitalizados: cómo detectarlos, prevenirlos y/o erradicarlos

Online violence and cyberbullying, psychosocial risks in digitalized work environments: how to detect, prevent and/or eradicate them

3. ¿Qué consecuencias nocivas tiene la actualización del riesgo de violencia digital y ciberacoso en el mundo del trabajo?

La violencia digital y el ciberacoso en el trabajo comparte con su forma presencial las graves consecuencias nocivas tanto para las personas empleadas víctimas como para las empresas. Estas conductas afectan gravemente a la dignidad y a la salud psíquica (ansiedad, estrés, impotencia, miedo), física y sexual de aquellas personas, así como perturba la tranquilidad del entorno social y familiar, por la mayor injerencia o carácter intrusivo de los medios digitales (**ni siquiera el hogar o el tiempo entre personas amigas son ya refugio, por lo intrusivo de la tecnología**). Ni siquiera el abandono de la empresa (aspecto relacionado ampliamente con el acoso presencial) es una garantía de paz, pues, de nuevo, el carácter omnipresente de la tecnología permite continuar el hostigamiento. Además, puede perjudicar (aún más) gravemente, como se dijo, a la reputación, imagen, privacidad y protección de datos de las personas víctimas.

Asimismo, conviene recordar, como hace la exposición de motivos del C190 OIT, que toda forma de violencia y acoso, por lo tanto, también, e incluso más, el ciberacoso, son incompatibles con la promoción de empresas sostenibles. Estas conductas afectan de forma muy negativa igualmente a la organización del trabajo, las relaciones en el lugar de trabajo (ej. mayor absentismo; menor compromiso y mayor desentendimiento del trabajo por parte de las personas víctimas de ciberacoso laboral), al valor de la reputación de las empresas y la productividad (pérdida de calidad de sus servicios).

4. Fundamentos normativos de la obligación empresarial de prevenir el riesgo de violencia digital y ciberacoso laboral: un marco complejo (triple)

Consecuentemente, al margen de la ratificación del C190 OIT (hecha en 2021), el deber empresarial de prevenir la violencia digital y el ciberacoso en el trabajo como riesgos psicosociales emergidos es inequívoco. Así se deriva de la obligación de prevenir todos los riesgos psicosociales constatados por la evolución (art. 14 LPRL; **STJUE 11 de noviembre de 2021**) y así lo explicita para el ciberacoso la AEPD. Una exigencia expresa que también hace, si bien no lo adjetiva ni como violencia digital ni como ciberacoso, la **Ley 10/2021 de 9 de julio, de trabajo a distancia**.

Su preámbulo reconoce, y su art. 4.4 exige, una especial tutela para las personas teletrabajadoras en general, no solo en situaciones de vulnerabilidad especial (personas teletrabajadoras menores), por su mayor "susceptibilidad a los riesgos vinculados con esta forma (flexible) específica de organización" (digitalizada), como "fatiga" (para todo tipo de empresa en el **art. 88 LOPDGDD**), "aislamiento" (llama a garantizar formas de comunicación fluida con el resto de personas compañeras y la empresa) y eventuales "problemas de acoso en el trabajo". Al respecto, aquel art. 4.4 remite, a su vez, al marco normativo propio de la igualdad efectiva entre mujeres y hombres (**LOIEMH**). En el se establecen no solo la obligatoriedad de los (1) **Planes de Igualdad de Género** (arts. 45 y ss.) sino también de los (2) **Protocolos de gestión del (ciberacoso) por razón de sexo-género** (arts. 48 y 62 LOIEMH). Un instrumento de gestión (planes de igualdad) y otro (protocolos) hoy interactuarían con los "planes de prevención de riesgos laborales" (art. 16 LPRL), en virtud del marco reglamentario (**Anexo IV del RD 901/2020, 13 de octubre, planes de igualdad**), que exige integrar en las políticas antidiscriminatorias (incluye todo tipo de acoso) de las empresas un enfoque de salud laboral con equidad de género.

Violencia en línea y ciberacoso, riesgos psicosociales en entornos laborales digitalizados: cómo detectarlos, prevenirlos y/o erradicarlos

Online violence and cyberbullying, psychosocial risks in digitalized work environments: how to detect, prevent and/or eradicate them

Cierto, ni la violencia digital ni el ciberacoso en el trabajo se nominan en la Ley 10/2021 como riesgo psicosocial emergente en el trabajo, sino que, se contemplan como modalidades digitales de desenvolvimiento de la violencia y el acoso. Ahora bien, esta regla ha de interpretarse, a su vez, con la previsión de su art. 16.1 Ley 10/2021 (se ordena atender a los factores de riesgo psicosocial y organizativo inherentes al trabajo remoto, por ese uso intensivo de las NTIC) y en su art. 18 (derecho a políticas internas de usos razonables de los dispositivos electrónicos de uso productivo y derecho a la desconexión digital). Precepto este que replica el más general del art. 88 LOPDGGD.

En suma, la violencia digital y el ciberacoso en el trabajo son riesgos genéricos con la obligación de prevenirlos en el conjunto de los entornos laborales (ex arts. 14 y 16 LPRL; ex arts. 48 y 62 LOIEMH), pero serían específicos a gestionar para el trabajo a distancia, en especial el teletrabajo. El cuadro resultante (tabla 2) es complejo, pero debe garantizar la efectividad de la protección.

Tabla 3. El marco normativo complejo de la obligación preventiva de la violencia digital y el ciberacoso en el mundo del trabajo en España.

Marco regulador	PRL	LOIEMH	Protección de Datos y derechos digitales
Instrumento de gestión	Evaluación de riesgos y planificación	Planes de Igualdad Protocolos de acoso por razón de sexo	Políticas de usos razonables de las TIC
Preceptos específicos	Arts. 14-16 LPRL/ arts. 16 y 18 Ley 10/2021 (Trabajo remoto)	Arts. 45 y ss. Arts. 48 y 62 LOIEMH Anexo IV RD 901/2020	Art. 88 LOPDGDD Art. 4.4 Ley 10/2021 (Trabajo a distancia)

Violencia en línea y ciberacoso, riesgos psicosociales en entornos laborales digitalizados: cómo detectarlos, prevenirlos y/o erradicarlos

Online violence and cyberbullying, psychosocial risks in digitalized work environments: how to detect, prevent and/or eradicate them

5.

De las normas a las prácticas: cómo actualizar los protocolos preventivos del (ciber)acoso y las políticas internas de usos razonables de TIC

Visibilizados y delimitados los riesgos psicosociales de violencia y ciberacoso en el trabajo, y confirmado que nuestro marco normativo establece un consistente deber de prevención y erradicación (desde el sistema preventivo, de igualdad de género y el de protección de datos y derechos digitales), es momento de su identificación y prevención prácticas, en especial desde el sistema de seguridad y salud en el trabajo. Hasta ahora, sin embargo, la casi totalidad de los (más de 50) casos de violencia digital y ciberacoso en el mundo del trabajo registrados en la experiencia judicial han recibido una respuesta reactiva, esto es, sancionando las conductas consumadas (corrección disciplinaria a las personas que actúan como agresoras y reparación de los daños causados a la víctima). Apenas un puñado de casos conocen esta dimensión preventiva primaria o secundaria (auspiciada por la doctrina judicial, pero poco aplicada: —ej. STSJ Cantabria 51/2019, 21 de enero— niega que haya en el caso un ciberacoso vertical ascendente desde la representante sindical a la gerente del centro, al entender que se trata solo de una campaña de crítica sindical desabrida en red), sin llegar a la etapa más ineficiente, la prevención terciaria (disciplinario-asistencial).

No obstante, si bien tímidamente, ya podemos encontrar algunas experiencias de gestión empresarial preventivas de riesgos laborales que incluyen el ciberacoso entre los riesgos a gestionar. Haremos aquí una breve, pero ilustrativa selección, de aquellas que nos parecen más relevantes, y que deberían difundirse, sin perjuicio de mejoras en ellas. Así, en cuanto a las concretas medidas a adoptar en el seno de las organizaciones para prevenir, o al menos minimizar, estos riesgos de comunicación hostil en seno a través de las NTIC serían básicamente las previstas en el sistema de seguridad y salud en el trabajo complementadas con las políticas internas de usos razonables de las TIC:

1. **Información y formación de las personas trabajadoras sobre qué es y qué efectos en la salud tienen la violencia digital y el ciberacoso en el trabajo**, así como las formas de prevenirlos, atajarlos o corregirlos. También información clara sobre las consecuencias disciplinarias (y otras responsabilidades).

2. **La inclusión de la violencia digital y el ciberacoso en el protocolo de prevención de la violencia y el acoso en el trabajo**, pero no solo nominalmente, sino fijando reglas específicas.

   La declaración de principios y la política de tolerancia 0 a toda forma de violencia, en cualquiera de sus formas, en el seno de las organizaciones que incorporan de manera usual estos protocolos debe mencionar expresamente la violencia y el acoso digitales. Pero no bastará con nominarlos, deben visibilizarse reglas específicas, evitando la tutela indiferenciada, genérica. No solo debe incluir su prohibición, sino también un catálogo de las principales conductas que integran la violencia y el acoso digitales, así como un elenco de recomendaciones de buen uso de TIC y de las redes sociales, incluso privadas (aquí enlazarán con las políticas de usos razonables de las TIC ex arts. 88 LOPDGDD y art. 18 de la Ley de trabajo a distancia).

3. **Ejemplos de recomendaciones y buenas prácticas para los protocolos de gestión del (ciber)acoso y las políticas internas de usos razonables**.

   Más allá del **"Decálogo de ciberseguridad de empresas. Una aproximación para el empresario"** (Instituto Nacional de Ciberseguridad —INCIBE—), que puede ser útil para una primera aproximación de las empresas a las nuevas obligaciones preventivas (refleja un catálogo de obligaciones específicas en cuanto a la actividad en redes sociales para su uso adecuado sin poner en riesgo la reputación, el funcionamiento e información de la empresa), contamos con ejemplos concretos que tratan de ir más allá y concretar una política específica de gestión preventivo-correctora de la violencia digital y el ciberacoso en el mundo del trabajo. Entre ellos destacamos:

AEPD: ***"La protección de datos como garantía en las políticas de prevención del acoso: recomendaciones de la AEPD"*** (noviembre de 2019).

Es el más completo y preciso. A ella remite también su Guía *"La protección de datos en las relaciones laborales"* (2021, p. 67). Con la referida "Guía de protección frente al acoso (y ciberacoso) en el trabajo" aporta un espacio web con recomendaciones y herramientas prácticas de ayuda para la protección de datos respecto de políticas de prevención del ciberacoso, en empresas y AAPP. Pormenoriza cómo se puede integrar la protección de datos en las políticas de prevención del ciberacoso en el trabajo, fijando recomendaciones para actualizar (en forma de compromiso de tolerancia 0, medidas de prevención el deber de prevención y de erradicación) en protocolos de acoso y en los planes de igualdad.

En el destacamos, de un lado, el elenco ilustrativo de conductas típicas de ciberacoso digital, esto es, a través de un tratamiento ilícito de datos personales (Tabla 4).

Tabla 4. Conductas constitutivas de ciberacoso en el trabajo o acoso digital.

- La grabación de imágenes degradantes que afecten a la intimidad de las personas .
- La difusión de imágenes o videos de contenido sexual entre personas compañeras de trabajo (o entre terceras personas), aún recibidas de forma legítima ('porno venganza'), o en redes sociales.
- La publicación o difusión de mensajes o contenido audiovisual (imágenes, memes, etc.) que tenga por objeto menoscabar la dignidad y crear un entorno humillante u hostil.
- La publicación o difusión de comentarios despectivos, chistes ofensivos o demérito de la valía profesional de una persona trabajadora en redes de mensajería instantánea o sociales, tengan un carácter sexual (acoso sexual), ya estén relacionados con el sexo de aquélla (acoso por razón de sexo) o su orientación o identidad sexual, ya tengan un carácter general (acoso laboral).
- El envío de mensajes o insinuaciones ofensivas de carácter sexual realizadas por redes de mensajería instantánea o redes sociales.
- La difusión de insultos o de rumores falsos empleando redes.

De otro, llama la atención de la necesidad de aportar en los protocolos información relativa a los posibles mecanismos de reacción ante un tratamiento de datos personales derivable en un procedimiento de ciberacoso (ej. mecanismos de retirada de contenido de las principales plataformas en internet, políticas de privacidad, **canal prioritario** puesto a disposición del público por parte de la AEPD, entre otros). Finalmente, destaca el deber de articular medidas para erradicar las situaciones de ciberacoso cuando el riesgo de que pudiera suceder ya se haya actualizado en la vida social y laboral de las personas víctimas (deber de colaborar con las autoridades para la erradicación de estas situaciones; el deber de denunciar cuando sean conocedores de situaciones de ciberacoso de género; el deber de poner en marcha los mecanismos de actuación previstos en sus políticas de prevención).

Informes de Responsabilidad Corporativa del Grupo AXA España y Estado de Información No Financiera de AXA Seguros Generales de los años 2019 y 2020: "*Protegemos lo que importa*", así como su ***Protocolo de actuación en situaciones de acoso*** (sexual, por razón de género, moral) **o "*ciberacoso*".**

No solo contiene una definición (aunque no muy precisa), sino que incluye un catálogo ejemplificativo de conductas constitutivas de ciberacoso laboral. Establece el típico

Violencia en línea y ciberacoso, riesgos psicosociales en entornos laborales digitalizados: cómo detectarlos, prevenirlos y/o erradicarlos

Online violence and cyberbullying, psychosocial risks in digitalized work environments: how to detect, prevent and/or eradicate them

principio de corresponsabilidad de todas las personas de la empresa en la alerta frente a estas conductas: los deberes de colaboración en su corrección y de sujeción a eventuales responsabilidades por el mero reenvío digital

Cláusula de corresponsabilidad:

En el ciberacoso toda persona que sea conocedora de estos hechos tiene la responsabilidad de ponerlo en conocimiento inmediato de la empresa para que se tomen las medidas adecuadas. Cualquier persona que participe reenviando y/o difundiendo sin denunciarlo podrá ser considerado igualmente responsable".

II Protocolo de prevención y actuación contra el acoso y ciberacoso sexual, por razón de sexo, por orientación sexual y por identidad y/o expresión de género **en la UC3M** (aprobado por el Consejo de Gobierno en sesión de 14 de noviembre de 2019) (recientemente ha sido condenado un alumno —de edad madura— por ciberacoso sexual y sexista a tres profesoras de la Universidad de Cádiz, en virtud de una condena por tres delitos contra la integridad moral).

Otras Universidades han seguido su estela (**Granada**, Sevilla, La Rioja, etc.). De nuevo, después, en la política preventiva, no se resalta ni una sola especificidad respecto de las situaciones de ciberacoso sexual en el trabajo, que se va repitiendo en todos los ámbitos de actuación, pero sin singularidad alguna.

Protocolo de Prevención y Actuación frente a la Violencia en el Trabajo (con un origen externo, no interno —que tiene su protocolo propio, que también incluye la palabra ciberacoso, pero dentro del acoso sexual mediante actos no verbales o comunicación virtual—) **en las instituciones sanitarias del Servicio Madrileño de Salud** (RESOLUCIÓN 92/2019, de 1 de marzo, de la Dirección General del Servicio Madrileño de Salud).

4. **Incluir también explícitamente la violencia digital y el ciberacoso laboral en el régimen disciplinario de la empresa, en línea con la visualización sugerida o recomendada en el ámbito preventivo**

Como obligación (aún cualificada) de medios, no de resultados, cabría proponer como medidas:

- controles aleatorios en los sistemas de comunicación corporativos (chats) de mensajes inapropiados (insultos, falta de respeto, contenido de carácter sexual compartido de manera automatizada, etc.
- canal de denuncias anónimo dentro del propio sistema de comunicaciones (será el caso del protocolo de acoso y ciberacoso del Grupo Axa).

5. **Inclusión de la prevención de la violencia digital y el ciberacoso en el trabajo en las políticas internas de usos razonables de las TIC y de las redes sociales, internas y externas**

Un ejemplo de **política de usos adecuados de redes es el Grupo Capgemini**. En ella se establecen las expectativas del Grupo sobre cómo sus personas empleadas deben comportarse en sus cuentas sociales, eso sí, siempre que opinen o expresen mensajes que estén relacionados con su trabajo en la compañía. No obstante, piensa más en la imagen de empresa que en las personas, pero puede bien utilizarse en sentido más bidireccional, lo que será más probable si en vez de unilateral esta política se negocia con la representación laboral o sindical.

6.

Para saber más

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (2019). *La protección de datos como garantía en las políticas de prevención del acoso: recomendaciones de la AEPD*. https://www.aepd.es/sites/default/files/2019-12/recomendaciones-sobre-acoso-digital-aepd.pdf

ÁLVAREZ DEL CUBILLO, A. (2021). "El ciberacoso en el trabajo como categoría jurídica". *Temas Laborales*, n. 157/2021, pp.167-192.

MOLINA NAVARRETE, C (2019). "Redes sociales digitales y gestión de riesgos profesionales: prevenir el ciberacoso sexual en el trabajo, entre la obligación y el desafío". *Diario la ley*, n. 9452, 2019 https://diariolaley.laleynext.es/dll/2019/07/09/redes-sociales-digitales-y-gestion-de-riesgos-profesionales-prevenir-el-ciberacoso-sexual-en-el-trabajo-entre-la-obligacion-y-el-desafio

MOLINA NAVARRETE, C (2019). El ciberacoso en el trabajo, como identificarlo, prevenirlo y erradicarlo en las empresas. Editorial La ley, Wolters Kluwer

VICENTE PACHÉS, F (2020). "El Convenio 190 de la OIT y su trascendencia en la gestión preventiva de la violencia digital y el ciberacoso en el trabajo". *Revista trabajo y Seguridad social CEF*, n. 448/julio 2020.

PORNARI, C. D.; WOOD, J. 2010. "Peer and Cyber Aggression in Secondary School Students: The Role of Moral Disengagement, Hostile Attribution Bias, and Outcome Expectancies", en *Aggressive Behavior*,Vol. 36, págs. 81-94.

Webgrafía

BAREA, MERCEDES. **El ciberacoso laboral como riesgo psicosocial emergente** https://afforhealth.com/el-ciberacoso-laboral-como-riesgo-psicosocial/