Publicar fotos de compañeros sin permiso: el error digital que puede costarte muy caro

Derecho a la imagen, consentimiento y consecuencias legales explicados sin rodeos. Porque una foto publicada sin permiso no es solo un malentendido: puede ser un delito.

Publicar fotos de compañeros sin permiso puede violar el derecho a la imagen y acarrear sanciones graves. Descubre qué dice la ley y cómo protegerte.

ETIQUETAS: derecho a la imagen, consentimiento digital, privacidad en el trabajo, RGPD fotos, ciberseguridad personal, protección de datos empleados, redes sociales y trabajo, imagen y privacidad 2026

La foto que "no le importa a nadie" puede arruinarte el año

Imagina la escena: fiesta de empresa, almuerzo de equipo, evento de networking. Alguien saca el móvil, hace una foto del grupo y la publica en LinkedIn con el hashtag de la empresa. Treinta likes, algún comentario simpático, y todo el mundo tan contento.

Ahora imagina que en esa foto aparece una persona que ese día preferiría no haber estado ahí. Que quizás está atravesando un proceso personal complicado. Que no quería que su imagen apareciera asociada a esa empresa, a ese evento, o simplemente en internet. Que nadie le preguntó.

¿Parece una reacción exagerada? No lo es. Y en 2026, con la trazabilidad digital que existe, las implicaciones van mucho más allá de un malestar momentáneo.

Publicar una foto de otra persona sin su consentimiento no es solo una cuestión de buenas maneras. Es, en muchos contextos, una infracción legal. Y el hecho de que todo el mundo lo haga no lo convierte en algo legal.

El derecho a la imagen no es un concepto abstracto

En España, el derecho a la propia imagen está reconocido en el **artículo 18.1 de la Constitución** como un derecho fundamental. No es una cláusula menor: está al mismo nivel que el honor y la intimidad personal. La **Ley Orgánica 1/1982** lo desarrolla específicamente, estableciendo que cualquier captación, reproducción o publicación de la imagen de una persona sin su consentimiento puede constituir una intromisión ilegítima.

Añade a eso el **Reglamento General de Protección de Datos (RGPD)** de la Unión Europea, que entró en vigor en 2018 y sigue siendo el marco legal de referencia. La imagen de una persona es, a todos los efectos, un dato personal. Y los datos personales no se tratan sin base legitimadora. En el contexto laboral y profesional, esa base legitimadora es casi siempre el **consentimiento explícito, informado y libre**. No el consentimiento tácito. No el "si no dices nada, entiendo que sí". El consentimiento real.

¿La consecuencia práctica? Si publicas una foto de un compañero de trabajo sin que él o ella lo haya autorizado expresamente, puedes estar infringiendo su derecho fundamental a la imagen y violando la normativa de protección de datos al mismo tiempo.

El mito del "contexto público" y por qué no te protege

Uno de los argumentos más habituales cuando se explica este tema es el siguiente: "Pero si estábamos en un evento, en una sala, en un espacio público... ¿no se puede fotografiar lo que es público?"

La respuesta corta es: depende, y casi nunca de la forma que imaginas.

El hecho de que alguien esté en un espacio de acceso no restringido no implica que haya renunciado a su derecho a la imagen. La jurisprudencia española y europea es clara en este sentido: estar en un lugar accesible no equivale a consentir la captación y difusión de tu imagen. Hay una diferencia fundamental entre ser visto en un lugar y ser fotografiado, editado y publicado en internet con nombre, empresa y cargo.

En el entorno laboral, esta distinción es todavía más relevante. Un trabajador no puede ser considerado como que ha prestado consentimiento a la publicación de su imagen simplemente por acudir a una reunión de empresa, una formación, una comida de equipo o un evento corporativo. La asistencia no equivale a autorización de uso de imagen.

Esto tiene implicaciones directas para los departamentos de comunicación, marketing y recursos humanos de cualquier organización, pero también para el empleado de a pie que publica desde su cuenta personal.

Las consecuencias legales que casi nadie menciona

La teoría está bien, pero lo que de verdad importa son las consecuencias. Y estas pueden ser más serias de lo que parece a primera vista.

En el plano civil, la persona afectada puede reclamar una indemnización por daños morales. Los tribunales españoles han reconocido este tipo de reclamaciones en múltiples ocasiones, y el importe no es simbólico: puede incluir el daño reputacional, el impacto emocional documentado y los perjuicios derivados de la difusión.

En el plano administrativo, la Agencia Española de Protección de Datos (AEPD) tiene competencia para investigar y sancionar a personas físicas y jurídicas que traten datos personales, incluyendo imágenes, sin base legitimadora. Las multas bajo el RGPD pueden alcanzar los 20 millones de euros para empresas o el 4% de la facturación global anual,

aunque en infracciones menores las sanciones son proporcionalmente inferiores. Lo relevante no es solo el importe: una resolución de la AEPD es pública y puede tener un impacto reputacional significativo.

En el plano penal, en los casos más graves, la captación, reproducción o divulgación no consentida de imágenes que vulneren la intimidad puede constituir un delito bajo el **artículo 197 del Código Penal**, con penas de prisión. Es el extremo del espectro, pero existe.

Y más allá del marco legal estricto: en el entorno laboral, publicar imágenes de compañeros sin autorización puede derivar en procesos disciplinarios, conflictos de equipo e incluso constituir acoso, especialmente si las imágenes son utilizadas para ridiculizar, señalar o exponer a una persona en un contexto no deseado.

El consentimiento: cómo se da, cómo se retira y qué forma debe tener

El consentimiento en materia de imagen tiene características específicas que conviene conocer.

Para ser válido, debe ser **libre** (sin presión ni coacción, lo que implica que en relaciones laborales con asimetría de poder hay que tener especial cuidado), **informado** (la persona debe saber para qué se usará la imagen, en qué canales, con qué alcance y durante cuánto tiempo), **específico** (no vale un consentimiento genérico para "todo": debe ser para usos concretos) y **revocable** (puede retirarse en cualquier momento, y ese derecho no puede eliminarse contractualmente).

Una firma en un contrato laboral que diga genéricamente "el empleado consiente el uso de su imagen en comunicaciones de la empresa" es, en términos de RGPD, de dudosa validez. No porque no exista, sino porque la falta de libre elección en una relación laboral hace que ese consentimiento sea cuestionable. Las empresas deben buscar fórmulas más específicas y documentar cada autorización de uso.

Para particulares que publican desde cuentas personales, la lógica es la misma, aunque menos formalizada: antes de publicar, pregunta. Y si alguien te pide que retires una imagen, retírala. No hacerlo puede agravar la situación legal y deteriorar irreparablemente la relación profesional.

El ecosistema OSINT y la trazabilidad de las imágenes en 2026

Hay una dimensión de este problema que va más allá del momento de la publicación: la permanencia y trazabilidad de las imágenes en el entorno digital.

En 2026, las herramientas de búsqueda inversa de imágenes, combinadas con técnicas de OSINT (Open Source Intelligence), permiten rastrear una foto publicada en LinkedIn, identificar a la persona, cruzar esa información con otras fuentes públicas y construir un perfil detallado sin que nadie haya tomado una decisión deliberada de exponer a esa persona.

Una foto de empresa donde aparece alguien puede ser el primer eslabón de una cadena de correlación de datos que, en el peor de los casos, facilita desde acoso hasta suplantación de identidad. No es ciencia ficción: es la infraestructura de datos que ya existe y que se vuelve más sofisticada cada año.

Por eso, la decisión de publicar la imagen de otra persona no debería evaluarse solo en el contexto de ese momento, sino considerando qué parte de la superficie de exposición digital de esa persona estás ampliando sin su permiso.

Reflexión estratégica: cultura digital en el entorno profesional

El problema de fondo no es técnico ni legal. Es cultural.

Vivimos en un entorno donde compartir es la norma y el freno es la excepción. Las redes sociales han instalado en nuestra conducta digital un reflejo casi automático: si algo es memorable, se fotografía; si se fotografía, se publica. Y esa automaticidad choca frontalmente con los derechos individuales en el espacio digital.

Las organizaciones que entienden esto no se limitan a redactar una cláusula en el contrato y olvidarse del asunto. Construyen protocolos claros, forman a sus equipos, nombran responsables de comunicación que conocen la normativa y crean una cultura donde pedir permiso antes de publicar la imagen de alguien no se percibe como un trámite burocrático, sino como un estándar de respeto profesional.

Y los individuos que entienden esto, tanto en su rol de posibles publicadores como en el de potenciales fotografiados, empiezan a gestionar su presencia digital con la misma deliberación con la que gestionarían cualquier otro aspecto de su reputación.

La ciberseguridad no empieza cuando un hacker intenta entrar en tus sistemas. Empieza cuando alguien saca el móvil en una reunión y decide, en décimas de segundo, qué hace con lo que captura.

Tu próximo paso (no requiere ser abogado)

Tres acciones concretas que puedes hacer hoy:

Revisa las imágenes que tienes publicadas en redes profesionales donde aparezcan otras personas y verifica que dispones de su autorización. Si no la tienes, considera retirarlas o pedirla ahora. Si tienes responsabilidad sobre comunicación en tu empresa, introduce un formulario de autorización de imagen para eventos corporativos, sencillo y comprensible. Y antes de la próxima foto de equipo, pregunta. Es un gesto pequeño con un impacto grande, tanto en términos legales como de cultura de equipo.

Si este artículo te ha resultado útil, compártelo con tu equipo y con cualquier persona que gestione comunicación o redes sociales en su empresa. Una cultura digital más consciente es responsabilidad de todos. Visita el blog para acceder a más recursos gratuitos sobre seguridad digital aplicada y privacidad en entornos profesionales.

Isaac Ruiz Romero