

DIPUTACIÓ DE
VALENCIA



Protecció de Dades i Seguretat de la Informació



Boletín protección de datos

Boletín del Departamento de protección de datos y Seguridad
de la Información de la Diputación Provincial de Valencia

Boletín N.º 6 | Diciembre 2020

**CONSECUENCIAS ADMINISTRATIVAS, DISCIPLINARIAS, CIVILES
Y PENALES DE LA DIFUSIÓN DE CONTENIDOS SENSIBLES**



Í N D I C E



CONSECUENCIAS ADMINISTRATIVAS, DISCIPLINARIAS, CIVILES Y PENALES DE LA DIFUSIÓN DE CONTENIDOS SENSIBLES

	Página
INTRODUCCIÓN	2
¿EN QUÉ RESPONSABILIDADES PUEDE INCURRIR QUIEN DIFUNDA ILEGÍTIMAMENTE CONTENIDOS SENSIBLES DE TERCEROS?	3
¿CÓMO SOLICITO LA ELIMINACIÓN DE FOTOS O DE VÍDEOS PUBLICADOS EN INTERNET	5
MATERIAL COMPLEMENTARIO	8
NOTICIAS DE ACTUALIDAD	8



Os invitamos a trasladarnos aquellas temáticas que resulten de vuestro interés para los próximos boletines informativos. Estas peticiones deberán dirigirse a:

Diputación de Valencia

Dpto. de Protección de Datos y
Seguridad de la Información

Pl. de Manises, 4 46003 Valencia

email: dpdssi@dival.es

SUSCRIPCIONES

Si deseas suscribirse a nuestro Boletín informativo accede al siguiente

[enlace](#)



INTRODUCCIÓN

La proliferación de dispositivos móviles y el acceso generalizado a Internet están propiciando la difusión, en muchas ocasiones de manera ilegítima y descontrolada, de nuestros datos personales a través de perfiles en redes sociales, aplicaciones de mensajería y otros sitios web.

En este contexto, es cada vez más frecuente que se publiquen y se difundan audios, imágenes o videos, en ocasiones de carácter sexual o violento, incluso de menores de edad y de otros colectivos vulnerables.

De hecho, en la actualidad, la grabación y difusión de imágenes personales es uno de los instrumentos más utilizados en los casos de acoso, tanto en el entorno laboral – *mobbing* –, como en el escolar –*bullying* –, y su versión a través de internet – *cyberbullying* –.

Quien difunda ilegítimamente contenidos sensibles de terceros puede incurrir en distintos tipos de responsabilidad: disciplinaria, administrativa, penal o patrimonial. Además, en el entorno laboral, el empleador también podría llegar a ser sancionado, bien por no haber evaluado el riesgo laboral adecuadamente, incluidos los denominados riesgos psicosociales, o por no haber adoptado las medidas de prevención adecuadas.

Si bien los buscadores, foros, blogs y redes sociales más populares ofrecen mecanismos y formularios para comunicarles la vulneración de la privacidad o la publicación de contenidos inapropiados, para la atención de situaciones excepcionalmente delicadas, que estén poniendo en alto riesgo los derechos y libertades de los afectados, siempre que éstos sean ciudadanos españoles o se encuentren en España, y especialmente si se trata de menores de edad o de víctimas de violencia por razón de género, la Agencia Española de Protección de Datos (AEPD) ha habilitado el ‘Canal Prioritario’, al que pueden acudir tanto las víctimas como cualquier persona que tenga conocimiento de la difusión de este tipo de contenidos.



“QUIEN DIFUNDA ILEGÍTIMAMENTE CONTENIDOS SENSIBLES DE TERCEROS PUEDE INCURRIR EN DISTINTOS TIPOS DE RESPONSABILIDAD: DISCIPLINARIA, ADMINISTRATIVA, PENAL O PATRIMONIAL. ADEMÁS, EN EL ENTORNO LABORAL, EL EMPLEADOR TAMBIÉN PODRÍA LLEGAR A SER SANCIONADO, BIEN POR NO HABER EVALUADO EL RIESGO LABORAL ADECUADAMENTE, INCLUIDOS LOS DENOMINADOS RIESGOS PSICOSOCIALES, O POR NO HABER ADOPTADO LAS MEDIDAS DE PREVENCIÓN ADECUADAS.”



¿EN QUÉ RESPONSABILIDADES PUEDE INCURRIR QUIEN DIFUNDA ILEGÍTIMAMENTE CONTENIDOS SENSIBLES DE TERCEROS?

Como indicábamos, los ciudadanos que difundan de manera ilegítima contenidos sensibles de terceros pueden incurrir en distintos tipos de responsabilidad.

RESPONSABILIDAD DISCIPLINARIA

En el ámbito laboral, las personas trabajadoras que lleven a cabo estas conductas podrían incurrir en responsabilidad disciplinaria (art. 58 del Estatuto de los Trabajadores; art. 93 del Estatuto Básico del Empleado Público), pudiendo acarrear el despido o la separación del servicio.

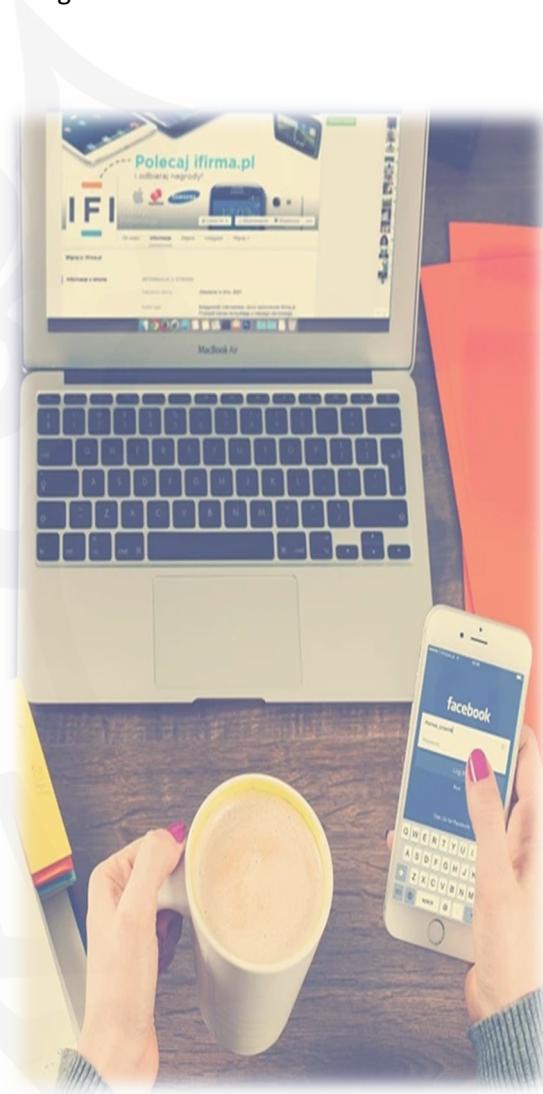
RESPONSABILIDAD ADMINISTRATIVA

La difusión de datos especialmente sensibles de una persona física (en contenidos tales como imágenes, audios o vídeos de carácter sexual o violento que permitan identificarla), publicados en diferentes servicios de internet sin consentimiento se considera un tratamiento ilícito de datos personales.

La Agencia Española de Protección de Datos es competente para investigar este tipo de actuaciones, y si considera que se ha infringido la Ley, podrá incoar el correspondiente procedimiento sancionador contra quienes lo han difundido o han contribuido a la difusión.

Infringe el RGPD (Reglamento General de Protección de Datos) y la LOPDGDD (Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales) quien obtiene ilícitamente los datos personales (imágenes, vídeos, audios u otros contenidos) o quien los difunde (es decir, quien los reenvía, publica en internet) sin consentimiento del interesado.

Estas conductas se pueden sancionar con multas que en los casos más graves pueden alcanzar los 20 millones de euros.





RESPONSABILIDAD PENAL

Los casos que entrarían en el marco de lo que se denomina “*sexting, ciberacoso o ciberbullying*” generan consecuencias de varios tipos. El Código Penal engloba estos comportamientos en diferentes tipos delictivos.

La difusión y la cesión a terceros de imágenes o vídeos sin consentimiento, que menoscaben la intimidad de una persona física, son constitutivas de delito castigado con pena de prisión de tres meses a un año o multa de seis a doce meses en aquellos casos en que se hayan obtenido con la anuencia de la persona afectada en cualquier lugar fuera de la mirada de terceros, cuando la divulgación menoscabe gravemente la intimidad personal de esa persona (art. 197.7 del Código Penal).

Asimismo, podrían constituir un delito contra la integridad moral, castigado con pena de prisión de seis meses a dos años (artículo 173.1 del Código Penal).

Cuando se cometan por menores de edad la Ley Orgánica de Responsabilidad Penal del Menor (LORPM) prevé en su artículo 71, un amplio abanico de medidas que se pueden adoptar y que dependerá de las circunstancias del menor: desarrollo evolutivo, antecedentes..., y que normalmente son la realización de servicios en beneficio de la comunidad, o tareas socio educativas, pudiendo llegar a la libertad vigilada e incluso a la privación de libertad (internamiento en centros o permanencia de fin de semana).

RESPONSABILIDAD PATRIMONIAL

Los ciudadanos podrían tener que indemnizar a la víctima por los daños y perjuicios que se deriven de la conducta ilícita, tanto materiales como morales. En el caso de los menores, responderían solidariamente con ellos sus padres o tutores, acogedores y guardadores legales o de hecho.

Igualmente, están obligados a responder de la misma forma por los daños materiales y morales causados cuando se produzcan por menores de 14 años, ante la jurisdicción civil.

“INFRINGE LA NORMATIVA DE PROTECCIÓN DE DATOS QUIEN OBTIENE ILÍCITAMENTE LOS DATOS (IMÁGENES, VÍDEOS, AUDIOS U OTROS CONTENIDOS) O QUIEN LOS DIFUNDE (ES DECIR, QUIEN LOS REENVÍA, PUBLICA EN INTERNET) SIN CONSENTIMIENTO”



¿CÓMO SOLICITO LA ELIMINACIÓN DE FOTOS O DE VÍDEOS PUBLICADOS EN INTERNET?

La difusión de imágenes o vídeos publicados en diferentes servicios de internet sin que exista legitimación para tratar este dato es un asunto que se plantea con frecuencia ante la AEPD.

El RGPD reconoce a las personas el ejercicio del derecho de supresión, por lo que, si fuera posible, habría que contactar con quien subió el contenido solicitándole su eliminación.

Si no consiguieras tu objetivo, deberías necesariamente solicitar el borrado a la plataforma que ha proporcionado los medios para la publicación, esto es, la red social o el portal de video en que se han publicado esas imágenes o vídeos, acreditando tu identidad e indicando qué enlaces son los que contienen los datos que quieras cancelar.

Se debe resolver sobre la solicitud de supresión en el plazo máximo de un mes a contar desde la recepción de la misma. Transcurrido ese plazo sin que de forma expresa respondan a la petición o si consideras que esa respuesta es insatisfactoria, se podría interponer la correspondiente reclamación ante la correspondiente autoridad de control, acompañando la documentación acreditativa de haber solicitado la supresión ante la entidad de que se trate.

Las redes sociales más populares, por su parte, disponen de mecanismos establecidos para comunicarles vulneraciones de la privacidad o contenidos inapropiados mediante sus propios formularios. Por ejemplo:

Google



La compañía dispone de una página desde la que se puede solicitar la retirada de contenido de sus diferentes servicios. En el caso del servicio de vídeos YouTube, se ofrecen diferentes opciones en caso de abuso o acoso, vulneraciones de la privacidad, denuncia de contenidos sexuales, contenidos violentos u otros problemas. Por otro lado, si consideras que un vídeo colgado en YouTube incluye un contenido inapropiado puedes utilizar el ícono con forma de bandera (Denunciar) para avisar del contenido y que la empresa lo revise.

Facebook



La red social ofrece un servicio de ayuda para avisar de fotos o vídeos que puedan infringir el derecho fundamental a la protección de datos. Facebook ofrece varias opciones en función de las circunstancias de cada caso concreto. También permite denunciar una conducta abusiva mediante el enlace Denunciar, que aparece situado junto a la mayoría de los contenidos publicados en Facebook.

Twitter



La red aglutina diferentes formas de informar sobre diversos incumplimientos, entre los que se encuentran la publicación de información privada en Twitter, la usurpación de identidad o el acoso.



Por último, las personas tienen derecho a solicitar, bajo ciertas condiciones, que los enlaces a sus datos personales no figuren en los resultados de una búsqueda en internet realizada por su nombre. La sentencia del Tribunal de Justicia de la UE confirmó que las personas tienen derecho a limitar la difusión universal e indiscriminada de sus datos personales en los buscadores generales cuando la información es obsoleta o ya no tiene relevancia ni interés público, aunque la publicación original sea legítima (en el caso de boletines oficiales o informaciones amparadas por las libertades de expresión o de información).

“EL RGPD RECONOCE A LAS PERSONAS EL EJERCICIO DEL DERECHO DE SUPRESIÓN, POR LO QUE HABRÍA QUE CONTACTAR CON QUIEN SUBIÓ EL CONTENIDO SOLICITÁNDOLE SU ELIMINACIÓN. SI NO, SE DEBERÍA SOLICITAR EL BORRADO A LA PLATAFORMA QUE HA PROPORCIONADO LOS MEDIOS PARA LA PUBLICACIÓN. LAS REDES SOCIALES MÁS POPULARES DISPONEN DE MECANISMOS PARA COMUNICARLES VULNERACIONES DE LA PRIVACIDAD O CONTENIDOS INAPROPIADOS.”

Este canal se ha habilitado para actuar con celeridad ante situaciones excepcionalmente delicadas, cuando los contenidos tengan carácter sexual o muestren actos de agresión y se estén poniendo en alto riesgo los derechos y libertades de los afectados, siempre que éstos sean ciudadanos españoles o se encuentren en España, especialmente si se trata de menores de edad o de víctimas de violencia de género. Pueden acudir a este canal tanto el afectado como cualquier persona que tenga conocimiento de la difusión de este tipo de contenidos.

Ahora bien, la AEPD hace hincapié en que únicamente debe acudirse a este canal ante una situación de excepcional gravedad de las señaladas anteriormente, pues fuera de estos supuestos existen otras vías para solicitar la retirada de contenidos. Se refiere a los mecanismos y formularios que los buscadores, foros, blogs y redes sociales más populares ofrecen para comunicarles la vulneración de la privacidad o la publicación de contenidos inapropiados, a los que hacíamos referencia en el apartado anterior.

Podrás presentar tu solicitud a través de la sede electrónica si dispones de un certificado válido o de cualquiera de los medios de autenticación soportados. Si no dispones de medios de autenticación, podrás imprimir el formulario generado al final del proceso y presentarlo en cualquier oficina de asistencia en materia de registros, en las oficinas de correos o en las representaciones diplomáticas y oficinas consulares de España, si te encuentras en el extranjero.



La solicitud deberá describir detalladamente las circunstancias en que se ha producido la difusión no consentida de los contenidos, indicando en particular si la persona afectada es víctima de violencia de género, abuso o agresión sexual o acoso y si pertenece a cualquier otro colectivo especialmente vulnerable: menores de edad (especificando si es menor de catorce años), personas con discapacidad o enfermedad grave o en riesgo de exclusión social u otros. Además, si el contenido está siendo difundido a través de Internet, también deberás copiar la dirección o direcciones web de acceso o identificar claramente el perfil social a través del que se están difundiendo. La AEPD también necesitará conocer si has llevado a cabo acciones para denunciar los hechos ante las instancias policiales (detallando, en tal caso, las instancias administrativas o judiciales concretas y la referencia de los procedimientos que se estén tramitando) o para limitar la difusión de los datos personales, identificando, en tal caso, a los prestadores de servicios (la red social, el portal de vídeo o de blogs...) a los que te has dirigido.

Una vez enviada la solicitud, junto a los documentos que consideres relevantes para la tramitación de la reclamación, la AEPD analizará la reclamación de forma prioritaria y, en su caso, ordenará la retirada del contenido al prestador del servicio o plataforma donde se esté difundiendo. Además, si hay indicios de delito, lo pondrán en conocimiento de la Fiscalía.



MATERIAL COMPLEMENTARIO

- “Consecuencias administrativas, disciplinarias, civiles y penales de la difusión de contenidos sensibles”, de la AEPD. Consulta el documento en [este enlace](#).
- “Eliminar fotos y vídeos de internet”, de la AEPD. Consulta [este enlace](#).
- Servicio de ayuda de Facebook para avisar de fotos o vídeos que puedan infringir el derecho fundamental a la protección de dato. Consulta [este enlace](#).
- Cómo retirar contenido de Google. Consulta [este enlace](#).
- Cómo denunciar incumplimientos en Twitter. Consulta este enlace.
- La sentencia del Tribunal de Justicia de la UE que establece que las personas tienen derecho a limitar la difusión universal e indiscriminada de sus datos personales en los buscadores generales cuando la información es obsoleta o ya no tiene relevancia ni interés público. Consulta la Sentencia en [este enlace](#).
- La protección de datos como garantía en las políticas de prevención del acoso: recomendaciones de la AEPD. Consulta el documento en [este enlace](#).
- Canal prioritario de retirada de contenidos sensibles de la AEPD. Consulta [este enlace](#).
- Infografía de la AEPD sobre el Canal Prioritario. Consulta la infografía en [este enlace](#).
- Preguntas Frecuentes sobre la difusión ilegítima de contenidos sensibles, de la AEPD. Consulta las FAQs en [este enlace](#).

NOTICIAS

- **Nueva sanción (apercibimiento) impuesta por la AEPD a un Ayuntamiento por no haber nombrado Delegado de Protección de Datos.** Las Administraciones públicas deben atender las obligaciones que el RGPD detalla, entre las que se incluye, la obligación de nombrar a un delegado de protección de datos y comunicarlo a esta AEPD. En el presente supuesto, la AEPD requiere al Ayuntamiento para que en el plazo de un mes acredite el cumplimiento de designar un Delegado de Protección de Datos, de conformidad con el artículo 37.1 del RGPD. Consulta la Resolución en [este enlace](#).
- **El Instituto Nacional de Ciberseguridad (INCIBE) nos da las claves para evitar riesgos de ciberseguridad desde el puesto de trabajo.** Fuga de datos, pérdida de información confidencial, infecciones por malware o deslices en el uso del correo electrónico o las redes sociales son algunos de los riesgos a los que nos enfrentamos en el puesto de trabajo. Es importante conocer las situaciones más comunes que se dan en el ámbito laboral, relacionadas con la seguridad del entorno de trabajo de los empleados para poder así minimizar el riesgo de fuga o pérdida de datos. Consulta el artículo en [este enlace](#).
- **INCIBE nos habla de las amenazas y riesgos a los que nos enfrentamos a través de códigos QR y nos ofrece consejos para evitar ser víctimas de ataques.** Con motivo de la nueva normalidad y las exigencias en materia sanitaria establecidas por parte del Ministerio de Sanidad, se ha producido un cambio de paradigma. Entre las medidas acordadas, destacan la eliminación de las cartas de menú o de los trípticos informativos en museos u oficinas de turismo, entre otras. Entre las alternativas que se han presentado para sustituir estos elementos, tenemos las aplicaciones para dispositivos móviles o el uso de códigos QR. No obstante, debemos plantearnos si esta alternativa es segura y las recomendaciones a seguir para no ser víctimas de ciberataques a través de esta. Consulta el artículo en [este enlace](#).
- **La AEPD aprueba su primer Código de Conducta bajo el RGPD.** El Código de Conducta de Tratamiento de Datos en la Actividad Publicitaria ha sido presentado por la Asociación para la Autorregulación de la Comunicación Comercial (AUTOCONTROL), y su contenido principal es el establecimiento de un sistema extrajudicial para tramitar reclamaciones sobre protección de datos y publicidad, ágil, eficaz y gratuito para los consumidores. Consulta el documento en [este enlace](#).