Práctica 2

Análisis de los casos 1 y 6

**Grupo 2D2**

**Participantes:**

* **David Arnal García**
* **Víctor Fayos Momparler**
* **Ángel Pérez González**
* **Josep Molina Martínez**

Caso 1: Un repartidor intenta ligar con una clienta a través de su nº de WhatsApp

1. Primer paso: noticias relacionadas

**Enlaces:**

* [**2000 euros de multa a instalador de fibra por mandar WhatsApp a una clienta**](https://www.adslzone.net/2018/07/18/multa-whatsapp-instalador-fibra/) **(ADSLZone, 2018)**
* [**Si te comunicas con tus clientes por WhatsApp también puedes ser multado por la AEPD**](https://www.pymesyautonomos.com/legalidad/si-te-comunicas-con-tus-clientes-por-whatsapp-tambien-puedes-ser-multado-por-la-aepd) **(Pymes y autónomos, 2018)**
* [**Las tres cosas que nunca debe hacer tu empresa si usa WhatsApp**](https://www.lasexta.com/tecnologia-tecnoxplora/internet/empresas/empresas-que-usan-whatsapp-que-debes-hacer_2014042557f784fb0cf2fd8cc6aa856c.html) **(La Sexta, 2014)**

**Explicación:**

La primera noticia está relacionada debido a que tampoco se respeta la privacidad del cliente, como en el caso original, ya que, de nuevo, un instalador de fibra óptica contacta con el cliente a través de WhatsApp sin su consentimiento.

La segunda noticia se relaciona con el caso mostrando qué papel tiene la Asociación Española de Protección de Datos (AEPD) en cuanto a la privacidad de los usuarios y sus consecuencias si son violadas, aspectos de vital importancia en el caso original debido a que se viola la privacidad del cliente.

Y la última noticia también está relacionada con el caso, ya que muestra cómo debe actuar correctamente una empresa a través de WhatsApp si cuenta con datos personales de clientes, es decir, como debería haber sido correcta una posible comunicación entre cliente y empresa, así como sus errores más comunes.

**Transcripciones:**

* **Noticia 1:**

# [**2000 euros de multa a instalador de fibra por mandar WhatsApp a una clienta**](https://www.adslzone.net/2018/07/18/multa-whatsapp-instalador-fibra/)

# **26/06/2018 - 16:53**

La **Ley de Protección de Datos** impide que una empresa pueda utilizar información que ha obtenido tras prestar un servicio para uso personal. Esto es lo que no debió entender un **instalador de fibra**, que **contactó por WhatsApp a una clienta** tras haberle realizado una instalación con el objetivo de **ligar con ella**, lo cual ella rápidamente denunció a la policía.

## **Intentó ligar con una clienta por WhatsApp tras instalar la fibra**

Así lo ha desvelado [**Samuel Parra**](https://www.samuelparra.com/2018/07/17/2000-euros-de-multa-al-instalador-de-movistar-que-utilizo-los-datos-de-la-clienta-para-ligar-con-ella/), abogado especialista en privacidad y protección de datos, en su blog. El demandado, tras haberle realizado una instalación de Movistar a la clienta, pasó a enviarle **mensajes con objetivo personal y sexual** mediante WhatsApp, en los cuales hacía **referencia a sus atributos físicos y le proponía quedar.**

La afectada fue rápidamente a **denunciar lo ocurrido a la Policía Nacional y a la Agencia Española de Protección de Datos**, ya que se sintió **acosada** por una persona que **conocía su dirección, su nombre y sus horarios**. El instalador, que fue contactado posteriormente por la AEPD, **no negó haber contactado a la clienta**, y se defendió argumentando que “lo hacía con **buenas intenciones** y con el fin de **subirle la autoestima** a la clienta”.

Esto no exime al instalador de no haber cumplido con el **artículo 6 de la Ley Orgánica de Protección de Datos**, que establece que “el tratamiento de los datos de carácter personal requerirá el **consentimiento inequívoco del afectado,** salvo que la ley disponga otra cosa.”. Además, el **artículo 4.2** determina que “los **datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos**”. Por ello, el instalador no podía contactar a la clienta por motivos que no estuvieran relacionados con la instalación que le iba a realizar ese día.

## **2.000 euros de multa que podrían haber sido mucho más**

Tratar los datos de personas sin su consentimiento puede llegar a ser **multado con entre 40.000 y 300.000 euros**, pero en este caso se ha dejado la cuantía en **2.000 euros**, de los cuales se abonarán **1.600 por pronto pago**. En el caso de que hubiera reconocido responsabilidad, la multa habría sido un 20% inferior, pero no ha sido así.

Esta sanción supone un caso **ejemplarizante para evitar que este tipo de conductas se repitan.** Por desgracia, este comportamiento está muy extendido en instaladores o repartidores que van a viviendas de los clientes. Sin embargo, mientras que un repartidor es un trabajador de una empresa, en este caso el instalador iba como persona física a realizar una actividad personal y doméstica.

Por ello, los mensajes iban a persona física a persona física, aunque para obtener esos datos se utilizó un **fichero que tiene como objetivo contactar con el cliente** para realizar una **actividad profesional** y distinta de la que lo utilizó el instalador, que fue intentar ligar con la afectada.

* **Noticia 2:**

**Si te comunicas con tus clientes por WhatsApp también puedes ser multado por la AEPD**

**21 Marzo 2018. Actualizado 28 Marzo 2018, 00:16**

La AEPD ha sancionado recientemente a [Facebook y WhatsApp](https://www.genbeta.com/actualidad/no-seria-descabellado-pedirle-1-000eur-a-facebook-y-whatsapp-que-podemos-hacer-tras-la-multa-de-la-aepd) con 300.000 euros a cada compañía por cruzar datos entre ellas sin el consentimiento expreso de los usuarios. Ahora bien, son muchas las empresas que utilizan la aplicación de mensajería instantánea de **WhatsApp para comunicarse con sus clientes, ¿podrían también ser multadas?** Todo esto siempre que las citadas empresas no acaben recurriendo y acaben por darles la razón, algo poco probable por otro lado.

Aquí hay que tener en cuenta dos cuestiones. Por un lado ¿quién es el responsable de la gestión de los datos de los clientes? Y por otro si se ha recogido el consentimiento escrito o no del cliente para el tratamiento de dichos datos y cómo se ha realizado. Hasta ahora la sanción afecta solo a las empresas que han realizado un tratamiento incorrecto de los datos personales, Facebook y WhatsApp. Pero todo cambia a partir de la entrada en vigor del [nuevo RGPD](https://www.pymesyautonomos.com/legalidad/perdido-con-el-nuevo-reglamento-de-proteccion-de-datos-la-aedp-acude-al-rescate-con-estas-guias).

A partir del próximo 25 de mayo, fecha de entrada en vigor del nuevo reglamento, **los autónomos y empresa que utilicen WhatsApp con sus clientes podrían ser multados** al ser éstos los responsables del tratamiento de los datos de sus clientes, sobre todo si no se ha requerido el consentimiento del afectado de forma libre, informado y específico. Es decir, hay que advertir que WhatsApp puede compartir sus datos con la red social de forma clara para que el usuario acabe consintiendo dicho traspaso de información.

Lo malo es que en muchas ocasiones **la comunicación no se realiza desde un teléfono de empresa**, sino que en muchos casos es el propio empleado el que facilita el suyo en algún momento para [facilitar la comunicación con los clientes](https://www.pymesyautonomos.com/tecnologia/por-que-estamos-usando-mal-whatsapp-con-nuestros-clientes). Lo cierto es que es algo que agiliza mucho la comunicación, que todo el mundo tiene instalado y por ello es fundamental recoger correctamente los consentimientos de los usuarios.

La otra opción es utilizar otras aplicaciones de mensajería instantánea que mejoren la privacidad pero a cambio se pierde la comodidad de que sea una **solución que todo el mundo utiliza ya en sus teléfonos** y se fuerza al cliente a utilizar aquella que nosotros decidimos. Mejor redactar de forma adecuada los consentimientos para seguir utilizando como hasta ahora WhatsApp.

* **Noticia 3:**

# **Las tres cosas que nunca debe hacer tu empresa si usa WhatsApp**

**25/04/2014**

Con el crecimiento y expansión de WhatsApp en todo el mundo, muchas empresas han echado mano de esta aplicación para hacer su negocio más atractivo y fácil de encontrar. Aunque puede resultar una buena herramienta para empresas, hay algunas prácticas que tu empresa jamás debe hacer.

WhatsApp es una aplicación que se ama y se odia a partes iguales. No hay duda que todo el mundo con un smartphone la usa, o por lo menos la ha usado hasta hace relativamente poco, según atestigua el número de [500 millones de usuarios activos al mes](http://www.tecnoxplora.com/empresas/whatsapp-acalla-rumores-cierre-anunciando-que-llega-500-millones-usuarios_2014042300080.html). Pero no solo hay 500 millones de personas conectadas intercambiando fotos y vídeos, también hay empresas.

Muchas de ellas han visto en WhatsApp una forma de comunicarse con potenciales clientes. Con que te tengan en tu libreta de contactos ya es suficiente para poder comunicarse contigo, y eso ha provocado que empresas, tanto grandes como pequeñas, usen la app para hablar con sus clientes, quizá creando un vínculo más personal entre ambos y mejorando el negocio.

Con un vistazo rápido a Twitter podemos encontrar cientos de menciones de empresas y negocios que usan WhatsApp para por ejemplo [hacer reservas](https://twitter.com/search?q=whatsapp%20reservas&src=typd&mode=photos), o incluso empresas de reparación que agregan el número de teléfono [para comunicar errores](http://instagram.com/p/msXVoKshUJ/).

Pero como empresas, hay que tener mucho cuidado con lo que se comunica mediante mensajería.

**Errores más comunes**

El primer error que las empresas cometen es el uso de WhatsApp en sí. La aplicación, aunque popular, se ha demostrado continuamente que es insegura para transmitir datos importantes y privados. La seguridad de tus clientes o de tus usuarios debería serlo todo, y usar WhatsApp crea una vía rápida de comunicación, pero **muy insegura** (para muestra, [el último caso](http://www.tecnoxplora.com/apps/whatsapp-confirma-otro-fallo-seguridad-donde-vives-donde-trabajas_2014042100094.html)).

Como parte de esta inseguridad, es una locura compartir documentos importantes de tu empresa mediante WhatsApp, y mucho menos información que pueda comprometer tu negocio.

Otro de los errores más comunes que se han encontrado es **la gestión desde un solo número** en servicios que muchas personas podrían usar. Contrata varias líneas y gestiona desde diferentes equipos o personas las incidencias, esto no hará que se queden una larga lista de incidencias o mensajes por leer. Divide y vencerás.

Muchos de los problemas de brechas de seguridad que tienen WhatsApp y otras aplicaciones de mensajería usadas para conectar con clientes y trabajadores de una misma empresa es el uso del terminal como algo personal. Esto es algo muy normal hoy en día: es el llamado [BYOD](http://es.wikipedia.org/wiki/BYOD) -Bring Your Own Device (“trae tu propio dispositivo”)- en el que cada vez más, en las empresas se permite el móvil personal como dispositivo de trabajo.

Pero cuando un móvil se usa para comunicarse con clientes eso es un gran error. Nunca deberías usar un dispositivo dedicado a la comunicación de esta forma como tu propio móvil. Sobre todo usarlo para descargar decenas de aplicaciones 'para probar' ya que en plataformas como Android es un riesgo: se han visto casos de aplicaciones que usaban los datos de la aplicación WhatsApp o Telegram para quién sabe qué.

**Protección de datos**

Lo más preocupante del uso de WhatsApp por parte de empresas es sin duda **el desconocimiento de la Ley de Protección de Datos.** Esta Ley es muy dura con empresas que comentan o usan datos personales de clientes por canales que jamás deberían pasar. Y menos por canales inseguros.

[En los términos de uso de WhatsApp](http://www.tecnoxplora.com/empresas/esto-que-firmas-lees-cuando-das-alta-whatsapp_2013110600445.html) se indica que no pueden garantizar la seguridad de los datos que se transmiten, y es el usuario el que asume el riesgo de la información que estás a punto de compartir.

Usar datos personales mediante WhatsApp se puede considerar como un incumplimiento de las obligaciones de las empresas ante la protección de datos, **con unas multas que pueden llegar desde los 900€ hasta los 600.000€.** Esto incluye desde el número de teléfono, el estado, la fecha y hora de conexión e incluso la foto de perfil. “Las empresas son responsables jurídicas de los datos personales que custodian de sus clientes y, como tales, están sujetas a la Ley Orgánica de Protección de Datos, que contempla como dato personal cualquier información que identifica o hace identificable a una persona física”, explica Natalia Esteban-Zazo, abogada de [DAS](http://www.das.es/es) acerca de la protección de datos en estas plataformas.

Quizá la mejor herramienta de la empresa ante esta situación, de seguir queriendo usar WhatsApp o cualquier aplicación de mensajería para comunicarse con clientes, es obtener el consentimiento del cliente para el uso de este tipo de aplicaciones, incluyéndose como una cláusula en contratos para que ambas partes autoricen los canales de comunicación. El problema es, que en muchos negocios donde no hay contratos de por medio, esto es prácticamente imposible de lograr.

1. Segundo paso: legislación

Para este caso, se podría decir que la legislación oportuna es:

[Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales](https://www.boe.es/buscar/pdf/2018/BOE-A-2018-16673-consolidado.pdf)

Esto se puede inducir debido a que dicha ley está relacionada con la protección de los datos personales de las personas, así como la garantía de los derechos digitales, y se puede relacionar con el caso en el artículo número 6, que regula el tratamiento basado en el consentimiento del afectado, observando que se llega a incumplir el punto 3: *«No podrá supeditarse la ejecución del contrato a que el afectado consienta el tratamiento de los datos personales para finalidades que no guarden relación con el mantenimiento, desarrollo o control de la relación contractual.»,* así como el artículo número 5, específicamente el punto 1: *«Los responsables y encargados del tratamiento de datos así como todas las personas que intervengan en cualquier fase de este estarán sujetas al deber de confidencialidad al que se refiere el artículo 5.1.f) del Reglamento (UE) 2016/679»,* punto cuya referencia incluye el reglamento (UE) 2016/679:

[REGLAMENTO (UE) 2016/ 679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO - de 27 de abril de 2016](https://www.boe.es/doue/2016/119/L00001-00088.pdf)

que incluye el citado artículo número 5, cuyo punto 1. f) hace referencia a que los datos personales serán: *«tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»).»,* pudiendo extraer, como conclusión, que el acusado no cumple ningún artículo de los citados anteriormente, ya que no se cumple la confidencialidad del cliente al utilizar sus datos personales, así como tampoco se respeta su privacidad vulnerando sus derechos como persona.

1. Sentencias (y procedimientos de la AEPD)

Como procedimiento relacionado se puede indicar la que realizó la AEPD en el caso de que un instalador de fibra óptica contactó, de igual forma, violando la privacidad y los derechos de un cliente de la compañía a través de la aplicación de comunicación instantánea WhatsApp comunicando su agrado por las facciones físicas de dicha cliente, así como su deseo de tener una cita con ella: [Procedimiento Nº: PS/00185/2018 RESOLUCIÓN R/01341/2018 DE TERMINACIÓN DEL PROCEDIMIENTO POR PAGO VOLUNTARIO](https://www.samuelparra.com/wp-content/uploads/2018/07/PS-00185-2018_ORI.pdf)

De igual forma, otro procedimiento relacionado es el siguiente: [Procedimiento Nº PS/00412/2018 RESOLUCIÓN: R/00326/2019 En el procedimiento sancionador PS/00412/2018](https://www.aepd.es/es/documento/ps-00412-2018.pdf) en cuyo caso se realizó debido a que otra compañía telefónica (en este caso, Telefónica) no estaba utilizando correctamente los datos personales de un cliente, pasando a su vulneración realizando acciones como el envío masivo de SMS (sin su consentimiento) a su línea telefónica, así como utilizar su número de teléfono para realizar pruebas, contrataciones no solicitadas y gestionar incidencias no comunicadas por dicho cliente. En este procedimiento, además, queda constatado que poco antes de su realización, se interpusieron otras denuncias a través de la AEPD, las cuales dieron lugar a la tramitación de los siguientes expedientes sancionadores: PS/446/2017, PS/276/2017 y PS/567/2015.

Por último, se puede mencionar también la siguiente sanción del Tribunal Supremo sobre la vulneración de los datos personales: [STS 531/2018 - ES:TS:2018:531](http://www.poderjudicial.es/search/documento/TS/8307741/proteccion%20de%20datos%20de%20caracter%20personal/20180305), como ejemplo de sanción sobre los datos personales, que podría haber ocurrido de la misma manera en el caso estudiado, si se hubiera actuado a través de tal órgano elegido.

1. Bibliografía

Agencia Española de Protección de Datos (2018). RESOLUCIÓN: R/01341/2018. *Reclamación contra técnico de Movistar por violar la intimidad y la privacidad de uno de los clientes de la compañía.* Madrid, España: Agencia Española de Protección de Datos.

Agencia Española de Protección de Datos (2018). RESOLUCIÓN: R/00326/2019. *Reclamación contra la compañía de telecomunicaciones “Telefónica” por no respetar los datos personales de un cliente.* Madrid, España: Agencia Española de Protección de Datos.

Sentencia respecto a la protección de datos. STS 531/2018 (Tribunal Supremo. Sala de lo Contencioso, 20 de febrero de 2018).

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 26 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE. *PARLAMENTO EUROPEO y CONSEJO DE LA UNIÓN EUROPEA.* Bruselas, Unión Europea: Diario Oficial de la Unión Europea.

Jefatura del Estado. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. *Boletín Oficial del Estado*, *294,* de 6 de diciembre de 2018.

ADSLZone (18 de julio de 2018). [2000 euros de multa a instalador de fibra por mandar WhatsApp a una clienta](https://www.adslzone.net/2018/07/18/multa-whatsapp-instalador-fibra/). Recuperado el 3 de abril de 2020 de ADSLZone: [2000 euros de multa a instalador de fibra por mandar WhatsApp a una clienta](https://www.adslzone.net/2018/07/18/multa-whatsapp-instalador-fibra/).

Pymes y Autónomos (28 de marzo de 2018). Si te comunicas con tus clientes por WhatsApp también puedes ser multado por la AEPD. Recuperado el 3 de abril de 2020 de Pymes y Autónomos: [Si te comunicas con tus clientes por WhatsApp también puedes ser multado por la AEPD](https://www.pymesyautonomos.com/legalidad/si-te-comunicas-con-tus-clientes-por-whatsapp-tambien-puedes-ser-multado-por-la-aepd).

La Sexta (25 de abril de 2014). Las tres cosas que nunca debe hacer tu empresa si usa WhatsApp. Recuperado el 3 de abril de 2020 de La Sexta: [Las tres cosas que nunca debe hacer tu empresa si usa WhatsApp](https://www.lasexta.com/tecnologia-tecnoxplora/internet/empresas/empresas-que-usan-whatsapp-que-debes-hacer_2014042557f784fb0cf2fd8cc6aa856c.html).

Caso 6: Una aplicación de una aseguradora da acceso a información de clientes a cualquier mediador

1. Primer paso: noticias relacionadas

**Enlaces:**

* [**La 'app' de Metrovalencia deja al descubierto los datos de 60.000 usuarios**](https://valenciaplaza.com/la-app-de-metrovalencia-deja-al-descubierto-los-datos-de-60000-usuarios) **(Valencia Plaza, 2018)**
* [**Facua denuncia a Google ante Protección de Datos por una posible filtración de datos de usuarios de Google+**](https://www.europapress.es/sociedad/noticia-facua-denuncia-google-proteccion-datos-posible-filtracion-datos-usuarios-google-20181029130707.html) **(Europa Press, 2018)**
* [**¿Nos pagará Facebook 200€? Admitida la demanda de OCU contra la red social**](https://as.com/meristation/2019/07/11/betech/1562855210_634373.html) **(As, 2019)**

**Explicación:**

La primera noticia está relacionada directamente con el caso de estudio por ser un caso similar entre aplicaciones con fallos de seguridad filtrando información a terceros no autorizados.

La segunda noticia está relacionada por la filtración de datos de carácter personal por parte de Google en su ya cerrada red social Google+. FACUA procedió a denunciar por vulnerar la Ley Orgánica de Protección de Datos de Carácter Personal.

La tercera noticia está relacionada por la cesión de datos personales de usuarios a terceros con el agravante en este caso de que Facebook se lucró económicamente de ello y de que estos datos fueron utilizados para decantar elecciones democráticas, principalmente.

**Transcripciones:**

* **Noticia 1:**

# **La 'app' de Metrovalencia deja al descubierto los datos de 60.000 usuarios**

**20/12/2018**

Las aplicaciones para móvil de **Metrovalencia** y el **TRAM** tienen al descubierto los datos de 60.000 usuarios del servicio de transporte de la Generalitat. Así lo ha denunciado en un juzgado de Valencia un ingeniero informático que señala a Ferrocarrils de la Generalitat Valenciana (FGV) y a la empresa de *software* que realizó la *app* por presunta violación del derecho de protección de datos de carácter personal.

***Valencia Plaza*** pudo comprobar este miércoles como el ingeniero, que pide mantener su anonimato, accedía de forma aparentemente sencilla a través del programa *Postman* a todos los datos de los usuarios registrados excepto el número de tarjeta de crédito, que sospecha que también se podría conseguir si tratara de realizar un pago aunque no lo ha probado para no incurrir en un delito.

En plena locura por el cumplimiento de la ley de Protección de Datos la situación parece muy grave, ya que el agujero informático generado en la aplicación permite que cualquier persona a través de internet pueda no solo acceder sino también manipular libremente la información de los usuarios registrados –59.894 en el momento de la denuncia–, incluyendo su dirección de correo electrónico, NIF, nombre completo, sexo, fecha de nacimiento, dirección postal completa y número de teléfono.

El informático que ha presentado la denuncia, que también ha remitido un escrito a la Agencia Española de Protección de Datos (AEPD), adjunta en la misma una auditoría donde explica, punto por punto, el problema que lleva a que estos datos estén en abierto. Según afirma radica en la API, interfaz de programación de aplicaciones, que está disponible de forma pública en internet. Esta API carece de autenticación, es decir, no reconoce quién realiza las peticiones, por lo que cualquiera puede acceder a los datos de todos los usuarios.

"La autenticación es un requisito indispensable en todo *software* de acceso público que maneja información privada y en este caso se ha optado por no implementar ningún tipo de autenticación sin pensar en las consecuencias. Se puede afirmar sin lugar a dudas que no se trata de un fallo de seguridad; el *software* se ha concebido así directamente porque no ha sido desarrollado por profesionales cualificados", asegura este ingeniero en la auditoría.

#### **Seguimiento de los viajes**

No solo son los datos personales los que quedan al descubierto, también las tarjetas de transporte asociadas a cada usuario y, por tanto, sus movimientos en el metro o tranvía, fecha, hora y tipo de acciones como entrada o salida. Estos datos permiten conocer la ubicación exacta de todos los usuarios y establecer sus patrones de movimiento. También es posible ver las compras realizadas por cada usuario, incluyendo el título de transporte recargado, el importe y la fecha.

En su denuncia, el informático aporta datos de los movimientos de una persona elegida al azar, residente en un municipio de La Ribera, que todos los días coge el metro a la misma hora para trasladarse a su trabajo en el centro de València –su dirección de correo electrónico revela dónde trabaja–, y que por la tarde regresa a su pueblo desde la misma estación, la de Plaza de España.

Más grave aún es que también permite el acceso a la fecha de caducidad y la marca de las tarjetas, lo que permitiría realizar pagos. "Esto supone la realización de recargas no autorizadas de tarjetas de transporte y, por tanto, de cobros ilícitos con tarjeta bancaria, siempre y cuando la pasarela de pago no tenga autenticación de doble factor", recoge la auditoría. No obstante, el denunciante avisa de que este último punto es teórico ya que es ilegal realizar la comprobación.

De hecho, apunta incluso a la posibilidad de realizar una recarga indicando importes de distinto cobro y de recarga, por lo que entiende que es posible recargar 10 euros en una tarjeta pagando solo 0.01, por ejemplo. Según la denuncia, también sería factible cambiar la contraseña de los usuarios, realizar devoluciones de pagos y eliminar o añadir tarjetas de crédito.

"El hecho de aceptar pagos con tarjetas bancarias exige el cumplimiento de unos estándares de seguridad muy estrictos, véase Payment Card Industry Data Security Standards, que ni el *software* ni la infraestructura de Ferrocarrils de la Generalitat Valenciana cumplen", asegura.

#### **Solución: desactivar la 'app'**

En la auditoría también se proponen medidas para solucionar la situación. En primer lugar, desactivar los servicios de la *app* con efecto inmediato hasta que se cumpla la legislación. Por otro lado, realizar una investigación para descubrir si la información pública ha sido descargada o explotada por terceras partes. A esta cuestión suma la necesidad de emitir nuevas tarjetas de los usuarios afectados con nueva numeración para que si alguien ha descargado su información, no se pueda seguir monitorizando, además de auditar su nuevo *software* y poner la auditoría a disposición de los usuarios.

También señala la necesidad de condenar "duramente" este tipo de situaciones y exigir que profesionales cualificados se encarguen de diseñar e implementar los productos que la sociedad utiliza en el día a día, siendo la informática una pieza esencial en la misma. "Si el estándar de calidad de FGV es el que ha quedado patente en esta pequeña auditoría, ¿qué garantías tienen los ciudadanos de que el resto de *software* e infraestructura informática cumplen con la legislación?", se pregunta.

**FGV no sabe nada**

Este periódico preguntó este miércoles a la empresa pública FGV, que aseguró que no han recibido notificación alguna ni del juzgado ni de la AEPD. Reconoce que hubo algún fallo cuando se lanzó la *app* el pasado mes de marzo, pero asegura que, tras ser advertidos por algún usuario a través de las redes sociales, estos fallos fueron corregidos.

Las fuentes consultadas se mostraron muy extrañadas porque la empresa pública utiliza el servidor de la Generalitat. La *app* fue desarrollado por la empresa leonesa Proconsi, que ganó el concurso convocado por la Gerencia de FGV al ofrecer 49.750 euros.

* **Noticia 2:**

# **Facua denuncia a Google ante Protección de Datos por una posible filtración de datos de usuarios de Google+**

**29/09/2018**

Facua-Consumidores en Acción ha anunciado que ha presentado una denuncia ante la Agencia Española de Protección de Datos (AEPD) contra Google por la posible filtración de datos de usuarios de su red social Google+ (G+). A principios de octubre, la compañía anunció el cierre de la parte para usuarios de la red social Google+ después de identificar un fallo de seguridad relacionado con la posibilidad de que aplicaciones externas accedan a información privada de 500.000 personas. "No ...

Leer más: [Facua denuncia a Google ante Protección de Datos por una posible filtración de datos de usuarios de Google+](https://www.europapress.es/sociedad/noticia-facua-denuncia-google-proteccion-datos-posible-filtracion-datos-usuarios-google-20181029130707.html)

(c) 2020 Europa Press. **Está expresamente prohibida la redistribución y la redifusión de este contenido sin su previo y expreso consentimiento.**

* **Noticia 3:**

# **¿Nos pagará Facebook 200€? Admitida la demanda de OCU contra la red social**

[**11/07/2019 - 16:29**](https://as.com/tag/fecha/20190711/)

## OCU pide que todos los usuarios de Facebook reciban, al menos, 200 euros de compensación por daño moral.

En mayo de 2018, [tras escándalos de Facebook como el de Cambridge Analytica](https://as.com/betech/2018/09/28/portada/1538153919_132828.html), una mala praxis de uso de datos que le costó a Mark Zuckerberg dos asistencias al Congreso de los EEUU y una a la Comisión Europea, la Organización de Consumidores y Usuarios (OCU), junto con sus organizaciones hermanas de Portugal, Bélgica e Italia, decidió lanzar una demanda colectiva contra Facebook, solicitando una compensación de, al menos, 200 euros para los usuarios de la red social por el uso indebido de sus datos.

### **La OCU demanda a Facebook**

Desde el comienzo del escándalo de datos, **las organizaciones del grupo Euroconsumers de España (OCU), Portugal (Deco-Proteste), Italia (Altroconsumo) y Bélgica (Test-achats) responsabilizan a Facebook** y le enviaron una advertencia con algunas demandas muy claras en nombre de los más de un millón y medio de consumidores que representan.

Por un lado, las Organizaciones pidieron a Facebook **aclarar cómo tenía pensado compensar, no solo a las víctimas del escándalo de Cambridge Analytica, sino también a todos los demás consumidores** cuyos datos estaban siendo mal utilizados por la plataforma. Y por otro, que explicara cómo pensaba situar a los consumidores en el centro del control de sus datos, permitiéndoles realmente decidir dónde, cuándo y con quién quieren compartirlos, cuándo quieren dejar de hacerlo y cuándo los quieren recuperar.

Cinco meses después de aquello, y tras las denuncias de los últimos escándalos, y la vulneración de los derechos y la privacidad de los consumidores, **OCU presentó en octubre de 2018 una demanda colectiva contra Facebook, por cesión irregular de datos.** En esta demanda, presentada en el Juzgado de lo Mercantil de Madrid, OCU actúa en defensa de todos los usuarios de la red social, a quienes no se ha informado ni solicitado autorización expresa para utilizar sus datos. Para OCU, **Facebook ha incumplido (entre otras) la Ley de Protección de Datos**, y no solo con los usuarios afectados por el escándalo de Cambridge Analytica o similares, sino con todos los usuarios de Facebook en España, cuyos datos han sido recopilados e intercambiados sin que hayan sido informados ni otorgado su conformidad expresa.

### **Compensar económicamente a todos los usuarios españoles**

[En la demanda presentada](https://www.ocu.org/consumo-familia/derechos-consumidor/noticias/presentacion-demanda-facebook), la OCU pide **la nulidad de ciertas cláusulas de los términos y condiciones de Facebook**, por ser abusivas o por su falta de transparencia, y también se exige que cese su incorporación y se prohíba que se incorporen esas cláusulas en el futuro. La OCU solicita al Juzgado que condene a Facebook a cesar su conducta desleal y prohibir que en el futuro reitere esa conducta. Y por último, La OCU pide que se condene a Facebook **a resarcir a los miembros de la red social con la cantidad de, al menos, 200 euros para cada uno de los usuarios españoles.**

Como vemos, la demanda colectiva de OCU no se limita solo a los usuarios afectados por el escándalo de Cambridge Analytica, sino que representa “*a todos los usuarios de Facebook en España. En este sentido, la Organización considera que, al haber permitido una gran recopilación e intercambio de datos de sus usuarios sin que estos hayan sido informados ni expresado su conformidad expresa, Facebook ha infringido la Ley de Protección de datos”*. Apoyada por los socios de la OCU y *“los los más de 36.000 consumidores que se han sumado a la acción de OCU Mis datos son míos“*.

### **Una demanda admitida**

Casi un año después, este caso vuelve a ser noticia porque no se ha quedado en sólo una denuncia, sino que el juzgado de lo mercantil nº 5 de Madrid, [ha admitido a trámite la demanda](https://www.ocu.org/organizacion/prensa/notas-de-prensa/2019/admision-demanda-facebook) **de OCU contra Facebook** por incumplir, entre otra normativa, la **Ley de Consumidores y Usuarios y la normativa de protección de datos** al no solicitar la autorización expresa, ni informar a los usuarios sobre la utilización de sus datos, haciendo un uso abusivo de sus condiciones de la contratación. ¿Acabará ganando la OCU y recibiremos todos 200€ y una disculpa por parte de la red de Zuckerberg?

1. Segundo paso: legislación

De nuevo, estamos en un caso en la que la legislación oportuna es la citada Ley Orgánica del anterior caso: [Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales](https://www.boe.es/buscar/pdf/2018/BOE-A-2018-16673-consolidado.pdf).

De igual forma, sucede que se está violando la privacidad y la intimidad de las personas, así como los derechos digitales, vulnerando distintos apartados de dicha ley, ya que no se están respetando los datos personales de los clientes. Específicamente, se está incumpliendo el artículo número 5, en el punto 1, donde indica: *«Los responsables y encargados del tratamiento de datos así como todas las personas que intervengan en cualquier fase de este estarán sujetas al deber de confidencialidad al que se refiere el artículo 5.1. f) del Reglamento (UE) 2016/679»*, que, igual que sucedía en el caso anterior, nos conduce de nuevo al Reglamento (UE) 2016/679: [REGLAMENTO (UE) 2016/ 679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO - de 27 de abril de 2016](https://www.boe.es/doue/2016/119/L00001-00088.pdf), más en concreto, al punto 5.1. f), que dice así: *«Los datos personales serán: tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»)»,* cuyo punto también se incumple, como el caso anterior, debido a que no se garantiza la seguridad de los datos personales. Además, en este caso, entra en juego la Ley 26/2006 de mediación de seguros y reaseguros privados: [Ley 26/2006, de 17 de julio, de mediación de seguros y reaseguros privados](https://www.boe.es/buscar/pdf/2006/BOE-A-2006-12916-consolidado.pdf), en la que se puede observar que se incumple el artículo 62 (correspondiente a la quinta sección), específicamente, el punto 1, y aún más, el apartado 1. b), que dice así: *«A los efectos previstos en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal: Cuando el cliente hubiera firmado un contrato de seguro, los agentes de seguros vinculados y los operadores de banca-seguros vinculados deberán tratar los datos del contrato de forma que únicamente puedan ser conocidos por la entidad aseguradora con la que se hubiera celebrado el contrato, sin que puedan tener acceso a dichos datos las restantes entidades aseguradoras por cuenta de las cuales actúen.»*, que indica que los datos únicamente pueden ser conocidos por la entidad aseguradora, cosa que también se incumple en el artículo donde se acusa a Allianz.

Por otra parte, indicar también que la Ley anterior conduce a otra Ley Orgánica, 15/1999, de 13 de diciembre, que se citará a continuación: [Documento BOE-A-1999-23750](https://www.boe.es/buscar/doc.php?id=BOE-A-1999-23750), la cual contiene un punto también incumplido, el punto 10, en el que se indica: *«El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo.»,* incumplido debido a falta de secreto profesional, así como su tratamiento.

1. Tercer paso: Sentencias

Vamos a indicar como documento relacionado el procedimiento sancionador realizado por la AEPD para tal caso, con número: PS/00305/2016 y teniendo como número identificador de resolución: R/03198/2016: [Procedimiento Nº PS/00305/2016 RESOLUCIÓN: R/03198/2016 En el procedimiento sancionador PS/00305/2016](https://www.aepd.es/es/documento/ps-00305-2016.pdf) en el que se denuncia a la compañía de seguros Allianz por el tratamiento y la cesión de datos personales sin el debido consentimiento del denunciante.

Y, además, por otra parte, como sentencia relacionada, citaremos la sentencia que realizó el Tribunal Supremo en relación con Allianz: [STS 1272/2019 - ES:TS:2019:1272](http://www.poderjudicial.es/search/AN/openDocument/09e04eaeb1a3f988/20190503) en la que se podrá observar acusaciones como delito de estafa y falsedad en documento mercantil, por el que se podrá obtener una mejor visión de hechos que suceden en torno a la compañía de Allianz.

1. Bibliografía

Agencia Española de Protección de Datos (2018). RESOLUCIÓN: R/03198/2016. *Reclamación contra la compañía de seguros Allianz por un uso inadecuado en el tratamiento de datos personales.* Madrid, España: Agencia Española de Protección de Datos.

Sentencia en relación a Allianz. STS 1272/2019 (Tribunal Supremo. Sala de lo Penal, 23 de abril de 2019).

Jefatura del Estado. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. *Boletín Oficial del Estado*, *294,* de 6 de diciembre de 2018.

Jefatura del Estado. Ley Orgánica 26/2006, de 17 de julio, de mediación de seguros y reaseguros privados. *Boletín Oficial del Estado*, *170,* de 18 de julio de 2006.

Jefatura del Estado. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. *Boletín Oficial del Estado*, *298,* de 14 de diciembre de 1999.

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 26 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE. *PARLAMENTO EUROPEO y CONSEJO DE LA UNIÓN EUROPEA.* Bruselas, Unión Europea: Diario Oficial de la Unión Europea.

Valencia Plaza (20 de diciembre de 2018). La 'app' de Metrovalencia deja al descubierto los datos de 60.000 usuarios. Recuperado el 3 de abril de Valencia Plaza: [La 'app' de Metrovalencia deja al descubierto los datos de 60.000 usuarios](https://valenciaplaza.com/la-app-de-metrovalencia-deja-al-descubierto-los-datos-de-60000-usuarios)

Europa Press (29 de octubre de 2018): FACUA denuncia a Google ante Protección de Datos por una posible filtración de datos de usuarios de Google+. Recuperado el 3 de abril de Europa Press: [Facua denuncia a Google ante Protección de Datos por una posible filtración de datos de usuarios de Google+](https://www.europapress.es/sociedad/noticia-facua-denuncia-google-proteccion-datos-posible-filtracion-datos-usuarios-google-20181029130707.html)

As (11 de julio de 2019): ¿Nos pagará Facebook 200€? Admitida la demanda de OCU contra la red social. Recuperado el 3 de abril de As: [¿Nos pagará Facebook 200€? Admitida la demanda de OCU contra la red social](https://as.com/meristation/2019/07/11/betech/1562855210_634373.html)