Practica 2

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

**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) (Valenciaplaza, 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)

(Europapress, 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 red social Google+.FACUA procedió a denunciar por vulnerar la Ley Orgánica de Protección de Datos de Carácter Personal.

La tercera noticia esta 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 que estos datos fueron utilizados para decantar elecciones democráticas principalmente.

**Transcripción:**

**Primera noticia:**

**20/12/2018 -**

VALÈNCIA. 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 València 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.

(...)

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 válida quién realiza las peticiones, por lo que cualquiera puede acceder a los datos de todos los usuarios.

(...)

#### **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.

(...).

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.

(...).

"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.

(...)

#### **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.

(...)

**Segunda noticia:**

MADRID, 29 Oct. (EUROPA PRESS)

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 accedieron a información privada** de 500.000 personas.

(...)

En este sentido, la asociación ha apuntado que el **Reglamento Europeo 2016/679**, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos, recoge que el tratamiento sólo será lícito si "el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos", entre otros.

Según recalca Facua, el artículo 32 de la misma normativa establece que "el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo", entre otras, "la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento".

De igual forma, ha indicado que la **Ley Orgánica de Protección de Datos de Carácter Personal (LOPD)** indica que los responsables de los ficheros "deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado".

Además, ha insistido en que tanto el **Reglamento 2016/679 como la LOPD prohíben el tratamiento de datos personales que revelen "el origen étnico y racial", "las opiniones políticas" y "las convicciones religiosas o filosóficas", entre otras**, salvo "consentimiento expreso y por escrito del interesado".

"Dado el carácter de una red social como Google+, caben muchas posibilidades de que los datos personales que fueron filtrados entren en esta categoría de datos especialmente protegidos, teniendo en cuenta el tipo de información que suelen subir los usuarios a las redes sociales (fotografías, información personal e íntima, etc.)", ha subrayado.

(...)

**Tercera noticia:**

En mayo de 2018, tras escándalos de Facebook como el de Cambridge Analytica, 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.

(...)

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.

(...)

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“.

(...)

(Nota: (...) son fragmentos que no interesan a lo que el caso se refiere)

**Legislación:**

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos

Personales y garantía de los derechos digitales.(BOE)

<https://www.boe.es/buscar/pdf/2018/BOE-A-2018-16673-consolidado.pdf>

Explicación: En él se detalla cómo debe tratarse la información personal.

REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 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 (Reglamento general de protección de datos) <https://www.boe.es/doue/2016/119/L00001-00088.pdf>

Explicación: Se relaciona ya que dicta cómo se tienen que tratar los datos de personas físicas en el territorio de la unión europea.

**Sentencias:**

**Bibliografía:**

Valenciaplaza. (20 de diciembre de 2018). 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>

Europapress. (29 de octubre de 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>

As. (11 de julio de 2019). ¿Nos pagará Facebook 200€? Admitida la demanda de OCU contra la red social.

<https://as.com/meristation/2019/07/11/betech/1562855210_634373.html>

Noticias Jurídicas (24 de julio de 2019)El Supremo confirma la vulneración de los datos personales en el proceso de venta de vivienda pública en Madrid.

<http://noticias.juridicas.com/actualidad/jurisprudencia/14264-el-supremo-confirma-la-vulneracion-de-los-datos-personales-en-el-proceso-de-venta-de-vivienda-publica-en-madrid/>

Iberley (28 de Enero de 2020) Sentencia ADMINISTRATIVO Audiencia Nacional, Sala de lo Contencioso, Sección 1, Rec 619/2016.

<https://www.iberley.es/jurisprudencia/sentencia-administrativo-an-sala-contencioso-sec-1-rec-619-2016-28-01-2020-48130038?voces%5B0%5D=Protecci%C3%B3n+de+datos&noIndex>

BOE (22 de mayo de 2019) Interpuesto por el Defensor del Pueblo respecto del apartado primero del artículo 58 bis de la Ley Orgánica 5/1985, de 19 de junio, del régimen electoral general, incorporado por la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales.

<https://www.boe.es/buscar/doc.php?id=BOE-A-2019-9548>