Práctica 2 - caso extra

**Grupo 2D2**

**Autor del entregable:**

* **David Arnal García**

Caso extra: [Una filial del antivirus gratis Avast vende todas las búsquedas, cada clic, cada compra en cada sitio de sus usuarios](https://www.xataka.com/seguridad/filial-antivirus-gratis-avast-vende-todas-busquedas-cada-clic-cada-compra-cada-sitio-sus-usuarios)

1. Primer paso: noticias relacionadas

**Enlaces:**

* [No solo en sus antivirus gratis: Más problemas para Avast y AVG](https://www.adslzone.net/noticias/seguridad/antitrack-avas-avg-problemas-seguridad/) (ADSLZone, 2020)

# [Cuidado con este popular antivirus gratis: ahora recoge más datos que nunca](https://www.softzone.es/noticias/seguridad/avast-2020-comparte-datos-usuarios/) (Softzone, 2020)

* [Kaspersky antivirus “confirmado como malicioso”. La guerra fría en la que perdemos todos](https://empresas.blogthinkbig.com/kaspersky-antivirus-malicioso-ciberseguridad/) (Telefónica, 2018)

**Explicación:**

La primera noticia está directamente relacionada con el caso, ya que es una continuación del problema de privacidad generado por Avast. Empezó vendiendo datos personales a través de una subsidiaria, y a raíz de este artículo, se puede saber que sus problemas no dejaron de aparecer. Esta vez no solo a Avast, sino también a su otra firma de antivirus asociada, AVG, quienes a través de su software Anti Track (supuestamente creado para el antirastreo) hacían a los ordenadores más vulnerables.

El segundo artículo es de fecha posterior al primero, y la manera en la que está relacionado con él es que después de saber que la recopilación de datos se había confirmado públicamente y haber prometido una solución, en una nueva versión del programa se tiene activado por defecto el envío de todos los datos comprometidos anteriormente sin ningún tipo de previo aviso.

Por último, se relaciona con el caso del antivirus Kaspersky, que fue confirmado como *malicioso* por la UE y desaconsejado para instituciones públicas debido a compartir información privada y, este caso, no solo datos personales o de navegación, sino datos que van más allá para ser utilizados por las Agencias de Inteligencia de donde procede el antivirus, Rusia.

**Transcripciones:**

* **Noticia 1:**

# [**No sólo en sus antivirus gratis: Más problemas para Avast y AVG**](https://www.adslzone.net/noticias/seguridad/antitrack-avas-avg-problemas-seguridad/)

**11/03/2020 - 14:00**

Los problemas siguen acumulándose para los [antivirus gratis](https://www.adslzone.net/listas/windows/mejores-antivirus-windows-10/) de Avast y AVG. Los sonados casos de espionaje destapados en las primeras semanas del año todavía siguen coleando y son muchos los que buscan [alternativas a Avast](https://www.adslzone.net/listas/mejores-programas/alternativas-avast/) para sus ordenadores. Para más inri, se acaban de conocer más problemas para la reputación de esta empresa. En este caso, son problemas con el software **Anti Track**, complementario a los antivirus gratis de Avast y AVG. Aunque pensado para proteger nuestra privacidad, parece que estaba haciendo todo lo contrario. Os damos todos los detalles tras el salto.

La compañía de seguridad ha intentado calmar los ánimos con el lanzamiento de **Avast Free Antivirus 2020**. Esta nueva versión cuenta con nuevos ajustes de privacidad, además de no instalar de forma automática las extensiones para el navegador. La sección mejorada de privacidad permite desactivar la recolección de datos personales, aunque es algo que viene activado por defecto.

## **¿Qué pasa con el software Anti Track?**

David Eade ha publicado un informe de seguridad sobre la existencia de una vulnerabilidad en el software Avast y AVG Anti Track que abre el ordenador a ataques Man-in-The-Middle (MiTM) y robo de datos. Esta afecta a todas las versiones de esta herramienta **anteriores a Avast AntiTrack 1.5.1.172 y AVG AntiTrack 2.0.0.178**. Los atacantes no necesitan acceso local para aprovechar la vulnerabilidad ni tampoco software especial.

Este software de Avast y AVG está diseñado para bloquear los rastreadores de publicidad y para evitar la monitorización invasiva de los usuarios. Se puede probar de forma gratuita, aunque se precio anual es de **49,99 euros al año**. Según la web de Avast, nos permitirá saber en todo momento si nos están rastreando, mantener nuestra identidad en secreto, evitar la publicidad personalizada y borrar el rastro automáticamente.

El problema es que parece que no estaba haciendo su trabajo correctamente. El primer problema está causado por la forma de validar los certificados, lo que permite ataques Man-in-The-Middle (MiTM). El segundo problema, según este investigador de seguridad, es que **“degrada” los protocolos de seguridad del navegador a TLS 1.0**. Incluso si un servidor web soporta TLS 1.2, este software lo ignorará y utilizará TLS 1.0.

El tercer problema es que falla al proteger las claves de sesión. En el caso de Internet Explorer y Edge, el investigador de seguridad explica que *“ignora las nuevas medidas de seguridad en favor de cifrados antiguos que se consideran inseguros hoy en día”.* Un atacante con un proxy malicioso podría robar el tráfico HTTPS de la víctima e incluso **clonar las cookies de sesión.**

El problema está solucionado en las versiones Avast AntiTrack 1.5.1.172 y AVG AntiTrack 2.0.0.178, por lo que todos los usuarios deberán actualizar para no sufrir estas vulnerabilidades. David Eade confirma que informó a Avast de su existencia el 7 de agosto de 2019, pero que no se han solucionado hasta el **9 de marzo de 2020.**

* **Noticia 2:**

# [**Cuidado con este popular antivirus gratis: ahora recoge más datos que nunca**](https://www.softzone.es/noticias/seguridad/avast-2020-comparte-datos-usuarios/)

**03/03/2020 - 09:15**

Hay determinados tipos de software en los que sus desarrolladores deberían poner más cuidado, el menos en lo que a términos de **seguridad y privacidad** se refiere. En concreto nos referimos, por ejemplo, a las soluciones antivirus, donde entran en juego una buena cantidad de propuestas, entre ellas Avast, del que os hablaremos ahora.

De hecho este es uno de los antivirus más populares de los últimos años, aunque también se ha visto envuelto en algunas polémicas recientes. Para que nos hagamos una idea de todo ello, hace poco se supo que el **programa de seguridad** había recopilado y vendido datos de sus usuarios a terceros a través de su filial **Jumpshot**. Tras los informes que revelaron todo esto, el software ha cesado las operaciones esta filial mencionada y ha presentado una disculpa.

## **Las polémicas con el antivirus Avast, no cesan**

Es evidente que esto es algo bastante serio, ya que en teoría los usuarios confían ciegamente en el [**software antivirus que protege sus equipos**](https://www.softzone.es/programas/antivirus/mejores-antivirus-windows/). Pues bien, después de esta polémica de venta de datos que os hemos comentado, hace unos días Avast lanzó una nueva actualización del producto. Se trata del nuevo **Avast Free Antivirus 20.1.**

Cabe mencionar que ahora esta nueva actualización ya no instala las extensiones de los navegadores, ya que fueron retiradas recientemente por **Google y Mozilla** de sus tiendas. Al mismo tiempo esta nueva versión incluye nuevas configuraciones de confidencialidad que vienen activadas por defecto y muestra más anuncios. Estos últimos están relacionados con diversos productos de la misma firma y de terceros.

Para los que no conozcan la polémica, una investigación descubrió que **Avast** está recopilando los datos de navegación de los usuarios en el **antivirus gratuito.** Posteriormente los vende a terceros a través de Jumpshot. Lo peor del caso es que se pudo ver que los datos recogidos no son completamente anónimos. Esto se debe a que pueden ser rastreados para identificar a un usuario en concreto del programa.

## **La nueva versión gratuita del antivirus sigue compartiendo datos**

Pues bien, hace una semana la empresa lanzó Avast 20.1 con varias correcciones de errores. Así, como Avast prometió que detendría la recogida de datos, esto se ha reflejado a través de nuevas configuraciones de **privacidad** en el antivirus. Eso sí, estas vienen habilitadas por defecto, como podemos ver en la captura adjunta.

También hay que destacar que las **extensiones** de los navegadores no son instaladas por Avast automáticamente, ya que las de Mozilla y Google desaparecieron de las tiendas oficiales. Pero al mismo tiempo, la firma dejó entrever que los usuarios de la versión gratuita verán ventanas emergentes sobre **Avast Cleanup Premium.** Es decir, que se han incluido nuevos anuncios en esta nueva versión del software.

Por otro lado os diremos que ahora, a través de la nueva **configuración de privacidad**, podemos desmarcar la recogida de datos en Opciones / Privacidad personal. Y es que aquí encontramos varias opciones relativas a la compartición de datos que podemos desactivar. De hecho vienen activadas por defecto para compartir información sobre amenazas y diversos datos de uso.

Más concretamente Avast comparte los datos de uso de la aplicación para mostrar anuncios sobre aplicaciones de terceros, como Chrome. En resumidas cuentas, la manera en la que Avast trata a los usuarios de su versión gratuita, no va a cambiar. Ya que de hecho en esta ventana de **configuración** que os comentamos, se deja claro que esa recopilación de datos personales es exclusiva de Avast Free Antivirus.

* **Noticia 3:**

# **Kaspersky antivirus “confirmado como malicioso”. La guerra fría en la que perdemos todos**

**18/06/2018**

Según la Unión Europea, el *software* de Kaspersky Lab (y su antivirus) es malicioso. **Así, literalmente.** [**Ya no puede ser utilizado en sus instituciones oficiales. Se le aparta y ya no es una herramienta bienvenida.**](https://www.infosecurity-magazine.com/news/european-lawmakers-vote-ban/) El último capítulo de una leyenda y extraño efecto dominó de acusaciones que, como bola de nieve, ha tomado tracción en los últimos años. Como en el imaginario cinematográfico durante la guerra fría de los 80, los rusos son los “sospechosos habituales”. Pero (como también se desprendía de “Juegos de guerra” en los 80), seguir presionando en esta contienda de tensiones reprimidas, **culmina en un juego en el que no solo no hay ganadores,** **sino que todos pierden**. Porque en un mundo de [***malware* globalizado**](https://empresas.blogthinkbig.com/caso-kaspersky-y-la-globalizacion-de/), descartar una tecnología como la de Kaspersky (que como tal, es neutra) no parece buena idea.

## ¿Qué ha pasado?

El Parlamento Europeo ha votado a favor de una moción relativa a la normativa en ciberdefensa en la que, literalmente, se puede leer:

***76. Calls on the EU to perform a comprehensive review of software, IT and communications equipment and infrastructure used in the institutions in order to exclude potentially dangerous programmes and devices, and to ban the ones that have been confirmed as malicious, such as Kaspersky Lab;***

Una frase que empieza bien, pero acaba raro. Obviamente es necesario que la comunicación e infraestructura en las instituciones excluya programas potencialmente peligrosos, y que se eliminen los confirmados como tal. Hasta ahí, correcto. Pero el ejemplo explícito de Kaspersky Lab (que incluye lógicamente su antivirus) levanta alguna que otra ceja. Suena a una constatación innecesaria en ese contexto. *“Malicioso”* es una palabra muy fea. Podríamos pensar que:

* Es malicioso porque contiene actividad maliciosa en su código. Pero, podría apostar fuerte por ello, no parece el caso. Hubieran sido descubiertos, y no se juegan su prestigio por algo tan peregrino como código dañino en un producto así.
* Se considera malicioso **porque a un antivirus se lo das todo.** Confías a nivel técnico y estratégico. Confías porque tiene todo el poder sobre la infraestructura, y confías a nivel estratégico porque le estás dando la potestad de decidir qué es bueno y qué es malo en tu equipo. **Puede ser un guardián eficaz, pero ¿y si está entrenado por alguien del que no te fías y que puede llegar a influir demasiado en él?**

Creemos que se trata del segundo supuesto, pero entonces no es que sea malicioso, sino que es inadecuado para unos intereses concretos. Y, al contrario que el *malware*, esto es bastante más subjetivo. En resumen, l**o que se quiere decir con esa frase, no es que el problema esté en el *software*, sino evidentemente, de dónde viene.** Lo que quieren decir es que no les gustaría que la información que tiene que utilizar un antivirus para realizar su trabajo, vaya a los servicios de inteligencia rusos y puedan usarla en su contra. O también teme que se sigan patrióticas instrucciones del gobierno Ruso para crear *malware* que Kaspersky no detecta a propósito, y espiar al resto que lo utiliza como herramienta protectora. Y es que Kaspersky podría, como antivirus instalado en una institución, además incluso tener acceso privilegiado a otro potencial *malware* creado por terceros. Imaginemos que alguien ataca a esa institución con un sofisticado APT. Kaspersky podría jugar con ventaja y cazarlo, estudiarlo, analizarlo y utilizar esa información como arma de espionaje incluso sin avisar al propio afectado.

Y esto es lo que se ha votado en el Parlamento Europeo. **No tanto sobre el *software* malicioso (en una horrible elección de adjetivos) sino que las herramientas de vigilancia contra el *software* malicioso, deben provenir de fuentes fiables.** Y ¿qué es “fiable”? Puedes ser fiable tecnológicamente, pero no geoestratégica o políticamente. Y en el fondo, esta afirmación mancha la reputación de una tecnología, que, **como tecnología, siempre es neutra.** Lo que es inocuo para algunos, será mal visto por otros. Y así, perdemos todos.

## No solo se renuncia al *software*

Como es lógico, la reacción de Kaspersky no se ha hecho esperar. Dejan de colaborar con la Europol y con NomoreRansom.org (organización en la que ElevenPaths también colabora). Con la renuncia a su *software*, a su tecnología, también se renuncia a sus conocimientos y experiencia. Y es que Kaspersky no es solo un antivirus con uno de los motores más potentes sino que es un laboratorio donde se detecta, investiga, y analizan las amenazas más relevantes de los últimos años. Desde [**Stuxnet**](https://www.kaspersky.com/blog/stuxnet-victims-zero/6775/), pasando por [**Duqu**](https://www.kaspersky.com/about/press-releases/2015_duqu-is-back-kaspersky-lab-reveals-cyberattack-on-its-corporate-network-that-also-hit-high-profile-victims-in-western-countries-the-middle-east-and-asia)**,** [**Careto**](http://blog.elevenpaths.com/2014/02/careto-mask-la-ciber-arma-posiblemente.html)**,** [**The Flame**](https://unaaldia.hispasec.com/2012/05/theflame-reflexiones-sobre-otra.html)… En los últimos años, se ha convertido en una de las pocas casas de antivirus capaz de poner el foco en el *software* como sistema de espionaje, la ciberguerra, donde no todos los analistas pueden arrojar luz. Como afirman, **venían colaborando con Europol y han ayudado a desenmascarar a cibercriminales de carne y hueso, además de campañas muy sonadas.** ¿Otros podrán hacerlo? Sin duda. Pero Kaspersky lo hacía ya muy bien, y (como demostró con su experimento de 2010), **es un claro referente tecnológico para otras casas antivirus. Se rompe así un equilibrio que no sabemos dónde acabará y, sobre todo, si aporta un beneficio mayor que la situación actual.**

## De dónde viene esto: 2010, un pequeño experimento

En la votación del Parlamento Europeo, hablando de “*software* malicioso” han manipulado el lenguaje. Han usado, siendo claros, la confusión como argumento. Pero esto viene de lejos… Kaspersky siempre estuvo en la polémica. Por empezar por algún sitio (y sin ánimo de ser exhaustivo), Kaspersky siempre ha sido claramente un referente en el mundo de la detección estática en casas antivirus. [**Y lo demostró con un experimento realizado en 2010**](https://empresas.blogthinkbig.com/se-desvela-una-guerra-sucia-en-el-mundo_26/)**.** Creó unos cuantos ficheros benignos e hizo que su motor se detectara en VirusTotal como *malware*. Era una mentirijilla, un “falso positivo” controlado para ver cómo reaccionaba el resto de casas. **Diez días después, 14 motores más detectaban este “no *malware*“, en un efecto dominó que dejaba claro quién se fijaba en quién a la hora de marcar con una firma un supuesto *malware*.** Hicieron público el experimento y denunciaron la situación, no sin cierta polémica. Este juego, aunque sirviese como muestra, no “demostraba” por sí solo. Además empañaron la imagen de cara a los usuarios y desacreditaban en cierta manera la función de una herramienta de seguridad no infalible pero sí imprescindible para muchos.

De dónde viene esto: 2014, un primer golpe técnico

Kaspersky fue atacado y [**el atacante vivió en su red durante un buen periodo de 2014.**](https://www.kaspersky.com/blog/kaspersky-statement-duqu-attack/8997/) En 2015, cuando descubrieron que llevaban meses con sus sistemas intervenidos y en un elogiable trabajo de transparencia, publicaron detalles muy concretos del ataque sin mencionar en ese momento que fueron los israelíes, como más tarde se confirmó.

## De dónde viene esto: 2015, un segundo golpe al prestigio

Dos antiguos trabajadores de Kaspersky acudieron a Reuters para denunciar (de forma anónima) que cuando trabajaban en el laboratorio Kaspersky mantenía un plan a gran escala mucho más sutil y maquiavélico que el anterior experimento puntual de 2010, [**para que los competidores cayeran en el falso positivo detectando ficheros importantes y/o comunes como *malware***](https://empresas.blogthinkbig.com/se-desvela-una-guerra-sucia-en-el-mundo_26/)**.** Microsoft, AVG y Avast confirmaron que, efectivamente, observaron estas tácticas de inducir a detectar falsos positivos pero quizás no solo de Kaspersky. Obviamente, ellos lo negaron.

## De dónde viene esto: 2017, todo mal viene de Rusia

Comenzó el año con la acusación de espionaje y ciberataques por parte de Rusia a las elecciones de EEUU. A Kaspersky aquí no se le atribuía ninguna responsabilidad, pero el incidente ayudó a dibujar a los rusos en general (y cualquier herramienta suya) como un actor importante que ya aprovechaba las redes como armas donde influir políticamente.

A finales de 2017 el New York Times publicaba un reportaje con un título que ya juzgaba a los actores: *“How Israel Caught Russian Hackers Scouring the World for U.S. Secrets”*. [**Afirma que espías israelíes detectaron a agentes del gobierno Ruso (espías)**](https://empresas.blogthinkbig.com/caso-kaspersky-y-la-globalizacion-de/), buscando en una especie de “buscador de *malware*” perteneciente a Kaspersky nombres de programas de inteligencia americano (tipo Eternal Blue, para entendernos) y documentos clasificados. Espías israelíes vigilando a espías rusos que vigilaban a espías estadounidenses. Los israelíes avisaron a los estadounidenses y en septiembre de 2017 se decretó a Kaspersky como sistema de protección prohibido entre las agencias de inteligencia americanas. Kaspersky obviamente negó que ofreciera estos “servicios” a la inteligencia rusa y a partir de aquí, mucha especulación, porque nunca se evidenció nada. En realidad, nunca se ha mostrado una sola evidencia final de todo esto.

Kaspersky se vio obligada a reaccionar. [**Lanzó su iniciativa de transparencia**](https://www.kaspersky.com/about/press-releases/2017_trust-first-kaspersky-lab-launches-its-global-transparency-initiative). En ella, fundamentalmente pondría a disposición de terceros el código de sus herramientas para que fueran auditadas. Las injerencias rusas en todas las votaciones (tanto las de final de 2017 en Estados Unidos como incluso las españolas) también se hicieron populares. Rusia y el ciber mal parecen ya una misma cosa en el imaginario colectivo.

## De dónde viene esto: 2018, la desconfianza salta el charco

Ganada ya la desconfianza de Estados Unidos tras las elecciones y el choque diplomático entre servicios de inteligencia, avivado el intento de desprestigio entre las propias casas antivirus (a pesar de ser técnicamente reconocida) a través de una confesión anónima de dos supuestos ex trabajadores, **la desconfianza salta el charco**. A finales de 2017, el Reino Unido también [**prohíbe el uso de Kaspersky**](https://www.theregister.co.uk/2017/12/03/uk_government_bans_russian_anti_virus_software/) en entornos secretos. **Es totalmente legítimo verificar la seguridad de las herramientas a las que confías tu seguridad, pero el efecto dominó continúa sin pruebas.** A mediados de 2018 [**el gobierno holandés**](https://www.reuters.com/article/us-cyber-netherlands-kaspersky/dutch-government-to-phase-out-use-of-kaspersky-anti-virus-software-idUSKCN1IF2NV) se une al pacto y ahora, como hemos mencionado, toda la Unión Europea.

Durante 2018, como parte de su iniciativa de transparencia y tras los comentarios de los holandeses, Kaspersky [**mueve su central a Zurich**](https://www.theregister.co.uk/2018/05/15/kaspersky_labs_announces_move_to_zurich_dutch_government_questions_firm/) para intentar desvincularse de Rusia… conocedores de que las tensiones políticas relativas a su conexión con el bloque soviético son el centro de todos los rechazos.

## Conclusión

Como en las parejas de enamorados, **cuando la confianza se rompe, poco importa todo lo demás. Las habilidades técnicas no pueden borrar una herida (fundada en hechos o no) que tiene otro origen mucho más oscuro.** Todos quieren pensar que Kaspersky está al servicio de su país, y no solo de sus dueños técnicos o estratégicos. En tiempos de *revival* de guerra fría, se trata de llevar el conocido argumento, cercano a la propaganda (verdades a medias, o mentiras totales), al plano de la ciberseguridad.

Pero no estamos en los 80, sino en un mundo mucho más conectado y globalizado. ¿Tiene sentido una “ciberguerra fría”? En un mundo globalizado, tanto un *malware* como una peligrosa vulnerabilidad puede acabar en segundos en manos de los analistas, y de ahí a proteger a otros clientes porque precisamente, así nos protegen mejor a todos, gracias a la inteligencia colectiva de los “endpoint security”. **Y Kaspersky siempre ha sido un importante actor en todo este ecosistema global, tanto en el plano de la inteligencia como técnico.** Como ocurre en la economía global, se supone que podría ser un estímulo para un mundo mejor bajo un capitalismo ideal… Pero no, la globalización es despiadada. En la vida real, esos ficheros, documentos, o *exploits* detectados, las “ciberarmas” vuelan en segundos hacia sistemas centralizados, y de ahí en manos de “cualquiera”… incluso en manos de quien no confías. Así que, en un mundo global, volvemos a los aranceles, a los recelos. Son los pros y los contras del mundo de las ciberarmas y el *malware* globalizado. Igual que la globalización económica que en un principio se funda bajo lo que se suponen argumentos bienintencionados, en el fondo esconde algunos aspectos que no son tan beneficiosos.

Por otro lado, si Kaspersky retira su apoyo y deja de investigar, ¿quién los reemplazará? ¿Y si los sustitutos están también sometidos a presiones políticas que le obligan de alguna manera a ofrecer favores a cambio? ¿Están todas las casas antivirus preparadas desde el plano técnico para soportar esa responsabilidad? **¿El golpe económico que esto supone para la compañía, minará sus capacidades de protección para el resto del mundo? ¿Quién gana y quién pierde?** Volvemos a bascular, de un plano técnico hacia otro político, en donde las respuestas comienzan a ser más polémicas y discutibles. Porque a nivel político no existe un única y correcta verdad. Este es un viejo dilema y no se está descubriendo nada nuevo en realidad: hablamos del mundo de la seguridad “física” de toda la vida, trasladado a la red, a las armas inteligentes y sus controversias. Aunque todo sea dicho: **por fin, la ciberseguridad en las agendas políticas y gubernamentales.**

1. Segundo paso: legislación

Tratándose de protección de datos, 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), ya que en dicho documento se encuentra el título II, correspondiente a los principios de protección de datos, en los que, por ejemplo, se podría decir que se vulnera el artículo número 5, artículo específico para el deber de confidencialidad, específicamente el artículo número 1, que dice así:  *«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»).»,* artículos que Avast, así como AVG, estarían incumpliendo.

1. Sentencias (y procedimientos de la AEPD)

Tratándose de un caso tan reciente, no hay ninguna sentencia impuesta directamente relacionada con el caso (relacionado con el antivirus Avast o con AVG), pero se pueden mencionar algunas sentencias para añadir información adicional que incumplen los artículos anteriormente dichos.

Por ejemplo, y aunque se recalca que se va a incluir una sentencia no relacionada con los antivirus, se puede mencionar la siguiente sentencia realizada por la AEPD: [E-09388-2019 Resolución de fecha 04-11-2019 Artículo 32 RGPD](https://www.aepd.es/es/documento/e-09388-2019.pdf) en la que se describe el robo de un ordenador que almacenaba en servicios *cloud* datos de menores de un centro de educación, por lo que, si dichos datos salieran a la luz, estarían vulnerando los artículos citados anteriormente respecto a la privacidad y al derecho de confidencialidad de los datos personales.

Por otra parte, se va a dejar otra sentencia de la AEPD: [Procedimiento Nº: PS/00122/2019 RESOLUCIÓN: R/00192/2019 En el procedimiento PS/00122/2019, instruido por la Agencia Española](https://www.aepd.es/es/documento/ps-00122-2019.pdf), en la que se describe que un particular vendió su vehículo usado en Prim Torrecillas, concesionario de vehículos y, posteriormente, alguien ajeno a dicho concesionario utilizó su nombre, apellidos y número de DNI para redactar un contrato de compraventa falso, por el cual el reclamante vendía un vehículo usado a un tercero, vulnerando completamente el derecho a la confidencialidad de los datos, así como su debido tratamiento.

1. Bibliografía

Agencia Española de Protección de Datos (2018). PROCEDIMIENTO: E/09388/2019. *Procedimiento en el que se informa el robo de un ordenador con información personal en cloud de menores de edad.* Madrid, España: Agencia Española de Protección de Datos.

Agencia Española de Protección de Datos (2019). RESOLUCIÓN: R/00192/2019. *Reclamación contra Prim Torrecillas por uso indebido de tratamiento de datos, así como vulneración de privacidad.* Madrid, España: Agencia Española de Protección de Datos.

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 (11 de marzo de 2020). [No sólo en sus antivirus gratis: Más problemas para Avast y AVG](https://www.adslzone.net/noticias/seguridad/antitrack-avas-avg-problemas-seguridad/). Recuperado el 3 de abril de 2020 de ADSLZone: [Problemas con la función AntiTrack de los antivirus gratis de Avast y AVG](https://www.adslzone.net/noticias/seguridad/antitrack-avas-avg-problemas-seguridad/)

Softzone (3 de marzo de 2020). [Cuidado con este popular antivirus gratis: ahora recoge más datos que nunca](https://www.softzone.es/noticias/seguridad/avast-2020-comparte-datos-usuarios/). Recuperado el 3 de abril de 2020 de Softzone: [El antivirus gratis Avast 2020 recoge y comparte datos de sus usuarios](https://www.softzone.es/noticias/seguridad/avast-2020-comparte-datos-usuarios/)

Telefónica (18 de junio de 20º8). Kaspersky antivirus “confirmado como malicioso”. La guerra fría en la que perdemos todos. Recuperado el 3 de abril de 2020 de Telefónica: [Kaspersky antivirus “confirmado como malicioso”. La guerra fría en la que perdemos todos](https://empresas.blogthinkbig.com/kaspersky-antivirus-malicioso-ciberseguridad/)