Medidas para minimizar el seguimiento en internet

Septiembre 2020

Introducción

Al utilizar internet existen prácticas que afectan a nuestra privacidad, como es el caso del seguimiento de la actividad de navegación que se produce al visitar un gran número de páginas webs. Este seguimiento habitualmente se lleva a cabo a través de las cookies, principalmente de publicidad o analíticas. El objetivo que persiguen es la elaboración de perfiles para ofrecer publicidad ajustada a los intereses y características concretas de cada individuo, además de recopilar información estadística de acceso a los servicios web.

Cuando visitamos una página web no solo accedemos a un único sitio de internet, sino que al mismo tiempo somos redirigidos en paralelo a múltiples servidores de terceras partes, que generalmente ofrecen servicios de publicidad y analítica de datos al sitio web principal. Este acceso a terceras partes es lo que permite que puedan instalar y acceder a la información vinculada a las cookies[1] que realizan el seguimiento de la actividad de cada usuario. Este es el motivo por el cual la mayoría de las técnicas que se usan mejorar el control del usuario sobre el seguimiento en internet se basan en la posibilidad de minimizar las cookies de terceros, o directamente evitar que se acceda a esos terceros.

Aun siendo el método más conocido, las cookies no son los únicos que se emplean para seguir a una persona a través de su navegación web. Existen otras técnicas para conseguir el mismo propósito, como las basadas en identificadores únicos de publicidad[2], o las implementadas mediante obtención de la huella digital del dispositivo[3]. En los navegadores, el Local Storage e IndexedDB permiten también almacenar y recuperar información en el dispositivo mientras se navega, y pueden ser utilizadas también para el seguimiento de la actividad de los usuarios.

Los logs (registros de actividad) de los servidores también podrían ser explotados en este sentido mediante la correlación de la información almacenada en diversos sitios. De esta forma, evitar el acceso a aquellos servicios que realizan este tipo de prácticas sin las garantías adecuadas es el método más efectivo de protección de la privacidad.

Hay que tener presente que estas técnicas de seguimiento de usuarios no son privativas de los navegadores presentes en los ordenadores personales. Móviles, tabletas y otros dispositivos inteligentes, como las Smart TV, utilizan identificadores únicos de publicidad. Estos identificadores se envían a servidores de internet cuando se usa una App y ante determinados eventos, permitiendo la singularización y el seguimiento del usuario.

Otro elemento a tener en cuenta es que los navegadores web y los dispositivos también permiten iniciar sesión, por ejemplo, con una cuenta de correo electrónico. De esta forma se permite acceder directamente al correo, a muchas otras aplicaciones directamente desde la interfaz y opciones del propio navegador, así como a mantener opciones de personalización de los servicios. Con la sesión de usuario iniciada, el historial de navegación puede estar siendo enviado automáticamente al proveedor de ese servicio.

También es posible el seguimiento de la actividad del usuario a través de los servicios de autenticación federada que ofrecen grandes compañías de internet y redes sociales. Esto sucede cuando para iniciar sesión en una web o en una aplicación concreta se puede utilizar la cuenta de Facebook, Google u otras.

[1] Guía sobre el uso de las cookies. AEPD.

[2] Nota técnica: Control del usuario en la personalización de anuncios en Android. AEPD.

[3] Estudio Fingerprinting o huella digital del dispositivo. AEPD.

agencia española protección datos

Recomendaciones básicas

Las recomendaciones básicas para usuarios sin conocimientos avanzados que permiten minimizar la exposición indeseada de datos de carácter personal son las siguientes:

1. Ten en cuenta la privacidad como una de las características deseables a la hora de elegir un navegador y las aplicaciones que instalas y utilizas en tus dispositivos. Debido a la constante evolución de estos productos debes consultar los últimos análisis que se publican sobre ellos.

2. Evitar instalar aplicaciones innecesarias en tu navegador, eso minimizará los riesgos.

3. Mantén actualizado tu navegador para disfrutar de las últimas tecnologías de protección anti-rastreo.

4. Si el navegador dispone de protección avanzada anti-rastreo/seguimiento[4], activa o mantén activada esta configuración. Estas opciones permiten varios niveles de protección, elige el nivel más elevado y que, a la vez, se ajuste a tus preferencias. En todo caso, si así lo consideras, puedes habilitar la opción para enviar a los sitios web la señal "Do not track"[5], indicando tu deseo de no ser rastreado.

5. Si así lo consideras, puedes configurar el navegador para bloquear las cookies de terceros[6], o como mínimo para bloquearlas cuando navegues en modo privado. En navegadores con protección anti-rastreo/seguimiento, estas opciones estarán integradas en la misma configuración.

6. Sopesa la utilidad de tener dos navegadores distintos instalados, uno con una configuración más restrictiva y otro configurado con mayores permisos. De esta forma, si las configuraciones anteriores te impiden acceder a algún servicio concreto, puedes seguir accediendo a ese servicio con el otro navegador minimizando la exposición de tus datos.

7. Otra opción para navegar en sitios que te exigen un mayor acceso a tus datos es añadir una excepción en la configuración del navegador que estás usando, pero recuerda que estarás exponiendo información personal con los sitios incluidos en la excepción.

8. Puedes configura el navegador de tal manera que al cerrarse se eliminen las cookies. Si esta medida te resulta incómoda para navegar en tus sitios favoritos, puedes optar por borrarlas manualmente cada cierto tiempo.

9. Evita en lo posible iniciar sesión en el navegador, identificándote con un usuario, o al menos, evita que la sesión se mantenga abierta de forma indefinida. Además, configura el navegador para no sincronizar tus datos de navegación con tu usuario de sesión.

10. Si el navegador no dispone de protección avanzada anti-rastreo/seguimiento, se pueden instalar extensiones que realicen esta función. No obstante, instala únicamente aquellos que ofrezcan garantías. En general, instalar software de terceros en el navegador puede introducir riesgos.

11. Configura las opciones de tu dispositivo para que, si así lo deseas, no se utilice el identificador de publicidad para crear perfiles o mostrar anuncios personalizados basados en la localización o el perfil. Si el dispositivo lo permite, también puedes cambiar[7] el identificador de publicidad cada cierto tiempo desde las opciones de configuración de privacidad.

12. Revisa y configura las opciones de personalización, perfiles y publicidad de aquellas aplicaciones, servicios y redes sociales[8] que utilices.

[4] Protección de rastreo en Mozilla Firefox y Microsoft Edge.
[5] Configuración de señal "Do Not Track" en Chrome, Firefox y Edge.
[6] Bloqueo de cookies de tercera parte en Chrome, Firefox y Edge.
[7] Cambiar/Restablecer identificador de publicidad en Android e iOS.
[8] Control personalización de anuncios Twitter, Facebook y Google.

Recomendaciones para usuarios avanzados

Para alcanzar un mayor nivel de control y de protección ante el seguimiento no deseado en internet se puede hacer uso de técnicas avanzadas, entre otras:

1. Configurar en la red doméstica un bloqueador de consultas DNS, como por ejemplo PiHole[9], que permite agregar listas de dominios a los que se restringe la conexión desde los dispositivos que tenemos en la red.

2. Navegar a través de una VPN (red privada virtual) o la red TOR[10]. Utilizar estos servicios de forma inapropiada puede suponer otros riesgos a la privacidad y a la seguridad en nuestras conexiones.

3. Instalar máquinas virtuales en tu sistema, incluyendo únicamente un navegador de Internet y navegar en las sesiones virtuales.

4. Utilizar sistemas operativos diseñados para preservar la privacidad y el anonimato, como por ejemplo Tails[11] o QubesOS[12].

[9] https://pi-hole.net/
[10] https://www.torproject.org/es/
[11] https://tails.boum.org/install/
[12] https://www.qubes-os.org/intro/