

TECNOLOGÍA

Navegar sin ser rastreado: una aspiración difícil de conseguir en Internet

La privacidad y el rastreo de las actividades que se hacen en internet levantan preocupaciones alrededor del mundo. Respuestas a interrogantes sobre los datos que damos a los navegadores.

MARIANA MALEK
Jueves, 08 Abril 2021 04:00

Compartir esta noticia



Foto: Shutterstock

Este contenido es exclusivo para nuestros suscriptores.

Seis personas de cada 10 usan **Google Chrome** como su navegador de internet preferido, de acuerdo con Global Stats. Según esta consultora, en **Uruguay** esa cifra asciende a 8,5 usuarios. Sin embargo, cuestiones de **privacidad** de la información hace que los expertos se preocupen cada vez más sobre cómo se rastrea la actividad online.

De acuerdo con el especialista en tecnología del *New York Times*, Brian X. Chen, es hora de que los usuarios de internet presten atención al navegador que utilizan para surfear la red y evalúen las opciones que ofrece el mercado, en particular, aquellas nuevas que se presentan como "navegadores (o *browsers*) privados".

Esto se debe a que algunas marcas menos conocidas que las populares – **Chrome de Google, Safari de Apple o Edge de Microsoft**–, como **Brave o DuckDuckGo**, minimizan la cantidad de datos que se brindan a sitios y navegadores e incluso son capaces de bloquear las tecnologías que rastrean la actividad en línea.

Gennie Gebhart, directora de Electronic Frontier Foundation, una organización sin fines de lucro de derechos digitales que se ocupa de los problemas de privacidad en línea, dijo al *New York Times* que este es un momento clave: "Las empresas que mantienen las luces encendidas haciendo publicidad a los usuarios, incluido **Google**, están luchando por ver cuál es la próxima jugada. También es un momento para que los usuarios estén informados y tomen una decisión".

Gratis (pero no tanto)

Para **Roberto Ambrosioni**, catedrático de **Ciberseguridad** de la Facultad de Ingeniería de la Universidad ORT y encargado de ciberseguridad de MAPFRE, los usuarios deben comprender la relación entre costo y beneficio que tiene el rastreo de datos que hacen los navegadores. En este sentido, deben informarse, ante todo, sobre qué datos se les otorgan.

"Los **navegadores** son un servicio y como todo servicio tiene un costo. Más allá de que no sea monetario, todos los navegadores a la larga venden anuncios y funcionan en base a esos datos", aseguró el especialista.

Ambrosioni sostuvo que, si no se trata de una "masacre a la **privacidad**", no tiene sentido quejarse de que el navegador se quede con datos y explicó a El País: "Con 'masacre a la privacidad' me refiero a cuando te sacan muchísimos datos, como el posicionamiento, etc. Eso no sucede en los navegadores comunes".

El experto enfatizó que el usuario debe ser consciente de que todo lo que se hace en internet queda guardado en la red de alguna manera.

Además, señaló que parte de los datos almacenados son utilizados para mejorar el servicio que ofrecen las diferentes plataformas. "Los errores o las búsquedas y sus respuestas ayudan a mejorar el funcionamiento de ese servicio al que accedemos", detalló.

El catedrático no niega de que el registro de esos datos viole la privacidad, pero entiende que forma parte de las reglas de juego del uso de internet. "Si el servidor se da cuenta que te gusta la **playa** y te da publicidad de playas, tal vez te moleste, pero no es nada grave. El problema es que muchas personas no los usan con fines que quieran que se conozcan y es entonces cuando se quejan", agregó.

Para el docente, nunca debe perderse de vista que los navegadores usan esa información para sustentarse, porque son un negocio

La transparencia como diferencial

Ambrosioni señaló que hace unos años hubo un cambio de paradigma sobre los datos que se almacenan en la red. "La seguridad está antes que la privacidad", destacó.

Como parte de su trabajo, el catedrático de **Ciberseguridad** de Universidad ORT prueba todas las nuevas tecnologías y, entre ellas, los nuevos navegadores que surgieron en los últimos años.

El "veredicto" de Ambrosioni es que jamás se deben usar navegadores que estén obsoletos.

"Si estás usando un navegador como **Internet Explorer** y ves que muchas plataformas bancarias te dicen que no sirve, eso es una señal de que está obsoleto. Entonces, como regla de seguridad no deben utilizarse", remarcó.

Usarlo no solo generará problemas de privacidad sino también conflictos adicionales: "Los atacantes acceden directamente tienen acceso a los datos".

La diferencia de los nuevos programas como **Brave, DuckDuckGo o Firefox Focus** es que en algunos casos están más encriptados que otros y eso implica que son menos vulnerables ante ataques.

"La gran diferencia que tiene la nueva generación de navegadores es que parecen ser más transparentes que el resto. Pero, de todos modos, te avisan que están rastreando datos porque ellos mismos lo hacen. Eso quiere decir que están más **aguijados** respecto a las normativas de protección de datos", concluyó.

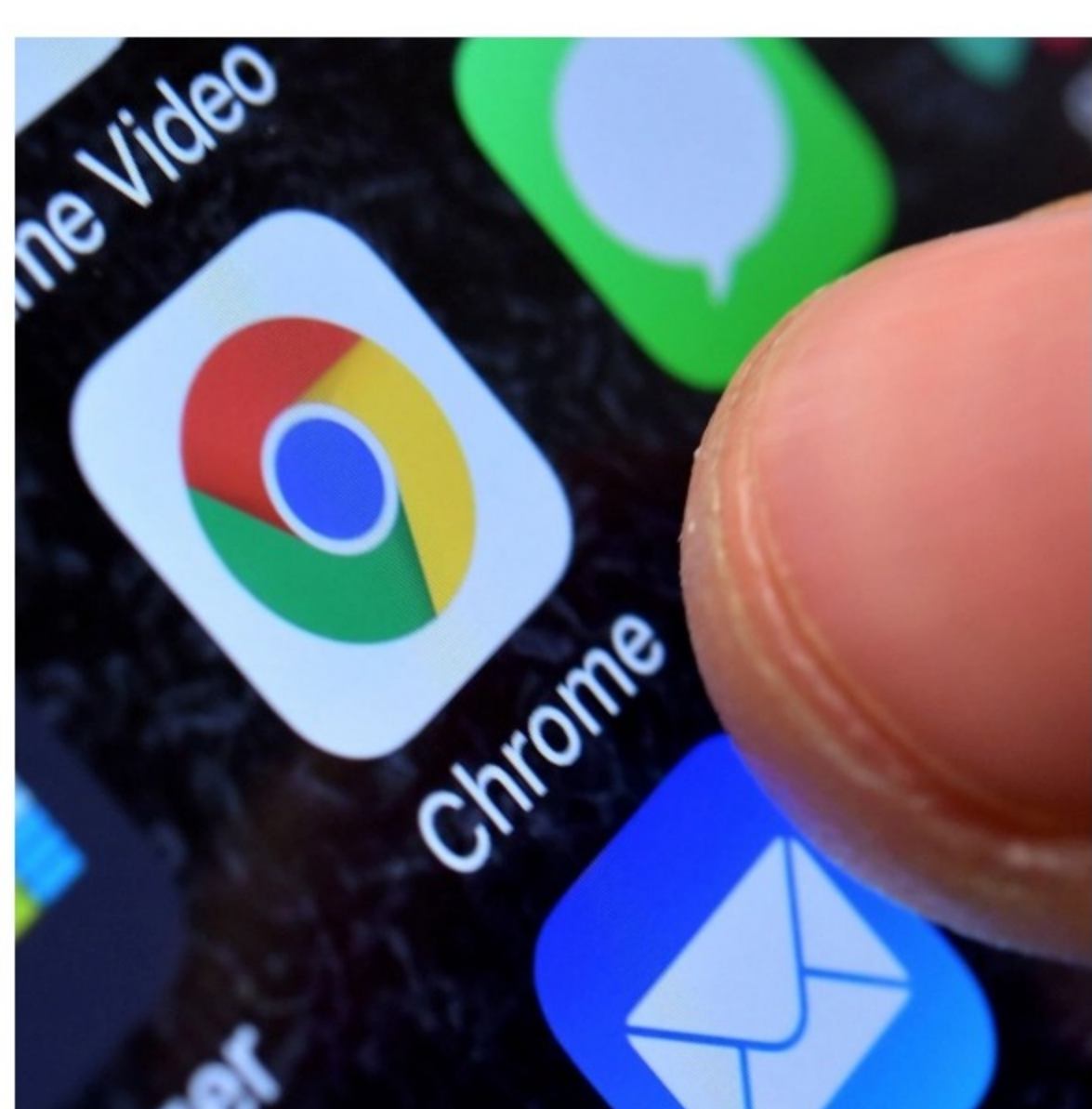


Foto: Shutterstock

¿Qué es un navegador privado?

Los navegadores privados incorporan tecnologías web que no son una novedad, pero lo importante es que las traen predeterminadas. Este tipo de plataformas funciona por defecto en **modo privado** o **incógnito** y no recuerda los sitios web visitados previamente. Además, utilizan bloqueadores para los rastreadores que incorporan los sitios web.

Cada vez que se visita una página, el software detecta esos rastreadores y les impide seguirlo de un sitio a otros. De todos modos, estos navegadores no impiden que su proveedor de internet vea los sitios web que visita, para ese tipo de protección, aún necesita conectarse a una **red privada virtual** (más conocida como **VPN**), que crea un túnel virtual que protege la información de navegación.

Cookies: ¿A qué le decís que si cuando las aceptás?

Entraste en un sitio web y te preguntaron si aceptabas las **cookies**? Si alguna vez visitaste sitios web esta situación sucedió en múltiples ocasiones. Las **cookies** según la página de soporte de **Google**, "guardan información de la navegación para hacer que tu experiencia en línea sea más sencilla. Con las cookies, los sitios pueden hacer lo siguiente: mantener tu acceso y recordar tus preferencias de sitios".

Los expertos definen a las cookies como los archivos que crean los sitios web donde se almacenan pequeñas cantidades de datos que se comparten a través del **navegador** con otros sitios de la web. A través de esos datos se crean los perfiles de usuarios para un funcionamiento más dirigido a los intereses de los usuarios, generalmente con un uso comercial.

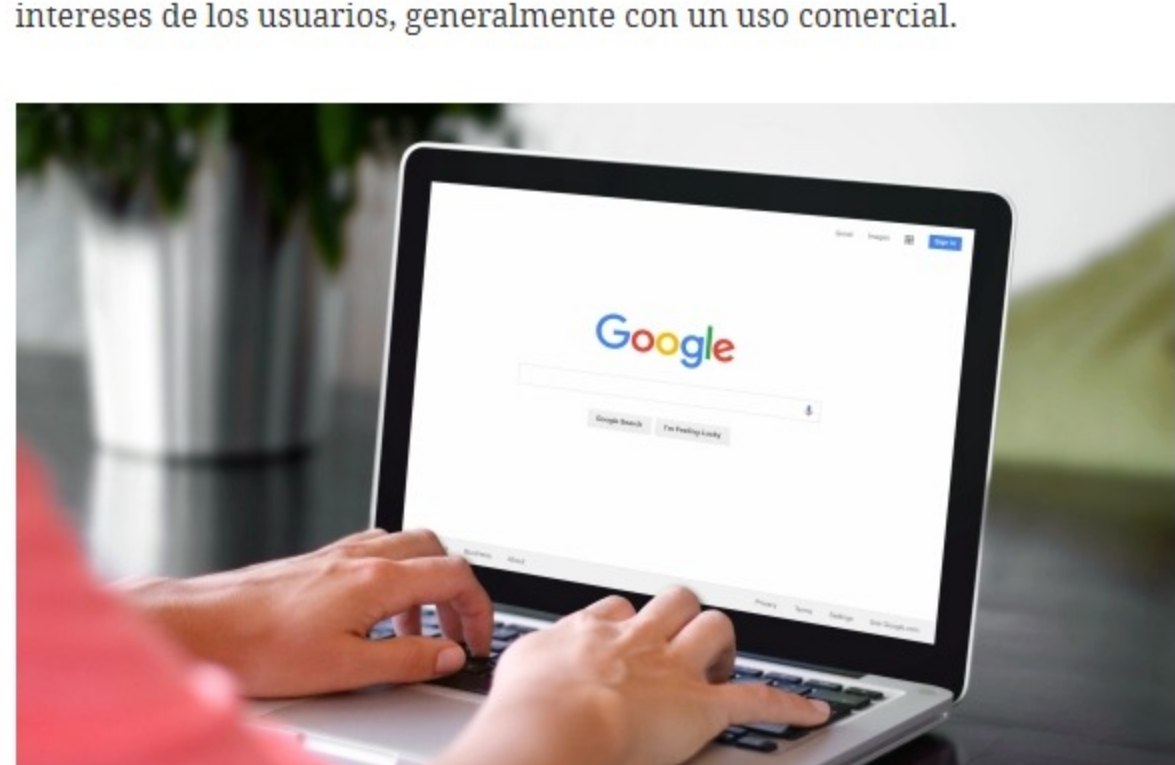


Foto: Shutterstock

¿Cómo se protegen los datos?

En Roberto Ambrosioni señaló que, desde hace algunos años, los gobiernos trabajan en los marcos legales que garantizan a los ciudadanos que sus datos son protegidos. La más sonada a nivel global fue el **Reglamento General de Protección de Datos (GDPR)**, por su título en inglés) que el parlamento europeo aprobó en 2016 y empezó a aplicar a partir de mayo de 2018.

Ambrosioni explicó que la fama de esta legislación tuvo impacto por su dureza. Uruguay protege los datos de sus ciudadanos desde 2008 a través de la **Ley 18.331** y establece que es un derecho humano previsto en la Constitución.

"La ley uruguaya fue actualizada en febrero de 2020 y se agregaron nuevas protecciones como que si hay un incidente cibernético en una empresa se debe avisar en un lapso de 72 horas a AGESIC; también se incorporó la figura del responsable de datos personales que las empresas deben tener. Esos dos puntos son importantes, porque en este momento donde hay muchos incidentes cibernéticos tenés que avisarle a tus clientes en un lapso de 72 horas y también a la unidad reguladora", destacó.

El especialista en ciberseguridad indicó que todos estos cambios en las condiciones de uso de los diferentes servicios son muy buenos desde el punto de vista de la protección del usuario porque brindan más garantías.

De todos modos, advirtió que cuando se habla en términos de privacidad no hay que ir contra el desarrollador de un navegador: "Es su negocio y así funciona. La clave es que el usuario sepa qué es lo que le está brindando a ese navegador", detalló el especialista.

¿Cuáles son los navegadores privados más destacados?

1. **Brave**: Se trata de un navegador de código abierto que está disponible desde 2016 y que popularizó su buen rendimiento. La plataforma asegura combatir el malware y el rastreo. Además, remarca que no comercializa los datos personales de sus usuarios y la navegación es privada.

2. **DuckDuckGo**: El navegador DuckDuckGo funciona en dispositivos móviles con Android o iOS y se puede instalar como extensión en Chrome. Su diferencial es que los anuncios no se basan en las cookies y evita que se carguen los rastreadores de anuncios. Además, permite borrar la sesión una vez que terminó de usarse.

3. **Firefox Focus**: Esta aplicación solo sirve en Android e iOS. Su diferencial es que cada vez que se sale de la aplicación el historial se purga automáticamente. Además, cuando carga un sitio web, el browser utiliza en una base de datos de rastreadores para determinar cuáles debe bloquear.

LAS MÁS VISTAS

