Protege tu privacidad en un mundo de vigilancia digital

- Cómo Google captura toda tu vida
- Cómo las aplicaciones móviles te rastrean constantemente
- 5 pasos fáciles para protegerte a ti y a tu familia

murena
choose freedom

En resumen

En la era digital actual, la privacidad se ha convertido en uno de los temas más cruciales para individuos y sociedades. Los dispositivos en los que confiamos —especialmente nuestros teléfonos inteligentes— recopilan una cantidad inmensa de datos personales y profesionales, a menudo sin nuestro pleno entendimiento o consentimiento genuino.

Gigantes tecnológicos como Google y Apple, junto con una amplia gama de aplicaciones móviles, tienen acceso a detalles íntimos de nuestras vidas, y los métodos que usan para rastrearnos representan amenazas significativas para nuestra privacidad y seguridad.

Este documento explora hasta qué punto empresas como Google y Apple recopilan datos de los usuarios, cómo las aplicaciones móviles rastrean a los usuarios a través de publicidad y subastas en tiempo real, y las posibles consecuencias de estas prácticas.
También ofrece pasos fáciles para ayudarte a protegerte contra la vigilancia digital.

Cómo Google recopila y utiliza los datos de los usuarios

Google, una de las mayores empresas tecnológicas del mundo, ha construido su imperio ofreciendo servicios "gratuitos" como Gmail, Google Search, YouTube y Google Maps, obteniendo enormes ganancias con la publicidad. Sin embargo, estos servicios tienen un costo significativo para la privacidad de los usuarios.

Cómo Google recopila tus datos:

- Rastreo de ubicación
- Historial de búsqueda y navegación
- Comunicaciones personales
- Aplicaciones de Google y Android

11,6 MB/día/usuario

La cantidad de datos personales recopilados por Google de teléfonos inteligentes Android.

Fuente: Digital Content Next – Prof. Douglas C. Schmidt, Universidad de Vanderbilt, agosto de 2018.

Cómo Google recopila y utiliza los datos de los usuarios

Rastreo de ubicación

Google rastrea tu ubicación incluso cuando no estás usando Google Maps. Recopila datos en tiempo real de dispositivos Android y puede inferir tu ubicación a través de direcciones IP, redes Wi-Fi y conexiones Bluetooth.

Cómo Google recopila y utiliza los datos de los usuarios

Historial de búsqueda y navegación

Cada búsqueda que realizas a través de Google Search y cada sitio web que visitas a través de Google Chrome es rastreado y registrado. Esto permite a Google construir un perfil detallado de tus intereses, hábitos y comportamientos.

Cómo Google recopila y utiliza los datos de los usuarios

Comunicaciones personales

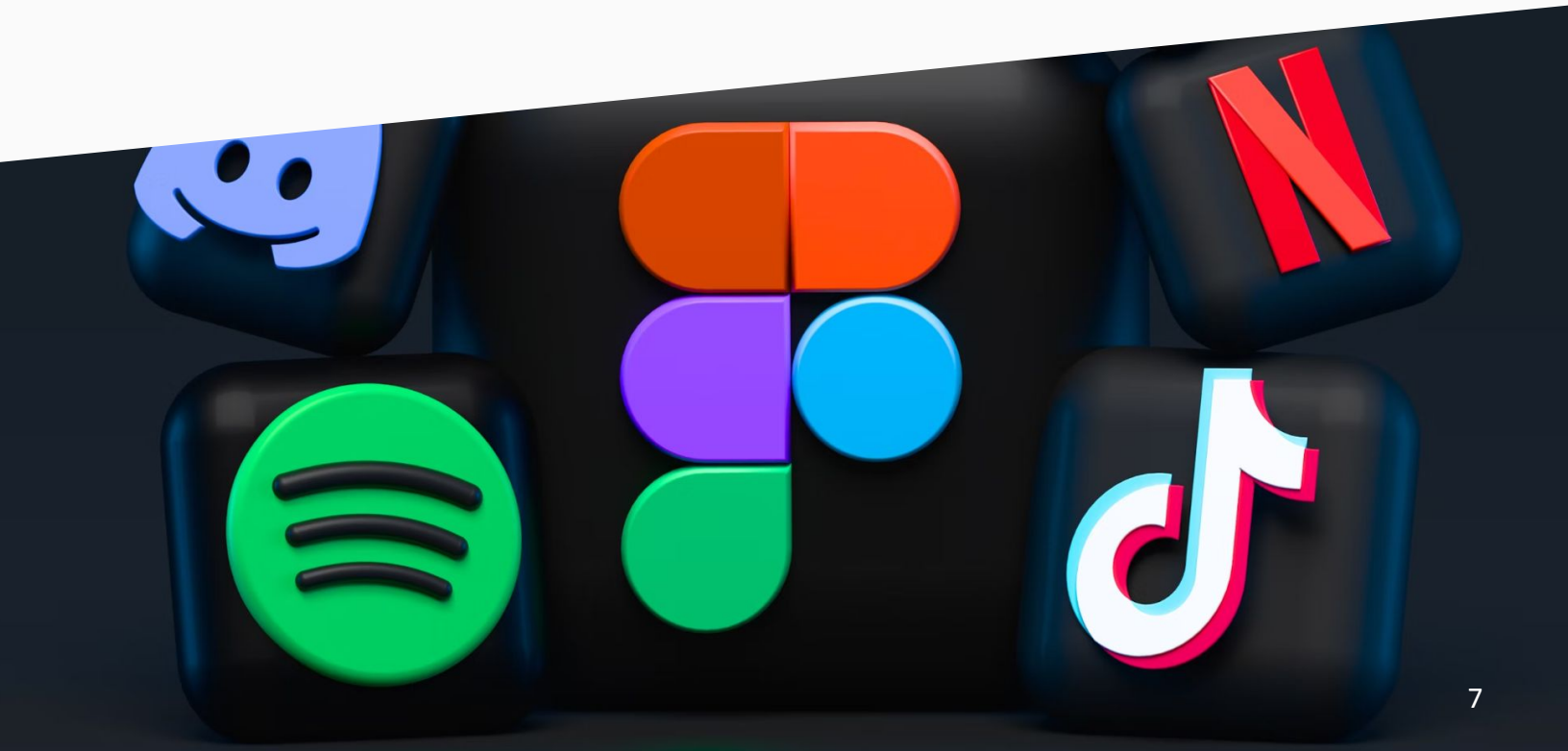
Si usas Gmail o Google Drive, el contenido de tus correos electrónicos y documentos puede ser escaneado y analizado por los algoritmos de Google para mejorar el direccionamiento publicitario. Google también recopila datos de mensajes de texto y llamadas de usuarios de Android sin consentimiento.

Fuente: "What Data Do The Google Dialer and Messages Apps On Android Send to Google?", Prof. Douglas Leith, Trinity College, Dublín, 2022.

Cómo Google recopila y utiliza los datos de los usuarios

Aplicaciones de Google y Android

La mayoría de los teléfonos Android están vinculados al ecosistema de Google, lo que significa que cada interacción con tu teléfono (como abrir aplicaciones, usar la cámara o comandos de voz) puede ser recopilada.
Los servicios de Google Play rastrean cómo y cuándo usas aplicaciones y sitios web, dando a Google acceso a amplios datos de comportamiento.

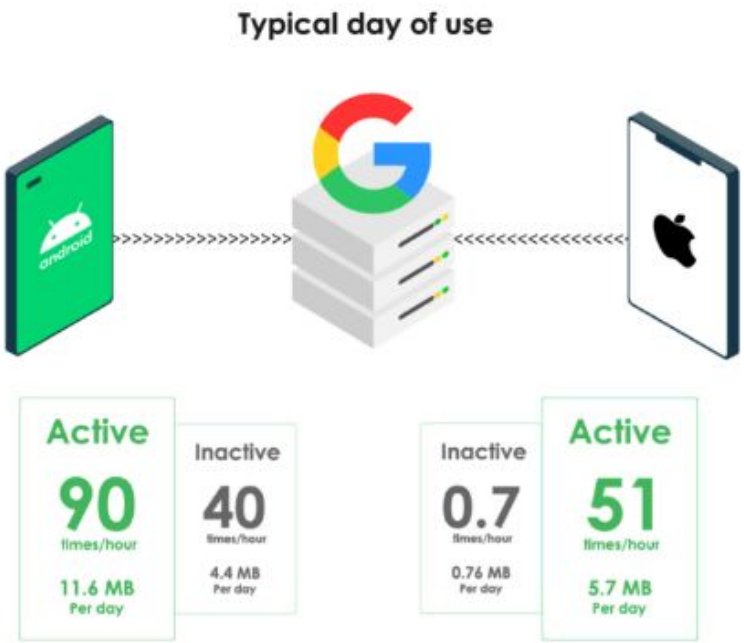


El enfoque de Apple en la recopilación de datos

Aunque Apple se comercializa como una empresa más enfocada en la privacidad, también participa en una recopilación significativa de datos. Apple no recopila tantos datos pasivamente como Google, pero aún recopila información a través de sus servicios como el App Store, iCloud y Apple Health.
Apple también recibe más de 25 mil millones de dólares por año de Google para hacer que Google Search sea el motor de búsqueda predeterminado de los dispositivos iOS.

Cantidades de datos recopilados:

- Un teléfono Android inactivo transmite entre 4,4 MB y 11,6 MB de datos personales por día a Google.
- Un dispositivo Apple envía entre 0,76 MB y 5,7 MB de datos por día a Google.
Fuente: Informe de la Universidad de Vanderbilt.



Consecuencias de la recopilación de datos por parte de Google y Apple

Los esfuerzos masivos de Google y Apple para recopilar datos permiten a estas empresas construir perfiles increíblemente detallados de individuos, incluyendo su historial de ubicación, historial de búsqueda, hábitos de comunicación y compras en línea. Esto genera preocupaciones importantes sobre la privacidad:

- **Economía de vigilancia:** Con datos tan completos, Google (y empresas tecnológicas similares) pueden moldear nuestras experiencias en línea, limitar el contenido que vemos y manipular nuestras decisiones, ya sea en compras, preferencias políticas o vida diaria.

- **Manipulación del comportamiento:** Con información precisa sobre el comportamiento de los usuarios, Google puede utilizar sus datos para influir no solo en los anuncios que los usuarios ven, sino también en lo que piensan o sienten, lo que representa serios riesgos para la autonomía.

- **Violaciones de datos:** Cuantos más datos recopila una empresa, más atractiva se vuelve para los piratas informáticos. Las violaciones de datos en empresas como Google pueden exponer información personal.

Cómo las aplicaciones móviles utilizan la publicidad y las subastas en tiempo real para rastrear a los usuarios

Además de Google y Apple, muchas aplicaciones móviles participan en prácticas invasivas de seguimiento a escala global, a menudo sin que los usuarios sean plenamente conscientes. Cómo las aplicaciones rastrean a los usuarios:

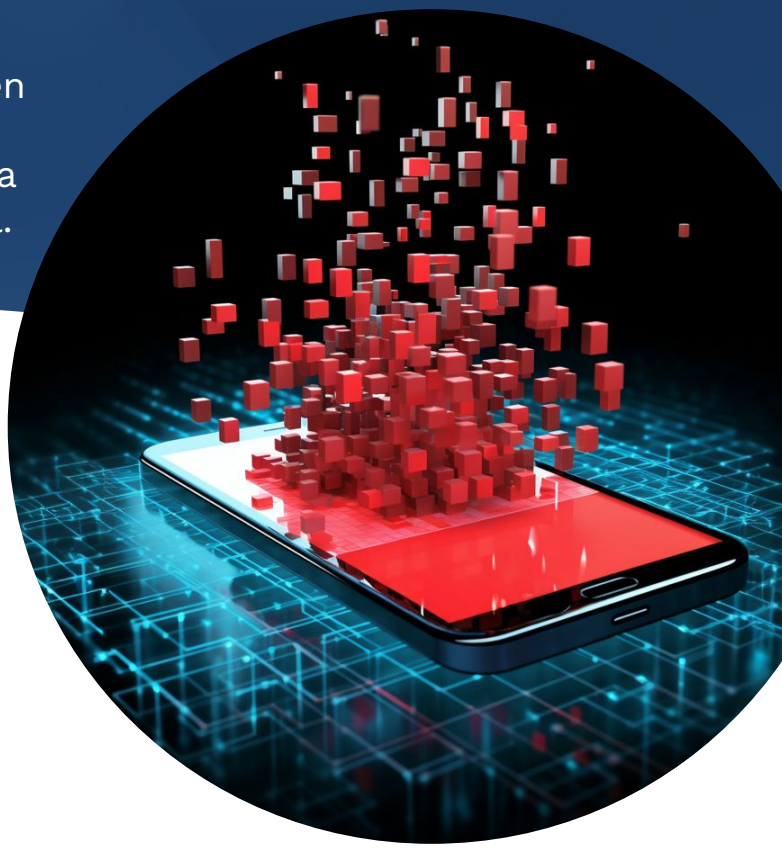
- **ID de publicidad:** Los dispositivos móviles tienen identificadores únicos, como el IDFA (Identifier for Advertisers) de Apple o el Advertising ID de Google, que permiten a las aplicaciones rastrear a los usuarios en diferentes plataformas. Estos ID se utilizan para mostrar anuncios dirigidos.

- **Subastas en tiempo real (RTB):** RTB es un sistema de subastas automatizado en el que los anunciantes pujan en tiempo real para mostrar anuncios a usuarios específicos. Cuando abres una aplicación o sitio web, los anunciantes reciben inmediatamente información sobre ti, como tu ubicación, dispositivo y comportamiento previo, y realizan pujas para mostrar anuncios. Este proceso ocurre millones de veces por segundo.

Consecuencias del seguimiento por aplicaciones móviles y subastas en tiempo real

Los datos recopilados por aplicaciones móviles y subastas en tiempo real representan amenazas graves para la privacidad de los usuarios:

- **Manipulación dirigida:** Los datos recopilados a través de RTB permiten a los anunciantes crear anuncios altamente dirigidos y personalizados. Si bien esto puede mejorar la relevancia de los anuncios, también permite a los anunciantes (o grupos políticos) manipular el comportamiento de los usuarios al proporcionar contenido específico y emocionalmente cargado.
- **Vigilancia constante:** Las aplicaciones pueden rastrear tu ubicación, el uso de aplicaciones y el comportamiento de navegación en tiempo real, a menudo sin tu consentimiento. Esto conduce a una vigilancia continua de tu vida digital.



- **Comerciantes de datos y erosión de la privacidad:** Los datos recopilados a través de RTB a menudo se comparten con intermediarios de datos de terceros, quienes pueden compilar perfiles completos de los usuarios. Estos intermediarios venden tus datos a anunciantes, gobiernos u otras entidades, lo que agrava aún más la erosión de tu privacidad.

Consejos para protegerte de la vigilancia digital

Afortunadamente, hay varios pasos que puedes seguir para protegerte de la vigilancia digital:

- **Desactiva el rastreo de ubicación:** Desactiva los servicios de ubicación para las aplicaciones que no lo necesiten y utiliza una VPN para ocultar tu dirección IP.
- **Bloquea rastreadores de publicidad:** Usa extensiones de navegador enfocadas en la privacidad. Desactiva los ID de publicidad en Android y iOS. El bloqueo de rastreadores en aplicaciones y la web también es una función predeterminada en /e/OS.
- **Minimiza los permisos de las aplicaciones:** Revisa regularmente los permisos de las aplicaciones y revoca el acceso a datos innecesarios para la funcionalidad básica de la aplicación.
- **Usa aplicaciones alternativas:** Sustituye tantas aplicaciones y servicios de Google como sea posible, especialmente Gmail y la búsqueda de Google.
- **Usa cifrado de extremo a extremo:** Opta por aplicaciones de mensajería como Signal, Matrix/Element o Threema, que ofrecen cifrado de extremo a extremo, asegurando que tu comunicación sea privada. Usa servicios de correo electrónico que ofrezcan cifrado de extremo a extremo completo, como ProtonMail.
- **Considera dispositivos enfocados en la privacidad:** Los teléfonos inteligentes Murena que ejecutan /e/OS están diseñados para respetar tu privacidad, evitando los mecanismos de rastreo de Google y los rastreadores publicitarios.

¡Seguridad NO es lo mismo que privacidad!

En el panorama digital actual, a menudo se confunden la seguridad y la privacidad. Aunque ambas son esenciales, sirven para diferentes propósitos:

- La seguridad se centra en proteger sistemas y datos contra accesos no autorizados.
- La privacidad tiene como objetivo limitar la recopilación y el intercambio de datos personales desde el principio.

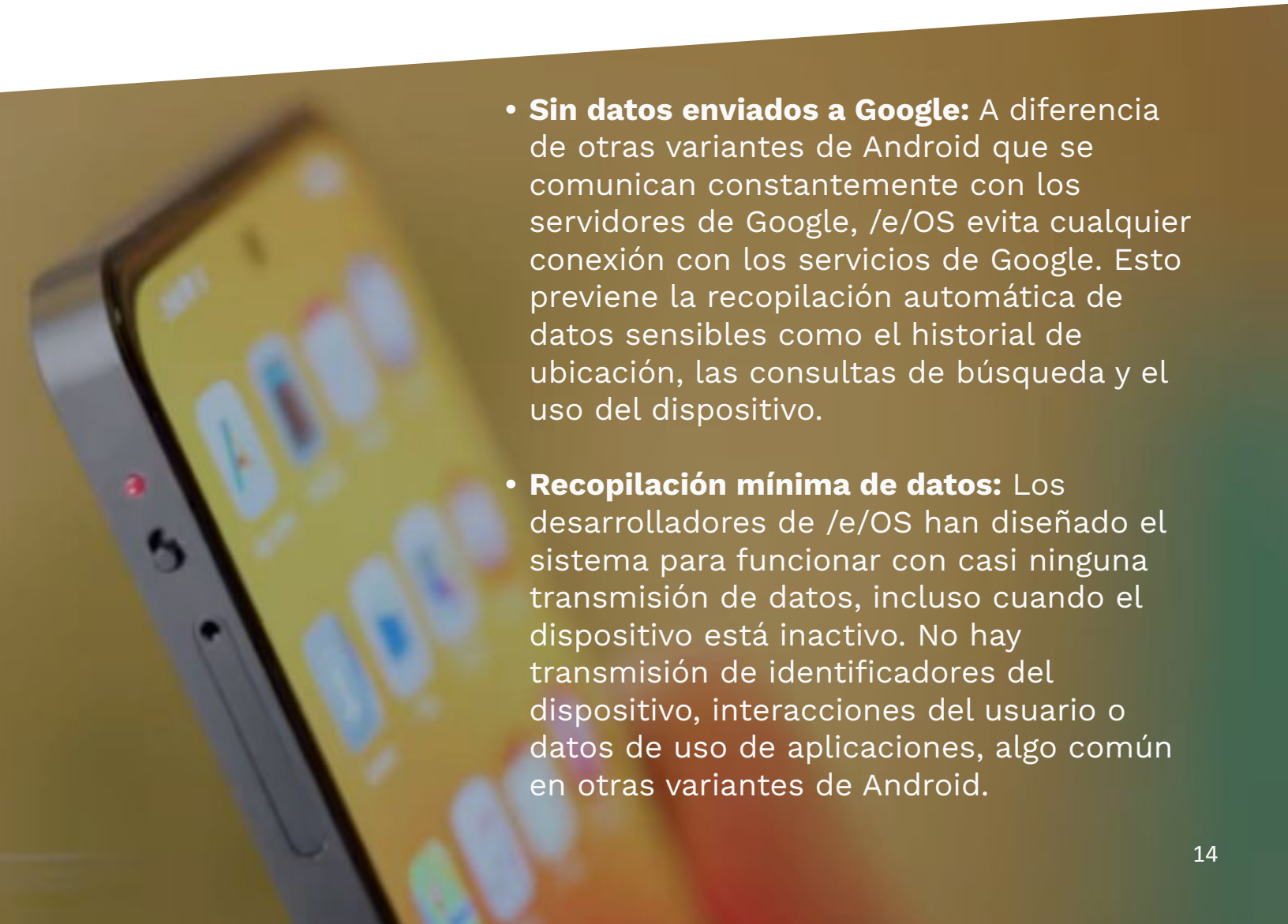
Un dispositivo puede ser seguro y aún así comprometer tu privacidad, ya que la seguridad no evita la recopilación de datos o la vigilancia por parte del propietario del sistema.

Ejemplos:

- **Software espía Pegasus en iPhones:** A pesar de la reputación de los iPhones como dispositivos seguros, Pegasus explotó vulnerabilidades para hackear a objetivos de alto nivel, incluidos un presidente europeo y activistas, sin interacción del usuario.
- **Hackeo por inteligencia rusa:** Durante el conflicto de Crimea, los teléfonos inteligentes de los soldados ucranianos fueron hackeados, permitiendo a los adversarios rastrear sus movimientos e interceptar comunicaciones, a pesar del uso de dispositivos encriptados de grado militar.
- **EncroChat y redes criminales:** Los teléfonos cifrados utilizados por redes criminales como EncroChat fueron hackeados por las fuerzas del orden europeas, lo que llevó al arresto de muchos criminales a pesar de que los teléfonos se consideraban "inhackeables".

Cómo Murena y /e/OS protegen la privacidad de los usuarios

A diferencia de los principales sistemas operativos móviles como Android de Google e iOS de Apple, /e/OS prácticamente no recopila datos personales de sus usuarios. Según un estudio, /e/OS se destaca como el sistema más respetuoso con la privacidad entre varias plataformas basadas en Android como Samsung, Xiaomi y Huawei.



- **Sin datos enviados a Google:** A diferencia de otras variantes de Android que se comunican constantemente con los servidores de Google, /e/OS evita cualquier conexión con los servicios de Google. Esto previene la recopilación automática de datos sensibles como el historial de ubicación, las consultas de búsqueda y el uso del dispositivo.
- **Recopilación mínima de datos:** Los desarrolladores de /e/OS han diseñado el sistema para funcionar con casi ninguna transmisión de datos, incluso cuando el dispositivo está inactivo. No hay transmisión de identificadores del dispositivo, interacciones del usuario o datos de uso de aplicaciones, algo común en otras variantes de Android.

Conclusión

En el mundo digital actual, nuestros datos personales se recopilan cada vez más a través de aplicaciones móviles y plataformas web. Grandes actores como Google y Apple recopilan enormes cantidades de datos de los usuarios, creando riesgos significativos a medida que los comportamientos y preferencias de los usuarios se rastrean y venden, a menudo sin su consentimiento claro.

Para proteger tu privacidad:

- Desactiva el rastreo de ubicación y usa una VPN.
- Sustituye los servicios de Google por alternativas respetuosas con la privacidad.
- Prefiere aplicaciones de mensajería con cifrado de extremo a extremo.
- Considera los teléfonos inteligentes Murena que ejecutan /e/OS, diseñados para respetar tu privacidad.