Denuncia contra LinkedIn: la plataforma habría espiado a millones de usuarios con un código oculto

09/04/2026

Un informe de la organización Fairlinked eV sostiene que LinkedIn espía a usuarios mediante un script denominado “BrowserGate”. Según el reporte, el sistema analizaba extensiones y generaba huellas digitales de los dispositivos. El alcance estimado supera los 405 millones de cuentas. La compañía rechazó las acusaciones y defendió el uso de herramientas de seguridad.

LinkedIn espía con “BrowserGate”: qué dice el informe sobre el análisis de extensiones

El informe de Fairlinked eV describe un mecanismo que habría operado en segundo plano dentro de los navegadores. Este

código, bautizado como “BrowserGate”, **habría permitido revisar más de 6.000 extensiones instaladas por los usuarios**. Entre ellas, se incluyen bloqueadores de anuncios, VPN y herramientas laborales.

Además del análisis de extensiones, el sistema habría recolectado información técnica del dispositivo, como sistema operativo, procesador y resolución de pantalla. Con estos datos, **se podría construir una “huella digital” única para cada usuario**. Según el reporte, esto plantea riesgos para la privacidad, especialmente en entornos profesionales.

Alcance del caso LinkedIn y debate por privacidad tras “BrowserGate”

El documento sostiene que **más de 405 millones de cuentas podrían haber sido afectadas**, con un aumento del uso del sistema entre 2024 y 2025. Este crecimiento se vincula con la implementación de la **Ley de Mercados Digitales de la Unión Europea**, que obligó a las plataformas a abrirse a servicios de terceros.

Desde LinkedIn, sin embargo**, negaron las acusaciones** y afirmaron que la detección de extensiones responde a fines de seguridad. La empresa aseguró que estos datos se utilizan para proteger tanto a la plataforma como a los usuarios, y cuestionó la credibilidad del informe.

El caso generó preocupación en organizaciones de privacidad, que **reclaman mayor transparencia y controles claros**. Expertos recomiendan revisar extensiones activas, limitar permisos y **reforzar políticas de seguridad**. La polémica reabre el debate sobre el equilibrio entre innovación tecnológica y protección de datos personales.

Fuente: La 100