

El fin de la privacidad: descubren que las señales de Wi-Fi pueden reconocerte y seguir tus pasos aunque tengas el celular apagado

02/06/2026



Durante años se asumió que la red wifi sólo servía para transportar datos entre aparatos. Un estudio del Instituto Tecnológico de Karlsruhe demuestra que las señales domésticas contienen información capaz de identificar a personas sin necesidad de que lleven un dispositivo encima. El hallazgo obliga a repensar la privacidad del entorno inalámbrico cotidiano.

Los autores se enfocaron en un componente poco conocido del protocolo: la **información de retroalimentación de beamforming** (BFI). Introducida con wifi 5, permite optimizar la dirección de la transmisión. Buena parte de esos paquetes viaja sin cifrar y contiene patrones físicos que, tras

procesarlos con aprendizaje automático, resultan sorprendentemente descriptivos.

Del ruido al rasgo: cómo funciona

En pruebas con 197 participantes, el sistema bautizado BFId logró identificar a individuos con una precisión cercana al 99,5% incluso cuando cambiaban de posición. A diferencia de trabajos previos que requieren acceso complejo a CSI, aquí se usaron routers comerciales y tarjetas corrientes, lo que acerca el concepto de **wifi biométrico** al equipamiento cotidiano.

La explicación física es simple en lo conceptual: las ondas se deforman al chocar con cuerpos, muebles y paredes, y esas microvariaciones se acumulan en patrones repetibles. La musculatura, la estatura y la manera de moverse dejan marcas radioeléctricas que el algoritmo usa como firma. Esa idea resume la noción de **wifi biométrico**.

Riesgos y recomendaciones

Los autores alertan sobre usos encubiertos: comercios, oficinas o servicios públicos podrían monitorizar identidades sin cámaras visibles. Ante ese riesgo proponen medidas en el estándar IEEE 802.11bf para limitar la captura o interpretación fácil de señales sensibles. La historia tecnológica muestra que herramientas útiles suelen reasignarse a finalidades menos benignas.

No es una cámara ni genera reconstrucciones tridimensionales precisas: BFId ofrece una firma estadística ligada a perturbaciones de señal, y su eficacia depende del entorno. Muebles, geometría del espacio e interferencias afectan el rendimiento, por lo que el sistema precisa entrenamiento previo y condiciones relativamente estables para alcanzar resultados elevados.

Investigaciones previas ya exploraban detección de presencia, respiración o caídas con señales inalámbricas, pero el avance clave es pasar de 'hay alguien' a 'sabemos quién'. Ese cruce transforma la discusión pública: no sólo se discute automatización o confort tecnológico, sino también derechos vinculados a identidad, anonimato y regulación del espacio digital.

El trabajo del Karlsruhe no implica vigilancia total inmediata, pero sí obliga a tomar medidas antes de que la técnica se despliegue masivamente. Reguladores, fabricantes y usuarios deben incorporar protecciones y transparencia.

Fuente: La 100