LA VENTANA INDISCRETA

LOS APARATOS QUE NOS VIGILAN

Una cámara en la esquina del techo siempre ha sido fácil de identificar y de evitar. En cambio, los nuevos sistemas de vigilancia no necesitan cámaras: utilizan el *router* wifi del salón, el altavoz inteligente de la cocina o la futura red móvil 6G, capaces de detectar nuestra presencia, nuestros movimientos y nuestra respiración a partir de las mismas ondas de radio que usamos para conectarnos o de ultrasonidos. Repasamos, de lo más visible a lo más invisible, el catálogo de aparatos y de señales que hoy nos observan, y el que se está diseñando para la próxima década.

TEXTO: **CARLOS JESÚS BERNARDOS CANO** INFOGRAFÍA: **DAMGOZ**

Glosario

- **ISAC / JCAS:** *Integrated Sensing and Communication* o *Joint Communication and Sensing*: uso de una misma señal de radio para comunicar y para detectar el entorno.
- **CSI (*Channel State Information*):** información sobre cómo se distorsiona una señal wifi al propagarse por un espacio; sus variaciones permiten inferir movimiento o presencia.
- **Efecto Doppler:** cambio de frecuencia de una onda (sonora o de radio) al reflejarse en un objeto en movimiento; es la base del *sensing* por ultrasonidos y de muchos radares.
- ***Backscatter*:** señal reflejada ("retrodispersada") por personas u objetos, que un receptor analiza para detectar su presencia o movimiento.
- **Biometría:** medición de rasgos físicos (rostro, huella, iris, voz) para identificar a una persona de forma automática.

Así ha evolucionado la mirada tecnológica

Si durante 40 años los circuitos cerrados de televisión apenas evolucionaron, en las siguientes décadas hemos asistido al vertiginoso desarrollo de unas tecnologías de vigilancia que ya apuntan a su perfecta y total integración en nuestras vidas.



1940-1970	1990-2000	2000-2010	2010-2020	2020-2024	2025-2026	2028-2030
Circuitos cerrados de televisión (CCTV) analógicos: se colocan las primeras cámaras de vigilancia con cable. No posibilitan la grabación de imágenes ni el análisis automático.	Digitalización e internet: surgen las cámaras IP, las *cookies* de rastreo en la web y los primeros programas espía (*spyware*).	El hogar seguro analógico-digital: se emplean alarmas con sensores de movimiento (PIR), contactos magnéticos y detectores de humo o calor vinculados a centrales de alarma.	Biometría de masas: se introduce el reconocimiento facial en aeropuertos, ciudades y redes sociales. La geolocalización permanente se generaliza mediante el *smartphone*.	Cámaras con IA integrada, timbres inteligentes y altavoces con micrófono siempre activo. Se inician las primeras pruebas de detección por wifi (*wifi sensing*) en viviendas.	(fase actual). La tecnología *wifi sensing* se estandariza bajo la norma IEEE 802.11bf y se integra en millones de *routers* domésticos distribuidos por las operadoras.	(6G). La red móvil incorpora la detección como un servicio nativo (ISAC). Las mismas antenas que proporcionan cobertura, se emplean para detectar personas, gestos o vehículos.



Fuentes: UIT-R (Rec. M.2160), 3GPP (TR 22.870, 2026), ETSI (GR ISC 001, 2025), IEEE (802.11bf-2025), NIST (NISTIR 8280, 2019), y C. Barroso-Fernández *et al.*, IEEE Wireless Communications (2026).

A

VIGILANCIA ÓPTICA:
Y LO QUE SE OBSERVA

- **Cámaras CCTV / IP.** Sistemas fijos y enlazados a la red; las cámaras realizan grabaciones continuas. Incorporan funciones de análisis automático de vídeo que permiten contar personas.
- **Webcams**. Se usan en casas y oficinas, integradas en ordenadores portátiles y monitores. Son objetivo frecuente de ataques *malware*.
- **Cámaras infrarrojas y térmicas.** Operan en oscuridad total. Las térmicas detectan el calor corporal, también con humo o niebla poco densos.
- **Reconocimiento facial.** Esta tecnología reconoce rasgos faciales para compararlos con bases de datos. El programa de evaluación del NIST (FRVT) examinó 189 algoritmos. El estudio mostró que la tasa de falsos positivos varía entre grupos demográficos en factores de 10 a más de 100 veces.

B

VIGILANCIA AMBIENTAL:
SENSORES Y DISPOSITIVOS DE DETECCIÓN

- **Sensores de movimiento PIR.** Detectores de infrarrojo pasivo, no emiten señales. Detectan variaciones rápidas en la radiación infrarroja del entorno.
- **Sensores de proximidad.** Pueden ser magnéticos, capacitivos (detectan objetos por variaciones en la energía eléctrica que almacenan), ópticos o ultrasónicos.
- **Detectores de calor.** Disparan la alarma al superar una temperatura fija o al percibir un aumento térmico muy rápido.
- **Detectores de humo.** Pueden ser ópticos (operan mediante la dispersión de luz por partículas de humo), o iónicos (registran variaciones en una corriente eléctrica ionizada).
- **Contactos magnéticos.** Formados por un imán y un interruptor de tipo *reed*. Permiten detectar la apertura de puertas o ventanas.

C

CIBERVIGILANCIA:
SISTEMAS DE MONITORIZACIÓN OCULTOS

- **Rastreo web.** Usan *cookies* de terceros y la huella digital del navegador para registrar los hábitos de navegación sin que el usuario se identifique.
- **Programas espía (*stalkerware* / *spyware*)**. Instalados en dispositivos para observar mensajes, ubicación, llamadas… (a menudo sin consentimiento).
- **Simuladores de estación base (*IMSI catchers*)**. Son como antenas de telefonía falsas para interceptar la identidad o las comunicaciones de terminales cercanos.
- **Lectores automáticos de matrículas (ALPR).** Cámaras con tecnología de reconocimiento óptico que capturan el paso de vehículos para identificar sus trayectos.
- **Geolocalización de *smartphones*.** Toman datos de GPS, redes wifi y antenas de telefonía para determinar la ubicación de alguien con precisión creciente.

D

LA FRONTERA:
LA RED TE VIGILA (RUMBO AL 6G)

- **El horizonte 6G ya está presente en** los organismos de estandarización.
- **La UIT (UIT-R) ha incluido** "Integrated sensing and communication" entre los seis escenarios de uso oficiales del marco para el 6G. Por su parte, el 3GPP recoge en el TR 22.870 (Release 20, 2026) más de veinte casos de uso de ISAC para 6G y admite que el sensing puede rastrear a personas que no llevan ningún dispositivo, lo que exige proteger su privacidad
- **El ETSI creó un grupo** específico (ISG ISAC) que en abril de 2025 publicó su primer informe (GR ISC 001) con 18 casos de uso avanzados para 6G, de los cuales nueve tienen la detección de personas como objetivo principal; el propio informe señala la privacidad y la confianza en los datos de sensing como uno de los retos centrales a resolver antes de desplegar la tecnología.