OPINIÓN

DESPUÉS DE LA PANDEMIA

¿Podría España prohibir redes sociales que basan su modelo de negocio en espiar a los ciudadanos?

Enrique Dans

Publicada 11 febrero 2026 02:41h

La pregunta no es retórica ni futurista, y tampoco es un simple ejercicio de provocación política. Aparece de forma recurrente cada vez que se destapan abusos, filtraciones o prácticas de vigilancia masiva normalizadas, y volvió a la agenda cuando Pedro Sánchez planteó públicamente la posibilidad de perseguir a los directivos de las grandes plataformas por los daños que causan.

El problema es que, en el marco jurídico actual de la Unión Europea, esa vía concreta no es viable. Pero que una opción no sea legal no significa que no existan otras, y ahí es donde empieza el debate que realmente importa.

La Unión Europea ha construido en los últimos años un armazón regulatorio que condiciona mucho lo que los Estados miembros pueden y no pueden hacer por su cuenta. El Reglamento General de Protección de Datos (GDPR) dejó claro que la vigilancia sistemática de los ciudadanos no es una actividad neutra ni inocua, y estableció límites, obligaciones y sanciones.

La Ley de Servicios Digitales (DSA) y la Ley de Mercados Digitales (DMA) han ido más allá, reservando a la Comisión Europea un papel central en la supervisión de las grandes plataformas y limitando la capacidad de los Estados para actuar de forma unilateral.

Eso tiene una consecuencia directa: España no puede decidir perseguir penalmente a los directivos de Meta o TikTok ni imponerles condiciones estructurales al margen del marco común europeo, por mucho que la tentación política exista.

Ahora bien, de ahí no se deduce que España tenga las manos atadas. Lo que no puede hacer es crear un régimen punitivo propio incompatible con la legislación comunitaria. Pero lo que sí puede hacer es aplicar con rigor las normas existentes, utilizar todas las herramientas administrativas disponibles y, sobre todo, impulsar debates que acaben trasladándose al nivel europeo, que es donde se decide lo esencial.

La pregunta relevante no es si España puede prohibir Instagram, Facebook, Threads o TikTok mañana por decreto, porque la respuesta honesta es que no, aunque sería fantástico hacerlo. La pregunta es si puede contribuir de forma decisiva a que ciertos modelos de negocio dejen de ser legales en Europa.

En ese contexto aparece con frecuencia una falsa solución que goza de gran popularidad política: prohibir el acceso a las redes sociales a los menores de 16 años. Es una idea intuitiva, aparentemente protectora y muy rentable en términos de titular, pero profundamente problemática.

No sólo no ataca el núcleo del problema, el modelo de vigilancia y extracción de datos, sino que introduce otros riesgos quizá más graves. Para prohibir el acceso por edad es imprescindible identificar a los usuarios de forma fiable, y eso plantea un dilema técnico y político de primer orden.

La identificación de edad en internet no es un problema trivial. Sin sistemas criptográficos avanzados, como credenciales anónimas verificables o pruebas de conocimiento cero, la única alternativa realista es algún tipo de registro centralizado: documentos de identidad, bases de datos, intermediarios que certifiquen quién es quién.

Es decir, justo lo contrario de lo que se dice querer proteger. Y pensar que ese tipo de soluciones se puede desplegar de forma segura y respetuosa con la privacidad en un país cuyo debate público apenas entiende qué es la criptografía, cómo funciona o por qué es esencial para los derechos digitales es, como poco, ingenuo.

Además, abrir la puerta a sistemas obligatorios de identificación para acceder a redes sociales no solo afecta a los menores. Crea una infraestructura de control que puede extenderse fácilmente al conjunto de la población. Hoy es para “proteger a los niños”, mañana “para combatir la desinformación”, pasado, para garantizar el “buen comportamiento” o la “seguridad nacional”.

La historia tecnológica está llena de ejemplos de herramientas creadas con fines supuestamente nobles que acaban utilizándose para vigilar, discriminar o reprimir. Introducir un mecanismo generalizado de identificación en redes sociales es regalar al Estado y a terceros un poder que cuesta mucho retirar después. Y nunca sabes quién puede llegar a gobernar.

Frente a eso, prohibir un modelo de negocio es algo muy distinto de prohibir a un colectivo. La vigilancia masiva con fines comerciales no es una ley natural ni una consecuencia inevitable de internet, sino el resultado de decisiones políticas y

refutatorias concretas tomadas (o no tomadas) anteriormente.

España, como Estado miembro, puede reforzar la aplicación del GDPR, dotar de medios reales a su autoridad de protección de datos, sancionar de forma sistemática prácticas abusivas y evitar que se traten las multas como un simple coste de hacer negocios. Puede actuar también en el ámbito de la protección del consumidor y de la competencia, cuestionando consentimientos ficticios, interfaces manipuladoras y mercados publicitarios opacos.

Y, sobre todo, puede liderar en Bruselas un debate que ya está latente: si la publicidad comportamental basada en la vigilancia de los usuarios debería seguir siendo legal. Porque este debate no afecta solo a las grandes redes sociales.

Si se cuestiona de verdad el modelo de vigilancia, entran en el foco Google, intermediarios publicitarios como Criteo y buena parte de los medios y servicios que hoy dependen de rastrear a sus usuarios de forma sistemática. Eso explica la resistencia: no estamos hablando de cuatro plataformas concretas, sino de una infraestructura económica entera construida sobre la extracción sistemática de datos personales.

España no puede, hoy por hoy, ilegalizar Instagram o TikTok por su cuenta, ni resolver el problema con prohibiciones simbólicas por edad que generan más riesgos de los que eliminan.

Pero sí puede abandonar los gestos grandilocuentes sin recorrido legal y apostar por una estrategia más incómoda y eficaz: aplicar la ley hasta el final, impulsar cambios normativos a nivel europeo y asumir que un modelo de negocio basado en espiar a los ciudadanos no es un daño colateral inevitable de la economía digital, sino una decisión política. La verdadera pregunta no es si se puede, sino si se quiere.

******Enrique Dans es Profesor de Innovación en IE University.***