


**IRENE
LEVY**

TELECOMUNICANDO



La verdad detrás de la “ley espía”

El nuevo artículo **30-B del Código Fiscal de la Federación** desató una tormenta mediática. Desde antes de su aprobación en la Cámara de Diputados, algunos medios y usuarios lo bautizaron como la “**ley espía**”, asegurando que el gobierno podrá acceder a todos nuestros datos digitales: las películas que vemos, con quién salimos en apps de citas, qué compramos. Pero el texto legal y su alcance real cuentan una historia más compleja.

El artículo obliga a las **plataformas digitales a permitir al SAT acceso en línea, en tiempo real y de forma permanente** a sus sistemas con el fin de verificar que cumplen con sus obligaciones fiscales. A simple vista, parece una medida sensata pero su redacción abre dilemas sobre **privacidad, proporcionalidad y transparencia**.

Lo que se exagera. No es cierto que el gobierno estará fa-

cultado para ver lo que cada usuario hace en internet. El artículo no autoriza al SAT a ello. El sujeto de la obligación es la empresa, no el usuario. El SAT lo aclaró en un comunicado: el objetivo es fiscalizar operaciones, no espiar a usuarios, y la versión aprobada del artículo sí acota la revisión a cuestiones fiscales. En ese punto, los titulares más alarmistas deforman la realidad.

Lo que el gobierno no dice. El discurso oficial también omite y distorsiona aspectos relevantes. En un **video difundido en redes**, Ernestina Godoy, consejera jurídica del Ejecutivo Federal, afirmó que las empresas “**entregarán información al SAT**”. Esa frase es imprecisa: el artículo no habla de entrega, sino de una **conexión permanente en tiempo real**. Esa diferencia es sustancial. Una conexión directa implica que el SAT pueda consultar datos de forma continua y,



aunque la ley limita el acceso a “información necesaria para comprobar obligaciones fiscales”, muchas plataformas no tienen sistemas que separen esos datos del resto de su base de usuarios por lo que, en la práctica, podrían verse obligadas a abrir más información de la que la norma pretende.

Bloqueo temporal o “kill switch”. La posibilidad de **bloquear** una plataforma, aunque se limita a plataformas extranjeras y existe desde 2021, es un punto crítico porque podría convertirse en una forma de **censura o presión económica** desproporcionada y al final los castigados serán los usuarios.

Análisis de datos. El último párrafo del 30-B permite que la ATDT realice “**gestión tecnológica o análisis de datos**”. Nadie ha explicado qué significa exactamente esto: ¿qué tipo de análisis?, ¿sobre qué información?, ¿con qué controles?, ¿dónde queda el **secreto fiscal**?

Un contexto que alimenta la desconfianza. El debate ocurre justo después de la aprobación de la **CURP biométrica**, que incorporará huellas,

rostro e iris en una base nacional. Aunque el gobierno ha dicho que es una herramienta de identidad y no de vigilancia, la coincidencia de ambas medidas refuerza la sensación de que el Estado acumula cada vez más acceso a los datos personales de los ciudadanos.

La zona gris. El artículo 30-B no es una ley espía, pero tampoco es inocuo. Su implementación sin límites técnicos claros en la ley -sin protocolos de acceso ni criterios de proporcionalidad- vulnera potencialmente derechos digitales. La falta de precisión en la comunicación oficial y la tendencia a negar cualquier riesgo, debilitan la confianza pública.

La exageración mediática desinforma; la distorsión gubernamental, también. Entre ambos extremos, hay un terreno que exige **transparencia, reglas técnicas y garantías efectivas de privacidad**. Porque en materia digital no basta con decir que “no se espía”, hay que acotarlo y los senadores aún están a tiempo.

Abogada, presidenta de Observatel y comentarista de Radio Educación.

X y Threads: @soyirenelevy

El debate ocurre justo después de la aprobación de la CURP biométrica, que incorporará huellas, rostro e iris.