Proyecto de Ley del Ministerio Federal del Interior

Proyecto de Ley para reforzar la ciberseguridad[1]

De ...

El Parlamento Federal alemán (Bundestag), con el consentimiento del Consejo Federal alemán (Bundesrat), ha aprobado la siguiente Ley:

[…]

Articulo 4

Modificaciones a la Ley relativa a la protección de datos y de la privacidad en el ámbito de las telecomunicaciones y los servicios digitales

La Ley de protección de datos en el ámbito de las telecomunicaciones y los servicios digitales, de 23 de junio de 2021 (Boletín Oficial Federal I, p. 1982; 2022 I, p. 1045), modificada en última instancia por el artículo 3 de la Ley de 10 de marzo de 2026 (Boletín Oficial Federal 2026 I, n.º 64), queda modificada como sigue:

1. Después del artículo 19, apartado 4, se añaden los apartados 5 y 6 siguientes:

(1) «Si un proveedor de servicios digitales tiene conocimiento de una interrupción que se derive de uno de sus servicios mientras un usuario lo está utilizando, deberá notificárselo inmediatamente al usuario, siempre que se conozca la identidad de este. En la medida en que sea técnicamente posible y económicamente razonable, el proveedor, dentro del ámbito de sus respectivas responsabilidades en relación con los servicios digitales prestados comercialmente, debe informar al usuario de los medios técnicos adecuados, eficaces y accesibles a través de los cuales pueda detectar y resolver la interrupción. Si la Oficina Federal de Seguridad de la Información (BSI, por sus siglas en alemán) ha notificado la interrupción al proveedor, este debe transmitir al usuario toda la información facilitada en la notificación de interrupción que pueda utilizarse para detectar y resolver la interrupción. El proveedor puede redirigir partes del tráfico de datos hacia y desde un servicio utilizado que esté experimentando una interrupción, en la medida en que sea necesario para notificar al usuario la interrupción.

(2) Si la Oficina Federal de Seguridad de la Información (BSI) informa a un proveedor de servicios digitales de amenazas concretas para la seguridad informática que se originen en el uso que un usuario haga de uno de sus servicios o que afecten a dicho uso, dicho proveedor deberá notificárselo inmediatamente al usuario, siempre que se conozca la identidad de este. Al hacerlo, el proveedor deberá, en particular, transmitir al usuario toda la información contenida en la notificación de la Oficina Federal de Seguridad de la Información (BSI), de conformidad con la primera frase, que permita identificar y prevenir las amenazas. Si un proveedor de servicios digitales tiene conocimiento de amenazas a la seguridad de las tecnologías de la información derivadas del uso de uno de sus servicios por parte del usuario o que afecten al mismo, podrá notificárselo al usuario. Siempre que sea técnicamente posible y económicamente razonable, el proveedor podrá informar al usuario de los medios técnicos adecuados, eficaces y accesibles con los que pueda identificar y prevenir estas amenazas.».

---

[1] El artículo 4 de la presente Ley está notificado de conformidad con la Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo, de 9 de septiembre de 2015, por la que se establece un procedimiento de información en materia de reglamentaciones técnicas y de reglas relativas a los servicios de la sociedad de la información (DO L 241 de 17.9.2015, p. 1).

[…]

Justificación

B. Parte especial

En relación con el artículo 4 (Modificaciones de la Ley relativa a la protección de datos y de la privacidad en el ámbito de las telecomunicaciones y los servicios digitales)

En relación con el punto 1

En virtud de los nuevos apartados 5 y 6, los proveedores de servicios digitales están obligados a informar a sus usuarios sobre las interrupciones (apartado 5) o las amenazas específicas (apartado 6) derivadas de alguno de sus servicios, así como a transmitir a sus usuarios la información de la Oficina Federal de Seguridad de la Información (BSI, por sus siglas en alemán) sobre amenazas específicas que afecten a los clientes de los proveedores, siempre que dicha información sea conocida y sea posible notificarla.

Las obligaciones de los apartados 5 y 6 corresponden esencialmente a las ya existentes para los proveedores de servicios de telecomunicaciones en el artículo 169, apartados 5 y 6, de la Ley de telecomunicaciones (TKG). Las obligaciones actuales de los proveedores de servicios de telecomunicaciones, establecidas en los apartados 5 y 6 del artículo 169 de la TKG, presentan lagunas a la hora de hacer frente a las amenazas correspondientes, ya que los sistemas cuyos operadores no están sujetos a la TKG se ven afectados con frecuencia. Sin embargo, la Oficina Federal de Seguridad de la Información (BSI) procesa a diario numerosos informes sobre sistemas vulnerables o comprometidos (proveedores de alojamiento web, proveedores de servicios de computación en la nube, proveedores de servicios de centros de datos, operadores de redes de distribución de contenidos, proveedores de servicios gestionados y proveedores de servicios de seguridad gestionados). Aunque estos resultados se envían actualmente a los proveedores, con mucha frecuencia estos no los transmiten a los usuarios afectados debido a la falta de obligación legal. Por lo tanto, no es posible hacer frente a la amenaza actual de manera eficaz y sistemática.

Los apartados 5 y 6 solo cubren las interrupciones o amenazas que emanan de un servicio durante el uso de dicho servicio por parte del usuario. Se refiere a los casos en los que un usuario, por ejemplo, utiliza un servicio de alojamiento para operar un sitio web o servicio de correo electrónico, y el sitio web o servicio de correo electrónico del que es responsable se ve comprometido y se utiliza indebidamente para distribuir correos electrónicos maliciosos o de phishing. Por lo tanto, se refiere a las interrupciones y amenazas que afectan a un usuario mientras utiliza un servicio. Entre los posibles ejemplos de incidentes relevantes se incluyen una cuenta de correo electrónico comprometida que se utiliza para enviar spam; un servidor comprometido que se utiliza para lanzar ataques DDoS; o un sitio web comprometido que se utiliza para distribuir malware.

El objetivo de esta obligación es prevenir los daños causados por servicios vulnerables o ya comprometidos. Este tipo de daños pueden afectar tanto al propio usuario como a otros usuarios de Internet si son objeto de ataques a través de los servicios afectados (por ejemplo, malware, phishing o ataques DDoS). Además, los proveedores de servicios digitales están obligados a notificar a aquellos usuarios cuyo uso de los servicios esté causando perturbaciones o que se encuentren en situación de riesgo —en la medida en que se tenga conocimiento de ello— y a transmitir a dichos usuarios cualquier información facilitada por la Oficina Federal de Seguridad de la Información (BSI).