Inquietud por la seguridad de los datos en el nuevo registro de viajeros

Algunos expertos ven en esa información un caramelo para los ciberdelincuentes

MÓNICA P. VILAR
REDACCIÓN / LA VOZ

Huéspedes de un hotel de Ferrol en una foto de archivo. JOSÉ PARDO

«Las empresas turísticas están asumiendo un riesgo muy importante al solicitar, transmitir y tener que guardar tantos datos de sus clientes». La afirmación es de Ramón Estalella, secretario general de la Confederación Española de Hoteles y Alojamientos Turísticos (Cehat), en referencia a la activación este pasado lunes de la obligatoriedad del nuevo registro de viajeros, que aumenta la información personal que hay que recabar de los viajeros. Además de los datos que ya eran obligatorios, como el nombre completo o el documento de identidad, ahora se solicitan otros como el correo electrónico, el teléfono o el parentesco entre el grupo de viajeros, si en él se incluye algún menor de edad. Deben registrarse también datos de pago, como el número y fecha de caducidad de la tarjeta bancaria o el IBAN de la cuenta corriente si se abona por transferencia.

«Cuando alguien paga con una tarjeta de crédito nosotros no nos quedamos con el número. De hecho, en el recibo la numeración aparece parcialmente oculta con asteriscos. Y si paga con el teléfono ni siquiera la vemos. Pero ahora vamos a tener que almacenar es información, y eso es peligrosísimo. Nos obliga a tener un nivel de seguridad para los ficheros digno de una entidad bancaria, cuando el 92 % de nuestros asociados son pymes», señala Juan Luis Barahona, presidente de la Federación Nacional de Vehículos de Alquiler (Feneval). Las empresas que alquilan coches sin conductor también están afectadas por los nuevos requerimientos de registro.

La nueva normativa, regulada por el Real Decreto 933/2021, marca, efectivamente, que las empresas no solo tendrán que recabar y comunicar los datos al Ministerio del Interior, para que estén a disposición de las fuerzas y cuerpos de seguridad del Estado. También tendrán que elaborar un registro informático y conservarlo durante tres años, con riesgo de sanción grave si no lo hacen. Interior alojará sus datos en servidores de la Secretaría de Estado de Seguridad. Pero cada establecimiento tendrá también que custodiar sus propios registros. Y ahí es donde algunos temen que se multipliquen los riesgos.

Y es que el conjunto de datos acumulados sobre una misma persona que dibuja el nuevo registro puede resultar muy apetecible para los delincuentes. «Un grupo de ciberdelincuencia busca tener información, y si saben que ciertos establecimientos acumulan un volumen de datos relevante, esto los convierte en un caramelo», señala Juan Carlos Rodríguez, CEO de DooingIT Ciberseguridad. Este experto resalta también que «hay un aumento de riesgo porque muchos establecimientos no tienen los medios suficientes para proteger esos datos: un pequeño alojamiento es posible que no tenga ciertas medidas de protección por mucho que sean recomendables ante una ciberdelincuencia creciente».

Mismo nivel de protección

Sin embargo, otro experto, el presidente del Colexio Profesional de Enxeñaría en Informática de Galicia, Fernando Suárez, señala que los establecimientos que recaban datos personales ya tenían que contar con herramientas para protegerlos. «O que se fai agora non difire tanto do que se facía, o nivel de seguridade tiña que ser o mesmo cando dabamos nome e DNI, que xa era moita información, que agora que se piden máis datos; xa tiñan que ter ferramentas de protección, ter en conta a ciberseguridade e ter persoal formado para manexar esa información. Se non tiñan a nosa información protexida, xa tiñan un problema, non aparece agora como algo novo», indica.

En ese sentido, considera que los ciudadanos deben ser muy conscientes de que son dueños de sus datos, y de que son muchas las ocasiones en las que los ceden de modo indiscriminado, por ejemplo, en la mayoría de las compras en línea: «Necesitamos máis concienciación social, saber qué datos damos e a quen, e esixir máis ás empresas, pero parece que só rachamos as vestiduras cando os datos nolos pide unha Administración pública, como se nos fosen espiar, cando é por motivos de interese público que vexo xustificados».

«Hay que ser realistas, una cosa es que se suponga que los negocios tienen que tener sistemas de seguridad y otra que los tengan o sean los adecuados, y no tiene las mismas posibilidades una gran cadena que un pequeño alojamiento», rebate Juan Carlos Rodríguez. Sin embargo, Fernando Suárez estima que cada vez son más las herramientas a disposición de las pequeñas empresas: «Hai servizos na nube, empresas especializadas no tratamento de datos, e cada vez con custes máis accesibles, non fai falta ter un departamento propio», defiende. Señala, además, que los delincuentes buscan un gran volumen de datos, lo que hace más tentadoras las grandes firmas, más protegidas.