LA TRIBUNA DEL EXPERTO

La confianza digital, activo para mejorar la competitividad y la cohesión social

ALBERTO VAQUERO GARCÍA

Ecobas-Gen-Universidade de Vigo. Codirector de Red Localis

En los últimos años, España ha alcanzado cotas históricas en el despliegue de infraestructuras digitales. Un 95 % de los hogares dispone de acceso a la red y un 89 % de la población de entre 16 y 74 años utiliza internet de forma habitual. Sin embargo, este despliegue masivo esconde una realidad compleja.

En un reciente estudio, elaborado para la Cátedra Economía de la Ciberseguridad USC-INCIBE, en el que compartimos autoría varios investigadores de las Universidades de Santiago de Compostela y Vigo, llegamos a la conclusión que la transformación digital en España se sostiene sobre un frágil equilibrio. Un gigante con los pies de barro.

Cibercrimen, opacidad e IA

El documento cataloga las principales amenazas que erosionan la certidumbre de los usuarios en el entorno virtual, dividiéndolas en incidentes técnicos y riesgos de carácter social y ético. En primer lugar, destacan los ataques cibernéticos, y muy especialmente los que se producen sobre el «Internet de la cosas» (IoT). Amenazas como el *ransomware* (retención de información a cambio de dinero tras un ataque digital), la suplantación de identidad mediante *phishing*, los ataques de denegación de servicio y las vulnerabilidades en dispositivos del IoT comprometen diariamente información confidencial y sistemas críticos y generan una carga de inseguridad y desconfianza en el uso de tecnologías digitales de gran calado. En segundo lugar, vigilancia y explotación de datos. La proliferación de brechas de seguridad, la vigilancia masiva mediante reconocimiento facial y/o algoritmos de supervisión (algo de los que nos llevan alertando desde hace muchos años), así como la venta o cesión no autorizada de datos personales generan un sentimiento generalizado de pérdida de control que desanima el empleo de las nuevas tecnologías. En tercer lugar, la desinformación y manipulación digital. La rápida difusión de contenidos falsos y/o sesgados mediante *deepfakes*, cuentas automatizadas (*bots*) y *trolls* (usuarios que publica comentarios provocadores u ofensivos) distorsiona la opinión pública y desgasta la credibilidad global de la información que se mueve en el ciberespacio. Todos conocemos el daño que está haciendo esta mala praxis.

De especial relevancia son las repercusiones en el ámbito económico. Aunque existe una confianza funcional en el comercio electrónico (del 76 %), la desconfianza reaparece ante las tecnologías emergentes. Solo un 30 % de la ciudadanía confía en sistemas de IA para la toma de decisiones que afecten a su vida personal o profesional. A tenor de las recientes noticias sobre las potenciales consecuencias del importante desarrollo de la IA —que incluso varios CEO han solicitado que se frene— no es de extrañar esta conclusión. Y seguro que más de uno recordara el argumento de alguna que otra película sobre un mundo futuro distópico controlado por las máquinas: «Sayonara, baby».

Brecha competencial y demográfica

A partir de los datos de la encuesta del INE sobre Equipamiento y Uso de Tecnologías de Información y Comunicación en los Hogares, nuestro trabajo señala que los obstáculos más frecuentes a los que tiene que enfrentarse cada día la ciudadanía se deben a la falta de competencias y soporte, y no tanto a la falta de conexión.

La edad es la variable determinante en la experiencia digital. Mientras que el 80 % de las personas de entre 65 y 74 años utiliza internet, la tasa cae al 40 % entre los mayores de 75 años. Además, casi 1 de cada 2 personas del grupo de 65 a 74 años presenta competencias digitales básicas o inferiores. Las dificultades técnicas de uso (instalación, configuración o compatibilidad) sufren un fuerte aumento con los años, provocando una penalización clara hacia las personas de edad avanzada.

Por lo que respecta a la estructura familiar, los hogares unipersonales registran una tasa de dificultad técnica del 65 % frente al 54 % observado en hogares con cinco o más miembros. Esto evidencia que la convivencia ofrece un soporte informal decisivo para resolver problemas del día a día. El conocimiento colectivo permite mejorar los niveles de confianza, frente a ser un «lobo digital». Finalmente, un 55 % de la población no utiliza ningún dispositivo o sistema domótico conectado en su hogar. Entre los motivos alegados destacan la ausencia de necesidad percibida, las dudas respecto a la privacidad y el temor a sufrir un ciberataque.

ILUSTRACIÓN MARÍA PEDREDA

Estrategias de intervención

Para las personas mayores nuestras recomendaciones pasarían por el envejecimiento activo y autonomía. Primero, alfabetización adaptada, basada en la formación presencial, en grupos reducidos y centrada en la prevención de fraudes y estafas bancarias. Segundo, conseguir entornos simplificados, esto es, impulsar interfaces accesibles, estándares claros de diseño y opciones de navegación simplificadas. Tercero, alcanzar una seguridad comprensible, por ejemplo, sustituyendo contraseñas complejas por autenticación biométrica (huella dactilar y/o reconocimiento facial). Y, finalmente, la puesta en marcha de centros físicos —y no solo digitales— de soporte y capacitación de familiares y cuidadores como mediadores.

Para la población de menos edad habría que promover el cambio desde ser usuarios instrumentales a personas críticas. Para ello es necesaria, una alfabetización integral, por ejemplo, apostando por una enseñanza activa para la verificación de datos ante las noticias falsas, así como comprensión del funcionamiento de los algoritmos y la recopilación masiva de datos personales. No todo lo que se publica es cierto y hay que saber discriminar. Segundo, es preciso contar con una ciberseguridad preventiva a través de la promoción de hábitos digitales seguros como la autenticación en dos pasos, contraseñas robustas y la evitar redes WiFi abiertas para cierto tipo de operaciones, por ejemplo, las que precisan el uso de información financiera. Y como colofón, apostar por una salud y ética digital, a través de estrategias de autorregulación del tiempo en las pantallas para prevenir la fatiga tecnológica; al mismo tiempo, es necesario apostar por campañas de concienciación contra el ciberacoso y el discurso de odio.

Para las zonas rurales es necesario apostar por la conectividad y cohesión territorial. Primero, es preciso contar con una infraestructura de alta velocidad digital y esto pasa necesariamente por garantizar fibra óptica rural y/o conexiones por satélite subvencionadas para erradicar las zonas grises de cobertura, factor clave para evitar el despoblamiento y garantizar la competitividad empresarial. La España vaciada sigue sufriendo mucho esta carencia a pesar los avances. También se hace necesaria una formación descentralizada, siendo vital acercar las capacitaciones técnicas y de ciberseguridad a través de la colaboración con ayuntamientos y diputaciones provinciales.

En resumen, la confianza digital debe entenderse como un activo estratégico. La sostenibilidad de la sociedad digital en España depende de situar la seguridad, la transparencia y la inclusión como pilares estructurales e insustituibles, tanto desde la perspectiva pública como privada. Desplegar tecnología sin capacitar a la ciudadanía ni garantizar una protección efectiva solo profundiza la brecha social y deteriora la legitimidad institucional. El «sentidiño» al que siempre acudimos los gallegos, es fundamental en este campo. En resumen, la confianza digital debe entenderse como un activo estratégico. La sostenibilidad de la sociedad digital en España depende de situar la seguridad, la transparencia y la inclusión como pilares estructurales e insustituibles, tanto desde la perspectiva pública como privada. Desplegar tecnología sin capacitar a la ciudadanía ni garantizar una protección efectiva solo profundiza la brecha social y deteriora la legitimidad institucional. El «sentidiño» al que siempre acudimos los gallegos, es un elemento fundamental en este campo.