LA LIBERTAD Correo

ESPECIAL

facebook correoperú
twitter @diariocorreo

UN FUTURO SIN BILLETES, PERO CON BILLETERAS

Opinión

MIRKO A. MALDONADO-MELÉNDEZ
Instituto Peruano de Buen Gobierno y Buena Administración

Cada vez más peruanos realizan transacciones mediante plataformas digitales. Es literalmente "moneda de cambio" su utilización cotidiana en comercios, tiendas por departamento, servicios de taxis, tiendas virtuales, entre muchos otros. La pandemia de la Covid 19 aceleró este proceso de digitalización y, según una reciente data proporcionada por Indecopi el 2023, las cifras alcanzan un poco más 154 empresas del sector fintech y más de 16 billeteras digitales, mediante diversos y singulares aplicativos para enviar dinero rápido en tiempo real: YAPE, PLIN, BIM, Agora PAY, Izipay YA, Waky, Kontigo, entre otras, cuya masificación en el país nos ha introducido de lleno en la realidad virtual del dinero digital y del monedero electrónico, cuya facilidad de acceso y uso puede considerarse como una nueva forma de democratización o inclusión de los ciudadanos, pero también constituye una forma de desmaterializar (desplazar) el uso del plástico (la tarjeta de débito o crédito según sea el caso). Sin embargo, ¿cuál es riesgo que corremos? y ¿cuál el precio que estamos dispuestos a pagar por este innovador servicio?. En un país cuyo ordenamiento jurídico ha sido diseñado para proteger derechos fundamentales (contenidos en los artículos 1, 2 y 3 de la Constitución Política) y las garantías que ofrece el pacto social (véase lo dispuesto en el artículo 44, 1er. párrafo parte infine de la misma), lamentablemente, a pesar de parecer estar escritos en piedra, lo cierto es que el sistema resulta insuficiente para otorgar garantías de protección y tutela de estos por parte de los poderes públicos.

Uno de los principales riesgos a la seguridad personal y patrimonial lo constituye la amenaza de vulneración de los datos, al igual que la suplantación de identidad, que tienen como objetivo final el acceso a los fondos o dinero de los usuarios de estos aplicativos. Por eso, resultaría de gran ingenuidad no hacerse las siguientes interrogantes: ¿Qué tan seguras son las billeteras electrónicas o aplicativos digitales de los bancos, cajas de ahorro o financieras?, ¿En qué medida el sistema legal nos protege de estos riesgos o amenazas? La respuesta salta a la vista si pensamos en la casi nula responsabilidad que asumen los bancos cuando somos víctimas de fraudes cibernéticos y cómo parece que la única manera de estar algo protegidos implica que tengamos que comprarle al mismo banco, seguros de protección de tarjetas y cuentas de ahorro.

Como si no bastase pagar impuestos que financien los servicios públicos y entre ellos la protección y seguridad por parte del Estado frente a la delincuencia y, en este caso, los delitos informáticos, muchos ciudadanos deben pagar su propia seguridad personal, sea que la ofrezca la policía en sus días de franco o, en el peor de los casos, determinados terceros cuya actividad no es tan santa que digamos. Mientras la ciberdelincuencia crea metodos cada vez más sofisticados para cometer sus crímenes, creando perfiles falsos y aplicaciones clonadas, las víctimas suelen ser los más vulnerables, entre ellas los adultos mayores y otros grupos etarios, cuyo escaso conocimiento del uso de la tecnología los expone enormemente a esta clase de delitos.

Ante esta situación, nos preguntamos: ¿resulta suficiente la legislación nacional para actuar de manera garantista para minimizar los riesgos mencionados?, ¿Están las instituciones del Estado peruano listas para afrontar una avalancha de denuncias en las comisarías, Indecopi y la Fiscalía Especializada en Ciberdelincuencia? Me temo que no.

Con la vigencia de la Ley N° 30096, de delitos informáticos, el Estado contempla y prevé una serie de conductas delictivas que van desde el "acceso ilícito", el "atentado contra la integridad de datos informáticos" y de los "sistemas informáticos", el "tráfico ilegal de datos", la "interceptación de datos informáticos", el "fraude informático", la "suplantación de identidad". Aunque estos delitos tipificados en la ley podrían multiplicarse de modo acelerado y no encuadrar nuevas conductas ilegales, y aunque esta norma no es suficiente del todo, constituye una herramienta (de momento útil) para que los operadores jurídicos puedan investigar la comisión de delitos y esclarecer los hechos, por parte de las fiscalias especializadas en delitos informaticos y de ciberdelincuencia, con fiscales y jueces capacitados, con investigaciones que sean rápidas, céleres y eficientes que acusen y condenen a los responsables, para desincentivar la comisión de este tipo de conductas infractoras, para lo cual será necesario contar con mecanismos de colaboración de todos los agentes intervinientes, como la Superintendencia de Banca y Seguros, los propios bancos y financieras e incluso el BCR, así como las potenciales víctimas que sean conscientes de los posibles riesgos derivados de la utilización de esta tecnología.

Un punto aparte merece la normativa de protección al consumidor y la propia legislación de la SBS respecto a los procedimientos administrativos en defensa de los usuarios afectados, pues en la actualidad muchos casos parecen proteger a los bancos o empresas que manejan la billetera electrónica. Es cierto que parte de la seguridad proviene del uso adecuado y cuidadoso de las aplicaciones por parte del usuario y pasa también por mantener a la vista el teléfono móvil, no compartir la contraseña ni compartir el token digital. Sin embargo, siendo que toda tecnología está sujeta siempre a riesgos de vulneración, hackeo, suplantación, entre otros, se requiere fortalecer el sistema legal a fin de que los ciudadanos no tengan que pagar con su propio patrimonio los riesgos de una digitalización que se ha implantado (ipso facto) de manera acelerada para minimizar los costos de operación de las empresas pero que, en caso de fraudes o robos, pareciera que casi siempre es asumido por las personas de a pie.

INNOVACIÓN. Billeteras digitales implementadas son de rápido acceso.

UNO DE LOS PRINCIPALES RIESGOS A LA SEGURIDAD PERSONAL Y PATRIMONIAL LO CONSTITUYE LA AMENAZA DE VULNERACIÓN DE LOS DATOS, AL IGUAL QUE LA SUPLANTACIÓN DE IDENTIDAD.