# Yo le di la llave al ladrón

**Desde el 2021 se incrementan los reportes de estafas virtuales en Sancti Spíritus a través de las plataformas de pago digital. *Escambray* intenta desandar las complejas rutas del dinero robado**

Mary Luz Borrego

—“Hoy es mi día”, pensó ingenuamente Luisa González*, sentada bien cómoda sobre su cama aquella calurosa tarde del 25 de julio del 2021.

Por casualidad, mientras revisaba las redes sociales, acababa de encontrar una oferta tentadora: alguien vendía Moneda Libremente Convertible (MLC) por transferencia a 61 pesos, cuando en ese momento su cotización en el mercado negro andaba por 65.

“Ese era el gancho para que uno cayera”, recuerda ahora esta mujer que en ese entonces intentaba comprar divisa con el propósito de adquirir un boleto para Haití. En un pestañazo ella mordió el anzuelo y se convirtió en víctima de una estafa virtual, que le costó perder 80 MLC y 36 300 pesos: “Cuando vi mis tarjetas en cero lloré, me subió la presión, casi me da un infarto”.

Solo les envió cándidamente una foto del carné de identidad y de sus tarjetas, además de las últimas 10 operaciones que había realizado, pero jamás dio su clave a nadie y ni siquiera abrió una cuenta por EnZona. No la necesitaron, en fracciones de segundo los ciberdelincuentes se la crearon y se apoderaron de todo su dinero.

### POR LA RUTA DEL DINERO

Esta lamentable experiencia se ha repetido, con sus matices, durante los últimos tiempos en buena parte del país. En Sancti Spíritus ese delito comenzó a crecer desde el pasado año, cuando se incrementaron los reportes de defraudaciones a usuarios a través de las plataformas de pago digital EnZona y Transfermóvil.

“Esas estafas siempre suceden cuando las personas les dan a ajenos datos de sus tarjetas magnéticas, generalmente para adquirir divisas por las redes y también para otras compras virtuales. Al inicio, EnZona tenía una debilidad: se podían operar varias tarjetas, aunque no fueran propias. Ya eso se rectificó y aun así sigue el problema”, asegura Yudeisy Martínez, jefa del Departamento de Banca Electrónica en el Banco de Crédito y Comercio (Bandec).

**¿Qué datos personales se necesitan para hacer una transferencia?**

“Únicamente se necesita el número de la tarjeta. No hay que dar el nombre exacto de la persona, ni la fecha de vencimiento. Todos esos datos los están propiciando, incluso están enviando fotos de la tarjeta matriz y hasta su pin”.

**Cuando ocurren este tipo de estafas, ¿a dónde deben concurrir las personas afectadas?**

“Al banco a cancelar su tarjeta para que no les sigan haciendo extracciones, ni la usen para estafar a otros. Además, hacer la denuncia en la Policía porque no podemos brindar información de terceros, ni decirles a dónde fue a parar su transferencia”.

La modernidad no solo ha sofisticado los medios de comunicación y pago, sino también a los estafadores, personajes inteligentes, hábiles y bien escurridizos, con avanzados conocimientos informáticos, que utilizan ardides para lograr sus propósitos.

“Ningún banco de este país pide tantos datos para hacer una transferencia. Estos ciberdelincuentes empiezan a solicitar información, por ejemplo, le dicen a la víctima: ‘Ya te envié el dinero y el tuyo no me ha llegado, revisa’. Incluso llegan a enviar capturas de pantalla y hasta correos falsos. También borran el nombre a las tarjetas, las falsifican. Y las personas les empiezan a dar poco a poco toda su información”, detalla Mavy González, jefa del Departamento de Asesoría Jurídica en Bandec.

**¿Existen formas de pescar a estos embaucadores?, ¿una estafa virtual es demostrable?**

“Sí claro, el dinero va a una tarjeta final y a esa es a la que hay que llegar. A Instrucción Policial le corresponde citar a los implicados, nosotros le informamos de todo el movimiento del dinero, sus recorridos, por la trazabilidad que queda. Pero también empiezan a pasar dinero de una tarjeta a otra y lo mueven no en la misma cuantía que lo robaron, sino fragmentado para diferentes tarjetas de distintos bancos. Esa es la parte que Instrucción tiene que despejar”.

**¿El sistema bancario no brinda seguridad a sus clientes del dinero que tienen en las tarjetas?**

“Sí; pero, ¿cómo nosotros sabemos realmente si ese cliente que se dice estafado realizó la operación o no?, porque lo que aparece en su estado de cuentas es una transferencia a otro número y él pudo haberla realizado. El titular no debe dar su información personal a un tercero. Puso el dinero en el banco, pero quien hizo uso de ese efectivo o quien permitió que se hiciera uso de ese efectivo fue él y ante esos casos solo un Tribunal puede determinar. La afectación le va a persistir, se trata de una compraventa de divisa, que es una actividad ilícita, y eso no se resarce ni en la vía judicial”.

Aunque actualmente el país —por las difíciles circunstancias económicas que atraviesa— no ha dispuesto un lugar oficial donde los cubanos puedan adquirir MLC, ni en los Tribunales todavía se ha juzgado un caso de este tipo, la Fiscalía confirmó a *Escambray* que cuando la estafa es de naturaleza ilícita no genera responsabilidad civil, es decir, que no se le restituirá el dinero a la víctima.

### LA OTRA GRAN ESTAFA

Mucho ha llovido desde que las pantallas de cine estrenaron con gran éxito la película norteamericana *La gran estafa*, donde un plan perfecto permitía robar varios casinos de Las Vegas en una sola noche. Ahora no se trata de un *remake* de ese filme, pero estos timadores bien podrían motivar el argumento de una cinta moderna.

“Están usando tarjetas ya estafadas para lavar el dinero ajeno proveniente de nuevos desfalcos y así hacer más larga la cadena, que se pierda la ruta de ese dinero y sea difícil encontrarlo. Están utilizando tarjetas puente y así se va enmascarando el real estafador, muchas veces cuesta bastante trabajo encontrarlo”, comenta Alicia Ramos, oficial de cumplimiento en Bandec.

Los expertos recomiendan algunos mecanismos de seguridad para impedir el acceso de terceros: no llevar en la cartera todos los documentos juntos, chequear sistemáticamente las cuentas personales, utilizar el doble factor de autenticación, diseñar contraseñas de pago fuertes y atender las alertas vía correo electrónico sobre intentos de acceder a su dinero.

Las ciberestafas no solo afectan a los clientes, sino también la credibilidad del sistema bancario al generar inseguridad en los usuarios, quienes piensan que los avances de la informática siempre puedan generar formas más avanzadas para estas simulaciones.

En el Código Penal vigente se reconoce el delito de estafa, al cual se le fija una sanción de privación de libertad de tres meses a un año, pena que puede incrementarse hasta una década si se suman determinadas agravantes.

Algunos consideran que los timadores actúan en red, pero, especulaciones aparte, estos hechos continúan aquí, donde se han reportado defraudaciones incluso superiores a los 100 000 pesos, a pesar de que, probablemente, muchos timados no realicen la denuncia por temor a que se les convierta en un bumerán: de acusadores se conviertan en acusados por tráfico ilegal de divisas.

No pocos se cuestionan por qué en otros países el propio banco investiga estos casos, devuelve el dinero y en Cuba, no: “Cuando se abre la cuenta con el cliente se le dice bien claro que es responsable de las operaciones que haga con su tarjeta y si luego da sus datos personales eso no es responsabilidad del banco. Nosotros ayudamos brindando el estado de cuentas, pero para investigar está la Policía”, se defiende Yailén Pentón, jefa del Departamento Jurídico en el Banco Popular de Ahorro, donde también toca puertas este delito.

Y justamente hasta la Estación de Policía del municipio de Sancti Spíritus llegó *Escambray*. Aquí se registra el mayor número de casos de esta naturaleza —casi todos relacionados con la compra de MLC, pero también algunos con la adquisición de criptomonedas—, y hasta ahora ninguno se ha esclarecido de forma total.

**¿Por qué resulta tan difícil llegar a la punta de la madeja en este tipo de delito?**, inquiere el periódico al primer teniente Yasiel Faldraga, jefe del área de Investigación.

“Las redes sociales son de libre acceso a nivel internacional, se crean perfiles falsos y ofrecen información no útil. Estos delincuentes también usan tarjetas de otras víctimas y hasta sus fotos para interactuar y engañar a otros usuarios. Hemos recibido más de 50 denuncias de este tipo.

“Estos casos son bastante trabajosos, tenemos que estar en constante despacho con el banco, siguiendo las trazas de las tarjetas utilizadas. Los estafadores tienen conocimientos bancarios, de las redes sociales. Pasan el dinero por diferentes tarjetas y luego pueden sacarlo en un cajero automático de otro territorio”.

**Por su experiencia, ¿considera posible esclarecer algunos de estos casos?**

“Sí es posible. Cada caso es único, tienen cosas similares, pero también diferentes. Vamos de un escalón a otro siguiendo la travesía de ese dinero. A algunos posibles autores o receptadores del dinero sustraído ya los tenemos circulados en otras provincias, fundamentalmente orientales, desde Ciego de Ávila hasta Holguín, pero aún no hemos podido darles captura.

**¿Existe la probabilidad de que algunos de los estafados puedan ser juzgados por tráfico ilegal de divisas?**

“Habría que ver cada caso de forma independiente. Tratamos de proteger a quien viene a acusar porque nadie se va a incriminar a sí mismo. Por una única vez que alguien compre divisa ilegalmente no se le va a juzgar, pero si se prueba que se dedica a eso ya sería diferente. Hasta ahora todos los estamos trabajando por estafa”.

Han transcurrido casi ocho meses desde que Luisa González cayó en la trampa como mansa paloma: “Me vi obligada a utilizar esta vía porque legalmente no existe un lugar donde pueda comprar MLC. Tenía que pagar el pasaje con esa moneda, además de que hace falta para comprar comida, aseo. El que no tenga quien le ponga euros tiene que comprar en la calle, pero la identidad de uno no se le puede dar a nadie. Yo le di la llave al ladrón”.

***Para proteger la identidad de la entrevistada se utilizó un nombre falso, pero su historia es completamente real.**