“Gota a gota virtual”: la intimidación detrás de los préstamos por internet

Fuente: El Espectador

La necesidad de dinero llevó a un ciudadano a tramitar un crédito y terminó siendo víctima de estafa, acoso cibernético y extorsión. Su situación se repite por todo el país. El caso está en manos de la Fiscalía por estafa, pero la persecución legal de este delito es difícil.

Actualmente, la Superintendencia de Industria y Comercio (SIC) tiene en la mira alrededor de 50 aplicaciones de préstamos por internet. Sin embargo, solo en dos de los casos se ha avanzado a una formulación de cargos. / Ilustración de Éder Leandro Rodríguez

Se imagina que a sus contactos les empiece a llegar su foto con la leyenda “se busca estafador, páguele a Credibús”; que les escriban a familiares, amigos o hasta al jefe diciendo que usted tiene una deuda, o que todos los días lo llamen, acosen y amedrenten por una deuda que ha pagado tres veces. Esa es la pesadilla que viven los ciudadanos que, en medio de una

urgencia, cayeron en las trampas de las aplicaciones (“apps”) de préstamos por internet, que prometen créditos sin papeleos. Lo grave: a pesar de las denuncias, es un fenómeno difícil de controlar.

Este problema, así como los delitos informáticos, se dispararon en pandemia. Los creadores de estas “apps” aprovecharon la situación económica de los hogares y las escasas habilidades digitales para montar un “negocio”, que hoy angustia a cientos de colombianos. Operan de forma simple: en redes sociales ofrecen préstamos sin papeleos, rápido desembolso, a bajas tasas y amplios plazos. Luego, cuando la víctima descarga la aplicación, aprovechan que la mayoría no lee los términos y condiciones, para camuflar una autorización que le da total acceso al dispositivo: fotos, agenda, ubicación... todo queda a disposición del dueño de la “app”. Información más valiosa que un pagaré.

Pesadilla

Esto le pasó a un bogotano que, en septiembre, cuando revisaba redes sociales, vio el aviso “préstamos rápidos, sin documentación”. Apareció en un momento de necesidad. “Le di clic, descargué la ‘app’ Credibús y cometí mi primer error: no leí los términos ni revisé los permisos que pedían para acceder a mi celular. Llené la solicitud, di mi número en Nequi para el desembolso y envié la foto de mi cédula. Ese fue mi segundo error”. Tras cumplir el trámite, le informaron el monto aprobado, el cual supuestamente pagaría en 90 días y con 3 % de interés.

Pero el clic, aceptando el crédito, lo sumió en una pesadilla. Segundos después llegó la primera sorpresa: le cambiaron las condiciones y tenía que pagar el doble del monto, en siete días. Sin opciones, reunió el dinero, pagó y eliminó la “app”. Lo asumió como una experiencia... un error que pagó con plata. Pero la historia no terminó. En enero le notificaron dos depósitos a su cuenta. “Como trabajo con proveedores y esperaba pagos, no verifiqué de inmediato. Lo tuve que hacer cuando llegó un mensaje diciendo que tenía dos días para pagar. Las ‘apps’ Credibús y Supercrédito consignaron sin autorización. Un fraude. Fui a la Policía a denunciar y me dijeron que pagara, que seguro la cosa terminaba ahí”.

La última semana de enero le cobraron por WhatsApp, de manera agresiva, como lo suelen hacer. Como había sido un préstamo no autorizado, él les dijo que les devolvería el dinero sin intereses, pero la respuesta fue una extorsión: tenía que pagar o enviarían fotos personales a sus contactos. Ya no se era un cobro hostil, sino un delito. "¡Tenían acceso a todo! Quedé congelado. Era mi privacidad, así que pagué". En febrero, otra sorpresa: dos nuevos depósitos desde Ezytransfer, por un monto mayor.

"Entré en pánico, pero era seguir en su estafa o mi privacidad. Me dieron hasta el 7 de febrero, a las 11:00 a.m. para cancelar, pero no pagué. Fui a de nuevo la Policía y me recomendaron cambiar mi número de teléfono y denunciar por la página web". Cuando salió de allí, tenía decenas de mensajes de cobro; uno con la lista de contactos frecuentes; habían llamado a 10 conocidos y distribuido su foto con la leyenda "ladrón y estafador". "Todo lo anexé en la denuncia. Doy a conocer mi caso, para que reflexionemos antes de acceder a cualquier 'app'".

Sin control

Esta historia se repite a lo largo y ancho del país. Una mujer en Nariño, por ejemplo, para aplacar el acoso de las "apps" Loco Cash, Vida Luja y Credibús, accedió a pagar $200.000 semanales por extensiones de plazo, hasta que no pudo más. Al final distribuyeron su foto, diciendo que pagaba sus deudas con favores sexuales. O en Manizales, el mensaje que envían a los contactos de la víctima es que, si no pagan, serían cómplices de fraude. Sus métodos de intimidación son como los de los peligrosos "gota a gota", pero virtuales.

Según el Gaula de la Policía, los ciberdelincuentes se caracterizan por aprovechar el desconocimiento de las víctimas o vulnerabilidades de sus sistemas informáticos, para acceder a la mayor información personal posible y tomar control de sus dispositivos. "La confianza, el escepticismo o el desconocimiento de cómo operan generan brechas de seguridad, que aprovechan para apropiarse de datos personales, bancarios y contraseñas, que luego usan para suplantar su identidad o extorsionar. Las consecuencias pueden ir desde el daño reputacional hasta la afectación del patrimonio".

Por estas situaciones, la alerta de los préstamos por internet está encendida, pero parece poco lo que se puede hacer. Por un lado, los préstamos entre particulares no están prohibidos. Así las cosas, las "apps" de préstamos digitales no son ilegales. Lo otro es que, a pesar de simular la actividad de un banco, no es una actividad que vigile la Superintendencia Superfinanciera, pues se supone que los recursos son de origen particular. Por lo tanto, esta transacción se cataloga como una actividad comercial, que le compete vigilar a la Superintendencia de Industria y Comercio (SIC).

Lo que sí viola la ley son las maniobras de cambiar condiciones, la estafa de desembolsar sin autorización para cobrar intereses, el uso irregular de los datos personales de los usuarios y los métodos agresivos a la hora de cobrar. Vale resaltar que las amenazas contra la honra y el buen nombre de las personas para cobrar una deuda son ilegales desde 1992. Ese año **la Corte Constitucional (T-412 de 1992)** prohibió los "chepitos", cobradores con un maletín, con el aviso de "deudor moroso", que perseguían al cliente, para someterlos al escarnio público y obligarlos a pagar. Lo de hoy podría ser similar, pero en la era digital y con un agravante: la amenaza es a vulnerar un derecho como la intimidad.

Desde entonces, la Corte resaltó que toda persona tiene derecho al respeto de su honra y su dignidad; que nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra y reputación, y que toda persona tiene derecho a la protección de la ley contra esos ataques. Aseguró que las empresas que incurran en estas conductas serían objeto de sanciones penales "como fraude a resolución judicial, prevaricato por omisión o en las sanciones penales a que hubiere lugar".

A pesar de ser clara la irregularidad y los delitos que comenten las "apps" de préstamos por internet, las investigaciones no van al ritmo de la tecnología y cada retraso es tiempo que ganan estos negocios para someter a más ciudadanos. Los resultados de la SIC, que es la primera llamada a ejercer control a través de su Dirección de Investigaciones de Protección de Datos Personales, demuestran la asincronía. A pesar de la cantidad de denuncias y de que hay 50 "apps" en la mira de la entidad, apenas dos

están en etapa de pliego de cargos: Nanocred Colombia S.A.S. (“app” Profin) y Construir Comundo (“app” Eastbay, Popcash, Móvil Crédito y Vida Luja). No obstante, sus procesos están en esa etapa desde mediados del año pasado.

Los otros procesos poco avanzan. Por ejemplo, pese a tener identificadas otras empresas como Ezytransfer (“app” Ricopréstamo), Saghlin S.A.S. (“app” Plata) y Rush Global Colombia S.A.S. (“app” Holacredy), están estancados, porque ninguna ha respondido a los requerimientos del ente de control. En el caso de Credibús y Doy Préstamo, pese a haber dado con un supuesto responsable, este negó haber desarrollado esas “apps”. Solo las investigaciones contra las “apps” Pez Crédito, Rápido Crédito, Loco Préstamo, Trueno y Finbee las remitieron a la Fiscalía.

A partir de ahí hay una larga lista de empresas y aplicaciones con denuncias que siguen bajo análisis, como Grolatech S.A.S. (“app” Librecash, Platahoy Ultracredit), Confiar Ees S.A.S. (“app” Acticrédito), El Dorado Network S.A.S. (“app” Parcecredit y Credifio), Microbank Colombia S.A.S. (“app” Suplata); Loco Cash, Flexiplata, Cop Más, Supercrédito, Plata Colombia, Patcecash, Firecrédito, Ya Dinero, Credissimo, Quickmoneypro, Efectivo Flower, Doblo, Fastrupee, Rapifinanciera, Nuevo Crédito, Línea Directa, Dinero Fabrica, Lana Hoy, Red Suelva, Préstamos Tackles y Atiemcrédito.

La explicación de la SIC de por qué es tan difícil poner en cintura estos negocios es que hay dificultades en la individualización del sujeto responsable del tratamiento de la información de cada “app”. “La Dirección de Investigaciones de Protección de datos Personales ha formulado pliego de cargos a dos responsables del tratamiento de datos. Seguimos con el uso de nuestras facultades legales para investigar y sancionar a los responsables. Desde la Superintendencia se seguirá insistiendo en la prevención, para que los ciudadanos identifiquen las aplicaciones y no las usen”, dice la entidad.

¿Y lo penal?

Con los relatos de las víctimas, es claro que, más allá de ser una mala práctica comercial que deba controlar la SIC, lo que se evidencia en el

relato de las víctimas es que las prácticas de esas aplicaciones transgreden el Código Penal y, a pesar de que varios casos han llegado a Fiscalía, no se conocen condenas. Una posible explicación: a la dificultad para identificar responsables, como lo señala la SIC, se suma que no tardan las autoridades en seguirle la pista a una "app", para que salgan al aire otras 10. Esto se refleja en los pocos resultados contra los crecientes delitos cibernéticos.

Entre 2019 y 2020, los delitos informáticos aumentaron 123 %, pasando de 22.023 a 49.359, según la DIJIN. En 2022 fueron 66.481, la mitad de las cuales fueron en Bogotá y Cundinamarca. Los principales delitos fueron hurto por medios informáticos (40 %), acceso abusivo a sistema informático (20 %), violación de datos personales (20 %) y suplantación de sitios web para capturar datos personales (9 %). De todo ese universo de denuncias, en 2019 alcanzaron a llevar 530 casos ante los jueces, pero solo hubo nueve condenas, y el año pasado, si bien triplicaron las imputaciones (1.502 casos), solo una terminó en sentencia.

El clamor de las víctimas de estas aplicaciones es tal, que el caso ya está en **la Corte Constitucional, que deberá pronunciarse** de nuevo ante los nuevos y peligrosos "chepitos" virtuales. En la Corte Constitucional, desde septiembre del año pasado, fue seleccionado para revisión un fallo de tutela, contra la empresa Construir Comundos S.A.S., dueña de las aplicaciones Eastbay, Popcash, Móvil Crédito y Vida Luja, la misma que está con pliego de cargos ante la SIC. La decisión de primera instancia la emitió el Juzgado 14 Civil Municipal de Cundinamarca y está en el despacho del magistrado Antonio José Lizarazo Ocampo, desde noviembre del año pasado.

¿Hay soluciones?

Los métodos de los que intimidan y estafan a través de internet son cada vez más sofisticados, mientras la alfabetización digital de la ciudadanía sigue siendo escasa. Al hacer una revisión en la tienda de Google (Playstore), se encuentra que al menos nueve de las 20 aplicaciones gratuitas de finanzas más descargadas son de préstamos por internet, a pesar de las denuncias y tener pésimas calificaciones.

Pero esta situación tendría una explicación. En Colombia hay una "ciudadanía digital inocente, en la que la falta de conocimiento y comprensión del dominio digital la conduce a excesos de confianza, esfuerzos preventivos débiles y una casi nula capacidad de anticipación, reacción y disminución de los daños causados por criminales y agentes amenazantes, de diferente magnitud, naturaleza y alcance", indicó César Restrepo, en su **columna Inseguridad cibernética.**

Un primer paso, según el columnista, es mejorar la competencia de los usuarios y promover una gestión de la ciberseguridad, dirigida a la prevención basada en los riesgos. "La lección del último año en ciberseguridad es que estamos frente a un riesgo enorme, con alto potencialidad de impacto en la vida de todos. Un escenario que enfrentamos en medio de una mezcla fatal de ignorancia y esfuerzos insuficientes", dice.

No obstante, hay un reto adicional por superar: la indiferencia de las autoridades ante los crímenes que ocurren en internet. Así lo advierte Catalina Moreno Arocha, coordinadora de inclusión social de la Fundación Karisma, quien resalta cómo están creciendo esas denuncias por violación a la privacidad y al buen nombre, lo que amerita ser atendidas de manera oportuna. Aclara, eso sí, que no se trata de que las autoridades salgan a bloquear aplicaciones sin control. "La SIC, por ejemplo, tiene una facultad de bloquear contenido en internet, cuando se habla de datos personales y deberían actuar de forma decidida y tomar decisiones motivadas, pero, insisto, en el marco del debido proceso".

Y se debe actuar de manera oportuna, porque, dice, la gente lo está pidiendo. "El problema es que las entidades encargadas de vigilar parecen indiferentes. Lo paradójico es que la Fiscalía y la Policía tienen herramientas y conocimiento para actuar de forma más oportuna. En este tema de aplicaciones de préstamos por internet sabemos que hay un proceso en la Corte Constitucional y hemos pedido conocer el expediente, para presentar argumentos como expertos y apoyar, pero el alto tribunal nos ha cerrado la puerta, dejando a la sociedad civil por fuera de un caso importante".

“Este tema de datos personales es muy grave, porque involucra muchos derechos fundamentales: la honra, el buen nombre, la intimidad... Si ven que hay muchos quejándose hay que actuar con celeridad, pero en el marco del debido proceso. Desafortunadamente todo esto pasa por un tema de falta de alfabetización digital, que aprovechan los cibercriminales. Está bien que hablemos de brecha digital y transformación digital e intentar conectar a la ciudadanía, pero también es necesario que enseñen a advertir los riegos de usar tecnología y a qué se expone la ciudadanía”, concluyó Moreno Arocha.

Por lo pronto, es importante que los ciudadanos conozcan la ruta en caso de ser víctimas. Lo primero es reportar la aplicación ante Google, por incumplimiento de los términos del servicio, ya que las plataformas que manejan datos sensibles deben usarlos lo menos posible; lo otro es denunciar en la Fiscalía por estafa, constreñimiento, amenaza y extorsión; promover las acciones de protección del consumidor y los datos personales ante la SIC y, finalmente, acudir a la tutela para defender el derecho a la honra.

El riesgo es claro y en un mundo cada vez más virtual, aumenta cada día más. Por eso, a la par de exigirles a las autoridades cumplir con su papel, hay cosas que un ciudadano puede hacer: mejorar las prácticas de seguridad cuando usan el celular, leer cada vez que vayan a dar un clic para aceptar y desconfiar, siempre desconfiar, para no terminar siendo una víctima más de los delincuentes que rondan su entorno digital.