

ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE COSTA RICA

PROYECTO DE LEY

“LEY PARA COMBATIR LAS ESTAFAS INFORMÁTICAS BANCARIAS”

LESLYE BOJORGES LEÓN

DIPUTADO

RECIBIDO EN LA SECRETARÍA DEL DIRECTORIO  
DE LA ASAMBLEA LEGISLATIVA

EXPEDIENTE N.º 23970

El: 02/10/2023.

A las: 04:05 pm Horas:

Recibido por: *[Signature]*

**PROYECTO DE LEY**  
**“LEY PARA COMBATIR LAS ESTAFAS INFORMÁTICAS BANCARIAS”**

Expediente N.º **023970**

**ASAMBLEA LEGISLATIVA.**

La realidad de las formas de delinquir, contra los sistemas financieros, se han ampliado, siendo que la estafa informática es una de las preocupaciones que ha afectado más a la banca costarricense y a sus clientes. El auge de la tecnología y la expansión de Internet han traído consigo numerosos beneficios, pero también han dado lugar a un aumento significativo en las estafas de esta índole, afectando no solo a individuos, sino a empresas y gobiernos en todo el mundo, complicando el panorama para los usuarios que requieren cada vez más de políticas públicas que busquen mitigar y reducir la tasa en la actividad delictiva de esta naturaleza.

Las estafas informáticas se han convertido en un problema global en la era digital, ya que la consumación de estos actos implican la lesión a diversos bienes jurídicos ya tutelados, donde podemos ver cómo se vulnera el patrimonio privado de las personas, así mismo la vulneración a sus datos personales o privados, por citar algunos ejemplos; y es que dentro de las estafas más comunes podemos encontrar prácticas conocidas como “*el Phishing*”, la cual es una forma de ciberataque en la que los atacantes intentan engañar a las personas para que revelen información confidencial, como contraseñas correos electrónicos, mensajes de texto o convencerlos de acceder a sitios web falsos para robar información personal, financiera o credenciales de inicio de sesión a las diferentes oficinas virtuales de los bancos comerciales nacionales, a razón de poder transferir dinero a otras cuentas y sacar el mismo de la pertenencia del usuario desde el cual accedieron.

Encontrar responsables en este tipo de actuaciones no suele ser tan fácil, siendo que los criminales digitales innovan en sus métodos y se vuelven casi indetectables, por lo que es importante identificar y encuadrar en un tipo penal a las acciones de los “cuenta destinos”, los cuales son definidos como aquella cuenta de ahorro, corriente o IBAN

pertencientes a la persona en donde son transferidos los fondos provenientes de una estafa informática (*“phishing”*) desde una determinada “cuenta origen”, cabe destacar que el alcance de la “cuenta destino” comprende únicamente la primera cuenta en la que se reciben los fondos procedentes de la cuenta origen.

Sobre la misma línea, el patrimonio personal y la propiedad privada son principios fundamentales y bienes jurídicos tutelados en nuestra sociedad, de manera que resulta menester legislar contra actuaciones que pretendan permitir que alguien lesione dichos bienes jurídicos, siendo que al igual que *el phishing*, *“el carding”* es otra de las prácticas más comunes ejecutadas por los criminales para apropiarse de los recursos económicos de otros usuarios, siendo una actividad de corte ilegal que implica **el uso no autorizado de tarjetas de crédito o débito para realizar compras fraudulentas** en línea. Los individuos que participan en el carding, son conocidos como “carders”, y utilizan la información que roban de las tarjetas de crédito o débito, como los números de tarjeta, fechas de vencimiento y códigos de seguridad (CVV), para realizar compras en línea sin el consentimiento del titular de la tarjeta.

El carding a menudo implica prácticas conducentes a la adquisición ilegítima de la información de las tarjetas de terceros, como el robo de datos, la compra de datos robados o el uso de “técnicas de ingeniería social” para engañar a las personas. y obtener su información financiera. Una vez que los carders tienen esta información, la utilizan para hacer compras en línea, descargar contenido digital o realizar otras transacciones fraudulentas.

El carding es una actividad delictiva que puede generar cargos por fraude y/o estafa, robo de identidad de los propietarios de las tarjetas y violaciones a los datos de las personas mediante técnicas de vulneración a la ciberseguridad de las bases de datos de los bancos o la respectiva institución financiera. Siendo que estos últimos deben de tomar medidas para detectar y prevenir el carding, siendo la constante monitorización de transacciones sospechosas y la implementación de medidas de seguridad adicionales, como la verificación en dos pasos, las principales herramientas que deben implementar los sistemas financieros; no obstante, en la mayoría de casos la inversión

en estos recursos no suele ser suficiente y ante la creciente profesionalización de los delincuentes a la hora de ejecutar sus estrategias de carding o de phishing, necesitamos contar con instrumentos jurídicos que permita castigar a quien realizan este tipo de actos.

Partiendo de la eventual violación al patrimonio privado y/o a los datos personales del titular legítimo del dinero y en la búsqueda del mantenimiento de la confianza en los sistemas financieros del país, es importa desalentar el crimen de esta naturaleza, mediante la sanción penal a las compras ilegales y las técnicas de ingeniería social que busca el "phishing" evitando la creación de incentivos para el crimen, ya que actualmente lo pueden visualizar como una actividad lucrativa y de bajo riesgo sancionatorio

En resumen, esta iniciativa de ley busca castigar a quien realice compras ilegales con tarjetas de crédito o débito que no son de su propiedad y, al mismo tiempo, condenar a quien utilice cuentas bancarias a su nombre para recibir, transferir o retirar los fondos provenientes de las acciones relacionadas a una estafa informática; todo esto con la intención de establecer un mecanismo jurídico penal esencial para mantener la integridad del sistema financiero, proteger a los titulares legítimos de las tarjetas y prevenir el delito financiero, además, es una forma de proteger la privacidad y la seguridad de las personas.

Por todo lo anteriormente expuesto, sometemos a consideración de esta honorable Asamblea Legislativa el presente proyecto de ley.

**LA ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE COSTA RICA****DECRETA****“LEY PARA COMBATIR LAS ESTAFAS INFORMÁTICAS BANCARIAS”**

**Artículo 1.-** Se adicionan los artículos 217 ter y 217 quater al Código Penal, N.º 4573, del 04 de mayo de 1970 y sus reformas, para que se lean de la siguiente manera:

**“Artículo 217 ter.-** Recepción de fondos a razón de Estafa Informática.

Quien facilite sus cuentas bancarias para recibir, transferir o retirar los fondos provenientes de las acciones relacionadas a una estafa informática.

Será sancionado de la siguiente forma:

1. Con prisión de uno a tres años, si el monto de lo defraudado no supera los cuatro salarios base.
2. Con prisión de tres a cinco años, si el monto de lo defraudado no supera los ocho salarios base.
3. Con prisión de cinco a ocho años, si el monto de lo defraudado supera los diez salarios base.

Las penas precedentes se elevarán en un tercio cuando los hechos señalados, los realice un empleado o encargado de administrar o dar soporte al sistema o red informática o telemática bancaria, o bien, que en razón de sus funciones tenga acceso a dicho sistema o red bancaria.”

**“Artículo 217 quater.-** Compras ilícitas mediante tarjetas.

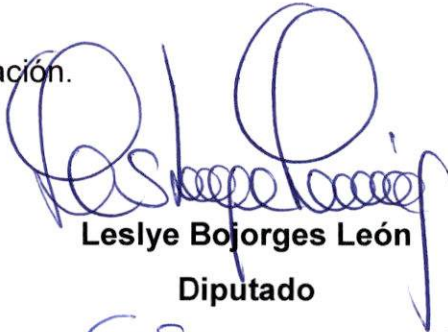
Quien adquiera bienes o servicios, a través del uso de una tarjeta de crédito o de débito no expedida en su favor, o mediante el uso de otro medio de pago electrónico, sin la autorización del titular.

Serán sancionados de la siguiente forma:

1. Con prisión de uno a tres años, si el monto de lo defraudado no supera los cuatro salarios base.

- 2. Con prisión de tres a cinco años, si el monto de lo defraudado no supera los ocho salarios base.
- 3. Con prisión de cinco a ocho años, si el monto de lo defraudado supera los diez salarios base.”

Rige a partir de su publicación.



**Leslye Bojorges León**  
**Diputado**

Alejandro Roldán Castro  
Carlos Felipe García

