## Fraude informático en Panamá

En la República de Panamá, el delito de **estafa cometido por medios informáticos** está consagrado en el Libro Segundo, sobre "Los Delitos", Título VI sobre Delitos contra el Patrimonio Económico, Capítulo III sobre la "Estafa y otros Fraudes", de la siguiente manera:

> *Artículo 220. Quien mediante engaño se procure o procure a un tercero un provecho ilícito en perjuicio de otro será sancionado con prisión de uno a cuatro años.*
> *La sanción se aumentará hasta un tercio cuando se cometa abusando de las relaciones personales o profesionales, o cuando se realice a través de un medio cibernético o informático.* (Código Penal, 2007, art. 289)

El artículo 220 del Código Penal de Panamá consagra la modalidad simple del delito de estafa. Pero también estipula algunas de las formas agravadas de este hecho delictivo. Una de las formas es cuando la estafa se realiza mediante medios informáticos, como lo son los ordenadores.

Por su parte, los delitos contra los medios informáticos están consagrados en el Capítulo I sobre Delitos contra la Seguridad Informática, Título VIII sobre **Delitos contra la Seguridad Jurídica de los Medios Electrónicos**. Específicamente en los artículos 289, 290, 291 y 292 del Código Penal de Panamá. El primer artículo en estudio señala lo siguiente:

> *"Quien indebidamente **ingrese** o **utilice** una **base de datos**, **red o sistema informático** será sancionado con dos a cuatro años de prisión."* (Código Penal, 2007, art. 289)

Primero se debe hacer un análisis exegético de la norma. La Real Academia de la Lengua Española defina **ingresar**, según su cuarta acepción, como *"Entrar en un lugar"* (Diccionario de la lengua española [DLE], 2018). Por lo que el verbo rector señala que el simple hecho de entrar a una base de datos, o entrar a una red informática, o entrar a un sistema informático, de manera indebida, constituye un hecho delictivo.

El verbo **utilizar** es definido como *"1. tr. Hacer que algo sirva para un fin. 2. tr. Aprovecharse de algo o de alguien."* (DEL, 2018). Por lo que utilizar significa sacar provecho de la base de datos o del sistema informático. Esto con el objetivo de lograr a algún fin específico. De esta manera, el propio verbo utilizar descarta la idea de una acepción culposa. No se puede sacar provecho o lograr un fin sin que primero se haya ideado. Por ejemplo, la persona que por error está frente a una base de datos puede idear en ese momento algún fin con la información que tiene frente a ella. Claro está, solo los delitos que lo dispongan taxativamente pueden acarrear una responsabilidad por culpa.

Este es un tipo penal *"básico, principal, de formulación casuística, monofensivo, anormal."* (Guerra, Villalaz & González, 2017, p. 228). Este delito consiste en el mero ingreso o uso de una base de datos de una red informática o de un sistema informático. Por ejemplo: A ingresa indebidamente a la computadora de B para ver la banca en línea de B y así saber la situación económica de B. El mismo solo puede realizarse mediante una acción dolosa, por lo que no es posible el ingreso indebido de una base de datos culposo. Por ejemplo, el profesor A le dice al estudiante B que copie de su memoria un artículo científico, pero B, de manera imprudente, abre el archivo con las calificaciones del resto de los estudiantes. En este supuesto, B realiza la acción de ingresar a una base de datos indebidamente, pero, lo hace sin intención, por lo que no sería posible castigar dicha conducta.

Definir el sujeto activo genera controversia en la dogmática penal panameña. Por un lado, se sostiene que *"el manejo de base de datos, red o sistema informático, requieren conocimientos y habilidades en el uso de los equipos informáticos, lo que nos permite señalar que* […] *por su calidad es propio o calificado"* (Guerra, Villalaz & González, 2017, p. 228). Sin embargo, otros autores sostienen que el *"sujeto activo o agente, puede estar conformado por cualquier persona"* (Sáenz, 2017, p. 342). Frente a este tema, la postura correcta, debe ser entender que el sujeto activo puede ser cualquier persona capaz de dominar conscientemente la realización de la conducta descrita en la norma en discusión. Es decir, no cabe la realización imprudente o culposa, pero tampoco es necesario que el ingreso o utilización sea realizado por un especialista en informática, sino que cualquier persona con

conocimientos básicos sobre informática puede hacerlo. Por ejemplo, un economista que trabaje para una empresa puede ver abierta la computadora de su jefe, e ingresar para ver los movimientos financieros de la empresa, con la finalidad de asesorar a empresas rivales.

Por su parte el objeto material *"es alternativ*[o]*"* (Guerra, Villalaz & González, 2017, p. 228). Por lo que puede cometerse contra *"una base de datos, una red informática o en un sistema informático."* (Guerra, Villalaz & González, 2017, p. 228). Sin desconocer lo anterior, también se puede utilizar un concepto amplio de dato y de sistema informático. Por lo que el objeto material puede dividirse en dos: los datos y los sistemas informáticos. El dato es la información almacenada, mientras que el sistema informático es el equipo que almacena el dato, lo que implica el componente físico (*hardware*) y el programa (*software*).

El diccionario del español jurídico define '**base de datos**' como *"memoria informática en la que pueden integrarse datos dispuestos de modo que sean accesibles individualmente por medios electrónicos o de otra forma. Base de datos bibliográfica, base de datos contable, base de datos enciclopédica."* (Real Academia Española & Consejo General del Poder Judicial, 2019).

Por su parte, define '**sistema informático**' como *"dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa".* (Real Academia Española & Consejo General del Poder Judicial, 2019).

Finalmente, define 'red informática' como *"conjunto de ordenadores y otros dispositivos, conectados por medios físicos o sin cables, con el objeto de compartir recursos, ya sean de hardware o de software."* (Real Academia Española & Consejo General del Poder Judicial, 2019).

Mientras que 'dato informático' es *"any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function"* (toda representación de hechos, información o conceptos en una forma adecuada para procesar en un sistema informático, incluido un programa adecuado para hacer que un sistema informático realice una función) (Consejo de Europa, 2001, Art. 1.b.)

Cabe destacar que este tipo penal, interpretado de manera amplia, puede dar lugar a puniciones absurdas. Por ejemplo, un trabajador de seguridad nocturna utiliza la computadora de una oficina para conectarse a internet y revisar su Facebook. En este caso, el trabajador estaría utilizando indebidamente una red informática. Sin embargo, debe analizarse con base en el principio de materialidad, es decir, que se trate de una lesión considerable del bien jurídico. Además, también se debe advertir que dicha lesión debe ser intencionada.

Por su parte, el bien jurídico tutelado es la seguridad jurídica de los medios electrónicos e informáticos, como se desprende del encabezado del título y capítulo respectivo. De lo anterior se deduce que lo que se protege es el dato almacenado en un sistema informático o red informática, y el propio sistema informático o la red informática.

Este delito consiste en *"ingresar o utilizar estos "instrumentos", documentos" o información de carácter electrónico, sin la autorización de los titulares, "usuarios" o "concesionarios" autorizados o legitimados para tener acceso a ellos."* (Gill, 2017, p. 450).

Por otro lado, el siguiente artículo relacionado a delitos contra la seguridad informática señala lo siguiente:

> *"Artículo 290. Quien indebidamente se* ***apodere****,* ***copie****,* ***utilice*** *o* ***modifique*** *los datos en tránsito o contenidos en una base de datos o sistema informático, o* ***interfiera****,* ***intercepte****,* ***obstaculice*** *o* ***impida*** *su transmisión será sancionado con dos a cuatro años de prisión."* (Lo resaltado y subrayado no es original).

Los verbos rectores son apoderarse, copiar, utilizar, modificar los datos. Estos pueden estar en tránsito dentro de una red informática o pueden estar almacenados en una base de datos. Otros verbos rectores contenidos en este artículo son, interferir, interceptar, obstaculizar e impedir la transmisión de dichos datos.

En cuanto al sujeto pasivo, es el *"Estado como titular de la seguridad informática y también las instituciones bancarias y financieras, personas naturales, también titulares de los derechos a la intimidad, al patrimonio, al honor."* (Guerra, Villalaz & González, 2017, p. 230). La definición anterior de sujeto pasivo prioriza al Estado como titular del bien jurídico, sin embargo, esta diferenciación no la hace la norma.

El objeto material puede ser *"datos en tránsito, bases de datos, sistemas informáticos, transmisión de información."* (Guerra, Villalaz & González, 2017, p. 230).

Por otro lado, el artículo 291 del Código Penal no contempla nuevas conductas delictivas, sino que establece las agravantes de las conductas previas, de la siguiente manera:

> *"Artículo 291. Las conductas descritas en los artículos 289 y 290 se* ***agravarán*** *de* ***un tercio a una sexta parte*** *de la pena si se cometen contra datos contenidos en bases de datos o sistema informático de:*
> *l.* ***Oficinas públicas*** *o bajo su tutela.*
> *2. Instituciones públicas, privadas o mixtas que prestan un* ***servicio público****.*
> *3. Bancos, aseguradoras y demás* ***instituciones financieras y bursátiles****.*
> *También se agravará la pena en la forma prevista en este artículo cuando los hechos sean cometidos* ***con fines lucrativos****.*
> *Estas sanciones se aplicarán sin perjuicio de las sanciones aplicables si los datos de que trata el presente Capítulo consisten en* ***información confidencial*** *de acceso restringido, referente a la* ***seguridad del Estado****, según lo dispuesto en el Capítulo I, Título XIV, del Libro Segundo de este Código.*

Este artículo establece una *"circunstancia agravante material, de lugar, específica, concomitante"* (Guerra, Villalaz & González, 2017, p. 231). Primero, se agrava la pena si el delito contra la seguridad jurídica de los medios electrónicos se comete en sistemas informáticos ubicados en oficinas públicas; o dedicados a la prestación de servicios públicos; o en instituciones financieras. Además, si las conductas se realizan para obtener algún beneficio económico, también será agravado. Cabe destacar que *"el fin de lucro es solamente un elemento accidental de los tipos penales descritos en esta sección."* (Gill, 2017, p. 452).

Por último, se establece una agravante cuando se trate de información confidencial sobre la seguridad del Estado, relativos al Título XIV sobre los delitos contra la Personalidad Jurídica del Estado, en el cual se estipulan delitos contra la Personalidad Internacional del Estado[1] y delitos contra la Personalidad Interna del

[1] Quien ejecute un acto para someter la República, en todo o en parte, a un Estado extranjero, aminorar su independencia o quebrantar su unidad e integridad será sancionado…

Estado[2]. Esta punición más severa se debe a que *"se trata de información confidencial, de acceso restringido referente a la seguridad del Estados"* (Gill, 2017, p. 450). Se debe aclarar que *"es sin perjuicio de las agravantes contenidas en el artículo 290"* (Gill, 2017, p. 452).

Para algunos autores el bien jurídico protegido *"es la seguridad informática que comprende la protección a la privacidad, a la fe pública, a la economía, a la propiedad intelectual, a las comunicaciones, los medios de transporte y la seguridad pública"* (Guerra, Villalaz & González, 2017, p. 230).

Finalmente, el artículo 292 establece otras modalidades de agravantes:

> *"Artículo 292. Si las conductas descritas en el presente Capítulo las comete la* ***persona encargada o responsable*** *de la base o del sistema informático, o la* ***persona autorizada para acceder*** *a este, o las cometió* ***utilizando información privilegiada****, la sanción se* ***agravará*** *entre* ***una sexta y una tercera parte****."*

Este artículo consagra una agravante de carácter *"personal, específica y antecedente"* (Guerra, Villalaz & González, 2017, p. 231). En este caso, la calidad de la persona sí determina si se la aplica o no algunas de las agravantes (persona encargada o responsable; persona autorizada para acceder). Sin embargo, cualquier persona puede cometer el delito utilizando información privilegiada. Es decir, no se requiere que tenga características especiales. Por ejemplo, a un economista le facilitan la contraseña de una computadora, y accede a la información de un ordenador. El economismo no es responsable ni está autorizada para acceder, pero logra hacerlo porque tiene información privilegiada.

## Referencias


Asamblea Nacional de Panamá. *Código Penal de Panamá*. G. O. 26519 de 2010.

Consejo de Europa. (2001). *Convention on Cybercrime*. Recovered on 13/08/2019 in: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561


[2] Quien promueva, dirija o participe en un alzamiento en armas para derrocar al gobierno nacional legalmente constituido o para cambiar violentamente la Constitución Política será sancionado...

Gill, H. (2017) *Comentarios al Código Penal de 2007*. Panamá, Panamá: Asesorías en ediciones gráficas.

Guerra, A., Villalaz, G. & González, A., (2017) *Compendio de Derecho Penal. Parte especial. 3ª edición*. Panamá: Cultural Portobelo.

Real Academia Española (2018). *Diccionario de la lengua española (22ª ed.)*. Edición del tricentenario.

Real Academia Española & Consejo General del Poder Judicial. *Diccionario del español jurídico*. Tomado el 5/8/2019 a las 5:45pm en: https://dej.rae.es/lema/base-de-datos

Sáenz, J. (2017). *Compendio de Derecho Penal Parte Especial.* Panamá: Jurídica Pujol S.A.

Sieber, U. (2009). *Los caminos de la armonización penal*. España: Editorial Tirant Lo Blanch.