INFOTEC CENTRO DE INVESTIGACIÓN E INNOVACIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

DIRECCIÓN ADJUNTA DE INNOVACIÓN Y CONOCIMIENTO
GERENCIA DE CAPITAL HUMANO
POSGRADOS

“PROTOCOLO DE ACTUACIÓN MINISTERIAL. INVESTIGACIÓN DEL DELITO DE DEFRAUDACIÓN FISCAL MEDIANTE EL EMPLEO DE CRIPTOMONEDAS”

PROPUESTA DE INTERVENCIÓN
Que para obtener el grado de MAESTRO EN DERECHO DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

Presenta:
Alfonso Moreno García

Asesor:
Mtro. Rafael Álvarez Chávez

Ciudad de México, mayo de 2020

Autorización de Impresión

INFOTEC
POSGRADOS

AUTORIZACIÓN DE IMPRESIÓN Y NO ADEUDO EN BIBLIOTECA

MAESTRÍA EN DERECHO DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

Ciudad de México, 9 de febrero de 2021.
INFOTEC-DAIC-GCH-SE-057/2021.

La Gerencia de Capital Humano / Gerencia de Investigación hacen constar que el trabajo de titulación intitulado

PROTOCOLO DE ACTUACIÓN MINISTERIAL. INVESTIGACIÓN DEL DELITO DE DEFRAUDACIÓN FISCAL MEDIANTE EL EMPLEO DE CRIPTOMONEDAS

Desarrollado por el alumno **Alfonso Moreno García** y bajo la asesoría del **Mtro. Rafael Álvarez Chávez**; cumple con el formato de biblioteca. Por lo cual, se expide la presente autorización para impresión del proyecto terminal al que se ha hecho mención.

Asimismo se hace constar que no debe material de la biblioteca de INFOTEC.

Vo. Bo.

Ing. Luis José Manuel Montaño Sánchez
Gerente de Capital Humano

Anexar a la presente autorización al inicio de la versión impresa del trabajo referido que ampara la misma.

C.p.p Servicios Escolares

Agradecimientos

a Cristina T. Ñeco
Gracias por tu acompañamiento
en mis metas académicas.

Tabla de contenido

Índice de cuadros

Introducción

Actualmente en el mundo existe un auge en el uso de las criptomonedas, basadas en la tecnología *blockchain*, que han permitido la compra y venta de las mismas y, por tanto, su especulación, así como instrumento de pago para la comercialización de bienes y servicios.

El Servicio de Administración Tributaria y la Procuraduría Fiscal se han mostrado preocupados con el empleo de las criptomonedas en dichas operaciones mercantiles, en virtud de que debido a su falta de fiscalización, pueden cometerse delitos fiscales, concretamente, el de defraudación fiscal.

El tema de las criptomonedas y su uso para la comisión de delitos como la defraudación fiscal es de la mayor relevancia y requiere de investigaciones realizadas bajo los estándares constitucionales y legales por parte del Ministerio Público.

El empleo de las tecnologías en las transacciones jurídicas y económicas es un tema de suma importancia. Cuando aparece una nueva, como lo es el *blockchain* y se utiliza como instrumento financiero o como un mecanismo de pago (similar a la moneda), por lo que requiere de una correcta comprensión, ya que debido a su difícil fiscalización, es fácil evadir impuestos y provocar el fraude fiscal.

La característica de las monedas virtuales es que no están respaldadas por gobierno ni banco central alguno; inclusive, no tienen poder liberatorio para el cumplimiento de obligaciones, como en cambio, sí lo tiene el peso de nuestro país y divisas extranjeras, en términos de los artículos 1º, 2º, 7º y 8º de la Ley Monetaria de los Estados Unidos Mexicanos, razón por la cual, desde un punto de vista estrictamente legal, ni siquiera puede llamársele “moneda”.

El pasado de 9 de marzo de 2018, se publicó en el Diario Oficial de la Federación la Ley para Regular las Instituciones de Tecnología Financiera, también conocida como Ley Fintech. Los aspectos relevantes de la citada Ley en cuanto a las criptomonedas, se encuentra sustentado en los artículos 30 a 34 y 88, donde se regulan diversas situaciones que ya suceden en nuestro país, a saber: la comercialización de productos y/o servicios mediante el pago en criptomonedas o

activos virtuales, la compraventa de activos virtuales mediante monedero electrónico (*Exchange)*, los riesgos que implica ello, el reconocimiento de que las mismas no son equivalentes a la moneda de curso legal o divisas extranjeras y, por ende, no están respaldadas por el gobierno federal y; la facultad del Banco de México para determinar las criptomonedas que deben ser utilizadas por las Instituciones de Tecnología Financiera.

En cuanto a la comisión de delitos informáticos se refiere, las criptomonedas merecen especial atención, pues ellas pueden ser el medio comisivo de conductas ilícitas como fraude, defraudación fiscal, operaciones con recursos de procedencia ilícita; Inclusive, las nuevas conductas delictivas establecidas en la nueva Ley para Regular las Instituciones de Tecnología Financiera, relacionadas con las criptomonedas.

Lizbeth Xóchitl Padilla Sanabria, menciona sobre los riesgos de la criptomoneda, relacionado con el lavado de dinero y la defraudación fiscal, pues menciona que

> "cualquier tipo de capital, cuya procedencia sea lícita o ilícita se convierta, a través de solicitudes anónimas hacia operadores expertos en tecnologías de sistemas que encripten la información económica y personal de sus clientes, en criptomonedas (sean *bitcoins*, *etherum*, *litecoin* o *ripple*), sin pasar por el sistema financiero mexicano (y por tanto por la dinámica de regulación financiera y fiscal), especulando para obtener ganancias sin que se haya tenido que pagar impuestos; además, trasladar dicho capital, convertido en moneda virtual, de un país a otro en cuestión de segundos a través de la red del internet, y su valor se podría convertir de nueva cuenta en cualquier tipo de divisa e incluso transformarse en bienes y servicios".[1]

[1] Padilla Sanabria, Lizbeth Xóchitl, *"Lavado de dinero y corrupción desde la perspectiva virtual"*, *El Heraldo de Puebla* del 10 de febrero de 2018, (*www.elheraldodepuebla.mx/archivos/28530).* Consultado el 06 de febrero de 2019.

En efecto, si el capital invertido en criptomonedas no ha sido fiscalizado y se desconoce su origen, estamos hablando eminentemente de una defraudación fiscal, y probablemente del delito de operaciones con recursos de procedencia ilícita.

El artículo 108 del Código Fiscal de la Federación establece el delito de defraudación fiscal genérico al establecer que lo comete quien con uso de engaños o aprovechamiento de errores, omita total o parcialmente el pago de alguna contribución u obtenga un beneficio indebido con perjuicio del fisco federal. El sujeto activo del delito es el contribuyente y el pasivo la Secretaría de Hacienda y Crédito Público, el bien jurídico tutelado el daño o posible daño a la hacienda pública.

En el engaño tiene que realizarse una conducta necesariamente, son actos por comisión, y en el aprovechamiento del error son actos por omisión. La esencia del trabajo consiste en la preocupación compartida con las autoridades fiscales en el sentido que mediante el empleo de las criptomonedas puede verificase esta conducta delictiva y las autoridades fiscales se encuentren en la posibilidad de tipificarla, en el ejercicio de sus facultades de comprobación fiscal.

En el caso, del delito de defraudación fiscal, surge la interrogante acerca de cuáles actos de investigación que debe seguir el Ministerio Público para la obtención de los datos de prueba necesarios para judicializar la carpeta de investigación.

Conforme al artículo 21 constitucional, es atribución del Ministerio Público la investigación de conductas posiblemente delictivas establecidas en las leyes penales, para lo cual debe llevar a cabo los actos de investigación con plena observancia de los requisitos constitucionales y legales que deriven en la obtención de datos de prueba que, en su caso, serán puestas del conocimiento del Juez de Control al judicializar la carpeta de investigación correspondiente.

El trabajo que se propone estará delimitado en cuanto a la legislación mexicana actualmente vigente (ámbitos espacial y temporal de validez) y sólo en cuanto a los actos de investigación que debe desarrollar el Ministerio Público para la obtención de datos de prueba cuando el delito de defraudación fiscal previsto en el Código Fiscal vigente sea realizado mediante el empleo de criptomonedas (ámbito material de validez).

Por tanto, el objetivo general del presente trabajo será determinar cuáles son los actos de investigación que deberá emplear el Ministerio Público, con auxilio de la policía especializada y los peritos, para la obtención de datos de prueba para establecer el delito de defraudación fiscal cometido mediante el empleo de criptomoneda.

Los objetivos específicos serán: 1) en cuanto a la tecnología en que se sustenta la criptomoneda, a) proporcionar una aproximación a la tecnología *blockchain* y, b) analizar la regulación legal en México relacionada con la criptomoneda conforme a la Ley para Regular las Instituciones de Tecnología Financiera; 2) en cuanto al delito de defraudación fiscal, a) analizar sus aspectos penales y, b) la criptomoneda como medio comisivo: 3) en cuanto a los actos de investigación relacionadas con la criptomoneda, a) determinar los actos que requieren control judicial, como con las solicitudes de información financiera y bancaria ante las instituciones financieras e instituciones de tecnología financieras y, b) determinar los actos de investigación que no requieren control judicial, como lo son la determinación del valor de la criptomoneda, la utilización de la tecnología *blockchain* y la determinación del daño o perjuicio a la hacienda pública.

En el presente trabajo se utilizan los métodos analítico y deductivo, a través del análisis documental de diversas fuentes de información.

En el primer capítulo, se realizará una explicación de la tecnología *blockchain* sobre la cual descansa la criptomoneda y las otras utilidades de dicha tecnología, haciendo una especial alusión a la criptografía y las razones de la posible confianza que deriva de ésta, para entonces finalizar con el análisis conceptual de la criptomoneda.

En el segundo capítulo, se estudiará el marco legal de la Criptomoneda en México, señalando sus aspectos financieros, fiscales y penales y la especial alusión que del tema realiza la Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita.

En ambos capítulos, la tecnología blockchain sobre la que descansa la criptomoneda y su regulación, es el punto de partida para los actos de investigación

que debe emplear el Ministerio Público a través de los peritos para determinar el uso de esta tecnología en el delito de defraudación fiscal.

En el tercer capítulo, se hará un análisis de los delitos informáticos relacionados con la criptomoneda, estableciendo el concepto de ésta, su clasificación y su relación con el Convenio de Budapest; se enunciarán los delitos informáticos existentes en la legislación federal y en algunas de las entidades federativas; se señalará cuáles son los bienes jurídicos tutelados por los delitos informáticos, y cuáles son los delitos informáticos que transgreden los bienes jurídicos tutelados, para así finalizar con el análisis de la criptomoneda como medio comisivo en los delitos informáticos, aspecto importante en el análisis de los actos de investigación en el delito de defraudación fiscal cuando es empleada ésta.

En el cuarto quinto, se hará un estudio de los actos de investigación relacionados con la criptomoneda, para lo cual se hará mención del proceso penal acusatorio, su principios y las etapas que la componen, poniendo énfasis en los actos de investigación en una carpeta de investigación; muy importante será la explicación de la problemática del derecho fundamental privacidad de la información financiera, pues de ello derivará en conocer cuáles son los actos de investigación que requieren de control judicial previo y en qué casos no es necesaria tal medida.

En el capítulo quinto, se hará el análisis dogmático del delito de defraudación fiscal y la criptomoneda como su medio comisivo, y así concluir con aspectos importantes en la Investigación de este delito mediante el empleo de criptomonedas, pues son los elementos de este tipo penal los que deberán establecerse mediante el empleo de los actos de investigación empleados por el Ministerio Público.

Finalmente, a manera de apéndice se adjuntará una propuesta de Protocolo de Actuación del Ministerio Público para la investigación del delito de defraudación fiscal cometido por medio del uso de criptomonedas.

Capítulo 1

Aspectos tecnológicos de la Criptomoneda

Capítulo 1. Aspectos tecnológicos de la Criptomoneda

1.1 Una aproximación a la Tecnología *Blockchain*

La tecnología Blockchain es una cadena de bloques que registra eventos electrónicos verificables, distribuida entre varios usuarios que no puede ser alterada ni suprimida y guarda la confidencialidad sobre el tipo de eventos y las personas que participaron.

> La principal característica de la tecnología es que permite crear y mantener un libro de contabilidad o registro de transacciones único, rápido, seguro, trazable y transparente, que es llevado de forma descentralizada o distribuida en los ordenadores (nodos) de todos aquellos que formen parte de la plataforma, con la que está en permanente interacción, y que no depende de ningún tercero de confianza para su existencia y mantenimiento, sino de los propios participantes. El registro, no puede ser borrado ni alterado, y sólo será legítimo y dado por válido si así lo decide la mayoría, dificultando enormemente los riesgos de falsificación de transacciones y de usurpación de identidad. Ese registro se va creando mediante la concatenación cronológica y sucesiva de bloques que forman una cadena. Cada bloque se cierra con una especie de firma criptográfica llamada *hash*, y ese mismo *hash* abre el siguiente bloque, a modo de sello lacrado. De esta forma, se certifica que la información, encriptada, no se ha manipulado ni se puede manipular.[2]

Esto es, la cadena de bloques registra todos los acontecimientos que se llevan a cabo en la red y las empaqueta en bloques. Un bloque contiene un conjunto de acontecimientos verificados y, en su caso, información adicional que se ha incluido en la cadena en forma criptográfica. Cada bloque está formado por dos códigos alfanuméricos, uno que enlaza con el bloque anterior, y otro que enlazará con el siguiente bloque (*hash*).

---

[2] García Mexia, Pablo, *Criptoderecho. La Regulación de Blockchain,* España, La Ley, 2018, p. 46.

La función hash permite conocer la integridad de la información y datos contenidos en un archivo electrónico, porque reduce el mensaje original a una secuencia de *bits*.

> Dichos algoritmos utilizan una serie de operaciones matemáticas sobre el mensaje original para calcular un valor de tamaño físico (128, 160, 256, 284 o 512 bits), utilizando una función de dispersión unidireccional (no se puede reconstruir el mensaje a partir de su compendio o huella digital) que cumple con una serie de propiedades criptográficas como son: 1) cualquier alteración del mensaje o datos originales influye en el resultado del compendio o huella digital; 2) no es posible la reconstrucción del mensaje a partir del compendio y 3) la posibilidad de encontrar dos mensajes con una misma huella digital es prácticamente nula.[3]

La función hash permite conocer si un archivo electrónico ha sido modificado o alterado, pues aun cambiando una sola letra del mensaje original, el archivo tendrá una huella digital diferente.

Un aspecto fundamental es que los acontecimientos deben ser verificados, lo que se lleva a cabo gracias a la red *peer to peer* (P2P). *Blockchain* es un sistema compartido y distribuido en la que todos los nodos son iguales entre sí, lo que impide pérdida o alteración de información, pues aunque un nodo falle, habría conexión a otros nodos por vías alternas; ello no sería posible en un sistema descentralizado y, menos aún, en un sistema concentrado.

Los nodos son ordenadores o procesadores que conectados a la red mencionada utilizan un software que almacena comparte y distribuye una copia actualizada en tiempo real de la cadena de bloques, de manera que cada vez que

[3] Lira Arteaga, Óscar Manuel, *Cibercriminalidad. Fundamentos de Investigación en México,* 3a. ed., México, Ubijus, 2018, p. 408.

un bloque se confirma, se añade a la cadena y se comunica a los demás nodos para que cada uno de ellos almacene una copia del bloque.[4]

La verificación de la información se lleva a cabo por medio de la minería que consiste en destinar potencia de procesamiento de un ordenador para realizar cálculos que verifiquen las transacciones. Para realizar esta actividad, los dueños del ordenador reciben un incentivo, una compensación económica en criptomoneda que pueden cambiar por divisas como euros o dólares.

Lo anterior imposibilita que un bloque sea utilizado dos veces para dos o más acontecimientos o transacciones; que en el caso de ser utilizados como criptomonedas, significa la imposibilidad de hacerse un doble pago.

En virtud de que la información de la transacción –no del usuario ni del contenido- es pública, por medio de un explorador como blockchain.info se puede conocer su estado (*https://blockchain.info/*).

Las principales características de la tecnología son:

> Publicidad. Generalmente las transacciones que se registran en la cadena de bloques se generan con una firma digital y quedan a la vista de todos.
>
> Inmutabilidad. Las transacciones son, además, válidas e inmutables y no se pueden eliminar, lo que hace de *Blockchain* una herramienta óptima para la trazabilidad y la prevención del fraude.
>
> Descentralización. Las *Blockchain* suelen estar mantenidas por muchos nodos y mineros alrededor del mundo y ninguno tiene el poder para controlarla y aprobar o desaprobar transacciones por sí solo. Este funcionamiento descentralizado y consensuado hace innecesario la existencia de una autoridad central.

[4] Bit2me Academy, "*¿Cómo funciona el Blockchain-Cadena de Bloques?"*, *https://academy.bit2me.com/como-funciona-blockchain-cadena-de-bloques/*. Consultado el 06 de mayo de 2020.

Distribución. Cada nodo de la red *Blockchain* posee una copia completa y actualizada a tiempo real de toda la cadena de bloques.

Consenso. Las operaciones se validan por consenso generalizado de la red mediante la aplicación de algoritmos previamente pactados. Dicho consenso determina qué transacciones son válidas y cuál es el estado actual de la cadena.

Carácter abierto. Con la descarga del software, cualquiera puede enviar transacciones y acceder a la información registrada en la cadena.

Seguridad. La combinación de incentivos económicos para los mineros y la verificación criptográfica le confiere un alto grado de seguridad.[5]

1.2 Criptograma

La Real Academia Española define al criptograma como un "mensaje escrito en clave"[6], no obstante, para un mejor entendimiento del criptograma para efectos del presente trabajo resulta necesario a su vez definir el concepto de criptografía para entender el sistema *blockchain*.

Se ha definido a la criptografía como el arte de escribir con clave secreta, sin embargo, para efectos tecnológicos y matemáticos se puede definir la criptografía como la rama de la informática y las matemáticas que estudia los algoritmos utilizados para ocultar la información de quien no debe verla.[7]

La tecnología *blockchain* utiliza sistemas de criptografía asimétrica donde se "utiliza un mecanismo de claves que permite el intercambio de información sin que

[5] García Mexia, Pablo, *op cit.,* p. 47.
[6] Real Academia Española, "Criptograma", *http://buscon.rae.es/draeI/*. Consultado el 06 de febrero de 2019
[7] García Mata, Iñigo, *"Criptografía básica para entender la tecnología blockchain"*, *Medium.com*, *https://medium.com/@igmata/criptograf%C3%ADa-b%C3%A1sica-para-entender-la-tecnolog%C3%ADa-blockchain-eb94cdd64158*. Consultado el 06 de febrero de 2019

se requiera compartir la clave de forma previa. Este sistema utiliza dos elementos, uno privado y uno público. El privado lo guardamos en un lugar seguro, y el público se muestra a todo el mundo para que puedan interactuar con nosotros".[8]

Para mejor entendimiento de *blockchain,* el criptograma es el fragmento de mensaje cifrado en dos claves (clave privada y clave pública), en donde las dos claves pertenecen a la misma persona que recibirá el mensaje, así cuando se quiere enviar información a alguien, se requiere primero su clave pública, se genera el mensaje cifrado y se envía a la persona, quien podrá recuperarlo utilizando su clave privada.

En términos del artículo 2º, fracción XIII de la Ley de Firma Electrónica Avanzada, ésta es el conjunto de datos y caracteres que permite la identificación del firmante, que ha sido creada por medios electrónicos bajo su exclusivo control, de manera que está vinculada únicamente al mismo y a los datos a los que se refiere, lo que permite que sea detectable cualquier modificación ulterior de éstos, la cual produce los mismos efectos jurídicos que la firma autógrafa.

La firma electrónica utiliza la criptografía asimétrica para que el receptor de un mensaje identifique al emisor y puede corroborar que no fue modificado o alterado por quien lo originó.

De esta manera, para que Juan le envié un mensaje a Tomás, que solamente este último pueda leer, primero Juan tendrá que conocer cuál es la parte pública del par de claves generado por Tomás. Una vez conocida esa clave pública, Juan podrá calcular el mensaje cifrado que enviará por la red utilizando la clave pública que Tomás le ha hecho saber. Al recibir el mensaje, Tomás aplicará la operación de descifrado correspondiente con la parte privada de su clave a la que se tendrá que asegurar que solamente él tiene acceso.

1.3 Confianza

En las transacciones comerciales la confianza es un aspecto básico, pues todo consumidor necesita de esto para poder poner su dinero en un agente del que

[8] *Idem.*

espera la enajenación de un bien o la prestación de un servicio y, en contrapartida, el proveedor también necesita la confianza de que recibirá el dinero por dicha circunstancia.

Blockchain es una tecnología en la que los usuarios han depositado su confianza, pues una vez familiarizados con la misma, se han dado cuenta de que el registro, no puede ser borrado ni alterado, y solo puede ser validado por la mayoría, dificultando enormemente los riesgos de falsificación de transacciones y de usurpación de identidad.

Por tanto, la tecnología *Blockchain* tiene un alto grado de seguridad debido a su carácter descentralizado, a la criptografía y la publicidad de la información al mismo tiempo que se resguarda la privacidad de los usuarios, razones por las que estos pueden llevar a cabo sus transacciones de manera confiable.

Al respecto, Alejandro Francisco Herrán Aguirre y Antonio de Jesús Victorio López en cuanto al tema de confianza en la tecnología señalan:

> … actualmente se puede afirmar que la Blockchain ha transitado firmemente del extremo de lo no familiar a lo familiar y por ende produce la confianza necesaria en sus usuarios para alojar en su interior diversas criptomonedas, incluso archivos digitales, contratos inteligentes y la posibilidad de contar también con registros públicos. Una vez que las personas se informan de la naturaleza propia de la Blockchain se dan cuenta de que es prácticamente inmutable, inalterable, descentralizada pero a la vez que se trata de una red pública por cuanto una operación es visible de los usuarios si se siguen los protocolos de seguridad y que si bien es cierto no se encuentra vigilada por un ente central si lo está por todos aquellos que la componen, es decir,

la propia Blockchain se convierte en el depositario de confianza a través de la actuación de sus nodos.[9]

1.4 Las utilidades del *Blockchain*

Una de las utilidades de esta tecnología –no la única, pues puede servir en la transparencia gubernamental, integración de expedientes clínicos, almacenamiento de información; entre otros,- es servir como criptomoneda. En internet, se encuentran diversas criptomonedas, tales como *"bitcoin", "ethereum", "PeerCoin", "Ripple", "Litecoin", "Dogecoin", "Petro"*, entre otras. La mayoría no están respaldadas por activos o bienes con un valor intrínseco, salvo tal vez, la "*Petro*" que el gobierno de Venezuela lanzó, respaldada por petróleo, oro, gas y diamantes.

La moneda *fiat* es una moneda que por disposición legal de una autoridad central, representa un valor, a diferencia de la moneda fiduciaria que se basa en la confianza de que es aceptado por todos los agentes económicos como medio de cambio, sin necesidad de que un gobierno imponga obligadamente su uso.[10] La criptomoneda es una moneda fiduciaria, pues en la medida en que la confianza en ella no se rompa, se usará en la misma media que el dinero *fiat*.

Una criptomoneda puede aparecer mediante una *Initial Coin Offering* (ICO), que es una forma de financiamiento de un proyecto empresarial que en lugar de ofrecer acciones, emite criptomonedas, mismas que tendrán cierto valor al inicio, pero aumentará de valor conforme al éxito del proyecto, logrando un retorno importante de rendimientos a los inversionistas.

Las criptomonedas, se comercializan por medio de un monedero virtual, consistente en una plataforma tecnológica *exchange*, donde se pueden comprar y vender mediante el pago de una comisión a la empresa operadora de la misma.

---

[9] Herrán Aguirre, Alejandro Francisco y Victorio López, Antonio de Jesús, "*Blockchain y confianza: Un estudio desde el Derecho*", *Revista Iberoamericana de Producción Académica y Gestión Educativa*, vol.5, núm. 10, julio – diciembre 2018, *http://pag.org.mx/index.php/PAG/article/view/754*.
[10] Wikipedia, "Dinero Fiduciario", *https://es.wikipedia.org/wiki/Dinero_fiduciario*. Consultado el 06 de mayo de 2020.

Esta empresa operadora apertura una cuenta al usuario en el monedero virtual –similar a una cuenta bancaria-, quien deposita en la cuenta bancaria de ésta, una cantidad de dinero que aparecerá abonada en el *exchange*; posteriormente, el usuario adquiere una criptomoneda y la cantidad de dinero será cargada contra el abono de la cantidad de criptomoneda. El registro inverso acontecerá cuando venda la criptomoneda, esto es, cargo de la criptomoneda contra abono de dinero.

La utilidad de la *exchange*, consiste en ser un instrumento financiero *de facto*, sin reconocimiento ni protección legal, pues permite realizar una inversión en criptomoneda con la expectativa de que en la especulación –como en forma similar sucede con divisas como dólar o euro, por ejemplo-, se vea favorecido con un aumento en su valor que signifique ganancias para el adquirente de la misma cuando las venda.

Cualquier persona puede utilizar una criptomoneda como simple medio de pago y no necesariamente como instrumento financiero, o con ánimo especulativo. Fue ésta la idea original de la criptomoneda, pues su última finalidad fue evitar al intermediario bancario en el sistema de pagos entre proveedores y clientes.

Efectivamente, por medio del uso de la criptomoneda se elimina la intermediación del banco –también los administradores de tarjetas de crédito bancarias, como Visa y MasterCard- para el pago de bienes o servicios, pues basta con la transferencia de la criptomoneda para su adquisición para que el enajenante o prestador se considere pagado, sin la necesidad de la intermediación bancaria que normalmente acontece, máxime que con los avances tecnológicos actuales el comercio electrónico ha evolucionado rápidamente a través de internet que permite la comercialización de bienes o servicios en forma instantánea.

En este contexto, para el consumidor puede representar una ventaja al no tener que usar necesariamente su cuenta bancaria y también al proveedor que no deberá pagar una comisión a su banco. Inclusive, en comercialización de

bienes y servicios internacionales, se evitarían las comisiones bancarias por transferencias de fondos o remesas internacionales.

El uso de la tecnología de *Blockchain* en criptomonedas no es la única, pues ha sido utilizada en aspectos diversos que brindan soluciones específicas, como lo son, por ejemplo, para almacenamiento de información en la nube, verificación de identidad digital, reproducción y distribución de música, servicios públicos, transparencia gubernamental, expedientes clínicos en el sector salud, protección de derechos de autor, entre otros.

A continuación, se ofrecen dos de estos ejemplos:

Esta tecnología se podría utilizar en la integración de expedientes electrónicos de pacientes que contengan la información de la evolución de su estado de salud por toda la vida de pacientes, sin que pueda suprimirse ni alterarse la información y con toda la privacidad que ello requiere.

En cuanto a la transparencia gubernamental, se podría vigilar el correcto sistema de pagos y movimiento de cualquier tipo de recursos, propiciando que las personas puedan acceder al conocimiento de las operaciones.

Actualmente, el almacenamiento de la nube se hace de forma centralizada en plataformas (*DropBox, Google Drive, Box*, etc.) que administran la información, pero con *Blockchain* se podrá hacer de forma distribuida sin depender de un proveedor, aumentando la seguridad de la misma.

En el ámbito jurídico, el contrato inteligente *(smart contract)* es un acuerdo de voluntades capaz de ejecutarse de manera automatizada y hacerse cumplir por sí mismo –autoejecutable-. Las personas podrán programar a las máquinas para que realicen contratos, como en el caso de un refrigerador que detecta la ausencia de algún alimento y solicita al supermercado el producto (Internet de las Cosas).

Los contratos inteligentes son programas informáticos que ejecutan autónoma y automáticamente los términos del mismo. Sin la intervención humana

pueden obtener información y procesarla según las reglas establecidas y realizar las medidas que se requieran como consecuencia de ello.[11]

Algunos contratos inteligentes pueden ser préstamos mercantiles, se podrá dejar la instrucción del depósito de una cantidad dinero sujeta a una condición, que, de realizarse, se hará la transferencia. Una más puede acontecer en el comercio electrónico, donde un contrato puede supervisar que la mercancía haya llegado para liberar los fondos. Otros pueden ser los fideicomisos, testamentos, etcétera.

1.5 La Criptomoneda

Una de las utilidades de la tecnología *Blockchain,* como se señaló anteriormente, es servir como criptomoneda. Es importante establecer la diferencia conceptual entre dinero electrónico, moneda digital, criptomoneda y moneda virtual.

Tulio Rosembuj, establece que el dinero electrónico *"es un valor monetario almacenado en un formato electrónico, representado por un crédito exigible a su emisor, emitido por un valor igual a los fondos recibidos y convertible en dinero de curso legal al valor nominal. Es un medio de pago que se encuentra supeditado a la autoridad de un banco central de acuerdo a la intermediación bancaria y financiera convencional"*[12].

Por su parte, la moneda digital está basada en una tecnología descentralizada sin la intervención de una autoridad central, pero con base en protocolos de programas de cómputo (software). Con ello, se incentivan las transacciones en línea de persona a persona, y se resuelve el problema del doble gasto y cada una de las transacciones conformadas consta en un registro público entre los usuarios.[13]

La criptomoneda se basa en algoritmos matemáticos, que descifran las claves, pública y privada, para impedir el fraude o el abuso, y que son únicas para

[11] Oro y Finanzas, *¿Qué son los contratos inteligentes o Smart contracts? Bitcoin y Ethereum o el dinero programable*, 17 de noviembre de 2015, *https://www.oroyfinanzas.com/2015/11/que-son-contratos-inteligentes-smart-contracts/*. Consultado el 08 de agosto de 2019.
[12] Rosembuj, Tulio, *Bitcoin,* 1a. ed., Barcelona, el Fisco – G.L.E.T.S.L., 2015, p. 28.
[13] *Ibidem*, p. 29.

cada usuario.[14] En virtud de la firma electrónica, cada usuario tiene dos claves, la privada y la pública que se comparte en la red. Con la criptografía existe alto grado de seguridad en la transacción y permite la adición de un bloque en la cadena. La transacción entre las partes no es otra cosa que un mensaje cuyo contenido es la clave pública del receptor y la cuantía de moneda que envían y está firmado por la clave privada del remitente.

Finalmente, la moneda virtual "es el estado próximo y sucesivo de la criptomoneda digital. Es la integración del mundo digital y sintético en la economía real y en las instituciones que la organizan… la virtualidad, en su propia garantía, debe asimilarse a la moneda real, para su supervivencia."[15]

Cada vez más se popularizan las plataformas de pago electrónico y ello contribuye a un uso cada vez menor del efectivo[16], de ahí que tal vez en un futuro los bancos centrales estén obligados a proporcionar moneda virtual sin riesgo, para lo cual tendrá que reconocerse a través de las reformas legales.

En México, el artículo 30 de la Ley para Regular las Instituciones de Tecnología Financiera, también conocida como Ley Fintech, intentó conceptualizar a la criptomoneda como activo virtual y la define como ***"****la representación de valor registrada electrónicamente y utilizada entre el público como medio de pago para todo tipo de actos jurídicos y cuya transferencia únicamente puede llevarse a cabo a través de medios electrónicos.*"

A este respecto, dicha disposición establece que en ningún caso se entenderá como activo virtual la moneda de curso legal en territorio nacional, las divisas ni cualquier otro activo denominado en moneda de curso legal o en divisas; que las Instituciones de Tecnología Financiera solo podrán operar con los activos virtuales que sean determinados por el Banco de México y; que para realizar

---

[14] *Idem*.
[15] *Ibidem*, p. 39.
[16] Orcutt, Mike, *"Riesgos y ventajas de que los gobiernos lancen criptomonedas públicas"* trad. de Ana Milutinovic, *MIT Technology Review, 2019*, *https://www.technologyreview.es/s/10815/riesgos-y-ventajas-de-que-los-gobiernos-lancen-criptomonedas-publicas*. Consultado el 09 de febrero de 2019.

operaciones con los activos virtuales, dichas instituciones deberán contar con la previa autorización de éste.

El concepto establecido por ley, se encuentra muy lejos de lo que debe entenderse por criptomoneda, porque no se relaciona con alguna tecnología descentralizada, ni hace referencia a la criptografía, elementos de *Blockchain* que es con base en la cual se sustenta la criptomoneda, de ahí que más bien la definición legal se aproxime al concepto de dinero electrónico, conforme a los conceptos que antes se comentaron.

Por tanto, la legislación mexicana menos aun coadyuva a que la criptomoneda evolucione a una moneda virtual, pues con independencia de que se le haya denominado “activo virtual”, del concepto legal no parece que la idea sea la virtualidad, esto es, que este último en alguno momento se asemeje a la moneda real, o sea, al peso mexicano.

Por tanto, a pesar de que la intención de la autoridad legislativa fue el de regular la criptomoneda con el concepto de activo virtual, al final de cuentas el concepto legal quedó en mero dinero electrónico.

Capítulo 2

La regulación legal de la Criptomoneda en México

Capítulo 2. La regulación legal de la Criptomoneda en México

En México, con la entrada en vigor de la Ley para Regular las Instituciones de Tecnología Financiera se buscó regular la criptomoneda como un "activo virtual", pero aún son incipientes los esfuerzos en tal aspecto. Habrá que esperar algunos años más para advertir cómo se materializan en la vida cotidiana de los ciudadanos la regulación.

Con relación a la naturaleza jurídica de la criptomoneda, la mencionada ley las considera como activo virtual -no así como moneda virtual-, entendida como la representación de valor registrada electrónicamente y utilizada entre el público como medio de pago para todo tipo de actos jurídicos y cuya transferencia únicamente puede llevarse a cabo a través de medios electrónicos.

Por principio de cuentas, la criptomoneda no es dinero, porque el dinero es un bien o cosa mueble fungible y progresivamente inmaterial, puesto que aun cuando la criptomoneda también pueda reputarse como fungible, lo cierto es que no es una cosa mueble (corpórea) y si bien el dinero con los avances electrónicos, no necesariamente se tiene en papel, lo cierto es que tiene reconocimiento legal, situación que de ninguna manera tiene la criptomoneda[17].

La naturaleza jurídica es la de ser un medio de pago que no tiene reconocimiento legal -como sí lo tiene el dinero- y como característica que se registra, transfiere electrónicamente y no es reconocida ni respaldada por el Banco de México.

2.1 Aspectos financieros de la Criptomoneda

La característica de las criptomonedas es que no están respaldadas por gobierno ni banco central alguno; inclusive, no tienen poder liberatorio para el cumplimiento de obligaciones, como en cambio, sí lo tiene el peso de nuestro país y divisas extranjeras, en términos de los artículos 1º, 2º, 7º y 8º de la Ley Monetaria

[17] García Mexia, Pablo, *op. cit*., p. 250.

de los Estados Unidos Mexicanos, razón por la cual, desde un punto de vista estrictamente legal, ni siquiera puede llamársele “moneda”.[18]

El 9 de marzo de 2018, se publicó en el Diario Oficial de la Federación la Ley para Regular las Instituciones de Tecnología Financiera, también conocida como Ley Fintech, en la que, entre otras, se regulan a las criptomonedas.

Los aspectos relevantes de dicha Ley, en cuanto a las criptomonedas se refiere (artículos 30 a 34 y 88 de la Ley Fintech), son las siguientes:

1. La criptomoneda se considera activo virtual, entendida ésta como la representación de valor registrada electrónicamente y utilizada entre el público como medio de pago para todo tipo de actos jurídicos y cuya transferencia únicamente puede llevarse a cabo a través de medios electrónicos.

   Es equivocado el concepto legal, pues como se dijo al finalizar el capítulo anterior, el concepto legal se asemeja más al dinero electrónico que a la criptomoneda y menos aún que a la moneda virtual.

2. En ningún caso se entenderá como activo virtual la moneda de curso legal en territorio nacional, las divisas ni cualquier otro activo denominado en moneda de curso legal o en divisas.

3. Previa autorización del Banco de México, las Instituciones de Tecnología Financiera solo podrán operar con los activos virtuales que sean determinados por el Banco de México mediante disposiciones de carácter general. En dichas disposiciones, el Banco de México podrá establecer plazos, términos y condiciones que deberán observar las Instituciones de Tecnología Financiera para los casos en que los activos virtuales que este haya determinado se transformen en otros tipos o modifiquen sus características.

[18] Rodríguez, Darinka, *“Criptomonedas no son de uso legal en México: Banxico”*, *El Financiero*, 10 marzo 2014, *http://www.elfinanciero.com.mx/economia/criptomonedas-no-son-de-uso-legal-en-mexico-banxico.html.* Consultado el 15 de diciembre de 2018.

4. El Banco de México para la determinación de los activos virtuales tomará en cuenta, entre otros aspectos, el uso que el público dé a las unidades digitales como medio de cambio y almacenamiento de valor, así como la unidad de cuenta; el tratamiento que otras jurisdicciones les den a unidades digitales particulares como activos virtuales, así como los convenios, mecanismos, reglas o protocolos que permitan generar, identificar, fraccionar y controlar la replicación de dichas unidades.

5. Las Instituciones de Tecnología Financiera que operen con activos virtuales deberán estar en posibilidad de entregar al Cliente respectivo, cuando lo solicite, la cantidad de activos virtuales de que este sea titular, o bien el monto en moneda nacional correspondiente al pago recibido de la enajenación de los activos virtuales que corresponda.

6. En las Operaciones de compraventa o enajenación de activos virtuales que las Instituciones de Tecnología Financiera realicen con sus Clientes o a nombre de ellos, el contravalor deberá entregarse en el mismo acto en que dichas Operaciones se lleven a cabo, y deberán liquidarse en los términos y sujeto a las condiciones que, al efecto, establezca el Banco de México mediante disposiciones de carácter general.

7. Las Instituciones de Tecnología Financiera que reciban cantidades de dinero para la celebración de Operaciones de compra de activos virtuales deberán devolver dichas cantidades a los Clientes respectivos, en caso de que las Operaciones referidas no se lleven a cabo en los plazos señalados en dichas disposiciones.

8. El Banco de México definirá las características de los activos virtuales, así como las condiciones y restricciones de las Operaciones y demás actos que se pueden realizar con dichos activos, mediante disposiciones de carácter general que para tal efecto emita. Asimismo, el Banco de México establecerá las medidas a las que deberán sujetarse las Instituciones de Tecnología Financiera para la custodia y control que sobre los activos virtuales ejerzan al realizar tales Operaciones y actos. Se entiende por custodia y control de

activos virtuales a la posesión de las firmas, claves o autorizaciones que sean suficientes para ejecutar las Operaciones a que se refiere esta Ley.

9. Las Instituciones de Tecnología Financiera tendrán prohibido vender, ceder o transferir su propiedad, dar en préstamo o garantía o afectar el uso, goce o disfrute de los activos virtuales que custodien y controlen por cuenta de sus Clientes, excepto cuando se trate de la venta, transferencia o asignación de dichos activos por orden de sus Clientes.

10. Las Instituciones de Tecnología Financiera que operen con activos virtuales deberán divulgar a sus Clientes, los riesgos que existen por celebrar operaciones con dichos activos, lo que deberá incluir, como mínimo, informarles de manera sencilla y clara en su página de internet o medio que utilice para prestar su servicio, lo siguiente:

    - En virtud de que el activo virtual no es moneda de curso legal, no está respaldado por el Gobierno Federal, ni por el Banco de México;
    - La imposibilidad de revertir las operaciones una vez ejecutadas, en su caso;
    - La volatilidad del valor del activo virtual, y
    - Los riesgos tecnológicos, cibernéticos y de fraude inherentes a los activos virtuales.

Con lo anterior, se regulan diversas situaciones que ya suceden en nuestro país, a saber: la comercialización de productos y/o servicios mediante el pago en criptomonedas o activos virtuales, la compraventa de activos virtuales mediante monedero electrónico (*Exchange*), los riesgos que implica ello, el reconocimiento de que las mismas no son equivalentes a la moneda de curso legal o divisas extranjeras y, por ende, no están respaldadas por el gobierno federal y; la facultad del banco de México para determinar las criptomonedas que deben ser utilizadas por las Instituciones de Tecnología Financiera.

La importancia de la regulación de la criptomoneda radica en que los usuarios tendrán confianza en las que sean recomendadas por el Banco de México, y sabrán

de antemano de los riesgos que implican; asimismo, conocerán que las empresas que controlan los monederos electrónicos son entidades financieras autorizadas, y que existen mecanismos suficientes para acceder a ellos, sin que se pierdan sus activos.

Con la Ley Fintech, será posible realizar pagos con criptomonedas que representan un valor y no considerar que el pago así realizado equivale a una permuta en el caso de compraventa de bienes.[19]

En cuanto a las sanciones administrativas, el artículo 104, fracción I de la Ley Fintech, establece una multa de 30,000 a 150,000 UMA por realizar operaciones con activos virtuales o divisas sin contar con la previa autorización del Banco de México o por realizar Operaciones con activos virtuales distintos a los determinados por el Banco de México.

Ahora bien, el 10 de septiembre de 2018, se publicaron en el Diario Oficial de la Federación, las "Disposiciones de carácter general aplicables a las Instituciones de Tecnología Financiera" y las "Disposiciones de carácter general a que se refiere el artículo 58 de la Ley para Regular las Instituciones de Tecnología Financiera". De esa manera quedó conformada la normativa secundaria de la llamada Ley Fintech, publicada el pasado 9 de marzo, la cual contará con un claro marco normativo.

El objeto de las disposiciones de carácter general es establecer el marco normativo aplicable a la organización de las Instituciones de Tecnología Financiera, y la operación de las Instituciones de Financiamiento Colectivo. Contempla entre otros puntos relevantes, los siguientes:

1. Prever los requisitos que deberán observar las Instituciones de Financiamiento Colectivo para dar cumplimiento a las obligaciones de establecer y dar a conocer a los posibles inversionistas los criterios aplicados para la selección de los solicitantes y de los proyectos objeto de financiamiento.

[19] Flores Juárez, Othon, *"¿Se pueden comprar inmuebles con criptomonedas?", El Mundo del Abogado*, 1 de febrero de 2018*, http://elmundodelabogado.com/revista/posiciones/item/se-pueden-comprar-inmuebles-con-criptomonedas*. Consultado el 15 de diciembre del 2018.

2. Establecer las características mínimas que deberán contener las constancias electrónicas de conocimiento de riesgos.
3. Establecer los límites para la realización de operaciones en las Instituciones de Financiamiento Colectivo, tomando en consideración la regulación aplicable a otras figuras del sistema financiero.
4. Señalar los términos para la ejecución de los mandatos y comisiones que realicen, a fin de que sus clientes efectúen las operaciones.
5. Tener un plan de continuidad de negocio, el cual se deberá implementar en situaciones de contingencia, a fin de contar con estándares mínimos que reduzcan los riesgos a que están expuestas estas instituciones.

Por otro lado, las disposiciones de carácter general a que se refiere el artículo 58 de la Ley Fintech, son para regular las siguientes cuestiones:

1. Establecer las medidas y procedimientos mínimos que las Instituciones de Tecnología Financiera deberán observar para prevenir y detectar los actos, omisiones u operaciones que pudieran favorecer, prestar ayuda, auxilio o cooperación de cualquier especie para la comisión del delito previsto en el artículo 139 Quáter del Código Penal Federal o que pudiesen ubicarse en los supuestos del artículo 400 Bis del mismo código.
2. Prever la forma y los términos en que las Instituciones de Tecnología Financiera deberán presentar a la Comisión Nacional Bancaria y de Valores el Manual de Cumplimiento.
3. Señalar la forma, los términos y las modalidades conforme a los cuales las Instituciones de Tecnología Financiera deben presentar a la Secretaría de Hacienda y Crédito Público, por conducto de la Comisión Nacional Bancaria y de Valores, los reportes relacionados con:
    - Los actos, operaciones y servicios que realicen con sus clientes y las operaciones entre éstos, que pudieran estar relacionados con los supuestos previstos en los artículos 139 Quáter o 400 Bis del CPF.

- Los actos, operaciones y servicios que realicen los miembros de su consejo de administración o administrador único, sus directivos, funcionarios, empleados, comisionistas o apoderados, que pudiesen actualizar los supuestos señalados en el inciso anterior, así como contravenir o no dar cumplimiento a las obligaciones establecidas en estas disposiciones.

4. Precisar las características que deban reunir los actos, operaciones y servicios que deban ser reportados por las Instituciones de Tecnología Financiera.

5. Prever los casos, la forma y los términos en los cuales las Instituciones de Tecnología Financiera darán cumplimiento a las obligaciones previstas en la ley y en estas disposiciones, así como los plazos y medios a través de los cuales comunicarán o presentarán a la Secretaría de Hacienda y Crédito Público, por conducto de la Comisión Nacional Bancaria y de Valores, o a esta última, según corresponda, la información y documentación que así lo acredite.

Así, con estas disposiciones inicia el proceso para que todas las entidades del sector tecnológico financiero que deseen operar ya puedan solicitar la autorización de la Comisión Nacional Bancaria y de Valores.

Finalmente, se señala que las disposiciones de carácter general entraron en vigor a los 15 días de su publicación en el DOF, es decir, a partir del 25 de septiembre de 2018; mientras que las disposiciones que se refieren al artículo 58 de la Ley Fintech, entraron en vigor desde el 11 de septiembre de 2018. En ambos casos, con las excepciones contenidas en sus artículos transitorios.

En términos de la circular 12/2018 del Banco de México, relacionada con las Disposiciones de Carácter General aplicables a las operaciones a las Instituciones de Fondos de Pago Electrónico, publicada en el Diario Oficial de la Federación el 10 de septiembre de 2018, las instituciones de fondos de pago electrónico deberán solicitar al Banco de México su autorización para que puedan utilizar aquellas tecnologías asociadas a alguno de los activos virtuales.

Para que estas Instituciones de Fondos de Pago Electrónico interesadas puedan enviar dicha solicitud por correo electrónico, deberán contar con un Certificado Digital vigente y se prevé que las que no tengan acceso a los elementos necesarios para enviar las solicitudes firmadas digitalmente, podrán presentarlas a la Gerencia de Operación y Continuidad de Negocio de los Sistemas de Pagos, en original, por duplicado.

La solicitud deberá estar suscrita por personas cuya firma haya quedado previamente registrada ante la Gerencia de Instrumentación de Operaciones para la gestión de solicitudes diversas para el Banco de México, adicionando un comunicado en el que especifiquen el motivo por el cual se ven en la necesidad de enviar solicitudes por este medio alterno.

Las instituciones de fondos de pago electrónico podrán otorgar beneficios no monetarios a sus clientes en términos de lo pactado al efecto entre ambas partes. Para ello, deberán determinar y establecer en los contratos que celebren con sus clientes la paridad que tendrán los referidos beneficios no monetarios respecto a cantidades de dinero.

Ahora bien, en el Diario Oficial de la Federación el día 8 de marzo de 2019, el Banco de México, publicó la circular 4/2019 dirigida a las Instituciones de Crédito e Instituciones de Tecnología Financiera relativa a las Disposiciones de carácter general aplicables a las Instituciones de Crédito e Instituciones de Tecnología Financiera en las Operaciones que realicen con Activos Virtuales.

El objetivo de la circular es establecer las reglas para determinar los activos virtuales y sus características, con los que las Instituciones de Tecnología Financiera e Instituciones de Crédito podrán operar; establecer los términos, condiciones y restricciones de las Operaciones que dichas Instituciones podrán realizar con activos virtuales; y establecer plazos, términos y condiciones que deberán observar las Instituciones para los casos en que los activos virtuales con los que operen se transformen en otros tipos de activos virtuales o modifiquen sus características.

En la circular, el Banco de México sostuvo que los activos virtuales son volátiles y costosos para celebrar transacciones y difícilmente escalables; destacó la existencia de riesgos para los tenedores de estos activos, porque derivado de la complejidad de la tecnología que los soporta, en su opinión, los usuarios podrían no conocer la complejidad de los procesos matemáticos y criptográficos y los posibles problemas que podrían presentarse y dar lugar a la pérdida de sus recursos; el desconocimiento por los usuarios de los elementos que determinan la oferta y demanda de dichos activos, así como la falta de alguna referencia con la cual se pueda obtener una estimación de su precio.

No obstante ello, el Banco Central señaló que busca promover y aprovechar el uso de tecnologías que pudieran tener un beneficio cuando sean utilizadas en el contexto de la operación interna de las IFT e instituciones de crédito "… Es decir, la utilización de tecnología como registros distribuidos, cadena de bloques o incluso los propios activos virtuales en sus procesos internos podría llegar a ser factible, siempre y cuando los riesgos de los activos virtuales no impacten al consumidor final."

Por todo esto, en la regla tercera de la circular, se sostuvo que previa autorización, las Instituciones sólo podrán celebrar las Operaciones con Activos Virtuales que correspondan a Operaciones Internas, pero deberán impedir en todo momento que se transmita, directa o indirectamente, el riesgo de dichas Operaciones con Activos Virtuales a los Clientes de dicha Institución.

Aspecto por demás importante es el señalamiento de la no autorización de Operaciones con activos virtuales para prestar de manera directa a sus Clientes servicios de intercambio, transmisión o custodia de activos virtuales.

Un aspecto esencial es lo establecido en la regla cuarta, relacionado con las características que deben reunir los activos virtuales, a saber:

1. Ser unidades de información, unívocamente identificables, incluso de manera fraccional, registradas electrónicamente, que no representen la titularidad o derechos de un activo subyacente o bien, que representen dicha titularidad o derechos por un valor inferior a estos.

2. Tener controles de emisión definidos mediante Protocolos determinados y a los que se pueden suscribir terceros, y
3. Contar con Protocolos que impidan que las réplicas de las unidades de información o sus fracciones se encuentren disponibles para ser transmitidas más de una vez en un mismo momento.

El hecho de que la circular 4/2019 haya establecido que solo pueden ser autorizadas las operaciones con activos virtuales que correspondan a operaciones internas, y que no serán autorizadas operaciones con activos virtuales para prestar de manera directa servicios de intercambio, transmisión o custodia de activos virtuales, constituye un auténtico obstáculo para la comercialización e intercambio de criptomonedas.

2.2 Aspectos penales de la Criptomoneda

Lizbeth Xóchitl Padilla Sanabria, menciona sobre los riesgos de la criptomoneda, relacionado con el lavado de dinero y la defraudación fiscal, pues señala que:

> cualquier tipo de capital, cuya procedencia sea lícita o ilícita se convierta, a través de solicitudes anónimas hacia operadores expertos en tecnologías de sistemas que encripten la información económica y personal de sus clientes, en criptomonedas (sean *bitcoins*, *etherum*, *litecoin* o *ripple*), sin pasar por el sistema financiero mexicano (y por tanto por la dinámica de regulación financiera y fiscal), especulando para obtener ganancias sin que se haya tenido que pagar impuestos; además, trasladar dicho capital, convertido en moneda virtual, de un país a otro en cuestión de segundos a través de la red del internet, y su valor se podría convertir de nueva cuenta en cualquier tipo de divisa e incluso transformarse en bienes y servicios.[20]

[20] Padilla Sanabria, Lizbeth Xóchitl, *Op. cit*.

En efecto, si el capital invertido en criptomonedas no ha sido fiscalizado y se desconoce su origen, estamos hablando eminentemente de una defraudación fiscal, y probablemente del delito de operaciones con recursos de procedencia ilícita, pues bien podría existir un concurso de ideal de delitos, inclusive, el artículo 109 del Código Fiscal de la Federación establece que "*El delito de defraudación fiscal y el delito previsto en el artículo 400 Bis del Código Penal Federal, se podrán perseguir simultáneamente. Se presume cometido el delito de defraudación fiscal cuando existan ingresos o recursos que provengan de operaciones con recursos de procedencia ilícita.*"

Si la tecnología *blockchain* permite la falta de identificación del usuario, es perfectamente posible que los recursos para la adquisición de la criptomoneda permanezcan ocultos y con ello se transformen en dinero y/o se adquieran bienes o servicios, lo que provoca que el origen del dinero no quede revelado y sean muy difícil su rastreo.

En la circular 4/2019 del Banco de México, publicada en el Diario Oficial de la Federación el 8 de marzo de 2019, se puso especial énfasis en que los activos virtuales conllevan un riesgo importante en materia de prevención de operaciones con recursos de procedencia ilícita, lavado de dinero y financiamiento al terrorismo, debido a la facilidad para transferir los activos virtuales a distintos países, así como la ausencia de controles y medidas de prevención homogéneos a nivel global.

Con la criptomoneda ha surgido la necesidad de establecer tipos penales que prevean conductas relevantes, pues la sustracción de las mismas de un monedero virtual no se ajusta a la descripción del delito de robo y tampoco del fraude informático (sustracción de dinero electrónico de las cuentas bancarias).

Con la promulgación de la Ley Fintech, existe ya la posibilidad de considerar conductas penalmente relevantes, aquellas como la sustracción de criptomonedas de un monedero virtual sin autorización de su titular.

En cuanto a los delitos, relacionados con las criptomonedas, la Ley Fintech contiene los siguientes dos tipos penales, establecidos en los artículos 119 y 133:

Artículo 119.- A quien en forma indebida utilice, obtenga, transfiera o de cualquier otra forma, disponga de los recursos, fondos de pago electrónico o activos virtuales de los Clientes de las ITF, de las sociedades autorizadas para operar con Modelos Novedosos o de los recursos, fondos de pago electrónico o activos virtuales de éstas, será sancionado con prisión de tres a nueve años de prisión y multa de 5,000 a 150,000 UMA.

Si quien realiza la conducta prevista en el párrafo anterior es accionista, socio, consejero, funcionario, directivo, administrador, empleado o proveedor de una ITF, de una sociedad autorizada para operar con Modelos Novedosos o es un tercero ajeno pero con acceso autorizado por éstas a sus propios sistemas, será sancionado con prisión de seis a dieciocho años y multa de 10,000 a 300,000 UMA.

Artículo 133.- Al que sin autorización obtenga, extraiga o desvíe recursos, fondos de pago electrónicos o activos virtuales por medio de los sistemas o equipos de informática de las ITF o de las sociedades o Entidades Financieras u otros sujetos supervisados por alguna Comisión Supervisora o por el Banco de México, autorizados para operar con Modelos Novedosos, se le impondrán las siguientes sanciones:

I. Cuando el monto de los recursos o el valor de los fondos de pago electrónicos o activos virtuales en el momento en que se cometa la conducta a que se refiere el presente artículo, según corresponda, exceda de 2,200 y no de 57,000 UMA; se sancionará con prisión de cuatro a diez años y multa de 7,000 a 170,000 UMA.

II. Cuando el monto de los recursos o el valor de los fondos de pago electrónicos o activos virtuales en el momento en que se cometa la conducta a que se refiere el presente artículo, según corresponda, exceda de 57,000, pero no de 400,000 UMA, se sancionará con prisión de cinco a once años y multa de 9,000 a 200,000 UMA.

III. Cuando el monto de los recursos o el valor de los fondos de pago electrónicos o activos virtuales en el momento en que se cometa la conducta a que se refiere el presente artículo, según corresponda, exceda de 400,000 UMA, se sancionará con prisión de seis a doce años y multa de 10,000 a 250,000 UMA.

No es este el momento para hacer un estudio dogmático penal de ambos a la luz de la teoría del delito, y saber si existe un concurso de delitos, pero sí dejar anotado que ambos tipos penales tienen como bien jurídico protegido el patrimonio. La diferencia entre ambos tipos penales es que el primero protege el patrimonio de los Clientes de las Instituciones de Tecnología Financiera y de las Sociedades Autorizadas para operar con Modelos Novedosos, mientras que el segundo, el patrimonio de estas últimas y no de los clientes.

Lo relevante radica en que con la entrada en vigor de la ley en comento, las criptomonedas tendrán un reconocimiento legal y las sociedades mercantiles que operen los monederos electrónicos *Exchange* serán parte del sistema financiero. Sin embargo, bajo el principio de especialidad de la Ley, el delito no será el fraude informático, previsto en el Código Penal Federal o en los Códigos Penales de las Entidades Federativas, sino alguno de los establecidos en la Ley Fintech.

2.3 Aspectos fiscales de la Criptomoneda

El objeto de la Ley del Impuesto Sobre la Renta es gravar los ingresos, y la base gravable es en forma muy simple, la suma de los ingresos del contribuyente, menos la suma de las deducciones autorizadas por la ley, adicionadas con la participación de los trabajadores en las utilidades de la empresa. Asimismo, se amortizarán las pérdidas fiscales de ejercicios anteriores y al resultado obtenido, se le aplicará la tasa del impuesto del 30% de conformidad con lo previsto en las fracciones I y II, por el artículo 9 de la Ley del Impuesto Sobre la Renta en vigor.

Cuando se comercializa la criptomoneda y alguien vende en un precio superior al de su adquisición hay utilidad y eso es indudable. El problema radica en cómo determinar esa utilidad que deberá ser objeto de tributación.

Al respecto, la Ley del Impuesto sobre la Renta no prevé mecánica o procedimiento alguno sobre la manera de calcular el impuesto correspondiente, tratándose de la compraventa de criptomoneda como instrumento de inversión. No es posible aplicar analógicamente las disposiciones, relacionadas con la ganancia o pérdida en la compra y venta de divisa extranjera, pues la criptomoneda no es divisa.

No cabe duda que es necesario reformar la ley de la materia, para establecer un procedimiento para determinar la base gravable del Impuesto sobre la Renta, máxime cuando, a diferencia de las divisas extranjeras, no hay parámetros certeros del valor de la criptomoneda. Por ejemplo, en el caso del dólar, la base del impuesto se calcula teniendo como fuente el valor de la divisa publicada en el Diario Oficial de la Federación diariamente.

Sin embargo, las criptomonedas, no tendrán una publicación oficial en cuanto a su valor. Es cierto que existen varias fuentes en la red que nos pueden dar noticia de su valor, pero éstas no son confiables al no ser oficiales y no dan certeza de los datos que conforman los parámetros de su valoración; inclusive, hay incertidumbre de la persona capacitada para determinar ello, a saber; ¿Deberá ser una persona con conocimientos financieros?; ¿Un ingeniero en sistemas, en virtud del conocimiento tecnológico en las fuentes de información, relacionados con los datos del valor de ellas?; ¿Un corredor público, por la experiencia de las operaciones mercantiles que implican la compraventa de las monedas virtuales?. No queda claro.

Lo anterior es importante, porque el valor de adquisición y venta de las criptomonedas pudo haberse realizado en un valor distinto de lo que la información en internet arroja, todo lo cual impacta en la determinación de la base gravable.

Otro aspecto de suma relevancia es el relacionado con la “monetarización” de las operaciones mercantiles y/o civiles con criptomonedas, pues con la nueva Ley Fintech, los contribuyentes podrán pactar el cumplimiento de sus obligaciones en estos activos virtuales.

Esto es, las adquisiciones, enajenaciones de bienes, los consumos de servicios mediante su pago con criptomonedas, como materiales, mercancías, vehículos, restaurantes, servicios médicos y cualquier otro profesional.

¿Cómo se determinarán el Impuesto sobre la Renta, cuando el valor de la criptomoneda quede en entredicho?, ¿Podrá pagarse el Impuesto sobre la Renta en criptomoneda?, ¿El Servicio de Administración Tributaria recibirá el pago del impuesto en dicho activo virtual?, o bien, ¿Tendrá que valuarse la misma, con los problemas indicados, para recibir el pago en moneda de curso legal?

La Ley del Impuesto sobre la Renta, necesita una reforma legal para regular los aspectos indicados, pues la criptomoneda es un activo virtual con el cual cada vez más estaremos en contacto, como medio de pago en las transacciones económicas.

Una posible solución para el caso del intercambio de criptomoneda y peso mexicano, podría ser el establecer que en la mecánica del cálculo del impuesto para obtener la base gravable, el precio de venta en moneda nacional en que el usuario la transmite, menos la suma del precio de su adquisición actualizado en moneda nacional, adicionado con las comisiones pagadas a la Institución de Tecnología Financiera que opera el intercambio, evidenciaría la utilidad del contribuyente sobre la cual se aplicará la tasa de ley, siendo que los valores de compra y venta por el usuario pueden ser conocidos de manera cierta a través de la Institución de Tecnología Financiera. Podrá establecerse que sea la IFT que opera el *Exchange* quien retenga el monto del impuesto causado.

Un aspecto importante para advertir el verdadero precio de las criptomonedas, en el caso de usarlas para pago de bienes y servicios con ella, es que se otorguen facultades a las autoridades fiscales para presumir su valor, a través del monto de la comisión que se cobre a los clientes por las Instituciones de Tecnología Financiera; pues al ser el monto de dicha comisión un porcentaje, se puede obtener el verdadero valor de la criptomoneda comercializada. Inclusive, podría dotarse de las mismas facultades presuntivas a las autoridades fiscales para que dicho valor lo realicen a través del promedio de valor en un momento

determinado en que se hayan comercializado un determinado tipo de criptomonedas mediante las Instituciones de Tecnología Financiera dedicadas al intercambio de las mismas y que aparezca un listado en la página web del Servicio de Administración Tributaria.

2.4 La Criptomoneda y La Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita

El objeto de la Ley de la Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita es crear e implementar medidas y procedimientos con la intención de prevenir y detectar actos, omisiones y operaciones que involucren recursos de procedencia ilícita y delitos relacionados con los mismos. Aunque sea cierto que el sistema financiero sea el principal medio en donde se mueven recursos económicos, también considera a otras actividades de servicio para que identifiquen e informen acerca de operaciones relevantes. Por actividades relevantes se entienden los actos, operaciones y servicios que realizan las actividades financieras y prestadoras de servicios y que son susceptibles de usarse como medio para mover dinero ilícito.[21]

En el Decreto del 9 de marzo de 2018, por el cual se expidió la Ley Fintech, se formaron y adicionaron diferentes disposiciones legales de diversos ordenamientos, entre ellos, se adicionó la fracción XVI del artículo 17 de la Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita para establecer como actividad vulnerable el ofrecimiento habitual y profesional de intercambio de activos virtuales por parte de sujetos distintos a las Entidades Financieras, que se lleven a cabo a través de plataformas electrónicas, digitales o similares, que administren u operen, facilitando o realizando operaciones de compra o venta de dichos activos propiedad de sus clientes o bien, provean medios para custodiar, almacenar, o transferir activos virtuales distintos a los reconocidos por el Banco de México en términos de la Ley para Regular las Instituciones de Tecnología Financiera.

[21] Orozco-Felgueres Loya, Carlos; *Efectos Fiscales en Materia de Prevención de Lavado de Dinero,* Dofiscal Thomson Reuter, México 2013, p. 96.

Se establece que serán objeto de Aviso de dicha operación ante la Secretaría de Hacienda y Crédito Público, cuando el monto de la operación de compra o venta que realice cada cliente de quien realice la actividad vulnerable sea por una cantidad igual o superior al equivalente a seiscientas cuarenta y cinco Unidades de Medida y Actualización.

Lo importante de tal adición a la Ley, obedece al hecho de considerar como actividad vulnerable las operaciones de compra venta de activos virtuales o criptomonedas, realizadas mediante las plataformas electrónicas, esto es, se reconoce que este tipo de operaciones son altamente riesgosas, pues presentan la posibilidad de que los fondos provengan de operaciones ilícitas.

El pasado 2 de octubre de 2019, se publicó en el Diario Oficial de la Federación, la Resolución que modifica la diversa por la que se expiden los formatos oficiales de los avisos e informes que deben presentar quienes realicen actividades vulnerables, esto es, los formatos de avisos e informes que las plataformas tecnológicas que realizan la compra y venta de criptomonedas tienen que entregar a las autoridades.

2.5 Comentarios Finales

México ha iniciado el camino de la regulación de criptomonedas, porque en la Ley para Regular las Instituciones de Tecnología Financiera ya hay disposiciones específicas sobre el “activo virtual”, entendido como la representación de valor registrada electrónicamente y utilizada entre el público como medio de pago para todo tipo de actos jurídicos y cuya transferencia únicamente puede llevarse a cabo a través de medios electrónicos.

Los aspectos relevantes son el reconocimiento en el sentido de que no puede considerarse al activo virtual como moneda de curso legal, ni como divisas ni cualquier otro activo denominado en moneda de curso legal o en divisas y que se necesita de autorización del Banco de México, para que las Instituciones de Tecnología Financiera operen con activos virtuales que solo lo serán los determinados por el propio banco central mediante disposiciones de carácter general.

No obstante ello, la circular 4/2019 del Banco central limitó las operaciones con activos virtuales a las operaciones internas, excluyendo de autorización a las operaciones con activos virtuales para prestar servicios de intercambio, transmisión o custodia de activos virtuales, con lo que se restringió a las Instituciones de Tecnología Financiera de las operaciones con el público en general para este tipo de actividades.

Es comprensible la precaución con la que el Banco de México actúa, porque es un hecho cierto que las criptomonedas son altamente riesgosas, pues presentan la posibilidad de que los fondos provengan de operaciones ilícitas, pero ello limita a la ley que a final de cuentas permitía dicha circunstancia, lo que inclusive podría ser cuestionado a la luz del artículo 89 fracción I constitucional, porque la regla no puede restringir la ley.

Y es que con el empleo de criptomonedas, puede realizarse diversas conductas criminales que como operaciones con recursos de procedencia ilícita y defraudación fiscal, fraudes entre otras, de ahí que es loable que el Banco de México advierta este aspecto.

Capítulo 3

Los delitos informáticos y la Criptomoneda

Capítulo 3. Los delitos informáticos y la Criptomoneda

Es indiscutible que el desarrollo de las nuevas tecnologías ha traído ventajas a la sociedad, pero también ha puesto de manifiesto desafíos. La tecnología en sí misma considerada es neutra, pues son las personas quienes pueden utilizarla para propósitos loables, pero también para causas perjudiciales.

El comportamiento criminógeno siempre ha existido en la medida que atenta contra los valores más preciados de la sociedad. Los criminales han utilizado la tecnología para realizar conductas ilícitas, razón por la cual los países han tenido que tipificar nuevas conductas en las leyes penales y esforzarse en la investigación de éstas o de las conductas delictivas tradicionales mediante el empleo de tecnologías.

Un delito cometido con el uso de criptomonedas es informático, como se verá más adelante y con ellas se corre el riesgo de realizar conductas relacionadas con operaciones con recursos de procedencia ilícita y/o defraudación fiscal en la medida en que con ellas se realizan operaciones que tienden a ocultar el origen de los recursos y la omisión del pago de las contribuciones que la ley establece.

3.1 Concepto de “Delito informático”

En 1983, la Organización para la Cooperación y el Desarrollo Económico (OCDE)[22], estableció que el *Computer Crime* es “...cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesado automático de datos y/o transmisiones de datos”[23]

[22] Fueron Estados miembros originales de la Organización para la Cooperación y el Desarrollo Económico: Alemania, Austria, Bélgica, Canadá, Dinamarca, España, Estados Unidos, Francia, Grecia, Irlanda, Islandia, Italia, Luxemburgo, Noruega, Países Bajos (Holanda), Portugal, Reino Unido, Suecia, Suiza y Turquía. Posteriormente se han incorporado mediante adhesión: Japón (28 de abril de 1964), Finlandia (28 de enero de 1969), Australia (7 de junio de 1971), Nueva Zelanda (29 de mayo de 1973), México (18 de mayo de 1994), República Checa (12 de diciembre de 1995), Hungría (7 de mayo de 1996), Polonia (22 de noviembre de 1996), Corea (12 de diciembre de 1996) y Eslovaquia (14 de diciembre de 2000).

[23] Organización para la Cooperación y el Desarrollo Económico, Computer related criminality: analysis of legal policy in the OECD Area, ICCP, 1984, p. 35.

En la obra "*Criminalita e Tecnología"*, Carlos Sarzana, señala que los crímenes por computadora comprenden "cualquier comportamiento criminógeno en el cual la computadora ha estado involucrada como material o como objeto de la acción criminógena, o como mero símbolo".[24]

María de la Luz Lima establece que un delito electrónico "en un sentido amplio, es cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin, y en un sentido estricto, el delito informático es cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel como método, medio o fin".[25]

Para Julio Téllez Valdez, los delitos informáticos son aquellas actitudes contrarias a los intereses de las personas que no se encuentran tipificadas en la legislación penal, en que se tiene a las computadoras como instrumento o fin (concepto atípico) o las conductas típicas, antijurídicas y culpables en que se tiene a las computadoras como instrumento o fin y que están descritas en el tipo penal (concepto típico).[26]

El mismo autor establece como característica de dichos antijurídicos que son conductas delictivas de cuello blanco, porque se requieren conocimientos técnicos; son acciones ocupacionales por realizarse cuando el sujeto activo labora, y son acciones de oportunidad pues se aprovecha la ocasión o el universo de funciones y organizaciones de un sistema tecnológico y económico.[27]

De lo anterior, puede formularse un concepto propio de delitos informáticos como cualquier conducta, típica, antijurídica y culpable, realizada por cualquier sujeto, con conocimiento técnico para su ejecución, aprovechando los medios

---

[24] SARZANA, Carlo, "Criminalità E Tecnologia en Computers" *Crime, Rassagna Penitenziaria e Criminologia*, año 1, Roma, 1979, p.5, *http://www.rassegnapenitenziaria.it/.* Consultado el 06 de febrero de 2019.
[25] Lima de la Luz, María, "Delitos Electrónicos", *Criminalia*, Academia Mexicana de Ciencias Penales, México, Porrúa, no. 1 - 6, año L, enero - junio 1984, p.100.
[26] Téllez Valdés, Julio, *Derecho informático*, 3a. ed., México, McGraw-Hill, 2004, p. 188.
[27] *Idem.*

electrónicos que se encuentran conectados a internet y que a través de la red logra ejecutar acciones que se encuentran fuera de la ley.

Son elementos esenciales, los siguientes:

1. Conducta ilícita para que se pueda considerar delito.
2. Medios electrónicos, como medio comisivo del delito.
3. Conocimiento técnico para su ejecución.
4. Tiene que ser por medio de la red de internet para su ejecución.

Es importante destacar que este tipo delitos informáticos, son principalmente cometidos mediante medios electrónicos y procesos informáticos, con computadoras, teléfonos, tabletas, etcétera, los cuales tendrán que estar conectados a internet para realizar la conducta ilícita ya que hoy en día es el medio principal por el cual surgen la mayoría de estos delitos.

En cuanto a los conceptos de electrónica, informática y cibernética, si bien no son sinónimos, en el ámbito de las nuevas tecnologías que son utilizadas para la realización de conductas típicas, se complementan.

La electrónica es entendida como una rama de la física aplicada que comprende la física, la ingeniería, la tecnología y las aplicaciones que tratan con la emisión, el flujo y el control de los electrones en el vacío y la materia.[28] Por su parte, la informática es aquella disciplina encargada del estudio de métodos, procesos, técnicas, desarrollos y su utilización en computadoras, con el fin de almacenar, procesar y transmitir información y datos en formato digital.[29]

Finalmente, la cibernética es la especialidad científica que compara el funcionamiento de una máquina y el de un ser vivo, sobre todo en lo referente a la comunicación y a los mecanismos de regulación.[30]

[28] Wikipedia, “Electrónica”, *https://es.wikipedia.org/wiki/Electr%C3%B3nica*. Consultado el 15 de abril de 2019.
[29] Ecured, “Informática”, *https://www.ecured.cu/Informática*. Consultado el 15 de abril de 2019.
[30] Definicion De, “Cibernética” *https://definicion.de/cibernetica/*. Consultado el 15 de abril de 2019.

Los delitos electrónicos son aquellos que utilizan la electrónica como medio para la realización de conductas delictivas, pero se considera que es más propio hablar de delitos informáticos, porque los sujetos activos utilizan a las tecnologías hoy existentes mediante los sistemas computacionales. No se considera correcto hablar de ciberdelitos en tanto que aun cuando en la comisión de delitos interviene la voluntad humana, no es el ámbito de la conducta criminal la comparación de la máquina con el ser humano, dado que lo importante desde el punto de vista penal es la intervención de la persona y la máquina o computadora como su herramienta.

Además, importa precisar que muchos de los delitos informáticos el bien jurídico tutelado son los datos almacenados en computadoras y más propiamente la información, o bien, las consecuencias que la vulneración de la información tiene en la dignidad, patrimonio, privacidad de las personas, entre otros.

De ahí que en los delitos informáticos estén presente los sistemas y procesos computacionales que involucran los datos e información almacenados en la computadora que necesitan de la electrónica para su procesamiento, flujo y transmisión.

Ahora bien, aun cuando los delitos informáticos puedan realizarse sin estar conectados necesariamente a internet, por ejemplo, algún delito cometido por medio de drones, o bien, la intervención de comunicaciones telefónicas, en la gran mayoría de los casos, el internet es un medio indispensable, pues hoy en día cada vez más el ecosistema en donde se desarrolla la actividad humana es mediante el uso de redes y el internet.

En esta línea de ideas, los delitos informáticos son más bien una subespecie de los delitos electrónicos que tiene como denominador común el uso de las computadoras para realizar actividades criminales tradicionales tales como robo, fraude, falsificaciones, daños, estafa, sabotaje, etcétera.

Asimismo, debe destacarse que el uso de las computadoras ha propiciado, a su vez, la necesidad de regulación por parte del derecho para sancionar nuevas conductas, tales como el fraude informático, delitos cometidos mediante la destrucción o alteración de datos, programas o documentos electrónicos contenidos

en redes o sistemas informáticos, los nuevos delitos contenidos en la nueva Ley para Regular las Instituciones de Tecnología Financiera, entre otros.

3.2 Clasificación de los delitos informáticos

Pocos son los autores que se han esforzado en realizar una clasificación de los delitos informáticos. Se considera que la más acertada es la de Alberto Nava Garcés, quien propone una clasificación en atención a si la tecnología y la electrónica son un medio o fin para cometer las conductas penalmente relevantes, como se verá a continuación:[31]

Los delitos informáticos que se pueden cometer por medio de la tecnología y la electrónica son:

a) Falsificaciones, en los que a través de la digitalización de documentos, puede crearse un documento que no corresponde al original del cual se obtuvo.

b) Robo de identidad, pues por medio de las computadoras y la red se puede tener acceso a datos personales de una persona y crear un perfil falso y hacer uso del mismo indebidamente.

c) Ingeniería social (para simular una identidad falsa), porque a través del análisis de sitios visitados, fotografías, etcétera que se encuentran en internet, se puede engañar a una persona y obtener de sus datos personales suficiente para llevar a cabo alguna conducta ilícita.

d) Conductas precursoras del abuso sexual, de la trata o del secuestro, *grooming*, acoso, *stalking*, *trolling*, esto es, conductas que con información de cuerpo desnudo y conversaciones con menores se ponen en venta a través de internet, con el consecuente abuso infantil en muchas de las ocasiones.

[31] Nava Garcés, Alberto Enrique, *Delitos Informáticos*, 3ª. Ed., México, Porrúa, 2016, pp. 112 y 113.

e) Transferencia de fondos, como lo es el fraude informático que consiste en vulnerar los sistemas informáticos de los bancos y poder acceder a las cuentas de usuarios para obtener los fondos ahí depositados.

f) Extorsión, porque a través de llamadas telefónicas, se busca obtener recursos mediante la intimidación o la violencia.

g) Intervención y grabación ilícita de conversaciones, en donde un tercero distinto de los intervinientes y sin su autorización, mediante la vulneración de la red, obtiene información de la comunicación para diversos fines.

h) Amenazas, pues cada vez más se llevan a cabo mediante el envío de mensajes a través de internet.

i) Clonación de tarjetas, en el cual una persona utiliza la tecnología para duplicar los plásticos que las Instituciones Bancarias entregan, vulnerando las medidas de seguridad que contienen.

j) Fraude, *phishing*, *pharming*, porque por medio de ingeniería social, logran obtener datos personales y con ello engañar a las personas logrando la obtención de dinero.

k) Pornografía infantil, pues existen sitios en internet que venden imágenes y videos de niños y niñas con cuerpo desnudo.

l) Delitos en materia de propiedad intelectual, porque en internet es posible encontrar diversas obras protegidas por el derecho de autor que se ponen a la venta sin la retribución a los autores.

Los delitos informáticos que tienen a la tecnología y electrónica como un fin son:

a) Robo de datos o de información, ya que la información alojada en computadoras y servidores en muchos de los casos es confidencial o bien puede representar un secreto comercial.

b) Robo o reproducción ilícita de programas de cómputo, también protegida por derecho de autor, puede representar una desventaja competitiva a sus titulares.

c) Daño a los programas de cómputo, porque en muchos de los casos, se busca que no funciones correctamente lo que puede poner en riesgo a las empresas.

d) *Malware*, modificar o alterar información, provocar pérdida de información, conseguir que no se pueda acceder a la información, secuestro de información, ataque a las páginas web o a los servidores.

Se considera acertada la clasificación anterior, porque tener a la tecnología como medio o fin, resulta muy orientador para entender la tipificación de los delitos informáticos.

De esta manera, los delitos que tienen a la tecnología como un medio para su realización, son aquellos que pueden ser cometidos inclusive sin el uso de la tecnología como son los ya mencionados y que, en todo caso, ésta ha servido como un elemento que los ha exponenciado en la época actual; así el fraude ha existido sin la tecnología y el uso de las computadoras y el internet, pero en virtud de ellos se ha presentado con mayor frecuencia.

Por su parte, los delitos que tiene a la tecnología como un fin, han tenido que regularse mediante la tipificación de conductas específicas que solo se entienden por el auge de las tecnologías, como lo son las antes mencionadas.

En el tema en cuanto a este trabajo se refiere, la defraudación fiscal por medio del empleo de criptomonedas es un delito informático, porque la tecnología *blockchain* será solo el medio o instrumento para causar el daño patrimonial. No será necesario establecer dentro de la descripción típica del tal ilícito la utilización de tal tecnología, pues para el tipo penal lo relevante es el resultado que la conducta cause, esto es, el perjuicio a la Hacienda Pública y no el medio empleado.

En todo caso, la tecnología usada adquiere relevancia en la investigación del delito, porque de ello depende poder establecer la omisión del pago de

contribuciones que, mediante engaño o aprovechamiento del error, se haya cometido con el resultado antes señalado.

3.3 México y el Convenio de Budapest

En virtud del avance tecnológico, en muchos de los casos, la comisión de delitos se realiza a través del uso de la tecnología, mediante computadoras e internet y es esta es la característica de los delitos informáticos.

Al respecto, debe cuestionarse cómo los países hacen frente a tal circunstancia, así como la regulación internacional es necesaria para estandarizar las conductas penales, los procedimientos y la cooperación entre países.

El Convenio de Budapest fue firmado el 23 de noviembre de 2001 y constituye el intento internacional de poner en marcha un andamiaje jurídico internacional para hacer frente a la cibercriminalidad. Es el primer tratado internacional creado con el objetivo de proteger a la sociedad frente a los delitos informáticos, mediante la elaboración de leyes adecuadas (artículos 2 a 10), la mejora de las técnicas de investigación (artículos 15, 16 y 17) y el aumento de la cooperación internacional (artículos 26 a 34). Son ya 56 países los que se han adherido a este instrumento internacional.

En términos del artículo 133 de la Constitución Mexicana, los tratados internacionales firmados por el Presidente de la República y aprobados por el Senado son ley suprema de la Unión. En el caso que México decida adherirse al Convenio de Budapest, será vinculante para él y deberá ajustar su legislación a las disposiciones del tratado. El artículo 1º de nuestra Constitución Federal, sitúa a los tratados internacionales en materia de derechos humanos al mismo nivel jerárquico de las leyes federales e incluso de la propia Carta Magna, por lo que dichos tratados son incorporados al orden jurídico nacional, debiendo prevalecer en caso de

conflicto entre éstos y aquella, las “restricciones expresas contenidas en la Constitución”.[32]

Alex Seger, responsable de la división de ciberdelincuencia del Consejo de Europa y secretario del Comité del Convenio de Budapest, sostuvo que desde 2007, México expresó su interés de cooperar con otros países para luchar contra el cibercrimen, pero desafortunadamente nunca ha finalizado el procedimiento para adherirse al Convenio de Budapest, porque en México, las leyes requieren grandes cambios y lograrlo es difícil y complicado, porque hay diferentes intereses entre las autoridades mexicanas.[33]

En la exposición de motivos, se señala la necesidad de establecer una política penal común con el objeto de proteger a la sociedad frente a la ciberdelincuencia, mediante la adopción de una legislación adecuada y mejora en la cooperación internacional. Queda claro que el Convenio de Budapest significa establecer en todos los países las reglas del derecho penal y disposiciones relacionadas al área de los delitos informáticos, así como establecer medidas para que la cooperación entre países sea rápida y eficaz.

La adhesión al convenio puede ser un avance importante en la investigación de delitos informáticos, ya que aportará herramientas y procedimientos para seguir luchando contra la delincuencia informática. Para México se espera la adhesión al convenio más que por la tipificación de delitos que ya existen en la legislación mexicana, por el intercambio internacional de información que ello significaría.

El Código Penal Federal, ya contiene delitos relacionados con el acceso ilícito a sistemas y la integridad de la información, el fraude informático, pornografía infantil, y propiedad intelectual, como se verá más adelante. Sin embargo, el convenio puede representar para México la cooperación internacional necesaria para el intercambio de información.

---

[32] Jurisprudencia 2a./J. 163/2017 (10a.), *Gaceta del Semanario Judicial de la Federación*, Décima Época, Libro 49, t. I, diciembre de 2017, p.487.

[33] Hernández, Aura, *“Piden a México en Convenio de Budapest, ser más que un observador”*, *El Excelsior*, 07 de diciembre de 2016, *https://www.excelsior.com.mx/hacker/2016/12/07/1132670*. Consultado el 15 de diciembre de 2018.

El convenio tiene cuatro capítulos y se establecen tres aspectos fundamentales para hacer frente a los delitos informáticos:

El primero, es el relacionado con estos delitos, con el objetivo de establecer un catálogo de conductas penalmente relevantes que definen los delitos y que los clasifica en cuatro categorías[34]:

a) Delitos que tienen a la tecnología como fin: son aquellos que atentan contra la confidencialidad, integridad o disponibilidad de la información. Por ejemplo, el daño informático, el acceso ilícito a un sistema, etc.

b) Delitos que tienen a la tecnología como medio: se refiere a delitos ya conocidos, que se cometen a través de un sistema informático. Son delitos comunes, que ya se encuentran tipificados en la mayoría de las legislaciones, ampliados a los medios digitales. Por ejemplo, el fraude informático o la falsificación de datos digitales.

c) Delitos relacionados con el contenido: establece como delitos diversos aspectos de la producción, posesión y distribución electrónica de pornografía infantil.

d) Delitos relacionados con infracciones a la propiedad intelectual: se refiere a la reproducción y difusión en Internet de contenido protegido por derechos de autor, sin la debida autorización. Por ejemplo: infracciones a la propiedad intelectual, piratería, etc.

El segundo, es el relacionado con las normas procesales, con el objetivo de precisar los procedimientos para la obtención y conservación de la evidencia digital y evitar su manipulación. Esto aplica a cualquier delito cuyo medio comisivo sea la informática y cualquier tipo de evidencia electrónica.[35]

---

[34] Pastorino, Cecilia, "Convenio de Budapest: Beneficios e implicaciones para la seguridad informática", *We Live Security*, ESET Enjoy Safer Tecnology, 06 diciembre 2017, *https://www.welivesecurity.com/la-es/2017/12/06/convenio-budapest-beneficios-implicaciones-seguridad-informatica*. Consultado el 15 de abril de 2019.
[35] *Idem.*

El último aspecto, es el relacionado con la cooperación internacional, que son reglas de cooperación entre países para investigar cualquier delito que involucre evidencia digital, ya sean delitos tradicionales o informáticos. Regula la localización de sospechosos, recolección o envío de evidencia digital y, también la extradición de personas.[36]

Entre las obligaciones de los países adherentes, se destacan la designación de un punto de contacto para la red 24×7 con la finalidad de proveer apoyo y cooperación de forma rápida y efectiva, así como un proceso de adecuación de normas y legislación al convenio de Budapest.[37]

Se debe revisar y armonizar la legislación penal mexicana sustantiva a la luz de los delitos señalados en el Convenio de Budapest, porque cuando este último se firmó, no estaban presente aún las redes sociales, los teléfonos inteligentes y sus aplicaciones, entre otros.

Refiere Alberto Nava Cortés, que el convenio pone a salvo la protección de los derechos y libertades fundamentales de los usuarios; sin embargo, con la Ley *Patriot* de los Estados Unidos de América, cuyo objetivo es ampliar la capacidad de control del Estado para combatir el terrorismo, mejorando la capacidad de las distintas agencias de seguridad estadounidenses al coordinarlas y dotarlas de mayores poderes de vigilancia contra los delitos de terrorismo, se puede vigilar y cancelar cualquier cuenta de correo electrónico cuyo servidor se encuentre alojado en éste.[38]

En un país como México, el Convenio de Budapest conlleva verdaderos riesgos, porque al tener una democracia aún incipiente, puede significar retrocesos en los derechos humanos, toda vez que México a pesar de tener un marco constitucional de observancia a los mismos, no tiene una política basada en ellos, pues las autoridades se han mostrado proclives a su vulneración.

---

[36] *Idem.*
[37] *Idem.*
[38] Nava Garcés, Alberto Enrique, *op. cit.* p. 138.

Si tenemos en cuenta que en años recientes el gobierno ha hecho uso de programas para intervenir los sistemas informáticos, como fue el caso del software de espionaje "*pegasus*" y con ello se logró intervenir de manera ilegal las comunicaciones de periodistas y activistas, bien podría justificar esas acciones precisamente en las investigaciones de delitos que a manera de pretexto permitan llevar esas acciones ilegales.

El problema del convenio de Budapest es que permite que los gobiernos de los estados tengan un margen de actuación tan amplio que conlleva a la arbitrariedad y provoque verdaderas acciones delictivas por parte del gobierno con servidores públicos encargados de vigilar los derechos fundamentales.

Asimismo, el Convenio de Budapest señala la necesidad de establecer conductas delictivas, pero es tan amplio el margen para que las autoridades tipifiquen las mismas que conceptos como "ilícitamente", "ilegítimamente" o similares pueden significar la violación a los principios de legalidad y exacta aplicación de la ley penal.

Danya Centeno de la Red en Defensa de los Derechos Digitales (R3D), considera que México debe cumplir con dos aspectos fundamentales. Por una parte, que se implemente en la legislación nacional los tipos penales que el tratado prevé de conformidad con el principio de exacta aplicación de la ley penal. Por otra, que la implementación se realice con transparencia y con una perspectiva de derechos humanos que incorpore los comentarios y observaciones de las múltiples partes interesadas, particularmente de la sociedad civil.[39]

El principio de legalidad en materia penal significa que la utilización precisa y cierta de la norma penal, al caso dado, descarta cualquier tipo de interpretación

[39] Centeno, Danya, *México y Convenio de Budapest: Posibles Incompatibilidades*, Red de Defensa de los Derechos Digitales, México, Junio 2018, *https://www.derechosdigitales.org/wp-content/uploads/minuta_r3d.pdf.* Consultado el 15 de diciembre de 2018.

basada en la costumbre y la analogía con otras leyes. Esto implica que la única fuente del derecho penal es la ley dictada por el Congreso de la Unión.[40]

Para que una norma responda al principio de legalidad, ella debe ser escrita, para que no queden dudas acerca de su contenido; estricta, significa que debe describir concretamente la conducta que es delito y; previa, debe ser anterior al hecho delictivo.

La exacta aplicación de la ley, es un principio que se encuentra previsto en el artículo 14 de la Constitución Federal, mismo que dispone: "*En los juicios del orden criminal queda prohibido imponer, por simple analogía, u aún por mayoría de razón, pena alguna que no esté decretada por una ley exactamente aplicable al delito de que se trata*.". Esta disposición impone un grado de precisión importante de la ley penal y excluye la analogía en cuanto perjudique al ciudadano, de tal manera que se evite la burla de la ley, dotando con ello de seguridad jurídica para obstaculizar la utilización de cláusulas generales indeterminadas.

El principio de legalidad está contenido en la Constitución en los artículos 16, 18 y 19 y conforme a éste sólo podrá considerarse delito, aquel hecho que la ley lo declare expresamente y de manera clara y precisa.

Así las cosas, es importante que en la implementación de delitos informáticos se respete el principio de exacta aplicación de la ley penal. Se considera que conceptos como "ilícitamente", "ilegítimamente" pueden dotar de un grado de indefinición, en virtud de que tales conceptos son elementos normativos de valoración jurídica o social, que corresponde a los operadores jurídicos determinar su sentido o alcance.

Sería más benéfico que en lugar de la utilización de dichos conceptos, en el tipo penal se establecieran requisitos como "sin autorización" o "sin consentimiento" que evitarán la indefinición y la inseguridad que provocan los tipos abiertos.

[40] Donna, Edgardo Alberto, "Precisiones sobre el principio de legalidad", *Estudios en Homenaje a Héctor Fix-Zamudio*, México, UNAM, Instituto de Investigaciones Jurídicas, 2009, p. 18.

En cuanto a los delitos patrimoniales, concretamente el fraude informático, el Convenio de Budapest, establece:

> Artículo 8.- Fraude Informático.
>
> Las partes adoptarán las medidas legislativas o de otro tipo que resulten necesarias para tipificar como delito en su derecho interno los actos deliberados e ilegítimos que causen perjuicio patrimonial a otra persona mediante:
>
> a. La introducción, alteración, borrado o supresión de datos informáticos
>
> b. Cualquier interferencia en el funcionamiento de un sistema informático, con la intención, dolosa o delictiva, de obtener de forma ilegítima un beneficio económico para uno mismo o para otra persona.

La disposición anterior, establece cuáles son los actos “ilegítimos” que causan un perjuicio patrimonial o beneficio económico, lo que conlleva imprecisión, porque lo “ilegítimo” es un concepto que implica una valoración jurídica o social que deberá a analizarse a la luz de las disposiciones legales, o bien, de acuerdo a las reglas sociales para poder desentrañar en cada caso qué es lo ilegitimo, lo que depende de cada sociedad en un lugar y momento determinado.

Lo así establecido por el Convenio de Budapest, lejos de brindar seguridad jurídica, provoca arbitrariedad, porque las autoridades legislativas al establecer los delitos por los cuales se pueda causar un daño patrimonial, pueden establecer tipos penales con indefinición que no cumplan con el principio de exacta aplicación de la ley, previsto por el artículo 14 constitucional.

En México, con la nueva Ley Fintech, una de las cosas que se pretende es evolucionar de una ausencia de tipicidad con relación a la sustracción de criptomonedas de los monederos electrónicos, a una conducta penalmente relevante y tipificada cuando las criptomonedas sean sustraídas sin autorización de

los mismos y, no como sucedía, que en el mejor de los casos esa conducta solo podrá calificarse como acceso ilegal a los sistemas informáticos.

Ello, porque la sustracción de las criptomonedas no puede ser robo en la medida en que no hay corporeidad en el objeto material del delito, ni fraude informático, porque éste va dirigido al dinero electrónico y no a los activos virtuales o criptomonedas.

3.4 Los delitos informáticos en el ordenamiento jurídico mexicano

Hoy en día los problemas que surgen a través de la sociedad de la información, han exigido una delimitación en los ordenamientos jurídicos de los países, con la finalidad de que se tipifiquen nuevas conductas penales frente al uso de la informática.

México en estos casos no ha sido la excepción, dentro de su marco jurídico ha empezado a hacer cambios para regular estos Delitos informáticos.

3.4.1 Código Penal Federal

Se encuentran como delitos el acceso ilícito a los sistemas y equipos de informática en los artículos 211 bis 1 al 211 bis 7, (hacking informático); delitos contra derechos de autor como el establecido en el artículo 424 bis, fracción II (cracking informático), y el artículo 426, relacionado con la fabricación, importación, venta o arrendamiento en un dispositivo o sistema para descifrar una señal satelital cifrada, portadora de programa, sin autorización de distribuidor legítimo de dicha señal.[41]

Existe un tipo de fraude informático, previsto en el artículo 231, fracción XIV del Código Penal Federal, cuya conducta consiste en “para obtener algún beneficio para sí o para un tercero, por cualquier medio accese, entre o se introduzca a los sistemas o programas de informática del sistema financiero e indebidamente realice operaciones, transferencias o movimientos de dinero o valores, independientemente de que los recursos no salgan de la Institución”

3.4.2 Código Penal para la Ciudad de México

[41] Artículo adicionado mediante Decreto publicado en el Diario Oficial de la Federación el 24 de diciembre de 1996.

El artículo 336 del Nuevo Código Penal del Distrito Federal hoy Ciudad de México[42], relativo a la Producción, Impresión, Enajenación, Distribución, Alteración o Falsificación de Títulos al Portador, Documentos de Crédito Públicos o Vales de Canje, dispone que se impondrán de tres a nueve años de prisión y de cien a cinco mil días multa al que, sin consentimiento de quien esté facultado para ello, altere los medios de identificación electrónica de tarjetas, títulos o documentos para el pago de bienes y servicios (fracción IV); acceda a los equipos electromagnéticos de las instituciones emisoras de tarjetas, títulos o documentos para el pago de bienes y servicios o para disposición de efectivo (fracción V); adquiera, utilice o posea equipos electromagnéticos o electrónicos para sustraer la información contenida en la cinta o banda magnética de tarjetas, títulos o documentos, para el pago de bienes o servicios o para disposición de efectivo, así como a quien posea o utilice la información sustraída, de esta forma (fracción VI); y a quien utilice indebidamente información confidencial o reservada de la institución o persona que legalmente esté facultada para emitir tarjetas, títulos o documentos utilizados para el pago de bienes y servicios, o de los titulares de dichos instrumentos o documentos. (fracción VII).

El artículo 355 del Código Penal antecitado, dispone que se impondrán de cuatro a nueve años de prisión y de doscientos cincuenta a cuatrocientos días multa, al funcionario electoral que altere, expida, sustituya, destruya o haga mal uso de documentos públicos electorales o archivos oficiales computarizados o relativos al registro de electores que corresponda.

3.4.3 Código Penal de Jalisco

El Artículo 170-Bis del Código Penal para el Estado libre y Soberano de Jalisco[43], con relación a la Falsificación de Medios Electrónicos o Magnéticos, señala como conductas penalmente relevantes al que, sin consentimiento de quien esté facultado

[42] Publicado en la Gaceta Oficial del Distrito Federal el 16 de julio de 2002. La denominación del Capítulo I del Título Vigésimo Cuarto, del Libro Segundo; así como la adición de la fracción VIII del artículo 336 del Nuevo Código Penal para el Distrito Federal, fueron publicadas en la Gaceta Oficial del Distrito Federal el 20 de diciembre de 2004.

[43] Publicado en la Gaceta Oficial del Distrito Federal el 16 de julio de 2002. La denominación del Capítulo I del Título Vigésimo Cuarto, del Libro Segundo; así como la adición de la fracción VIII del artículo 336 del Nuevo Código Penal para el Distrito Federal, fueron publicadas en la Gaceta Oficial del Distrito Federal el 20 de diciembre de 2004.

para ello: produzca, imprima, enajene, distribuya, altere o falsifique, aun gratuitamente, adquiera, utilice, posea o detente, sin tener derecho a ello, boletos, contraseñas, fichas, tarjetas u otros documentos que no estén destinados a circular y sirvan exclusivamente para identificar a quien tiene derecho a exigir la prestación que en ellos se consigna, siempre que estos delitos no sean de competencia federal; altere, copie o reproduzca, indebidamente, los medios de identificación electrónica de boletos, contraseñas, fichas u otros documentos a los que se refiere la fracción I de este artículo; acceda, obtenga, posea o detente indebidamente información de los equipos electromagnéticos o sistemas de cómputo de las organizaciones emisoras de los boletos, contraseñas, fichas u otros documentos a los que se refiere la fracción I de este artículo, y los destine a alguno de los supuestos que contempla el presente artículo y; adquiera, utilice, posea o detente equipos electromagnéticos o electrónicos para sustraer en forma indebida la información contenida en la cinta magnética de los boletos, contraseñas, fichas u otros documentos a los que se refiere la fracción I del artículo.

3.4.4 Código Penal de Sinaloa

En el artículo 217 del Código Penal para el Estado de Sinaloa[44], señala como conducta penalmente relevante, la persona que dolosamente y sin derecho: Use o entre a una base de datos, sistema de computadores o red de computadoras o a cualquier parte de la misma, con el propósito de diseñar, ejecutar o alterar un esquema o artificio, con el fin de defraudar, obtener dinero, bienes o información; o Intercepte, interfiera, reciba, use, altere, dañe o destruya un soporte lógico o programa de computadora o los datos contenidos en la misma, en la base, sistema o red.

3.5 Bien Jurídico Tutelado en los delitos informáticos

En el presente apartado, se aborda el concepto de bien jurídico protegido penalmente, su ubicación y transcendencia en la teoría del delito. Se señalan cuáles pueden ser los bienes jurídicos protegidos en los delitos informáticos y se da noticia

[44] Decreto Número 539, Publicado en el Periódico Oficial No. 131 de 28 de octubre de 1992.

de algunos delitos de este tipo, señalando el bien jurídico que en específico se protege.

3.5.1 Concepto de Bien Jurídico como límite al *Ius Puniendi*

Se puede definir de manera general como “el objeto de protección de las normas de derecho”.

Pavón Vasconcelos señala que la “Entidad que constituye el objeto de protección de las normas penales, contra las acciones de los hombres encaminadas a su lección o destrucción. La tutela de la de los bienes jurídicos es la razón de ser de las normas sancionatorias del derecho penal y, en cierto sentido, es verdad que el bien jurídico constituye el objeto de la tutela de la ley penal y al mismo tiempo el objeto del ataque de la acción jurídica y culpable”.[45]

Asimismo, Mir Puig refiere que el bien jurídico constituye el punto de partida y la idea que preside la formación del tipo, y son bienes jurídicos “aquellos intereses de la vida de la comunidad a los que presta protección el derecho penal”, por cuanto “las normas jurídicas prohíben bajo pena aquellas acciones que resultan apropiadas para menoscabar de forma especialmente peligrosa los intereses de la vida de la colectividad. El tipo parte, pues, de la norma y ésta, del bien jurídico”.[46]

En forma concreta, se desprende de los conceptos anteriores que el Bien Jurídico Penal es simple y sencillamente el objeto o interés que protegen las normas penales, lo que a su vez constituye un límite al *ius puniendi*, a lo que nos referiremos a continuación.

Mir Puig sustenta que: “El derecho penal suele entenderse en dos sentidos distintos, objetivo y subjetivo. En sentido objetivo significa el conjunto de normas penales. El Derecho penal subjetivo – también llamado derecho a castigar o *ius puniendi* – es el derecho que corresponde al Estado a crear y aplicar el Derecho

[45] Pavón Vasconcelos, Francisco; *Diccionario de Derecho Penal, México,* Porrúa, 1997, p. 139.
[46] Mir Puig S. y Muñoz Conde F.; *Tratado de Derecho Penal, Parte General I;* Barcelona, Bosch, 1981, p. 350.

penal objetivo.[47] A este respecto, Porte Petit refiere que es: “la facultad del Estado para determinar los delitos, las penas y las medidas de seguridad.”[48]

Entonces, de acuerdo con los diversos autores, el *ius puniendi* es el derecho a castigar, mediante la imposición y ejecución de penas y medidas de seguridad, lo que se logra mediante la determinación en la ley de los delitos. Sin embargo, dicha potestad estatal no es ilimitada, sino por el contrario, se encuentra acotada mediante diversos principios, como el bien jurídico.

El derecho penal de un Estado ha de justificarse como sistema de protección de la sociedad. Los intereses sociales que por su importancia puedan merecer la protección del Derecho se denominan bienes jurídicos. Se dice entonces que el derecho penal sólo puede proteger bienes jurídicos[49], lo que se traduce en una limitación al *ius puniendi*, y ello implica que una conducta típica solo será materialmente antijurídica en la medida en que lesione o ponga en peligro un bien jurídico protegido por la norma penal. El concepto de “antijuricidad material” será explicado en el capítulo siguiente.

3.5.2 El Bien Jurídico en la Tipicidad y la Antijuricidad

Delito es la acción típica, antijurídica y culpable. El bien Jurídico es uno de los elementos objetivos del tipo penal; su existencia debe verificarse al realizar el juicio de tipicidad; sin embargo, es en la antijuricidad donde se advierte su lesión o puesta en peligro.

Para Porte Petit la antijuridicidad es “cuando habiendo tipicidad no existe una causa de justificación o licitud”[50]. Raúl Carrancá señala que es “la oposición a las normas de cultura, reconocida por el Estado. Es la contradicción entre una conducta concreta y un concreto orden jurídico establecido por el Estado”

[47] Mir Puig Santiago, *Derecho Penal, Parte General,* Barcelona, B de F; 2011, p. 42.
[48] Porte Petit Candaudap, Celestino, *Apuntamientos De La Parte General De Derecho Penal,* México, Porrúa, 1969, p. 18.
[49] Mir Puig, Santiago, *El Derecho Penal en el Estado Social y Democrático de Derecho,* Barcelona, Ariel, 1994, p. 159.
[50] Porte Petit, Celestino, *op. cit.*, p. 203.

Gómez Benítez indica que no hay posible antijuridicidad sin tipicidad, de donde se deduce que cuando se habla de una conducta antijurídica se presupone que también es típica; pero excepcionalmente puede haber, sin embargo, tipicidad sin antijuridicidad: esto ocurre precisamente cuando concurre una causa de justificación de la realización del tipo prohibitivo."[51]

Derivado de lo anterior se concluye, que la antijuricidad es el rechazo al ordenamiento jurídico en su conjunto que contiene una norma prohibitiva o de determinación, ante la ausencia de causas de justificación.

La antijuridicidad tiene un aspecto formal y material.

González Quintanilla indica que la antijuridicidad formal no es más que la oposición entre el hecho u omisión y el ordenamiento jurídico-positivo. En sentido "material", la acción es antijurídica cuando, habiendo transgredido una norma positiva, lesiona o pone en peligro el bien jurídico que el Derecho quería proteger.[52]

Así las cosas, mientras que la antijuridicidad formal es la contravención de la conducta al ordenamiento jurídico y positivo, el aspecto "material" se revela cuando habiendo transgredido una norma positiva, se lesiona o pone en peligro el bien jurídico que el Derecho quería proteger.

3.5.3 Bienes Jurídicos Protegidos en los delitos informáticos

Para Julio Téllez Valdez, los delitos informáticos son aquéllas actitudes contrarias a los intereses de las personas en que se tiene a las computadoras como instrumento o fin, o bien, las conductas típicas, antijurídicas y culpables en que se tiene a las computadoras como instrumento o fin.[53] El mismo autor establece como característica de dichos antijurídicos que son conductas delictivas de cuello blanco, porque se requieren conocimientos técnicos; son acciones ocupacionales por realizarse cuando el sujeto activo labora, y son acciones de oportunidad pues se

[51] Gómez Benítez, José Manuel, *Teoría Jurídica Del Delito, Derecho Penal Parte General, Madrid,* Civitas, 1984, p. 80.
[52] González Quintanilla, José Arturo, *Derecho Penal Mexicano,* México, Porrúa, 1991, p. 308.
[53] Téllez Valdés, Julio, *op. cit*. p. 163.

aprovecha la ocasión o el universo de funciones y organizaciones de un sistema tecnológico y económico.[54]

Nava Garcés, indica que el bien jurídico protegido en los delitos informáticos es la información, pero dado el desarrollo de las nuevas tecnologías pueden afectarse otros bienes como la salud, el patrimonio, la dignidad humana, la intimidad y la privacidad, entre muchos otros.[55]

3.5.3.1 Dignidad Humana

La Suprema Corte de Justicia de la Nación ha considerado el artículo 1o. de la Constitución Política de los Estados Unidos Mexicanos junto con los instrumentos internacionales en materia de derechos humanos suscritos por México, reconocen el valor superior de la dignidad humana, es decir, que en el ser humano hay una dignidad que debe ser respetada en todo caso, constituyéndose como un derecho absolutamente fundamental[56], entendida como el interés inherente a toda persona, por el mero hecho de serlo, a ser tratada como tal y no como un objeto, a no ser humillada, degradada, envilecida o cosificada.[57]

La jurisprudencia de la Corte Interamericana de Derechos Humanos, se ha referido con frecuencia la dignidad humana, en casos de ataques a la vida y la integridad física, incluido el límite que ella supone para acciones contra una persona privada de libertad, o bien cuando se refiere a la honra y cuando la ha elevado a criterio para la determinación de las reparaciones debidas.[58]

Incluso, la mencionada Corte cuando refirió al “proyecto de vida”, apuntó que un ser humano para desarrollarse plenamente debe no solamente existir sino tener una perspectiva de realización por medio de su plan vital. En ese sentido, se

---

[54] *Idem.*
[55] Nava Garcés, Alberto Enrique, *op. cit.,* p. 94.
[56] Tesis P. LXV/2009, Semanario Judicial de la Federación y su Gaceta, Novena Época, t. XXX, diciembre de 2009, P. 8.
[57] Jurisprudencia 1a./J. 37/2016 (10a.), Gaceta del Semanario Judicial de la Federación, Décimo Época, Libro 33, t. II, agosto de 2016, P. 633.
[58] Amezcua, Luis, “Algunos puntos relevantes sobre la dignidad humana en la jurisprudencia de la Corte Interamericana de Derechos Humanos”, *Revista Iberoamericana de Derecho Procesal Constitucional*, México, No. 8. Porrúa, 2007, *http://www.corteidh.or.cr/tablas/r24334.pdf*. Consultado el 06 de febrero de 2019.

pronunció por entender que el daño al proyecto de vida "atiende a la realización integral de la persona afectada considerando su vocación, aptitudes, circunstancia y potencialidades y aspiraciones que le permiten (a la persona) fijarse razonablemente determinadas expectativas y acceder a ellas".[59]

Los bienes jurídicos mencionados, merecedores de protección penal tienen su fundamento en la dignidad de las personas, pues ésta es el derecho del cual derivan todos los demás. Dado que los derechos humanos se encuentran relacionados entre sí, no puede existir uno de ellos, sin el de dignidad de las personas.

3.5.3.2 Privacidad

El concepto de derecho a la privacidad puede definirse como aquél que todo individuo tiene a separar aspectos de su vida privada del escrutinio público.[60] Hay conductas o espacios que, en principio, no le concierne a la autoridad, y no pueden hacerse del conocimiento público, pues corresponde a cada persona decidir al respecto, sin que nadie pueda reclamar su divulgación.[61]

El interior del domicilio, las relaciones familiares, el cuerpo de las personas, su estado de salud, información financiera, las comunicaciones, inclusive los secretos industriales merecen protección, pues son en principio aspectos privados que merecen protección, hasta en tanto no se vulnere alguna disposición legal.

3.5.3.3 Información

La información es el bien jurídico por excelencia de los delitos informáticos. Proviene del Latín *Informatio-onis*, acción y efecto de informar o informarse.[62] Es el "Conjunto

---

[59] Corte IDH, Caso Loayza Tamayo vs. Perú, fondo, sentencia de 17 de septiembre de 1997, Serie C No. 33. En sentido similar, Caso de los "Niños de la Calle" (Villagrán Morales y otros) vs. Guatemala, fondo, sentencia de 19 de noviembre de 1999, Serie C No. 63.

[60] García Ricci, Diego *Artículo 16 constitucional. Derecho a la Privacidad*, México, Suprema Corte de Justicia de la Nación, 2014, p.1, *https://archivos.juridicas.unam.mx/www/bjv/libros/8/3567/39.pdf. Consultado el* 06 de febrero de 2019.

[61] Muñozcano Eternod, Antonio, *El derecho a la intimidad frente al derecho a la información*, México, Porrúa, 2010, p. 3.

[62] Real Academia Española, "Información", *http://buscon.rae.es/draeI/*. Consultado el 06 de febrero de 2019.

de datos o conocimientos, a los que habiéndoseles dado forma y estructura determinada traen consigo un mensaje".[63]

La información para muchas personas y empresas constituye su objeto de trabajo; empresas con grandes bases de datos tienen especial cuidado en implementar medidas de protección para evitar su pérdida o manipulación; por ejemplo; los procesos de control interno, los inventarios, información contable, financiera y comercial, etcétera.

Especial relevancia en este aspecto constituyen los activos de información que la norma ISO 27001 entiende como los recursos necesarios para que la empresa funcione y consiga los objetivos que se ha propuesto la alta dirección.

Con el marco jurídico en materia de Protección de Datos Personales información en posesión de particulares y de sujetos obligados también entra en juego la privacidad de la información. El secreto bancario, fiscal, los secretos industriales son un claro ejemplo de ello, máxime cuando dado el avance de las nuevas tecnologías todo ello es almacenado electrónicamente.

Hoy en día, delitos como la violación de comunicaciones privadas, violación al secreto industrial, fiscal y bancario, se realizan en las más de las veces mediante aparatos o dispositivos electrónicos.

3.5.3.4 Patrimonio

El patrimonio es el conjunto de poderes y deberes, apreciables en dinero, que tiene una persona; tiene dos elementos: activo y pasivo; el activo se constituye por el conjunto de bienes y derechos; el pasivo por las cargas y obligaciones susceptibles de una apreciación pecuniaria.[64] "En Derecho Civil el patrimonio es el conjunto de

[63] Soto Gama, Daniel, *Principios Generales del derecho a la Información*, México, Instituto de Transparencia y Acceso a la Información Pública del Estado de México y Municipios, 2010, *http://www.infoem.org.mx/sipoem/ipo_capacitacionComunicacion/pdf/pet_tesis_003_2009.pdf. Consultado el* 06 de febrero de 2019.

[64] López Monroy, José de Jesús, *Diccionario Jurídico*, Instituto de Investigaciones Jurídicas de la Universidad Nacional Autónoma de México, México, Porrúa, 2004, Tomo II, p. 2353.

bienes, derechos, obligaciones y cargas apreciables en dinero, que constituyen una universalidad jurídica y que pertenecen a una persona física o moral."[65]

Delitos como el fraude, se realizan en las más de las veces, utilizando a la informática como medio para alcanzar los fines. Conductas como el *phishing* o *pharming*, pretenden engañar a personas para obtener su información y acceder a los sistemas bancarias y sustraer su patrimonio.

3.5.3.5 Protección de menores

No cabe duda que los menores deben gozar protección legal, su estabilidad, su normal desarrollo psicológico y sexual debe ser tutelado como el valor más preciado de la sociedad.

El Artículo 3, párrafo I, de La Convención de los Derechos del Niño, adoptada por la Asamblea General de las Naciones Unidas, el 20 de noviembre de 1989, establece que: "En todas las medidas… que tomen las instituciones públicas o privadas de bienestar social, los tribunales, las autoridades administrativas o los órganos legislativos, una consideración primordial a que se atenderá será el interés superior del niño".

El artículo 4, noveno párrafo de la Carta Magna establece:

> En todas las decisiones y actuaciones del Estado se velará y cumplirá con el principio del interés superior de la niñez, garantizando de manera plena sus derechos. Los niños y las niñas tienen derecho a la satisfacción de sus necesidades de alimentación, salud, educación y sano esparcimiento para su desarrollo integral. Este principio deberá guiar el diseño, ejecución, seguimiento y evaluación de las políticas públicas dirigidas a la niñez.

Es muy lamentable que en la actualidad se aprovechen las nuevas tecnologías y más concretamente el uso del internet para la realización de conductas delictivas como la pornografía infantil. Nuevas conductas han surgido

[65] Reynoso Dávila, Roberto, *Delitos patrimoniales*, México, Porrúa, 2001, p. 1.

como el *grooming*, especie de acoso sexual cometido a través el internet en contra de menores, por personas mayores con identidad falsa, con la finalidad de obtener imágenes pornográficas y extorsionarlos.

3.5.3.6 Seguridad nacional

La seguridad nacional no tiene un significado preciso, generalmente se refiere a "todos aquellos programas, medidas e instrumentos que cierto Estado adopta para defender a sus órganos supremos de un eventual derrocamiento violento por un movimiento subversivo interno o por una agresión externa".[66]

En los términos del artículo 3 de la Ley de Seguridad Nacional, son las acciones destinadas de manera inmediata y directa a mantener la integridad, estabilidad y permanencia del Estado Mexicano, que conlleven a:

> I.- La protección de la nación mexicana frente a las amenazas y riesgos que enfrente nuestro país;
>
> II.- La preservación de la soberanía e independencia nacionales y la defensa del territorio;
>
> III.- El mantenimiento del orden constitucional y el fortalecimiento de las instituciones democráticas de gobierno;
>
> IV.- El mantenimiento de la unidad de las partes integrantes de la Federación señaladas en el artículo 43 de la Constitución Política de los Estados Unidos Mexicanos;
>
> V.- La defensa legítima del Estado Mexicano respecto de otros Estados o sujetos de derecho internacional, y
>
> VI. La preservación de la democracia, fundada en el desarrollo económico social y político del país y sus habitantes.

Por su puesto que las nuevas tecnologías, cuando son mal empleadas para producir actos que conllevan a la desestabilización del Estado, por ejemplo, la utilización de redes sociales para infundir temor a la población que trastoca el orden

[66] Orozco Enríquez, J. Jesús, *Diccionario Jurídico*, *op. cit*., p. 2886.

público, la intervención no autorizada de sistemas de aviación, entre otros, repercute en la seguridad nacional.

3.5.4 Delitos Informáticos que transgreden los Bienes Jurídicos tutelados

Son variados los delitos informáticos existentes. A continuación, se enunciarán algunos y se señalará el bien jurídico que protege cada una de las conductas tipificadas.

3.5.4.1 Revelación de secretos

El artículo 211 Bis del Código Penal Federal, establece como delito la revelación, divulgación o utilización indebida de información o imágenes obtenidas en una intervención de comunicación privada.

El tipo penal tiene como bien jurídico no solo la privacidad, sino también la información misma.

3.5.4.2 Acceso ilícito a sistemas y equipos de informática

El artículo 211 Bis 1 del Código Penal Federal, señala como conducta delictiva la modificación, destrucción o pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad.

Igual que el delito anterior, el bien jurídico es no solo la privacidad, sino también la información misma.

3.5.4.3 Fraude

En los términos del artículo 386 del Código Penal Federal, existe fraude genérico, cuando mediante el engaño o aprovechamiento del error, una persona se hace ilícitamente de alguna cosa o alcanza un lucro indebido en perjuicio de otra.

Existen muchas conductas que mediante el uso de internet o dispositivos electrónicos, pueden ser fraudulentas, como lo es el *pharming* o *phishing*.

Existe un tipo de fraude informático, previsto en el artículo 231, fracción XIV del Código Penal Federal, cuya conducta consiste en: “para obtener algún beneficio para sí o para un tercero, por cualquier medio accese, entre o se introduzca a los sistemas o programas de informática del sistema financiero e indebidamente realice operaciones, transferencias o movimientos de dinero o valores, independientemente de que los recursos no salgan de la Institución”

Este delito fue creado específicamente para tipificar como delito el acceso ilícito a cuentas bancarias de usuarios de la banca y la sustracción de sus fondos.

No cabe duda, que el bien jurídico tutelado en este delito es el patrimonio.

3.5.4.4 Pornografía Infantil

En términos del artículo 202 del Código Penal Federal, comete el delito de pornografía infantil, quien procure, obligue, facilite o induzca, por cualquier medio, a realizar actos sexuales o de exhibicionismo corporal con fines lascivos o sexuales, reales o simulados, con el objeto de video grabarlos, fotografiarlos, filmarlos, exhibirlos o describirlos a través de anuncios impresos, transmisión de archivos de datos en red pública o privada de telecomunicaciones, sistemas de cómputo, electrónicos o sucedáneos. También la impresión, la reproducción, almacenamiento, distribución, venta, compra, arrendamiento, exposición, publicitación, transmisión, importación o exportación de dicho material.

La pornografía es un serio problema, porque atenta contra la niñez. Es evidente que el bien jurídico tutelado son los derechos del menor, su desarrollo psicológico y sexual.

3.5.4.5 Terrorismo

Esta conducta se encuentra tipificada en el artículo 139 del Código Penal Federal, y se comete cuando se utilizan sustancias tóxicas, armas químicas, biológicas o similares, material radioactivo, material nuclear, combustible nuclear, mineral radiactivo, fuente de radiación o instrumentos que emitan radiaciones, explosivos,

o armas de fuego, o por incendio, inundación o por cualquier otro medio violento, para la realización de actos en contra de bienes o servicios, ya sea públicos o privados, o bien, en contra de la integridad física, emocional, o la vida de personas, que produzcan alarma, temor o terror en la población o en un grupo o sector de ella, para atentar contra la seguridad nacional o presionar a la autoridad o a un particular, u obligar a éste para que tome una determinación.

Desafortunadamente, hoy en día, existen muchos ejemplos de terrorismo en el mundo, pero México no ha sido uno de los países en que haya impactado en forma constante esta conducta.

El objetivo de terrorista es producir alarma, temor o terror en la población o en un grupo o sector de ella. Para ello, en muchas de las veces se valen de las nuevas tecnologías, pues a través del internet difunden mensajes que producen pánico en la sociedad, lo cual impacta en el normal funcionamiento social, económico y político de la sociedad, generando una merma en la democracia.

Los bienes jurídicos tutelados son la seguridad nacional y la estabilidad nacional.

3.6 La Criptomoneda como medio comisivo de delitos informáticos

Dentro de la teoría jurídica del delito, el delito es una conducta típica, antijurídica y culpable. En la tipicidad existen los elementos objetivos, normativos y subjetivos del tipo. Los primeros, revelan todas aquellas externalidades perceptibles por los sentidos; como son, sujeto, objeto material, resultado, nexo causal, medios comisivos, entre otros.

Los medios comisivos por medio de los cuales se desarrolló la conducta típica siempre están presentes cuando se materializa la misma. Un aspecto especialmente importante en mencionar es que éstos pueden estar o no descritos en la ley. Cuando el legislador establece un especial medio comisivo en el tipo para afirmar la existencia de la conducta típica, deberá estar probada la actualización de éste en la carpeta de investigación correspondiente.

Lo anterior, no significa que en todos los casos el tipo penal deba o requiera de un medio comisivo específico, sino por el contrario, muchas conductas típicas no requieren de un medio comisivo específico, lo que provoca que el resultado pueda obtenerse por cualquier medio comisivo.

Por ejemplo, el delito de robo no requiere un medio comisivo específico, como en cambio, sí lo requiere el delito de fraude, pues este último solo puede cometerse mediante el engaño o aprovechamiento del error.

Los delitos informáticos mediante el uso de criptomonedas son informáticos, pues las conductas realizadas con las mismas, se utilizan las computadoras como medio para la comisión de conductas penalmente relevantes y la información que se obtiene a través de ellas sirve, para la obtención ilícita de un lucro o beneficio económico en tratándose de un delito patrimonial o fiscal.

Con las criptomonedas pueden cometerse múltiples delitos, pues al representar de facto un valor económico, se usan como medio para obtener el pago en delitos como el fraude, extorsión, robo, secuestro, etcétera, pues los sujetos activos con conocimientos técnicos y aprovechando que la tecnología *Blockchain* permite el anonimato, exigen entregas de cantidades en criptomonedas aprovechándose de internet.

En ese sentido, las criptomonedas son las herramientas con las que los sujetos se han valido para la realización de actividades con contenido económico y que son reprochables desde el punto de vista legal.

Como se advierte de manera inmediata, estos delitos no contienen algún medio comisivo en concreto, relacionado con las cantidades que deban ser entregadas, o con el daño o perjuicio causado, pero se realizan teniendo como medio comisivo la criptomoneda.

En la nueva Ley Fintech, se establecieron diversos delitos y algunos de ellos relacionados con criptomonedas, pero es importante mencionar aquí que existen tipos penales que ya establecen a la misma como elementos objetivos, bien sea como medio comisivo o como objeto.

Capítulo 4

Los actos de investigación relacionados con la Criptomoneda

Capítulo 4. Los actos de investigación relacionados con la Criptomoneda

Los delitos realizados mediante el empleo de criptomonedas requieren de una investigación compleja por parte del Ministerio Público, pues es quien tiene ese deber en términos del artículo 21 constitucional.

La complejidad radica en que con base en el nuevo proceso penal acusatorio y oral, el órgano investigador tiene el deber de realizar sus actos de investigación con base en los principios del sistema, respetando los derechos del imputado y de la víctima en los términos del artículo 20, apartados A, B y C constitucional y de conformidad con el Código Nacional de Procedimientos Penales.

En los delitos fiscales, el sujeto pasivo es el Estado y el activo el contribuyente quien al realizar operaciones mediante el uso de criptomonedas debe pagar los impuestos correspondientes, pero el ministerio público está obligado a observar los derechos fundamentales del particular al realizar su investigación, procurando que sus actos están ajustados conforme a las disposiciones constitucionales y legales.

Las técnicas de investigación cuando en los delitos fiscales se realizan mediante criptomonedas encierran un problema complejo, pues la información financiera como punto de partida para establecer la existencia del hecho que la ley marca como delito y la probabilidad de que el imputado intervino en su realización, es privada y protegida por el artículo 16 constitucional.

No obstante, no todos los actos de investigación inciden en la esfera de los derechos fundamentales del imputado, pues la actividad pericial para conocer sobre el empleo de la tecnología *blockchain*, la valuación de la criptomoneda y la cuantificación del daño patrimonial al fisco federal son actos de investigación que no contienen una repercusión en algún derecho protegido en favor del contribuyente.

A continuación, después de dar una nota sobre los principios rectores del proceso penal y sus etapas, se analizará la problemática del derecho fundamental

de privacidad en la información financiera y se establecerán qué actos son sujetos de control judicial.

4.1 El Proceso Penal Acusatorio y Oral

Con motivo del Decreto por el que se reforman los artículos 16, 17, 18, 19, 20, 21, 22; las fracciones XXI y XXIII del artículo 73; la fracción VII del artículo 115, y la fracción XIII del apartado B del artículo 123, todos de la Constitución Política de los Estados Unidos Mexicanos en materia de seguridad y justicia pena, mediante el cual se establecen las bases del nuevo Sistema de Justicia Penal en la República Mexicana, se implementó el nuevo sistema procesal penal acusatorio, dejando atrás el sistema tradicional que regía en el país. Posteriormente, por decreto publicado en el mencionado medio de difusión el día 5 de marzo de 2014, se expidió el Código Nacional de Procedimientos Penales, mismo que es de aplicación tanto a nivel federal como estatal.

Los principios que rigen al sistema procesal penal acusatorio son los siguientes:

1. Publicidad consistente en que las audiencias son públicas, con el fin de que accedan no sólo las partes que intervienen en el procedimiento, sino también el público en general, pues es una garantía de los sujetos en conflicto y la propia sociedad para la transparencia de las actuaciones judiciales, con las excepciones previstas la Ley, como son la protección a la intimidad y privacidad de la víctima, derechos de terceros, secretos industriales, información de seguridad nacional o pública. En todo caso, nunca podrá ser secreto para la acusación, la víctima, el imputado o su defensa.[67]
2. Inmediación que se traduce en que las audiencias deben desarrollarse íntegramente en presencia del Órgano jurisdiccional, así como de las partes que deban de intervenir en la misma, para que el primero reciba la información y las pruebas relacionadas con los hechos atribuidos al

[67] Eloy Morales Brand, José Luis, *Proceso Penal Acusatorio y Litigación Oral,* México, Rechtikal, 2014, p. 103.

imputado. Esto es, el Juez debe recibir la la prueba y los alegatos de los sujetos procesales en forma directa, sin interposición de cosa o persona.[68]

3. Contradicción que significa que las partes puedan conocer, controvertir o confrontar los medios de prueba, así como oponerse a las peticiones y alegatos de la otra parte. Este principio incluye la posibilidad de defensa, pues en virtud del principio de presunción de inocencia, la asistencia del abogado defensor debe existir en todo momento y nada puede ser ocultado al imputado para que controvierta y se defienda con igualdad procesal.[69]
4. Concentración para que las audiencias se desarrollarán preferentemente en un mismo día o en días consecutivos hasta su conclusión, esto es, que todas las actuaciones se lleven a cabo en una misma audiencia donde las partes proponen y el juez resuelve en forma inmediata.[70]
5. Continuidad ya que las audiencias deben llevarse a cabo de forma continua, sucesiva y secuencial, esto es, que debe privilegiarse su desarrollo integralmente.[71]

La oralidad no es un principio sino una característica del sistema y consiste en que las etapas procesales se desarrollan principalmente de esta manera y no por escrito, concretamente, las audiencias son orales y las partes no pueden en principio leer documentos completos, salvo los casos que dispone la ley.

Existen otros principios que son aplicables al sistema para asegurar el debido proceso, como son: legalidad, presunción de inocencia, igualdad, prohibición de doble enjuiciamiento, además existen principios adicionales relacionados con el régimen probatorio, como son: Libertad de prueba, Licitud de Prueba, y Libre valoración de prueba

[68] *Ibidem*, p. 100.
[69] *Ibidem*, p. 102.
[70] *Ibidem*, p. 103.
[71] *Ibidem*, p. 105.

Diferencias del procedimiento acusatorio con el procedimiento tradicional.

	Procedimiento Acusatorio	**Procedimiento Tradicional**
1	El Procedimiento acusatorio es de origen insular (Gran Bretaña) y propio del sistema de derecho común (*common law*)	El Procedimiento tradicional es de origen continental (Europa continental) propio del sistema romano canónico.
2	El Control de la información que se genera en los actos procesales es preponderantemente horizontal, de ahí la connotación adversarial.	El Control de la información tiene gran verticalidad e intervención directa del tribunal.
3	El Procedimiento Acusatorio toma como motivo conductor la audiencia judicial, esto es, "todo lo no expuesto en la audiencia no obra en el mundo"	El Procedimiento tradicional toma como motivo conductor el expediente, esto es, "lo que no obra en autos, no obra en el mundo"
4	Se privilegia la libertad como situación personal del imputado que enfrentará un proceso penal. Le corresponde al persecutor solicitar la aplicación de instrumentos procesales como providencias precautorias o medidas cautelares	Se privilegia la detención como situación personal del imputado que enfrentará un proceso penal o a quien se le sigue un proceso penal. Le corresponde al imputado solicitar su libertad a través de incidentes como el de libertad provisional bajo caución.
5	Existe un Régimen de libertad de prueba y libre valoración de prueba	Existe un régimen de tasación, respecto a prueba idónea y la forma en la que ha de valorarse.

Cuadro 1: Elaboración propia

Las razones por las cuales México implementó el proceso penal acusatorio y oral, son:

1. Cumplir con compromisos internacionales.
2. La tendencia existente en Latinoamérica que había tomado en cuanto al esquema procesal en materia penal.
3. El compromiso de los operadores políticos, esto es, por las decisiones tomadas y plasmadas en la propia constitución.

Las etapas del procedimiento penal son:

Primera. Etapa preliminar (llamada así por su ubicación) o etapa de investigación inicial (por su finalidad). Es competencia del Ministerio Público y del Juez de Control. Inicia con la presentación de una denuncia, querella o requisito equivalente y concluye con una resolución llamada cierre de investigación

Las fases de esta etapa son:

1. Investigación inicial. El propósito es la obtención por parte del Ministerio Público de la información necesaria para posteriormente ir a un tribunal y lograr obtener de este último un auto de vinculación a proceso y, en su caso, las medidas cautelares; o bien, en el caso del imputado y su defensa, evitar que se dicte dicho auto y no se impongan medidas o sean de menor alcance.
2. Investigación complementaria. El propósito es complementar la información para dar margen a una acusación y obtener a final de cuentas la existencia de delito y responsabilidad penal del acusado.

   Cuando el juez dicta el auto de vinculación al proceso, debe fijar un plazo para el cierre de la investigación y con esto termina la fase de investigación inicial e inicia la frase de investigación complementaria. Esta última termina con el cierre de la investigación, para dar margen a la acusación por parte del Ministerio Público.

Segunda. Etapa de preparación de juicio (llamada así por su finalidad) o intermedia (por su ubicación). Es competencia del juez de control.

1. Inicia con la acusación que por escrito formula el Ministerio Público. Si no se presenta la acusación se sobresee el procedimiento, imposibilitando seguir

con la acusación. Ante la existencia de la acusación, el tribunal tendrá por presentada la acusación y correrá traslado a las partes procesales, esto es, a la víctima u ofendido y su abogado, así como al imputado y su abogado defensor, además citará para la celebración de una audiencia intermedia.

2. Concluye con la dictación del auto de apertura a juicio oral. El propósito es adelgazar o disminuir los insumos del proceso, esto es, depurar los elementos que habrán de considerarse en un proceso, como son los hechos, elementos de convicción y el derecho.

Tercera. Etapa final (por su ubicación) o de juicio (por su finalidad). Es competencia del juez o tribunal oral. Una vez que el Juez de Control haya dictado auto de apertura a juicio oral, lo deberá remitir al juez o tribunal competente y distinto del Juez de Control.

Esta etapa Inicia con el auto de radicación por parte del Juez de enjuiciamiento, donde se pronunciará respecto a la recepción del auto de apertura, la citación a la audiencia de debate del juicio a los sujetos procesales a los órganos de prueba que deben comparecer (testigos y/o peritos) y el señalamiento del día y hora en que se deberá llevar a cabo la audiencia de juicio.

En la audiencia de debate de juicio oral, las partes alegarán y desahogarán las pruebas que les fueron admitidas. El juez emitirá su fallo valorando libremente las pruebas desahogadas en forma oral y condenará o absolverá, según sea el caso. Posteriormente, en el caso de un fallo condenatorio, el Juez de enjuiciamiento citará a una audiencia de sentencia de imposición de penas y graduación de sanciones.

4.2 Actos de Investigación

El objetivo de la investigación es la obtención de información, para ello el Ministerio Público debe realizar actos de investigación para advertir los datos que establezcan que se ha cometido un hecho que la ley señala como delito y que exista la probabilidad de que el imputado intervino en su comisión.

> A lo largo de la investigación, pueden ocurrir técnicas de investigación y actos de investigación, que el CNPP distingue, aunque de manera deficiente pues no lo hace bajo una metodología técnicamente sustentada e incluso resulta imprecisa al regular unos en donde habla de otras; baste ver que, en el capítulo destinado a las técnicas de investigación el CNPP señala los listados de los actos que requieren y de los que no requieren autorización judicial, que más adelante retoma al reglamentar, en título aparte, dichos actos. La dificultad deriva de la reforma constitucional penal 2008 en la parte que establece, en el artículo 16, que los jueces de control resolverán las solicitudes de medidas cautelares, providencias precautorias y técnicas de investigación de la autoridad, que requieran autorización judicial. Así entonces, las técnicas vienen a ser los procedimientos, pericias y habilidades que deberá aplicar el MP o las policías en la realización de los actos; algunas de ellas requieren de previa autorización judicial, otras no.[72]

Para el Código Nacional de Procedimientos Penales son técnicas de investigación: la cadena de custodia; el aseguramiento de bienes, instrumentos, objetos o productos del delito; y el decomiso, cuya regulación se encuentra detallada en los artículos 227 al 250 de dicho ordenamiento legal.

El acto de investigación puede estar o no sujeto a control jurisdiccional. Lo primero es la regla general, pues normalmente los actos de investigación no son de control judicial. El embalaje, las entrevistas, entre otros supuestos que señala el artículo 251 del Código Nacional de Procedimientos Penales, no se requieren de control judicial.

[72] Nader Kuri, Jorge; *La investigación en el Código Nacional de Procedimientos Penales en el Código Nacional de Procedimientos Penales. Estudios*, México, Instituto de Investigaciones Jurídicas de la Universidad Nacional Autónoma de México, *https://archivos.juridicas.unam.mx/www/bjv/libros/9/4032/8.pdf*. Consultado el 03 de enero de 2020.

Requieren de control judicial previo, cuando por la naturaleza de los actos de investigación, se traduzcan en un acto de molestia. El allanamiento (cateo) requiere de un control judicial, la intervención de comunicaciones privadas, entre otros supuestos que señala el artículo 252 del Código Nacional de Procedimientos Penales requieren de control judicial.

El artículo 20, apartado A, fracción IX, establece que "Cualquier prueba obtenida con violación a derechos fundamentales será nula", lo que se traduce en que el Juez deberá excluir toda prueba que se realice en contravención de derechos fundamentales. La razón de la exclusión se basa en las siguientes posiciones.

> I. La necesidad de impedir que la justicia penal deje de ser tal, al fundarse en procedimientos probatorios injustos
>
> II.- De las máximas de la experiencia policial se infiere que todo procedimiento investigativo que sobrepase las normas de respeto y protección de los derechos humanos, no puede aportar verdades jurídicas, sino solo renuncias de derechos por parte de los imputados en beneficio del interés del Estado, lo que obviamente no es garantía alguna de confianza y fidelidad de la evidencia obtenida.
>
> III.- El abrir espacio, so pretexto de la razón de Estado a los métodos policiacos para presentar culpables ofreciendo pruebas a costa de la disminución de las garantías del debido proceso, no es ni más ni menos que instaurar la corrupción operativa en sus agentes y contravenir abiertamente todos los principios y normas de la deontología profesional.[73]

Toda la información que se genera en la investigación, se registra por el Ministerio Público en la carpeta de investigación, en donde obran las entrevistas, documentos e informes periciales, series fotográficas, etcétera.

La *ratio essendi* de la investigación penal es la realización de actos que permitan a las partes allegarse de los elementos, conforme a los cuales se sustente

[73] Ojeda Velázquez, Jorge, *Derecho constitucional Penal*, México, Porrúa, 2011, t. III, p 1560.

a título demostrativo la persecución y la defensa. Registrar y conservar son los objetivos de este tipo de actos, en el entendido de que al contar con la información se estará en aptitud de tomar decisiones durante el curso del proceso.

4.3 La problemática del derecho fundamental de privacidad de la información financiera

El derecho fundamental a la privacidad y protección de datos personales debe ser respetado y garantizado en su efectividad por parte del Estado estableciendo las políticas públicas y el marco normativo por el cual se promuevan, respeten, protejan y garanticen en términos del artículo 1° constitucional.

Es de conocimiento generalizado los diversos casos que han existido en que se vulnera la privacidad y los datos personales de los ciudadanos como el robo de dispositivos móviles con información personal y acceso a internet, así como el espionaje gubernamental a los datos personales de los usuarios y la utilización de esta información para cambiar el pensamiento de votantes, entre otros.

Ante tales eventos, la privacidad y la protección de datos personales se encuentra en entredicho por la falta de educación tecnológica de las personas, por la poca importancia que le otorga el Estado a la protección de estos derechos, así como la falta de regulación y múltiple jurisdicción para la solución de los conflictos.

La privacidad es todo lo que una persona realiza en su ámbito reservado de vida, esto es, que cierta información propia no se encuentre dentro del alcance de otras personas, en virtud de la confidencialidad de la misma.

El ser humano está consciente que conforme pasan los días, la humanidad va evolucionando y de la mano de esta evolución vienen grandes cambios que nuestros antepasados pudieron llegar a considerar como imposibles, éstos pueden ser culturales, regionales, políticos o sociales y su principal detonante son los de tipo tecnológico.

Como es bien sabido, el crecimiento incipiente de la tecnología acarrea muchas consecuencias en todas las materias y viene de la mano con la implementación de las nuevas Tecnologías de la Información y Comunicación, así

como de la difusión masiva de datos compartidos por medio del internet, cuya práctica ha hecho que cada vez sea más común lidiar con la falta de privacidad.

El concepto de privacidad que antes conocíamos no puede ser el mismo al de la actualidad, ya que se pasó de tener que lidiar solamente con la gente indiscreta a hoy tener que proteger nuestro derecho a la privacidad, establecido en el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos. Este derecho a la privacidad, que se conocía como "derecho a no ser molestado" o "derecho a controlar la información propia" está compuesto de un elemento esencial, consistente en que el individuo debe poder tener el control sobre sus propios datos e información privada.

La Segunda Sala de la Suprema Corte de Justicia de la Nación con relación al derecho fundamental de la privacidad, sostuvo que el artículo 16 constitucional establece que la garantía de seguridad jurídica de todo gobernado a no ser molestado en su persona, familia, papeles o posesiones, sino cuando medie mandato de autoridad competente debidamente fundado y motivado, de lo que deriva la inviolabilidad del domicilio, cuya finalidad primordial es el respeto a un ámbito de la vida privada personal y familiar que debe quedar excluido del conocimiento ajeno y de las intromisiones de los demás, con la limitante que la Constitución Política de los Estados Unidos Mexicanos establece para las autoridades. Además, precisó que en un sentido amplio, dicho derecho fundamental puede extenderse a una protección que va más allá del aseguramiento del domicilio como espacio físico en que se desenvuelve normalmente la privacidad o la intimidad, de lo cual deriva el reconocimiento en dicha disposición, de un derecho a la intimidad o vida privada de los gobernados que abarca las intromisiones o molestias que por cualquier medio puedan realizarse en ese ámbito reservado de la vida.[74]

Es de vital importancia el reconocer que no existe la privacidad como tal, ya que aunque podemos vigilar el contenido de la información que compartimos por

[74] Tesis 2a. LXIII/2008, *Semanario Judicial de la Federación y su Gaceta*, Novena Época, t. XXVII, mayo de 2008, p. 229.

ejemplo, en las redes sociales, no estamos del todo exentos a que alguien pueda acceder a nuestra información personal y vulnerarla al decidir divulgarla, violentando de esta manera nuestra vida privada.

Se han verificado muchas situaciones que han vulnerado la privacidad e intimidad de las personas como consecuencia de no existir una efectiva protección de los datos personales de estas. Uno de los casos que puede desarrollarse a partir de la invasión a la privacidad de una persona y provocado por lo dependientes que somos los seres humanos a los dispositivos tecnológicos es cuando a alguien le roban su teléfono celular, ya que esa persona no solamente se está quedando en ese momento sin su equipo, contactos o correos, sino también lo están privando de fotografías, documentos y demás información privada como números de cuentas bancarias y los datos históricos de las ubicaciones compartidas por medio de las aplicaciones con acceso a internet.

Otro de los casos conocidos es el de Edward Snowden, quien decidió filtrar que el gobierno de los Estados Unidos de América espiaba a otros gobiernos y los medios de comunicación, teléfonos celulares, *tablets*, computadoras, entre otros de sus ciudadanos.

Fue muy conocido también el caso de *Cambridge Analytica*, quien por medio de aplicaciones obtenía datos personales proporcionados directamente por los usuarios para así comercializarlos e inferir perfiles psicológicos de cada usuario, con lo cual se logró saber cuál debía ser el contenido, tono y tema de un mensaje para influir en ellos y poder así cambiar su manera de pensar.

Igual de grave es el caso en que una persona irrumpe en las redes sociales de otra y sustrae sus datos personales para realizar fraudes, suplantar su identidad y robo de información de sus contactos.

Ahora bien, en cuanto a los delitos cometidos mediante el uso de criptomonedas la información bancaria y financiera es esencial, pues es necesario conocer los movimientos de cargo y abono tanto en los monederos virtuales como en los centros de intercambio entre la moneda nacional y las criptomonedas.

En este punto cobra especial el secreto bancario y financiero establecido en los artículos 142 de la Ley de Instituciones de Crédito y 73 de la Ley para Regular las Instituciones de Tecnología Financiera.

Dichas disposiciones establecen lo siguiente:

> ARTÍCULO 142.- La información y documentación relativa a las operaciones y servicios a que se refiere el artículo 46 de la presente Ley, tendrá carácter confidencial, por lo que las instituciones de crédito, en protección del derecho a la privacidad de sus clientes y usuarios que en este artículo se establece, en ningún caso podrán dar noticias o información de los depósitos, operaciones o servicios, incluyendo los previstos en la fracción XV del citado artículo 46, sino al depositante, deudor, titular, beneficiario, fideicomitente, fideicomisario, comitente o mandante, a sus representantes legales o a quienes tengan otorgado poder para disponer de la cuenta o para intervenir en la operación o servicio.
>
> Como excepción a lo dispuesto por el párrafo anterior, las instituciones de crédito estarán obligadas a dar las noticias o información a que se refiere dicho párrafo, cuando lo solicite la autoridad judicial en virtud de providencia dictada en juicio en el que el titular o, en su caso, el fideicomitente, fideicomisario, fiduciario, comitente, comisionista, mandante o mandatario sea parte o acusado. Para los efectos del presente párrafo, la autoridad judicial podrá formular su solicitud directamente a la institución de crédito, o a través de la Comisión Nacional Bancaria y de Valores.
>
> Las instituciones de crédito también estarán exceptuadas de la prohibición prevista en el primer párrafo de este artículo y, por tanto, obligadas a dar las noticias o información mencionadas, en los casos en que sean solicitadas por las siguientes autoridades:

(REFORMADA, D.O.F. 17 DE JUNIO DE 2016)

I. El Procurador General de la República o el servidor público en quien delegue facultades para requerir información, para la comprobación del hecho que la ley señale como delito y de la probable responsabilidad del imputado;

(REFORMADA, D.O.F. 17 DE JUNIO DE 2016)

II. Los procuradores generales de justicia de los Estados de la Federación y del Distrito Federal o subprocuradores, para la comprobación del hecho que la ley señale como delito y de la probable responsabilidad del imputado;

(REFORMADA, D.O.F. 17 DE JUNIO DE 2016)

III. El Procurador General de Justicia Militar, para la comprobación del hecho que la ley señale como delito y de la probable responsabilidad del imputado;

(REFORMADA [N. DE E. REPUBLICADA], D.O.F. 17 DE JUNIO DE 2016)

IV. Las autoridades hacendarias federales, para fines fiscales;

V. La Secretaría de Hacienda y Crédito Público, para efectos de lo dispuesto por el artículo 115 de la presente Ley;

VI. El Tesorero de la Federación, cuando el acto de vigilancia lo amerite, para solicitar los estados de cuenta y cualquier otra información relativa a las cuentas personales de los servidores públicos, auxiliares y, en su caso, particulares relacionados con la investigación de que se trate;

VII. La Auditoría Superior de la Federación, en ejercicio de sus facultades de revisión y fiscalización de la Cuenta Pública Federal y respecto a cuentas o contratos a través de los cuáles se administren o ejerzan recursos públicos federales;

VIII. El titular y los subsecretarios de la Secretaría de la Función Pública, en ejercicio de sus facultades de investigación o

auditoría para verificar la evolución del patrimonio de los servidores públicos federales.

La solicitud de información y documentación a que se refiere el párrafo anterior, deberá formularse en todo caso, dentro del procedimiento de verificación a que se refieren los artículos 41 y 42 de la Ley Federal de Responsabilidades Administrativas de los Servidores Públicos, y

IX. La Unidad de Fiscalización de los Recursos de los Partidos Políticos, órgano técnico del Consejo General del Instituto Federal Electoral, para el ejercicio de sus atribuciones legales, en los términos establecidos en el Código Federal de Instituciones y Procedimientos Electorales. Las autoridades electorales de las entidades federativas solicitarán y obtendrán la información que resulte necesaria también para el ejercicio de sus atribuciones legales a través de la unidad primeramente mencionada.

Las autoridades mencionadas en las fracciones anteriores solicitarán las noticias o información a que se refiere este artículo en el ejercicio de sus facultades y de conformidad con las disposiciones legales que les resulten aplicables.

Las solicitudes a que se refiere el tercer párrafo de este artículo deberán formularse con la debida fundamentación y motivación, por conducto de la Comisión Nacional Bancaria y de Valores. Los servidores públicos y las instituciones señalados en las fracciones I y VII, y la unidad de fiscalización a que se refiere la fracción IX, podrán optar por solicitar a la autoridad judicial que expida la orden correspondiente, a efecto de que la institución de crédito entregue la información requerida, siempre que dichos servidores o autoridades especifiquen la denominación de la institución, el número de cuenta, el nombre del cuentahabiente

o usuario y demás datos y elementos que permitan su identificación plena, de acuerdo con la operación de que se trate.

Los empleados y funcionarios de las instituciones de crédito serán responsables, en los términos de las disposiciones aplicables, por violación del secreto que se establece y las instituciones estarán obligadas en caso de revelación indebida del secreto, a reparar los daños y perjuicios que se causen.

Lo anterior, en forma alguna afecta la obligación que tienen las instituciones de crédito de proporcionar a la Comisión Nacional Bancaria y de Valores, toda clase de información y documentos que, en ejercicio de sus funciones de inspección y vigilancia, les solicite en relación con las operaciones que celebren y los servicios que presten, así como tampoco la obligación de proporcionar la información que les sea solicitada por el Banco de México, el Instituto para la Protección al Ahorro Bancario y la Comisión para la Protección y Defensa de los Usuarios de Servicios Financieros, en los términos de las disposiciones legales aplicables.

Se entenderá que no existe violación al secreto propio de las operaciones a que se refiere la fracción XV del artículo 46 de esta Ley, en los casos en que la Auditoría Superior de la Federación, con fundamento en la ley que norma su gestión, requiera la información a que se refiere el presente artículo.

Los documentos y los datos que proporcionen las instituciones de crédito como consecuencia de las excepciones al primer párrafo del presente artículo, sólo podrán ser utilizados en las actuaciones que correspondan en términos de ley y, respecto de aquéllos, se deberá observar la más estricta confidencialidad, aun cuando el servidor público de que se trate se separe del servicio. Al servidor público que indebidamente quebrante la reserva de las actuaciones, proporcione copia de las mismas o

de los documentos con ellas relacionados, o que de cualquier otra forma revele información en ellos contenida, quedará sujeto a las responsabilidades administrativas, civiles o penales correspondientes.

Las instituciones de crédito deberán dar contestación a los requerimientos que la Comisión Nacional Bancaria y de Valores les formule en virtud de las peticiones de las autoridades indicadas en este artículo, dentro de los plazos que la misma determine. La propia Comisión podrá sancionar a las instituciones de crédito que no cumplan con los plazos y condiciones que se establezca, de conformidad con lo dispuesto por los artículos 108 al 110 de la presente Ley.

La Comisión emitirá disposiciones de carácter general en las que establezca los requisitos que deberán reunir las solicitudes o requerimientos de información que formulen las autoridades a que se refieren las fracciones I a IX de este artículo, a efecto de que las instituciones de crédito requeridas estén en aptitud de identificar, localizar y aportar las noticias o información solicitadas.

ARTÍCULO 73.- La información y documentación relativa a las actividades y servicios que presten las ITF de conformidad con la presente Ley y las Operaciones que se realicen a través de ellas, tendrá el carácter confidencial, por lo que las ITF, en protección del derecho a la privacidad de sus Clientes que en este artículo se establece, en ningún caso podrán dar noticias o información de las actividades, Operaciones o servicios, sino al mismo Cliente, a sus representantes legales o a quienes tengan otorgado poder para disponer o intervenir en la Operación o servicio.

Como excepción a lo dispuesto en el párrafo anterior, las ITF estarán obligadas a dar las noticias o información a que se

refiere dicho párrafo, cuando lo solicite la autoridad judicial en virtud de providencia dictada en juicio en el que el Cliente sea parte o acusado. Para efectos del presente párrafo, la autoridad judicial podrá formular su solicitud directamente a la ITF, o a través de la CNBV.

Asimismo, las ITF estarán exceptuadas de la prohibición prevista en el primer párrafo de este artículo y, por tanto, obligadas a dar las noticias o información mencionadas, en los casos en que sean solicitadas por las autoridades siguientes:

I. El Procurador General de la República o el servidor público en quien delegue facultades para requerir información, a fin de reunir indicios para el esclarecimiento de los hechos y, en su caso, obtener datos de prueba para sustentar el ejercicio de la acción penal, la acusación contra el imputado y la reparación del daño;

II. Los procuradores generales de justicia o fiscales generales de las entidades federativas o los servidores públicos en quienes deleguen facultades para requerir información, en los términos de las disposiciones a que se refiere el último párrafo del presente artículo, a fin de reunir indicios para el esclarecimiento de los hechos y, en su caso, obtener datos de prueba para sustentar el ejercicio de la acción penal, la acusación contra el imputado y la reparación del daño;

III. El Procurador General de Justicia Militar, a fin de reunir indicios para el esclarecimiento de los hechos y, en su caso, obtener datos de prueba para sustentar el ejercicio de la acción penal, la acusación contra el imputado y la reparación del daño;

IV. Las autoridades hacendarias federales y estatales, para fines fiscales;

V. La Secretaría, para efectos de lo dispuesto en el artículo 58 de la presente Ley;

VI. El Tesorero de la Federación o el servidor público en quien delegue facultades para requerir información, en los términos de las disposiciones a que se refiere el último párrafo del presente artículo, cuando el acto de vigilancia lo amerite, para solicitar los estados de cuenta y cualquier otra información relativa a las cuentas personales de los servidores públicos, auxiliares y, en su caso, particulares relacionados con la investigación de que se trate;

VII. La Auditoría Superior de la Federación o sus homólogas en las entidades federativas, en ejercicio de sus facultades de revisión y fiscalización de la Cuenta Pública Federal o Local y respecto a cuentas o contratos a través de los cuales se administren o ejerzan recursos públicos;

VIII. Las autoridades investigadoras a que se refiere la Ley General de Responsabilidades Administrativas, o sus homólogos en las entidades federativas, para el esclarecimiento de los hechos, siempre que la información respectiva esté relacionada con la comisión de infracciones a que se refiere dicha Ley, y

IX. La Unidad Técnica de Fiscalización del Instituto Nacional Electoral, para el ejercicio de sus atribuciones legales, en los términos establecidos en la Ley General de Instituciones y Procedimientos Electorales. Las autoridades electorales de las entidades federativas solicitarán y obtendrán la información que resulte necesaria para el ejercicio de sus atribuciones legales a través de la Unidad Técnica de Fiscalización del Instituto Nacional Electoral.

Las autoridades mencionadas en las fracciones anteriores solicitarán las noticias o información a que se refiere este artículo en el ejercicio de sus atribuciones y de conformidad con las disposiciones legales que les resulten aplicables.

Las solicitudes a que se refiere el tercer párrafo de este artículo deberán formularse con la debida fundamentación y motivación, y a través de la CNBV. Los servidores públicos y las instituciones señalados en las fracciones I y VII del párrafo tercero de este artículo, y la Unidad Técnica de Fiscalización a que se refiere la fracción IX de dicho párrafo, podrán optar por solicitar a la autoridad judicial que expida la orden correspondiente, a efecto de que la ITF entregue la información requerida, siempre que dichos servidores públicos o autoridades especifiquen la denominación de la ITF, el número de cuenta o de identificación del Cliente, el nombre del Cliente y demás datos y elementos que permitan su identificación plena, de acuerdo con la Operación de que se trate.

En el caso de hechos que presumiblemente pongan en peligro la vida, la libertad o la integridad de las personas, las autoridades mencionadas en las fracciones I y II del párrafo tercero de este artículo, podrán requerir la información o documentación necesaria para actuar de manera inmediata, de acuerdo a los convenios o protocolos de emergencia que se establezcan para tal efecto entre dichas autoridades, agencias gubernamentales involucradas en el combate de este tipo de delitos, la CNBV y las ITF.

Los empleados y funcionarios de las ITF serán responsables, en los términos de las disposiciones jurídicas aplicables, por violación del secreto que se establece y las ITF estarán obligadas en caso de revelación indebida del secreto, a reparar los daños y perjuicios que se causen.

Los documentos y datos que proporcionen las ITF como consecuencia de las excepciones al primer párrafo del presente artículo, solo podrán ser utilizados en las actuaciones que correspondan en términos de ley y, respecto de aquellos, se

deberá observar la más estricta confidencialidad, aun cuando el servidor público de que se trate se separe del servicio. Al servidor público que indebidamente quebrante la reserva de las actuaciones, proporcione copia de las mismas o de los documentos con ellas relacionados, o que de cualquier otra forma revele información en ellos contenida, quedará sujeto a las responsabilidades administrativas, civiles y penales correspondientes.

Lo anterior, no afecta la obligación que tienen las ITF de proporcionar a la CNBV, toda clase de información y documentos que, en ejercicio de sus funciones de inspección y vigilancia, les solicite en relación con las Operaciones y demás actos que celebren y los servicios que presten, así como tampoco la obligación de proporcionar la información que les sea solicitada por otras Autoridades Financieras, en los términos de las disposiciones legales aplicables.

Las ITF deberán dar contestación a los requerimientos que la CNBV les formule en virtud de las peticiones de las autoridades señaladas en este artículo, dentro de los plazos y condiciones que esta determine. La CNBV podrá sancionar a las ITF que no cumplan con los plazos y condiciones que se establezcan en dichos requerimientos, de conformidad con lo dispuesto en las disposiciones del Título VI de la presente Ley.

La CNBV sancionará con multa administrativa de 1 a 15,000 UMA a las ITF por no dar respuesta en los plazos otorgados en el presente artículo para la atención de los requerimientos de información, documentación, aseguramiento, desbloqueo de cuentas, transferencia o situación de fondos formulados por las autoridades competentes señaladas.

La CNBV emitirá las disposiciones de carácter general en las que establezca las formalidades y los requisitos que deberán

> reunir las solicitudes o requerimientos de información que formulen las autoridades a que se refiere este artículo, a efecto de que las ITF requeridas estén en aptitud de identificar, localizar y aportar las noticias o información solicitadas por dichas autoridades.

Del análisis de las disposiciones antes transcritas, se advierte que ambas regulan el secreto financiero y bancario a favor de los usuarios de servicios financieros, con las limitaciones y en los términos que ahí se establecen.

El derecho de los particulares al secreto financiero y bancario se traduce en que las instituciones bancarias deben guardar confidencialidad sobre los datos e información financiera de sus clientes, esto es, no divulgarla a terceros distintos de los propios usuarios.

De los artículos 142 de la Ley de Instituciones de Crédito y 73 de la Ley para Regular las Instituciones de Tecnología Financiera, se advierte que el secreto financiero o bancario guarda relación con la vida privada de los gobernados, en su condición de clientes o deudores de las entidades bancarias, por lo que si bien no está consagrado como tal explícitamente en la Constitución Política de los Estados Unidos Mexicanos, al estar referido a la historia crediticia de aquéllos, puede considerarse como una extensión del derecho fundamental a la vida privada de la persona, familia, domicilio, papeles o posesiones de los gobernados, protegido por el artículo 16, primer párrafo, constitucional.[75]

El secreto financiero y bancario no es absoluto, porque los derechos fundamentales establecidos en la Constitución mexicana encuentran sus límites en la propia carta magna de modo directo y de manera indirecta o mediata en la legislación ordinaria, por la necesidad de preservar otros derechos o bienes protegidos constitucionalmente.

Por tanto, si bien el secreto financiero o bancario está protegido por la garantía de seguridad jurídica contenida en el artículo 16, primer párrafo, de la Carta

[75] Tesis 2a. LXIV/2008, *Semanario Judicial de la Federación y su Gaceta*, Novena Época, t. XXVII, mayo de 2008, p. 234.

Magna, en su vertiente de derecho a la privacidad o intimidad, como ya se ha dado cuenta, se encuentra delimitado por la protección que debe darse a otros bienes o derechos constitucionalmente resguardados, como es el de los bancos o instituciones de crédito, de los usuarios o de las sociedades de información, a tener conocimiento del historial crediticio de sus clientes o deudores a fin de realizar las operaciones propias de su objeto, tal y como se establece en los artículos 2o., 5o. y 20 de la Ley para Regular las Sociedades de Información Crediticia.

Esto es, que las instituciones financieras pueden proporcionar a las Sociedades de Información Crediticia (conocidas como buró de crédito), la información financiera necesaria para conocer el historial crediticio de los clientes para con base en éste, las propias instituciones estén en aptitud de calificar la posibilidad de otorgar créditos a los clientes.[76]

4.4 Actos de investigación que requieren control judicial

Frente a la regla general del deber de confidencialidad de la información y documentación relativa a las actividades y servicios que presten las instituciones financieras y las instituciones de tecnología financieras en protección del derecho a la privacidad de sus clientes que se traduce en la prohibición de dar noticias o información de las actividades, operaciones o servicios, sino al mismo Cliente, a sus representantes legales o a quienes tengan otorgado poder para disponer o intervenir en la operación o servicio; surge las excepciones, a saber:

Primera excepción. Deben proporcionar las noticias o información anteriores, cuando lo solicite la autoridad judicial en virtud de providencia dictada en juicio en el que el Cliente sea parte o acusado por sí o a través de la Comisión Nacional Bancaria y de Valores.

Segunda excepción. Deben proporcionar las noticias o información antes mencionadas, cuando lo soliciten las autoridades siguientes:

[76] Tesis 2a. LXX/2008, *Semanario Judicial de la Federación y su Gaceta*, Novena Época, t. XXVIII, agosto de 2008, p. 57.

1. El Fiscal General de la República o el servidor público en quien delegue facultades para requerir información, a fin de reunir indicios para el esclarecimiento de los hechos y, en su caso, obtener datos de prueba para sustentar el ejercicio de la acción penal, la acusación contra el imputado y la reparación del daño;
2. Los Procuradores Generales de Justicia o Fiscales Generales de las entidades federativas o los servidores públicos en quienes deleguen facultades para requerir información, en los términos de las disposiciones a que se refiere el último párrafo del presente artículo, a fin de reunir indicios para el esclarecimiento de los hechos y, en su caso, obtener datos de prueba para sustentar el ejercicio de la acción penal, la acusación contra el imputado y la reparación del daño;
3. El Procurador General de Justicia Militar, a fin de reunir indicios para el esclarecimiento de los hechos y, en su caso, obtener datos de prueba para sustentar el ejercicio de la acción penal, la acusación contra el imputado y la reparación del daño;
4. Las autoridades hacendarias federales y estatales, para fines fiscales;
5. El Tesorero de la Federación o el servidor público en quien delegue facultades para requerir información, en los términos de las disposiciones a que se refiere el último párrafo del presente artículo, cuando el acto de vigilancia lo amerite, para solicitar los estados de cuenta y cualquier otra información relativa a las cuentas personales de los servidores públicos, auxiliares y, en su caso, particulares relacionados con la investigación de que se trate;
6. La Auditoría Superior de la Federación o sus homólogas en las entidades federativas, en ejercicio de sus facultades de revisión y fiscalización de la Cuenta Pública Federal o Local y respecto a cuentas o contratos a través de los cuales se administren o ejerzan recursos públicos;
7. Las autoridades investigadoras a que se refiere la Ley General de Responsabilidades Administrativas, o sus homólogos en las entidades

federativas, para el esclarecimiento de los hechos, siempre que la información respectiva esté relacionada con la comisión de infracciones a que se refiere dicha Ley, y

8. La Unidad Técnica de Fiscalización del Instituto Nacional Electoral, para el ejercicio de sus atribuciones legales, en los términos establecidos en la Ley General de Instituciones y Procedimientos Electorales. Las autoridades electorales de las entidades federativas solicitarán y obtendrán la información que resulte necesaria para el ejercicio de sus atribuciones legales a través de la Unidad Técnica de Fiscalización del Instituto Nacional Electoral.
9. La Secretaria de Hacienda y Crédito Público para los efectos del artículo 115 de la Ley de Instituciones de Crédito y 58 de la Ley para Regular las Instituciones de Tecnología Financiera.

La segunda excepción antes apuntada resulta particularmente trascendental, toda vez que determina que las autoridades mencionadas puedan acceder a la información financiera que tiene el carácter privado para los clientes y usuarios de los servicios financieros.

Ante esto, cabe cuestionarse si la solicitud que hagan las diversas autoridades antes citadas, debe ser objeto de escrutinio judicial previo, esto es, sujeto a control judicial para su otorgamiento a éstas.

Y es que si se toma en cuenta que la información financiera de los clientes o usuarios financieros es de carácter privada y está protegida por el derecho fundamental de seguridad jurídica establecido en el artículo 16 constitucional, ello significa que la solicitud y eventual entrega por parte de las instituciones financieras e instituciones de tecnología financiera implica la irrupción al derecho a la privacidad de las personas que como derecho humano reconocido en la Constitución debe ser respetado y su eventual transgresión, solo puede ser autorizado por parte de la autoridad judicial y mediante el análisis de la solicitud que haga la autoridad correspondiente para conocer la finalidad del uso de esa información y la necesidad de la medida.

El tema es de mayor trascendencia por cuanto hace a las autoridades investigadoras en materia penal, como lo son la Fiscalía General de la República y las Fiscalías o Procuradurías de las entidades federativas, porque cuando al realizar un acto de investigación que implica afectar la esfera de derechos fundamentales de los particulares, deben necesariamente pasar por escrutinio judicial.

De esta manera, la solicitud de información financiera que realice el Ministerio Público Federal o el de las entidades federativas, además de realizarse a través del Fiscal General o el servidor público en quien delegue esa facultad, debe ser objeto de control judicial, lo que equivale a que las instituciones financieras e instituciones de tecnología financiera otorguen la información, pero previamente, el ministerio público debe contar con la autorización del juez de control, que solo podrá conceder el acceso a la información bancaria y financiera, como excepción al secreto bancario y financiero, si se justifica la necesidad de la medida, esto es, que se demuestre la finalidad perseguida, la relación con el objeto de la investigación penal y su proporcionalidad.

Sobre el tema, la Primera Sala de la Suprema Corte de Justicia de la Nación con relación al artículo 117, fracción II (actualmente 142) de la Ley de Instituciones de Crédito, sostuvo que dicha disposición viola el derecho a la vida privada.

Explicó el máximo tribunal que la disposición legal en comento, que prevé como excepción a la protección del derecho a la privacidad de los clientes o usuarios de las instituciones de crédito, la obligación de dar noticia o información, cuando las autoridades que la soliciten sean los procuradores generales de justicia de los Estados de la Federación y de la ciudad de México o subprocuradores, para la comprobación del cuerpo del delito y de la probable responsabilidad del indiciado, viola el derecho a la vida privada, toda vez que la permisión que otorga dicho precepto a la autoridad ministerial no forma parte de la facultad de investigación de delitos contenida en el artículo 21 de la Constitución Política de los Estados Unidos Mexicanos, ni de la extensión de facultades de irrupción en la vida privada expresamente protegidas por el artículo 16 de la propia Constitución.

También señaló que el acceso a dicha información implica que tenga la potencialidad de afectación del derecho a la autodeterminación de la persona, quien como titular de los datos personales es la única legitimada para autorizar su circulación; de ahí que la solicitud de información bancaria realizada por la autoridad ministerial debe estar precedida de autorización judicial.

Finalizó concluyendo que el carácter previo del control judicial, como regla, deriva del reforzamiento que en la etapa de investigación penal se imprimió al principio de reserva judicial de las intervenciones que afectan derechos fundamentales, toda vez que el lugar preferente que ocupan en el Estado se expresa a través de los controles que deben mediar para su afectación, como lo prevé en el artículo 1o. de la Constitución Federal.[77]

Con base en lo anterior, es posible señalar que los artículos 142 de la Ley de Instituciones de Crédito y 73 de la Ley para Regular las Instituciones de Tecnología Financiera son inconstitucionales en la medida que permiten a la autoridad investigadora penal, la obtención de información financiera y bancaria confidencial protegida por el derecho fundamental de privacidad establecido en el artículo 16 constitucional cuando ello se haga en virtud de la obligación de las instituciones financieras e instituciones de tecnología financieras de proporcionar los datos personales de los clientes y usuarios de servicios financieros.

No es óbice para lo anterior, que el artículo 142 quinto párrafo de la Ley de Instituciones de Crédito, y el diverso artículo 73 de la Ley para Regular las Instituciones de Tecnología Financiera párrafos quinto y sexto, establezcan que además de que las solicitudes de información a las Instituciones financieras e instituciones de tecnología financieras deben formularse con la debida fundamentación y motivación, a través de la Comisión Nacional Bancaria y de Valores, el Fiscal General de la República puede optar por solicitar a la autoridad judicial que expida la orden correspondiente, a efecto de que dichas instituciones entreguen la información requerida, siempre que dichos servidores públicos o

[77] Tesis 1a. LXXI/2018 (10a.), *Gaceta del Semanario Judicial de la Federación,* Décima Época, Libro 55, t. II, junio de 2018, p. 977.

autoridades especifiquen la denominación de la Institución, el número de cuenta o de identificación del Cliente, el nombre del Cliente y demás datos y elementos que permitan su identificación plena, de acuerdo con la operación de que se trate.

Lo anterior, porque dichas porciones normativas al señalar que dichas autoridad “podrán” les otorga un carácter potestativo para acudir ante el Juez de control para la autorización y eventual obtención de la información financiera privada correspondientes, cuando ello debió ser de carácter reglado y no discrecional, esto es, la disposición debió establecer como obligatorio el acudir ante el juez de control en asuntos del orden penal para obtener la autorización correspondiente y acceder a la información financiera confidencial y privada en posesión de las instituciones obligadas a proporcionarlas.

No obstante lo antes expuesto, cabe indicar que las autoridades ministeriales a pesar la inconstitucionalidad de tales disposiciones, se encuentran plenamente en posibilidad de acatar el artículo 16 constitucional y armonizar las mencionadas disposiciones legales con el dispositivo constitucional, respetando el secreto bancario y financiero como manifestación del derecho a la privacidad de las personas.

Efectivamente, las autoridades ministeriales deben de acudir previamente al Juez de Control y obtener la autorización correspondiente justificando la necesidad de la petición para la obtención de la información confidencial y una vez que sea obsequiada dirigirse ante las instituciones financieras e instituciones de tecnología financieras para el acceso a los datos e información de los clientes y usuarios de servicios financieros.

Solo de esta manera se logra el respeto al derecho fundamental de privacidad establecido en la constitución y su extensión en el secreto bancario y financiero, de ahí que a pesar de que las disposiciones legales sean proclives a violar la constitución, las autoridades investigadoras en materia penal tienen a su alcance que sus actos de investigación no sean violatorios de derechos fundamentales, si como se plantea, acudan ante el Juez de Control previamente a solicitar y tener acceso a la información financiera de carácter confidencial.

Lo anterior no es sólo una mera formalidad, pues no contar con la autorización del Juez de Control para el acceso y obtención de la información financiera, con la consecuente violación al derecho de privacidad establecido en el artículo 16 constitucional, genera una consecuencia trascendental, consistente en la nulidad de las actuaciones de e información obtenida con violación a derechos fundamentales.

El artículo 20, apartado A, fracción IX de la Constitución Política de los Estados Unidos Mexicanos establece como uno de los principios del proceso penal que “Cualquier prueba obtenida con violación de derechos fundamentales será nula”. En forma similar, el artículo 346, fracción II del Código Nacional de Procedimientos Penales establece el deber del Juez de Control de excluir los medios de prueba, entre otros casos, cuando “Por haberse obtenido con violación a derechos fundamentales”.

Lo que se traduce en que, si el Ministerio Público en su actuación no obtiene la autorización del Juez de Control para la obtención de la información financiera, estos datos de prueba en la investigación, se habrán obtenido con violación a derechos fundamentales y deben ser excluidos por el Juez de Control en la etapa intermedia y no podrán ser valorados ni tomados en cuenta para el enjuiciamiento del acusado.

No es aquí el momento para realizar un análisis del tema sobre la licitud probatoria, la teoría de los frutos del árbol envenenado y sus excepciones, pero basta decir para efectos de lo comentado hasta el momento, que sin la autorización previa del Juez de Control, los datos de prueba obtenidos con violación a derechos fundamentales son nulos y además por consecuencia, todos los demás datos de prueba obtenidos a partir de éstos, también lo serán.

En ese sentido, la autoridad investigadora penal, en observancia de su deber de investigación establecido en el artículo 21 constitucional, debe cuidar en extremo que la información financiera de carácter confidencial y protegida por el derecho fundamental de privacidad se haya obtenido legalmente, esto es, previa

autorización del Juez de Control, pues de otra manera será nula y nulos también todos los demás datos de prueba que de ella deriven.

De esta manera, la inobservancia de no respetar los derechos fundamentales en la obtención de los datos de prueba, puede viciar toda la investigación y no sólo la nulidad de los obtenidos sin la autorización judicial, pues muy grave es que además toda la información obtenida deriva del conocimiento de la información financiera confidencial, como lo es entrevistas con terceros con los que se tuvo operaciones comerciales, contratos mercantiles, que se conocieron como consecuencia de información financiera corre el riesgo latente de también ser nulos.

Todo lo anterior, impacta en el tema fundamental del presente trabajo, porque para conocer sobre la investigación de una defraudación fiscal con el uso de criptomonedas, necesariamente se necesita de información confidencial protegida por el secreto bancario y financiero.

Efectivamente, es necesario el conocimiento de operaciones civiles y mercantiles mediante el uso de criptomonedas, así como compra y venta de criptomonedas, que muy posiblemente se hicieron sin el pago de los impuestos correspondientes, lo que se logra conocer mediante la información financiera de cargos y abonos en los monederos virtuales de las criptomonedas y reflejados en los estados de cuenta, así como de los movimientos de cargo y abono en los centros de cambio virtuales *exchanges* en donde se comercializan las propias criptomonedas contra los estados de cuenta bancarios.

De ahí que para la investigación de un delito de defraudación fiscal por medio del uso de criptomonedas es absolutamente necesario el acceso a los estados de cuenta de los monederos virtuales, bancos y centros de cambio virtuales *exchanges*, información que sólo podrá accederse mediante la autorización judicial previa como ha quedado expuesto.

4.4.1 El caso de la Unidad de Inteligencia Financiera de la Secretaría de Hacienda y Crédito Público

Hasta aquí lo más importante con relación al tema de la privacidad y sigilo de la información bancaria y financiera y su trascendencia en la investigación penal. Sin

embargo, conviene no cerrar el presente tema sin antes hacer referencia a un tema de actualidad en la vida jurídica del país relacionado con la Unidad de Inteligencia Financiera de la Secretaría de Hacienda y Crédito Público.

Esta Unidad cuenta con las facultades establecidas en los artículos 15 del Reglamento Interior de la Secretaría de Hacienda y Crédito Público, así como del 3º del Reglamento de la Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita. En lo fundamental, sus atribuciones son:

1. Recibir reportes de operaciones financieras y avisos de quienes realizan actividades vulnerables;
2. Analizar las operaciones financieras y económicas y otra información relacionada; y
3. Diseminar reportes de inteligencia y otros documentos útiles para detectar operaciones probablemente vinculadas con el lavado de dinero (LD) o el financiamiento al terrorismo (FT), y en su caso, presentar las denuncias correspondientes ante la autoridad competente.

Existe una atribución adicional, derivada de los artículos 115 de la Ley de Instituciones de Crédito y 58 de la Ley para Regular las Instituciones de Inteligencia Financiera, consistente en expedir la lista de personas bloqueadas a que dichas disposiciones se refieren, facultad que se encuentra en el artículo 15, fracción XXXII del Reglamento Interior de la Secretaría de Hacienda y Crédito Público que establece: “Integrar la lista de personas bloqueadas, prevista en las leyes financieras, incluida la introducción y eliminación de personas en dicha lista, así como emitir los lineamientos, guías o mejores prácticas en la materia a que se refiere esta fracción.”.

Los artículos 115, noveno párrafo y 58 antes de los ordenamientos legales mencionados, establecen lo siguiente:

> Artículo 115…
>
> …

> Las instituciones de crédito deberán suspender de forma inmediata la realización de actos, operaciones o servicios con los clientes o usuarios que la Secretaría de Hacienda y Crédito Público les informe mediante una lista de personas bloqueadas que tendrá el carácter de confidencial. La lista de personas bloqueadas tendrá la finalidad de prevenir y detectar actos, omisiones u operaciones que pudieran ubicarse en los supuestos previstos en los artículos referidos en la fracción I de este artículo.
>
> …
>
> Artículo 58…
>
> …
>
> Las ITF deberán suspender de forma inmediata la realización de actos, Operaciones o servicios con los Clientes que la Secretaría les informe mediante una lista de personas bloqueadas que tendrá el carácter de confidencial. La lista de personas bloqueadas tendrá la finalidad de prevenir y detectar actos, omisiones u Operaciones que pudieran ubicarse en los supuestos previstos en la fracción I del párrafo primero de este artículo.
>
> …

Sobre el tema, la Segunda Sala de la Suprema Corte de Justicia de la Nación al resolver por unanimidad de votos el amparo en revisión número 806/2017, realizó una interpretación conforme del artículo 115 de la Ley de Instituciones de Crédito.

Distinguiendo el motivo que puede generar el bloqueo de cuentas bancarias, y del ejercicio de la facultad contenida en el artículo 115 de la Ley de Instituciones de Crédito –y ahora también el 58 de la Ley para Regular las Instituciones de Tecnología Financiera- en favor de la Unidad de Inteligencia Financiera de la Secretaría de Hacienda y Crédito Público.

En tal contexto, es preciso destacar que existen algunos tratados internacionales de los cuales nuestro país es parte, que establecen la obligación de asegurar determinados bienes, entre los que se encuentran las cuentas bancarias, como lo es la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional, establece en su artículo 12.2 que los Estados Parte: “Adoptarán las medidas que sean necesarias para permitir la identificación, la localización, el embargo preventivo o la incautación de cualquier bien a que se refiera el párrafo 1 del presente artículo con miras a su eventual decomiso”.

Entre las conductas a que se refiere la anterior obligación, se encuentra el “blanqueo de dinero”, tal y como se desprende de los artículos 6 y 7 de la propia Convención, aunado a que, en términos del numeral 13 de la misma, existe una obligación de cooperación internacional para fines de decomiso cuando exista una solicitud proveniente de otro Estado Parte.

Ello sin que para la Segunda Sala pasara desapercibido que la citada Convención indica que el “blanqueo de dinero” es un delito. Sin embargo, dicha sala reiteró que la acción de bloqueo de cuentas con motivo de una solicitud extranjera será de índole administrativa, con independencia de que tenga consecuencias penales en el país en que se generó.

En esas condiciones, es posible concluir que, en el supuesto de que el bloqueo de cuentas realizado a partir del contenido del artículo 115 de la Ley de Instituciones de Crédito –y también el artículo 58 de la Ley para Regular las Instituciones de Tecnología Financiera-, tenga como origen el cumplimiento de una resolución o pronunciamiento de un organismo internacional o bien, el cumplimiento de una obligación bilateral o multilateral asumida por nuestro país, no implica una invasión de facultades conferidas a la figura del Ministerio Público, ya que se realiza en cumplimiento a una solicitud internacional, lo cual, es de índole administrativo, con independencia de las consecuencias penales que ello implique en el país en que se origina la solicitud.

No obstante ello, no se satisface cuando el bloqueo de cuentas se realiza para cuestiones estrictamente nacionales, en tanto en estos supuestos,

efectivamente la medida cautelar no se impondría en relación con un procedimiento específico y determinado, aspecto que trastoca su validez constitucional.

Por ende, dichas consideraciones son aplicables cuando la Unidad de Inteligencia Financiera ejerce las atribuciones establecidas en el artículo 115 de la Ley de Instituciones de Crédito y 58 de la Ley para Regular las Instituciones de Tecnología Financiera en uso de la facultad que le confiere el artículo 15, fracción XXXII del Reglamento de la Secretaría de Hacienda y Crédito Público, para el bloqueo de cuentas bancarias y suspensión de operaciones bancarias y financieras con los usuarios de tales servicios, por guardar relación con la comisión del delito de operaciones con recursos de procedencia ilícita.

Asimismo, la Segunda Sala del Alto Tribunal en sesiones de catorce y veintidós de marzo, dieciocho de abril y diecinueve de mayo, todos de dos mil dieciocho, resolvió por unanimidad los diversos amparos en revisión 1150/2017, 1181/2017, 1231/2017 y 124/2018, de la que derivó una jurisprudencia,[78] donde se pone de manifiesto que el contenido del artículo 115 de la Ley de Instituciones de Crédito y 58 de la Ley para Regular las instituciones de Inteligencia Financiera, así como diversas disposiciones de carácter general que de él emanan, no son inconstitucionales, pero en una interpretación conforme, tienen aplicación únicamente en tratándose de solicitudes derivadas de procedimientos internacionales y no así, para el ámbito de autoridades locales, por lo que no pueden solicitar un bloqueo de cuentas bancarias con base en estas normas.

Lo anterior, al considerar que la atribución de la Unidad de Inteligencia Financiera de la Secretaría de Hacienda y Crédito Público, consistente en el bloqueo de cuentas a los clientes y usuarios de servicios financieros, únicamente puede emplearse como medida cautelar relacionada con los procedimientos relativos al cumplimiento de compromisos internacionales asumidos en nuestro país, lo cual se actualiza ante dos escenarios, a saber:

[78] Jurisprudencia 2a./J. 46/2018 (10a.), Gaceta del Semanario Judicial de la Federación, Décima Época, Libro 54, t. II, mayo de 2018, p. 1270.

1. Ya sea por el cumplimiento de una obligación de carácter bilateral o multilateral asumida por México, en la cual se establezca de manera expresa la obligación compartida de implementar este tipo de medidas ante solicitudes de autoridades extranjeras; o bien,

2. Por el cumplimiento de una resolución o determinación adoptada por un organismo internacional o por una agrupación intergubernamental, que sea reconocida con tales atribuciones por nuestro país a la luz de algún tratado internacional –a manera de ejemplo, para el cumplimiento de las resoluciones que en materia de terrorismo y proliferación de armas de destrucción masiva emite el Consejo de Seguridad de la Organización de Naciones Unidas–.

De ahí que la citada atribución, no puede emplearse cuando el motivo que genere el bloqueo de las cuentas tenga un origen estrictamente nacional, esto es, que no se realice para el cumplimiento de un compromiso internacional.

Inclusive, sobre el tema de la suspensión del acto reclamado, en Jurisprudencia[79] la misma Segunda Sala sostuvo que es procedente conceder la medida cautelar atendiendo a una ponderación del interés social, la no contravención a disposiciones de orden público así como al principio de apariencia del buen derecho. Sin embargo, dicha suspensión debe concederse de manera condicionada, esto es, no surtirá efectos si el bloqueo se emitió en cumplimiento de una obligación contraída con un gobierno extranjero o la ejecución de una resolución adoptada por un organismo internacional o agrupación intergubernamental cuyas atribuciones fueron reconocidas con base en una obligación asumida por el Estado mexicano.

Ahora bien, considerando la Jurisprudencia emitida por el máximo Tribunal del país, la Unidad de Inteligencia financiera solo puede hacer uso de su facultad de incluir en la lista de personas bloqueadas cuando éstas se encuentren relacionadas con el delito de operaciones con recursos de procedencia ilícita y

[79] Jurisprudencia 2a./J. 87/2019 (10a.), Gaceta del Semanario Judicial de la Federación, Décima Época Libro 66, t. II, mayo de 2019, 1270.

lavado de dinero establecido en el artículo 400 bis del Código Penal Federal y en cumplimiento de una resolución o determinación adoptada por un organismo internacional o por una autoridad extranjera y no cuando ello derive de una circunstancia estrictamente nacional.

A juicio del que suscribe, la diferencia en que la petición del bloqueo de activos, derechos, cuentas bancarias, etcétera, derive de una autoridad extranjera y no nacional no parece un criterio válido de distinción para considerar que en el primer caso se transgredió el principio de seguridad jurídica y en el segundo caso no.

El problema medular en lo que al presente trabajo se refiere, es que esta facultad de la Unidad de Inteligencia Financiera conlleva necesariamente el conocimiento de la información bancaria y financiera de las personas, lo que como se ha visto está protegido por el derecho fundamental de privacidad de y protección de datos personales, pues para bloquear las operaciones con las instituciones bancarias y financieras, evidentemente se necesita saber de los movimientos de cargo y abono.

Si dicha autoridad tiene conocimiento de los cargos y abonos y demás datos bancarios y financieros protegidos por el secreto bancario, debe considerarse que es necesaria autorización judicial previa para tal efecto y además al ser el Ministerio Público el órgano investigador, es este último quien debe realizar la solicitud correspondiente.

Si la Unidad de Inteligencia Financiera accede a la información bancaria y financiera sin que el Ministerio Público la haya solicitado ante el Juez de Control y la aporta en una carpeta de investigación, se corre el grave riesgo de que en un caso concreto la defensa solicita la ilicitud de los datos de prueba y el Juez no tendrá otra opción que considerarlos sin validez probatoria.

En todo caso, mientras no exista una solicitud de modificación de Jurisprudencia y/o modificación del marco legal y reglamentario, en los términos en que se encuentra el actual artículo 21 constitucional, la mencionada autoridad hacendaria debe presentar la querella correspondiente, aportar los datos de prueba

al Ministerio Público, y solicitar a éste que pida al Juez de Control la información financiera para que con los demás documentos, determinar sobre la necesidad de suspender las operaciones con el sistema bancario y financiero, así como bloquear las cuentas bancarias, pues de otra manera sería inconstitucional.

4.5 Actos de investigación que no requieren control judicial

No todos los actos de investigación requieren control judicial previo, pues como se indicó, el punto de partida para determinar si un acto requiere control judicial es la incidencia que el mismo pueda tener en los derechos fundamentales.

Así, por ejemplo, una orden de cateo requiere control judicial previo, porque inciden en la inviolabilidad del domicilio, un acceso a un teléfono móvil, también requiere control judicial, porque implica irrumpir en la privacidad de las personas.

Pero actos de investigación como entrevistas, inspección de lugares abiertos, etcétera; no requieren de control judicial alguno, pues no está en entredicho alguna vulneración de derechos fundamentales.

En los delitos fiscales, cobra especial relevancia la determinación del daño al fisco federal, lo cual en términos del artículo 92 fracción I del Código Fiscal de la Federación se realiza mediante la formulación de la querella correspondiente y en los términos del quinto párrafo de dicha disposición, la propia autoridad debe hacer la cuantificación correspondiente del daño o el perjuicio causado al fisco federal.

Asimismo, para la comprobación del delito de defraudación fiscal mediante el empleo de criptomonedas, se requiere el conocimiento cierto del valor de ésta, así como el empleo de la tecnología *blockchain* sobre la que descansa.

Tanto la determinación del daño a la hacienda pública, como la valuación de la criptomoneda y el empleo de la tecnología *blockchain* sólo puede comprobarse mediante dictámenes periciales en los que de manera técnica y con profesionistas calificados se determinen tales aspectos, pues en términos del artículo 368 del Código Nacional de Procedimientos Penales, la prueba pericial es necesaria cuando para el examen de personas, hechos, objetos o circunstancias relevantes para el

proceso, fuere necesario o conveniente poseer conocimientos especiales en alguna ciencia, arte, técnica u oficio.

En razón de lo anterior, para constatar el daño a la hacienda pública es necesaria la intervención de un profesionista en contabilidad que por sus conocimientos en la técnica contable analice la información financiera del contribuyente y cuantifique el monto de la obligación fiscal no pagada, esto es, de las contribuciones omitidas.

De igual forma, es imprescindible la intervención de un profesionista en sistemas computacionales para conocer de manera cierta la utilización de la tecnología *blockchain* con la cual se emplearon las criptomonedas con las características técnicas a que se hizo referencia en el capítulo primero.

Finalmente, también es importante la participación de un profesionista en materia de valuación de criptomonedas que determine el valor en el mercado de las criptomonedas empleadas, máxime que dependiendo del tipo de las mismas, el valor puede variar, pues no tiene el mismo valor la *bitcoin* que la *ethereum*, entre otras.

Sin embargo, las criptomonedas, no tienen una publicación oficial en cuanto a su valor. Es cierto que existen varias fuentes en la red que nos pueden dar noticia de su valor, pero éstas no son confiables al no ser oficiales y no dan certeza de los datos que conforman los parámetros de su valoración; inclusive, hay incertidumbre de la persona capacitada para determinar ello, a saber; ¿Deberá ser una persona con conocimientos financieros?; ¿Un ingeniero en sistemas, en virtud del conocimiento tecnológico en las fuentes de información, relacionados con los datos del valor de ellas?; ¿Un corredor público, por la experiencia de las operaciones mercantiles que implican la compraventa de las monedas virtuales?. No queda claro.

A juicio del que suscribe, para otorgar plena certidumbre jurídica, la valuación de la criptomoneda bien pudiera ser realizada por corredor público que cuente con registro vigente ante la Secretaría de Economía, pues una de las funciones de dicho profesionista es la valuación de bienes conforme a valor de mercado y

perfectamente puede allegarse de diferentes fuentes de información en la red para conocer el valor de alguna criptomoneda.

El artículo 369 del Código Nacional de Procedimiento Penales establece que los peritos deberán poseer título oficial en la materia relativa al punto sobre el cual dictaminarán y no tener impedimentos para el ejercicio profesional, siempre que la ciencia, el arte, la técnica o el oficio sobre la que verse la pericia en cuestión esté reglamentada; en caso contrario, deberá designarse a una persona de idoneidad manifiesta y que preferentemente pertenezca a un gremio o agrupación relativa a la actividad sobre la que verse la pericia.

El perito contable es el profesionista que a través de su experiencia y conocimientos mediante la realización de estudios, análisis, técnicas, pruebas o procedimientos utilizados en su especialidad y con el uso de las herramientas o equipos de los que dispone, dilucida una problemática en la técnica de su profesión y emite una opinión que servirá de orientadora a los operadores del sistema de justicia penal.

En el caso concreto, para conocer la determinación del daño o perjuicio a la hacienda pública, el empleo de la tecnología *blockchain*, así como la valuación de la criptomoneda, se necesita de un profesionista con título profesional en las materias de contabilidad, sistemas computacionales y financiera.

El dictamen que rinda deberá contener como requisitos:

1. Proemio, esto es, la mención de la calidad en que interviene el perito, su profesión, así como la parte quien lo designó, o bien, si es un perito tercero en discordia, en su caso.
2. Documentación a analizar: estudio y análisis de los documentos con base en los cuales se rinde el dictamen.
3. Consideraciones: son las bases, elementos y fundamentos, así como las técnicas, métodos y herramientas utilizadas, con base en las cuales se desarrolla el dictamen.

4. Conclusiones: es el resultado de la investigación dando su opinión respecto del problema que le fue planteado.
5. Respuestas al cuestionario, en el caso de que la prueba pericial verse sobre un cuestionario formulado por las partes.

Ahora bien, el dictamen pericial no está sujeto a control judicial, pues no es un acto que incida en los derechos fundamentales del contribuyente, sin embargo, para la determinación del daño a la hacienda pública, la valuación de la criptomoneda y el empleo de la tecnología *blockchain*, es necesaria la información financiera que previamente debió ser sujeta a control judicial, pues de no ser así, los datos de prueba serán ilícitos y en consecuencia también los dictámenes periciales que se realicen con base en esa información.

Lo anterior es así, pues no es posible que el dictamen pericial correspondiente se formule con base en información financiera que haya sido obtenida con violación a derechos fundamentales, pues como ya se mencionó, la información financiera está protegida por el derecho fundamental de privacidad establecido en el artículo 16 constitucional.

Con independencia de lo anterior, cabe dejar apuntado que el perito debe rendir su dictamen y las partes que ofrezcan la prueba pericial deben correr traslado a la contraparte antes de la audiencia intermedia para que se imponga de su contenido y ejerzan su derecho de contradicción con relación a la admisión o exclusión del medio de prueba. En la audiencia de juicio, el perito debe exponer las conclusiones de su dictamen en forma oral y las partes podrán interrogarlos y contrainterrogarlos al desahogar la prueba y en legítimo derecho del principio de contradicción.

Capítulo 5

La Criptomoneda y el Delito de Defraudación Fiscal

Capítulo 5. La Criptomoneda y el Delito de Defraudación Fiscal

Francisco Pavón Vasconcelos refiere que delito es: “la conducta o el hecho típico antijurídico, culpable y punible”[80]. Por su parte, Mario Alberto Torres López indica que los delitos fiscales son “todo ilícito que atente contra la hacienda pública federal, estatal o Municipal”.[81]

En opinión del suscrito, los delitos fiscales pueden verse desde dos perspectivas, a saber, formal y material. Desde el punto de vista del primero, los Delitos fiscales son aquellos delitos especiales que se encuentran previstos en las diversas leyes fiscales; desde la perspectiva material, son aquellos en que se afecta la recaudación, el patrimonio de la Hacienda Pública y el buen desarrollo del sistema tributario.[82]

Son varios los ordenamientos en los que se encuentran tipificados los delitos fiscales. En el Código Fiscal de la Federación (96 a 115), Ley del Seguro Social (artículos 307 al 316) y la Ley del Instituto Nacional del Fondo Nacional de la Vivienda para los Trabajadores (artículos 57 y 58).

Por cuanto al Código Fiscal de la Federación se refiere, en el título IV “De las Infracciones y Delitos Fiscales”, Capítulo II “De los Delitos fiscales”, se encuentran previstos diversos delitos, como lo son: encubrimiento (artículo 96); delito de funcionarios o empleados públicos (artículo 97 y 114); contrabando (artículos 102 a 107); defraudación fiscal (artículos 108 y 109); delitos por infracciones sobre el Registro Federal de contribuyentes (artículo 110); delitos relacionados con la presentación de declaraciones o contabilidad (artículo 111); delito de depositarios e interventores (artículo 112); delitos relacionados con la alteración o destrucción de aparatos de control, sellos, máquinas registradoras, etcétera (artículo 113); delito de expedición o comercialización de operaciones inexistentes, falsas o actos

[80] Pavón Vasconcelos, Francisco, *Derecho Penal Mexicano*, Parte General, México, Porrúa, 2000, p. 178.
[81] Torres López, Mario Alberto, *Teoría y Práctica de los delitos fiscales*, México, Porrúa, 2000, p. 38.
[82] Moreno García, Alfonso, *Efectos Penales de la Discrepancia Fiscal de las Personas Físicas*, Tesis de Maestría, Universidad Panamericana, 2018, p. 72.

jurídicos simulados (artículo 113 bis); delito de servidores públicos que visiten o embarguen sin mandamiento escrito (artículo 114); delito de servidores públicos que amenacen con formular, denuncia, querella o declaratoria de perjuicio (artículo 114-A); delito de servidores públicos que revelen información proporcionada por el sistema financiero (artículo 114-B); delito de robo o destrucción de mercancías en recinto fiscal o fiscalizado (artículo 115) y; delito para comercializadores o transportistas de gasolina o diésel sin especificaciones (artículo 115 bis).

En estrecha relación con el delito de defraudación fiscal, se encuentra el diverso de operaciones con recursos de procedencia ilícita y lavado de dinero, establecido en el artículo 400 bis del Código Penal Federal, más aun si se considera que en términos del tercer párrafo del artículo 108 del Código Fiscal de la Federación, ambos ilícitos pueden perseguirse simultáneamente.

Conviene precisar que por decreto publicado en el Diario Oficial de la Federación el 8 de noviembre de 2019, se reformaron, adicionaron y derogaron diversas disposiciones de la Ley Federal de Delincuencia Organizada, de la Ley de Seguridad Nacional, del Código Nacional de Procedimientos Penales, del Código Fiscal de la Federación y del Código Penal Federal, con los objetivos de inhibir de la expedición o comercialización de operaciones inexistentes, falsas o actos jurídicos simulados; evitar el fraude fiscal y; aumentar la recaudación.

La reforma fiscal penal está dirigida tanto a los emisores de comprobantes fiscales digitales (CFDI’s) que amparan operaciones inexistentes, falsas o actos jurídicos simulados, como a los receptores de los mismos quienes al dar efectos fiscales a los mismos, aprovechan la deducción y acreditamientos correspondientes.

Fueron varias las disposiciones que fueron afectadas por el decreto, a saber: de Ley Federal contra la Delincuencia Organizada, se reformó el artículo 2 fracción VIII y se adicionó el artículo 2 fracciones VIII Bis y VIII Ter; de la Ley de Seguridad Nacional, se reformaron las fracciones XI y XII del artículo 5 y se adicionó la fracción XIII; del Código Nacional de Procedimientos Penales, se reformaron los artículos 187 párrafo segundo, 256 párrafo tercero y se adicionaron los artículos 167 párrafo

séptimo fracciones I, II y II y 192 párrafo tercero; del Código Fiscal de la Federación, re reformó el artículo 113 bis y se derogó el artículo 113 fracción III y; del Código Penal Federal, se adicionó el artículo 11 Bis fracción VIII Bis.

La reforma fiscal penal está dirigida tanto a los emisores de comprobantes fiscales digitales (CFDI's) que amparan operaciones inexistentes, falsas o actos jurídicos simulados, como a los receptores de los mismos quienes al dar efectos fiscales a los mismos, aprovechan la deducción y acreditamientos correspondientes.

Los aspectos más sobresalientes de la reforma, fueron los siguientes:

1. Se considerará amenaza a la seguridad nacional y delincuencia organizada el fraude al fisco.
2. Se busca sancionar al beneficiario final de la expedición de CFDI's con operaciones inexistentes, falsas o simuladas.
3. Sanciones de cinco a ocho años de cárcel para quien adquiera CFDI's con operaciones inexistentes, falsas o simuladas.
4. Protección a personas que ayuden en la investigación (testigos protegidos).
5. A quienes expidan facturas falsas por hasta $7,804,239 no aplicará la prisión preventiva oficiosa ni serán tratados como delincuentes o crimen organizado.
6. La reforma entró en vigor el día 1 de enero del 2020.
7. Las conductas cometidas antes de que aplique la reforma legal para endurecer las penas a los defraudadores fiscales se continuarán investigando, juzgando y sentenciando, conforme a la normatividad vigente previo a la reforma.

5.1 Estudio Jurídico del delito de Defraudación Fiscal

El Diccionario Jurídico del Instituto de Investigaciones Jurídicas de la Universidad Nacional Autónoma de México señala que "la defraudación fiscal supone la intención de dañar, la realización de un acto voluntario o la ocultación (omisión) de cualquier circunstancia con relevancia fiscal con el propósito deliberado de sustraerse en todo o en parte a una obligación fiscal".[83]

[83] Jonhson Okhuysen, Eduardo, *Diccionario Jurídico*, *op. cit*., t. II p. 2886.

Este delito comparte con el delito de fraude establecido en el artículo 386 del Código Penal federal un rasgo importante, relacionado en que no basta el lucro indebido, el daño patrimonial o el perjuicio por sí mismos, sino además, se necesita la existencia del engaño o aprovechamiento del error, pues de otra manera, no se cumpliría la exigencia del artículo 17 constitucional, consistente en que "*Nadie puede ser aprisionado por deudas de carácter puramente civil.*".

El delito fiscal que ocupa el presente trabajo, tiene como conducta la omisión del pago de contribuciones, como sujeto activo al contribuyente y como sujeto pasivo al Estado, además del quebrando a la Hacienda Pública como resultado, sin olvidad el engaño o aprovechamiento del error propios de los delitos de fraude.

De tal manera que el delito de defraudación fiscal es la conducta típica, antijurídica y culpable que realiza el contribuyente quien teniendo la obligación de pagar contribuciones, mediante el engaño o aprovechamiento de error, no lo realiza u obtiene algún beneficio con el consecuente daño patrimonial al fiscal federal.

El delito de defraudación fiscal puede ser el genérico que prevé el artículo 108 del Código Fiscal de la Federación o el equiparado o específico del artículo 109 del mismo ordenamiento.

5.1.1 Defraudación Fiscal Genérica

El Código Fiscal de la Federación en el Título IV "De las Infracciones y Delitos Fiscales", en el Capítulo II "De Los Delitos Fiscales", tipifica en el artículo 108 el delito de defraudación fiscal genérico señalando "Comete el delito de defraudación fiscal quien con uso de engaños o aprovechamiento de errores, omita total o parcialmente el pago de alguna contribución u obtenga un beneficio indebido con perjuicio del fisco federal."

La disposición del artículo 108 en el segundo párrafo es un tanto imprecisa, debido a que señala que la contribución comprende tanto pagos provisionales como el impuesto del ejercicio, pero para proceder penalmente y, en su caso, iniciar la la carpeta de investigación es necesario que se determine el total del impuesto omitido, por lo que para que se dé esta hipótesis es necesario que se determine el impuesto omitido por ejercicios completos, y no por pagos provisionales, que como

su nombre lo indica son pagos a cuenta del impuesto definitivo; por tanto no son definitivos.

En el delito de defraudación fiscal, la persona que lo comete tiene la finalidad de conducirse con falsedad, valiéndose de maquinaciones y artificios contra el fisco en aras de encubrir la omisión del pago total o parcial de alguna contribución, o bien, obteniendo un beneficio indebido. El contribuyente engaña pretendiendo hacer creer que las obligaciones fiscales se cubrieron de manera correcta, o bien, oculta cierto beneficio que no le corresponde.

Este delito se comete necesariamente de forma dolosa, esto es, el contribuyente, teniendo pleno conocimiento de lo que hace, utiliza los medios necesarios para presentar hechos falsos como verdaderos y quiere tomar ventaja del fisco en caso de que éste se encuentre en estado de error. Evidentemente, este delito no admite la forma de comisión culposa.

Como elementos del delito de defraudación fiscal se tienen los siguientes:

a) Uso de engaño o aprovechamiento de errores. El engaño consiste en provocar en otro mediante artificios o maquinaciones una falsa apreciación de la realidad, En cambio, en el aprovechamiento del error el sujeto se vale de la falsa apreciación de la realidad pero no provocada por él, sino por la propia autoridad. Esto es, el engaño o aprovechamiento del error es el medio comisivo.

b) Omitir pagar total o parcialmente una contribución. El delito de defraudación fiscal se consuma en el momento en que se omite pagar la contribución correspondiente. Para determinar si existe omisión total o parcial de pago de contribuciones, es necesario que previamente exista la obligación de cubrir dichas contribuciones, es decir, que la persona física o moral a la que se pretende imputar dicho ilícito tenga la obligación, en términos de ley, de cubrir las contribuciones cuyo pago se dice omitió, ya que, si no existe dicha obligación de pago, no se puede hablar de falta de pago ni mucho menos de la comisión de una conducta delictiva. Para conocer ello, habrá que remitirse

a la ley fiscal específica y advertir los supuestos en los que se debe pagar y los plazos correspondientes.[84]

c) Obtener un beneficio indebido. Este caso se puede presentar, por ejemplo, si el fisco efectúa una devolución errónea de impuestos sin que el contribuyente aclare o devuelva dicha cantidad o si un contribuyente solicita la devolución de impuestos de forma engañosa.

   Este momento es el ejercicio mental en cuyo momento se puede determinar con precisión la comisión del ilícito, sin sancionar una acción de la ley como sería querellar por utilidades presuntamente obtenidas y determinadas éstas por la autoridad hacendaria.[85]

d) En perjuicio del fisco federal, esto es, se refiere al monto que la Hacienda Pública ha dejado de percibir, o bien, la afectación que ha sufrido con motivo de devoluciones indebidas.

En cuanto al tercer párrafo, se establece que los delitos de defraudación fiscal y operaciones con recursos de procedencia ilícita, previsto en el artículo 400 Bis del Código Penal Federal, se podrán perseguir simultáneamente. Asimismo, se contiene una presunción consistente en que se presumirá cometido el delito de defraudación fiscal cuando existan ingresos derivados de operaciones con recursos de procedencia ilícita.

Dicha presunción solo es aplicable al delito de defraudación fiscal genérico del artículo 108 del Código Fiscal de la Federación, no así a las distintas hipótesis delictivas del delito de defraudación fiscal equiparable contenidas en el artículo 109 de dicho ordenamiento, puesto que su redacción no las contempla. De igual forma esta presunción solo se aplica en un solo sentido, pues del delito de operaciones con recursos de procedencia ilícita se puede presumir la comisión del delito de defraudación fiscal, más no a la inversa.[86]

---

[84] Ambrosio, Michel Higuera, *Derecho Penal Fiscal*, México, Porrúa, 2012, p. 564.
[85] Urbina Nandayapa, Arturo, *Los Delitos Fiscales en México, El cuerpo de los Delitos Fiscales en el Derecho Positivo*, México, PAC, 2012, t. II, p. 96.
[86] Michel Higuera, Ambrosio, *op. cit*., p. 603.

Con independencia de lo anterior, lo grave del asunto es que la presunción comentada rompe con el principio de presunción de inocencia, pues al presumir la existencia del delito de defraudación fiscal, a partir de la existencia del delito de operaciones con recursos de procedencia ilícita, invierte la carga probatoria teniendo el agraviado que demostrar su inocencia, esto es, que no existió delito de defraudación fiscal y no la autoridad ministerial su culpabilidad.

5.1.2 Defraudación Fiscal Equiparada

La expresión “equiparable” se refiere a que las mismas penas que se encuentran establecidas en el artículo 108 del Código Fiscal de la Federación resultan aplicables para las figuras previstas por el diverso artículo 109.

El delito de defraudación fiscal equiparable se encuentra previsto en el artículo 109 del Código Fiscal de la Federación. En cuanto a la fracción I del precepto en comento contiene diferentes hipótesis delictivas, la primera se relaciona con datos que asientan en las declaraciones fiscales, como las deducciones y los ingresos, y la segunda hipótesis se refiere a una situación en que una persona realiza erogaciones que superan sus ingresos en un ejercicio fiscal.

Es conveniente precisar que existen dos formas de determinar créditos fiscales: a) la autodeterminación por parte de los contribuyentes obligados y b) mediante el ejercicio de facultades de comprobación de las autoridades fiscales de conformidad con los artículos 42 al 48 del Código Fiscal dela Federación.

Es importante tener presente la fracción I, porque dado que en nuestro sistema fiscal impera la regla de autodeterminación de las contribuciones por parte de los contribuyentes, normalmente el delito de defraudación fiscal que se actualiza es el equiparado del artículo 109, la fracción I para quien “Consigne en las declaraciones que presente para los efectos fiscales, deducciones falsas o ingresos acumulables menores a los realmente obtenidos o valor de actos o actividades menores a los realmente obtenidos o realizados o determinados conforme a las leyes…”

Los delitos contemplados como equiparables al de defraudación fiscal, al igual que su genérico, solo permiten una comisión dolosa, es decir, basta con

conocer y querer el resultado típico, y esta forma de comisión es contemplada en todas y cada una de las fracciones que establece el artículo 109 del Código Fiscal de la Federación.

5.1.3 Elementos

Por la forma en que se encuentra redactado el artículo 109, fracción I, primera parte, la defraudación fiscal equiparada es un delito de mera conducta, pues no exige la presencia de un resultado consistente en un perjuicio al fisco federal, como en cambio sí lo establece la defraudación fiscal genérica del artículo 108; sin embargo, este perjuicio se deduce de la propia descripción típica, por lo que si bien no se encuentra previsto este resultado expresamente dentro del tipo penal como uno de sus elementos, en los procedimientos penales la autoridad hacendaria debe acreditar dicho perjuicio al Fisco Federal mediante la determinación cuantificable del mismo, para los efectos de la imposición de las sanciones.[87]

Es claro precisar que los elementos de todo tipo penal se encuentran según la teoría del delito y la corriente finalista, en el elemento de la tipicidad, donde se suscriben los elementos objetivos del tipo entendiéndose por ellos todos aquellos que describe el propio tipo penal, así como los elementos normativos, que son aquellos que requieren una valoración que puede ser jurídica o cultural, así como los elementos subjetivos del tipo, en donde observamos el dolo o la culpa según la forma de comisión que requiera el tipo penal.

5.1.4 Elementos Objetivos

Los elementos objetivos de la primera hipótesis de la fracción I del artículo 109 del Código Fiscal de la Federación análisis de la presente tesis son:

a) Consignación en las declaraciones que se presenten para los efectos fiscales
b) Deducciones falsas o ingresos acumulables menores a los realmente obtenidos

[87] *Ibidem*, p. 44.

c) Valor de actos o actividades menores a los realmente obtenidos o realizados o determinados conforme a las leyes.[88]

De acuerdo con la fracción I del artículo 109 del Código Fiscal de la Federación, la conducta delictiva consiste en que el contribuyente consigne en sus declaraciones fiscales, deducciones falsas o ingresos acumulables menores a los realmente obtenidos o valor de actos o actividades menores y que no pague en forma correcta sus contribuciones.

Con dicha conducta equiparada a la defraudación fiscal, existe la posibilidad para que la autoridad ejercite acción penal en contra de contribuyentes que evadieron contribuciones en ejercicios anteriores[89], mediante el empleo de una forma muy específica de engaño, consistente en que en las declaraciones presentadas, se asienten datos incorrectos o falsos en los rubros de ingresos, deducciones y valor de los actos o actividades.

5.1.5 Elementos Normativos

Respecto de los elementos normativos es necesario precisar que dichos elementos requieren una valoración misma que puede ser jurídica o bien cultural. En el caso de la defraudación fiscal equiparada, se tienen los siguientes elementos normativos como son:

a) *Consignar*, de conformidad con el Diccionario de la Real Academia Española es asentar opiniones, votos, doctrinas, hechos, circunstancias, datos, etc. por escrito y a menudo con formalidad jurídica o de modo solemne.[90]

b) *Declaraciones*, según lo establecido por el artículo 6º del Código Fiscal de la Federación, los contribuyentes deben realizar el pago de sus contribuciones mediante declaración en los plazos que en tal disposición se señala. Declaración de impuestos: “es la manifestación que efectúa el

[88] *Ibidem,* p. 56.

[89] Ponce Rivera, Alejandro, *Nueva Responsabilidad fiscal penal*, México, Ediciones Fiscales ISEF, México 2000, pp. 167 a 196.

[90] Real Academia Española, “consignar”, *http://buscon.rae.es/draeI/*. Consultado el 10 de enero de 2020.

contribuyente por mandato de ley de sus obligaciones tributarias durante un ejercicio fiscal".[91] La declaración es el documento por medio del cual, el contribuyente señala a la autoridad fiscal los datos y cifras que tomó en cuenta para la determinación de la base correspondiente que aplicada la tasa o tarifa, derivó en la contribución a pagar.

c) *Deducciones*, es un concepto propio de la Ley del Impuesto sobre la Renta y que se encuentra regulado en los artículos 25 (deducciones autorizadas), 27 (requisitos de las deducciones) y 28 (gastos no deducibles), y representa los gastos y costo que el contribuyente tuvo en el ejercicio que restado de los ingresos del ejercicio determina la utilidad que menos las pérdidas fiscales de ejercicios anteriores, arroja la base correspondiente.

Es importante destacar que la descripción típica requiere de la existencia de deducciones falsas, esto es, operaciones que no son reales y cuyo valor el contribuyente dedujo; cuestión muy diferente a la circunstancia de que el gasto haya existido pero la ley lo considera no deducible, o bien permitiéndolo la ley, el contribuyente no cumplió con los requisitos legales para su deducibilidad, casos en donde la deducción no es falsa, sino más bien, improcedente.

d) *Ingresos,* según lo establecido por el artículo 16 de la Ley del Impuesto Sobre la Renta se entiende por ingreso la totalidad de los ingresos en efectivo, en bienes, en servicio en crédito o cualquier otro tipo que obtengan en el ejercicio. Mientras que el Diccionario de la Lengua Española señala que se entiende por ingreso el caudal que entra en poder de alguien y que le es de cargo en las cuentas.[92]

e) *Valor de los actos o actividades,* es un concepto propio de la Ley del Impuesto al Valor Agregado y que deriva del artículo 1º, porque se

[91] Carrasco Iriarte, Hugo, Diccionario de Derecho Fiscal, México, Oxford, 2008, p. 144.
[92] Real Academia Española, "ingreso", *http://buscon.rae.es/draeI/*. Consultado el 10 de enero de 2020.

establecen los diferentes actos o actividades objeto de imposición y la tasa aplicable, siendo 16% como regla general o la del 0% en los casos del artículo 2-A; el valor de los actos por regla general es la contraprestación por la enajenación del bien o la prestación del servicio, salvo las excepciones establecidas en Ley

Los elementos normativos antes mencionados son de valoración jurídica, pues remiten a otros ordenamientos jurídicos para su entendimiento en particular la Ley del Impuesto sobre la Renta, la Ley del Impuesto al Valor Agregado y el Código Fiscal de la Federación, ya que dichas legislaciones contemplan las figuras aquí analizadas.

5.1.6 Elementos Subjetivos

En la defraudación fiscal equiparada que prevé el artículo 109 fracción I del Código Fiscal de la Federación, es claro que no se encuentra plasmado ningún elemento subjetivo específico distinto al dolo, sin embargo, la configuración típica del delito supone un ánimo o intención por parte del autor de asentar datos incorrectos o falsos para hacer ver a la autoridad ingresos menores, deducciones falsas o valor de los actos o actividades menores, es decir, que el contribuyente, al momento de presentar las declaraciones para efectos fiscales ante la autoridad hacendaria está consciente de la discrepancia de datos que están consignando en las declaraciones con la realidad, de tal manera que en la conducta desplegada por el sujeto activo se encuentra presente el elemento volitivo de efectuar esa conducta típica con el resultado que la misma supone perjuicio al Fisco.

De ahí que de dicha conducta se desprenda que el sujeto activo actúa dolosamente, ya que conocía el carácter ilícito de su proceder como un aspecto cognoscitivo y, aun así, dispuso lo necesario para la presentación de dichas declaraciones fiscales a sabiendas de que las mismas contienen datos que no están apegados a la realidad con la intención de ocultamiento a la autoridad fiscal, es decir, un aspecto volitivo, de tal forma que consigna datos falsos en las declaraciones que se presentan para efectos fiscales configurándose el delito.

5.1.7 Punibilidad

La punibilidad es la cualidad de punible, es decir, aquella conducta a la que se tiene la posibilidad de aplicar una sanción o pena jurídica. La Punibilidad significa la posibilidad de aplicar pena, atendiendo a esto no a cualquier delito se le puede aplicar pena.

La punibilidad es conminación de privación o restricción de bienes del autor del delito, formulada por el legislador para la prevención general y determinada cualitativamente por la clase del bien tutelado y cuantitativamente por la magnitud del bien y el ataque a éste.[93]

Manuel Osorio, establece como punibilidad a aquella situación en que se encuentra quien, por haber cometido una infracción delictiva, se hace acreedor a un castigo. Sin embargo, hay circunstancias en que, aun existiendo la infracción penal y su autor, éste no puede ser castigado por razones previamente determinadas por el legislador.[94]

Por lo tanto, la sanción prevista para el delito de defraudación fiscal está contemplada en el artículo 108 del Código Fiscal de la Federación y, a su vez, el artículo 109 que establece la defraudación fiscal equiparada, remite al artículo 108 para las sanciones que a la letra establece:

> …
> El delito de defraudación fiscal se sancionará con las penas siguientes:
> I. Con prisión de tres meses a dos años, cuando el monto de lo defraudado no exceda de $1, 369,930.00.

[93] Solórzano de la Barreda, Luis, *Punibilidad, Punición y Pena de los Sustitutivos Penales*, México, Porrúa, 2000, p. 70, *http://biblio.juridicas.unam.mx/libros/2/854/5.pdf*. Consultado el 10 de octubre de 2018.
[94] Ossorio, Manuel, *Diccionario de Ciencias Jurídicas, Políticas y Sociales*, 27a. ed., Buenos Aires, Heliasta, 2000, p. 822.

II. Con prisión de dos años a cinco años cuando el monto de lo defraudado exceda de $1, 369,930.00 pero no de $2, 054,890.00.

III. Con prisión de tres años a nueve años cuando el monto de lo defraudado fuere mayor de $2, 054,890.00.

Es necesario precisar que en este último precepto legal se establecen las hipótesis calificativas para el delito de defraudación fiscal, así como el delito de defraudación fiscal equiparada.

….

El delito de defraudación fiscal y los previstos en el artículo 109 de este Código, serán calificados cuando se originen por:

a) Usar documentos falsos.

b) Omitir reiteradamente la expedición de comprobantes por las actividades que se realicen, siempre que las disposiciones fiscales establezcan la obligación de expedirlos. Se entiende que existe una conducta reiterada cuando durante un período de cinco años el contribuyente haya sido sancionado por esa conducta la segunda o posteriores veces.

c) Manifestar datos falsos para obtener de la autoridad fiscal la devolución de contribuciones que no le correspondan.

d) No llevar los sistemas o registros contables a que se esté obligado conforme a las disposiciones fiscales o asentar datos falsos en dichos sistemas o registros.

e) Omitir contribuciones retenidas o recaudadas.

f) Manifestar datos falsos para realizar la compensación de contribuciones que no le correspondan.

g) Utilizar datos falsos para acreditar o disminuir contribuciones.

Cuando los delitos sean calificados, la pena que corresponda se aumentará en una mitad.

5.1.8 Bien Jurídico Protegido

Von Liszt sostuvo que el bien jurídico puede ser definido como un "interés vital para el desarrollo de los individuos en una sociedad determinada que adquiere reconocimiento".[95]

El bien jurídico es protegido por el derecho, mediante una sanción para cualquier conducta que lesione o ponga en riesgo el bien protegido. Se puede deducir que el bien jurídico obtiene este carácter con la vigencia de una norma que lo proteja, pero si esta norma fuera derogada, éste no deja de existir, pero ya no estaría protegido por ésta.

> Esta característica proteccionista que brinda la normatividad para los bienes jurídicos, se hace notar con mayor incidencia en el Derecho Penal, por ser en esta rama del derecho en la que la norma se orienta directamente a la supresión de cualquier acto contrario a mantener la protección del bien jurídico.
>
> Es importante tener en cuenta que la protección del bien jurídico, si bien se puede observar con mayor fuerza en el Derecho Penal, lo cierto es que esta protección va de parte de todo el ordenamiento legal, pues sería totalmente contradictorio que mientras la norma penal sancione el homicidio, una norma civil o de cualquier otra índole, lo permitan o consientan.[96]

El Derecho Penal tiene como propósito la protección de los bienes jurídicamente tutelados para el derecho, es por ello que cada delito tipificado en el

---

[95] Von Liszt, Franz, *Tratado de Derecho Penal*, traducido de la 20a ed., trad. Luis Jiménez de Asúa, 4a.º ed., Reus, Madrid, 1999, t. II. p. 4.

[96] Santivañez, Juan José, *"Algunas Consideraciones sobre la Ley de Régimen Disciplinario del personal Policial"*, Asociación Peruana de Derecho Policial, 26 de septiembre de 2019 *https://juanjosesantivanez.blogspot.com/2009/09/algunas-consideraciones-sobre-la-ley-n.html*. Consultado el 15 de mayo de 2020.

Código Penal tiene una protección hacia el bien jurídico que ha de lesionar o bien tratar de lesionar, para configurar dicho delito y posteriormente ser sancionado.

Por lo tanto, y relacionado con el delito en estudio en el presente trabajo, el bien jurídico tutelado que protege el artículo 109 fracción I tercera hipótesis del Código Fiscal de la Federación, lo constituye la recaudación de los ingresos federales y el patrimonio de la Hacienda Pública.

5.2 La Criptomoneda como medio comisivo en el delito de Defraudación Fiscal

En la última parte del capítulo anterior, se señalaron los rasgos esenciales del "medio comisivo" en los delitos y se mencionó que como elemento del tipo penal, puede estar o no establecido en éste, cuando se establece, es porque el legislador tomó en cuenta la relevancia penal que tiene en la conducta.

Por el contrario, cuando no se establece medio comisivo alguno, es porque la conducta tendrá relevancia penal con independencia del medio comisivo empleado.

En la defraudación fiscal genérica del artículo 108 del Código Fiscal de la Federación y la equiparada del artículo 109, fracción I siguiente, las hipótesis jurídicas exigen que la conducta se realice mediante engaño o aprovechamiento del error en el primer caso, y mediante la consignación de datos y cifras en una declaración en el segundo caso.

Efectivamente, en el caso del artículo 108 citado, lo que tiene relevancia penal no es tanto dejar de pagar contribuciones u obtener un beneficio indebido en perjuicio del fisco federal, sino más bien que ello se haga mediante el engaño o el aprovechamiento de error, característica muy propia del delito de fraude y que en la defraudación fiscal no podía dejarse de lado.

En el caso de la defraudación fiscal equiparada del artículo 109 mencionado, también existe un engaño, pero éste se da en forma específica, esto es, se hace mediante el empleo de una declaración con cifras y datos falsos o incorrectos para dejar de pagar las contribuciones o para la obtención del beneficio, que es

propiamente un engaño, porque lo asentado en las declaraciones se hace en desapego a la realidad.

Ahora bien, el engaño propio de los delitos de fraude puede realizarse con criptomonedas, puesto aun cuando no es dinero, al servir como instrumento de pago en las transacciones económicas o como instrumento de inversión, es sumamente complicada su fiscalización.

Es decir, como instrumento de pago, puede ser que una persona que enajene un bien o presta un servicio, acuerde con el adquirente o prestatario que la obligación para cubrir la contraprestación se realice mediante el envío de criptomonedas del monedero virtual de este último al monedero virtual del primero.

Como instrumento de inversión, puede suceder que una persona decida adquirir criptomonedas con la expectativa de que al paso del tiempo incremente su valor y por tanto tener su dinero representado en criptomonedas.

En ambos supuestos, existe un serio problema para la recaudación de las contribuciones, puesto que en el primero, no existe una forma en que las autoridades fiscales tengan conocimiento de la operación y el monto de la misma de lo que depende la cuantificación de los impuestos, esto es, si el contribuyente presta un servicio y recibe criptomonedas por el mismo, simple y sencillamente las autoridades no tendrán conocimiento de ello.

Igual acontece con la inversión en criptomonedas, porque en el supuesto de que las mismas incrementen su valor frente al peso mexicano, las autoridades mexicanas no tendrán conocimiento de las ganancias devengadas por ello.

No cabe duda que este tipo de transacciones son objeto de impuesto sobre la renta y/o impuesto al valor agregado, pues la contraprestación es un ingreso para efectos del primer impuesto y el valor de los actos o actividades para efectos del segundo.

El problema se acentúa cuando los monederos virtuales y las plataformas de intercambio de criptomonedas por peso mexicano y divisas, en muchos de los casos

pueden no estar en México y no ser sujetas a la regulación y ámbito de competencia de las autoridades mexicanas.

Pero aun en el supuesto de que por alguna circunstancia, las autoridades tuvieran conocimiento de la transacción económica y el monto de las mismas en criptomoneda, aun existirá un problema por salvar, consistente en la determinación del valor de esa transacción en pesos mexicanos, porque las autoridades no pueden recibir el pago de los impuestos en criptomonedas.

Cobra especial relevancia que la tecnología *blockchain* sobre la que descansan las criptomonedas propician el anonimato, lo que hace que sea muy complicado la fiscalización de las autoridades fiscales de las transacciones realizadas por medio de las mismas.

Entonces, una persona puede realizar transacciones económicas, como la enajenación de un bien o la prestación de un servicio y recibir criptomonedas para satisfacer la contraprestación, consignar en sus declaraciones fiscales datos incorrectos o falsos (como lo es no declarar las transacciones de este tipo) para no cubrir el impuesto sobre la renta y el impuesto al valor agregado derivados de este tipo de transacciones, con lo cual engaña a las autoridades fiscales.

Este es el verdadero riesgo en la recaudación del país que trastoca las finanzas públicas y que debe ser evitada, pero sancionada con rigor e inclusive penalmente.

5.3 La Investigación del delito de Defraudación Fiscal mediante el empleo de Criptomonedas

Conforme al artículo 21 constitucional, es atribución del Ministerio Público la investigación de conductas posiblemente delictivas establecidas en las leyes penales, para lo cual debe llevar a cabo los actos y técnicas de investigación con plena observancia de los requisitos constitucionales y legales que deriven en la obtención de datos de prueba que en su caso serán puestas del conocimiento del Juez de Control al judicializar la carpeta de investigación correspondiente.

En el caso de las criptomonedas que son empleadas para la realización del delito de defraudación fiscal, se requiere de una compleja investigación por parte de Ministerio Público, así como el suministro de datos de prueba por parte de la Procuraduría Fiscal de la Federación para acreditar los elementos del tipo penal de defraudación fiscal genérico y/o específico.

En la investigación se involucran aspectos tecnológicos, contables y financieros que no son propios del perfil profesional del Ministerio Público y que requieren de profesionistas especializados en diferentes áreas que como peritos al elaborar los dictámenes correspondientes y ser examinados oralmente en juicio deben producir convicción en el Juez respecto de la comprobación de los elementos del tipo.

En el caso de la comercialización de diversos bienes a través compraventa de una plataforma electrónica, la empresa que cobró a los consumidores en criptomoneda y presentó su declaración sin considerar los ingresos, ni el valor de los actos o actividades por las ventas del ejercicio, no cabe duda que omitió el pago de contribuciones y engañó a las autoridades al consignar ingresos menores y valor de los actos o actividades menor a lo realmente obtenido.

En la investigación hay dos aspectos claves, el primero relacionado con los datos de prueba que debe obtener y el segundo con el análisis que de éstos deben hacer los profesionistas que emitan su dictamen.

De esta manera, se necesita un dictamen en informática para poder advertir que el pago de las transacciones comerciales se realizó mediante el empleo de criptomonedas; un dictamen en valuación de criptomonedas para advertir el monto de las transacciones en moneda nacional y un dictamen en contabilidad para cuantificar el daño al fisco federal también en moneda nacional.

Un cuidado extremo debe tener el Ministerio Público, quien debe cuidar que la recolección de los datos de prueba de carácter documental a las Instituciones de Instituciones de Tecnología Financiera, Instituciones bancarias, etcétera se lleve a cabo respetando las exigencias constitucionales y legales relacionadas con los secretos bancario y financiero.

Capítulo 6

Propuesta de la investigación

Capítulo 6. Propuesta de la investigación

6.1 Protocolo de actuación. Investigación de defraudación fiscal mediante el empleo de Criptomonedas

6.1.1 INTRODUCCIÓN

A la luz del sistema procesal penal acusatorio, con la promulgación en marzo de 2014 del Código Nacional de Procedimientos Penales (CNPP), la miscelánea penal emitida en junio de 2016 y la promulgación de protocolos y guías nacionales de actuación, entró en vigor un nuevo modelo no sólo de enjuiciamiento, de solución de conflictos o incluso de figuras novedosas de aceleración de soluciones litigiosas, sino también de investigación.

Sobre este aspecto, la investigación deberá realizarse de manera sistemática, ordenada, conjunta y científica, apegada a los axiomas que rigen el actuar de los servidores públicos de la Fiscalía General de la República, es decir, a los principios de certeza, legalidad, objetividad, imparcialidad, profesionalismo, honradez, lealtad, disciplina y respeto a los derechos humanos, y debe estar enfocada a la recopilación de datos que establezcan que se ha cometido un hecho que la ley señala como delito y que existe la probabilidad de que el indiciado lo cometió o participó en su comisión.

Sin embargo, la investigación no debe de concluir en lo inmediato, con la simple acreditación de los elementos que integran el hecho delictivo descrito en la ley y la probabilidad de que una persona intervino o participó en su ejecución, sino que es importante también realizar una indagatoria integral de los bienes que están relacionados con el hecho comisivo, puesto que de los mismos puede desprenderse la comisión de otro hecho que la ley señala como delito.[97]

En este sentido, la afectación al patrimonio de la Hacienda Pública por parte de los contribuyentes que intervienen en la comisión del delito de defraudación fiscal genérica o equiparada requiere de una investigación profunda y compleja, máxime

[97] López Lozano, Eduardo, *"Investigaciones Financieras Paralelas"*, Colegio de Contadores Públicos de México, 16 de julio de 2018, *https://veritasonline.com.mx/investigaciones-financieras-paralelas/*. Consultado el 15 de mayo de 2020.

cuando este delito es realizado mediante el empleo de criptomonedas como medio comisivo.

Para este supuesto, la investigación forense debe partir de la obtención financiera por parte de la autoridad investigadora que se encuentra protegida por el derecho a la privacidad de las personas establecido en el artículo 16 constitucional, información que es necesaria para la determinación del daño o perjuicio a la hacienda pública, el empleo de la tecnología con la cual se fundamenta la criptomoneda y la valuación de ésta.

Esto solo puede determinarse por profesionistas expertos en la técnica contable, en sistemas computacionales y en valuación de bienes que mediante los dictámenes periciales expresen su opinión sobre tales tópicos.

6.1.2 MARCO JURÍDICO

1. Constitución Política de los Estados Unidos Mexicanos
2. Código Fiscal de la Federación
3. Código Nacional de Procedimientos Penales
4. Código Penal Federal
5. Ley de Instituciones de Crédito
6. Ley para Regular las Instituciones de Tecnología Financiera
7. Ley General de Organizaciones y Actividades Auxiliares del Crédito
8. Reglamento de la Ley Orgánica de la Procuraduría General de la República

6.1.3 ALCANCE

Una investigación financiera y fiscal implica la recopilación, identificación, clasificación y análisis de toda la información disponible por parte del agente del Ministerio Público de la Federación (AMPF) con miras a remitirlas a las unidades especializadas para su análisis y, en su caso, judicializarla, sancionando a los responsables de la comisión de tales conductas y resarciendo el daño o perjuicio al Hacienda Pública.

Una investigación financiera y fiscal podría arrojar los elementos necesarios para investigar la probable comisión del hecho que la ley señala como delito y para identificar el empleo de la criptomoneda en las transacciones civiles y mercantiles por las que no se pagaron las contribuciones correspondientes.

6.1.4 OBJETIVOS DEL PROTOCOLO

6.1.4.1 Generales

El Protocolo busca homologar la actuación del AMPF estableciendo tácticas operativas básicas que describan cómo se debe proceder para iniciar una investigación y fiscal derivada de la persecución de otro hecho que la ley señala como delito de defraudación fiscal mediante el empleo de criptomoneda y determinar las técnicas de investigación que deberá emplear el Ministerio Público para la obtención de datos de prueba.

6.1.4.2 Específicos

1. En cuanto a la tecnología en que se sustenta la criptomoneda,
    - Proporcionar una aproximación a la tecnología *blockchain* y,
    - Analizar la regulación legal en México relacionada con la criptomoneda conforme a la Ley para Regular las Instituciones de Tecnología Financiera;
2. En cuanto al delito de defraudación fiscal,
    - Analizar sus aspectos penales y,
    - Analizar la criptomoneda como medio comisivo:
3. En cuanto a las técnicas de investigación relacionadas con la criptomoneda,
    - Determinar las técnicas que requieren control judicial, como con las solicitudes de información financiera y bancaria ante las instituciones financieras e instituciones de tecnología financieras y,
    - Determinar las técnicas que no requieren control judicial, como lo son la determinación del valor de la criptomoneda, la utilización de la tecnología blockchain y la determinación del daño o perjuicio a la hacienda pública.

6.1.5 POLÍTICAS DE OPERACIÓN

1. El AMPF, PFM y Peritos, en todo momento están obligados a promover, respetar, proteger y garantizar los derechos humanos de las personas implicadas.

2. Los actos de investigación deberán desarrollarse de manera obligatoria en todas las indagatorias de los AMPF en que la Secretaría de Hacienda y Crédito Público haya presentado querella por el delito de defraudación fiscal, a efecto de establecer si en el caso concreto existió daño a la Hacienda Público y su cuantía, así como advertir si para ello se empleó una criptomoneda como medio comisivo.

3. En todos los casos de las investigaciones financieras y fiscales deberán existir indicios fundados (como datos de prueba o elementos objetivos) de la comisión de un hecho que la ley señala como delito de manera previa.

4. En caso de que derivado de los actos de investigación se adviertan elementos de la posible comisión de un hecho que la ley señala como delito, distinto a la defraudación fiscal, como puede ser el delito de operaciones con recursos de procedencia ilícita, los AMPF deberán remitir mediante oficio la síntesis de los hechos que se investigan, así como el informe de resultados a la Unidad Especializada en Análisis Financiero (UEAF) de conformidad con el ámbito de sus competencias, para que esta determine la pertinencia de iniciar o no una Carpeta de Investigación.

5. En caso de que una de las unidades especializadas se declare incompetente, el AMPF deberá agotar la intervención de la otra unidad especializada.

6. La investigación financiera y fiscal deberá extenderse a todas aquellas personas físicas y jurídicas, así como a cualquier otro tipo de vehículos corporativos o financieros con los que la investigación tenga relación, incluyendo los beneficiarios, propietarios reales, titulares, cotitulares, fideicomisarios, fideicomitentes, firmantes y/o representantes legales de las

personas investigadas, así como a los proveedores de los recursos, derechos o bienes de cualquier naturaleza.

6.1.6 ROLES DE LOS PARTICIPANTES

Responsable	Descripción
Agente del Ministerio Público (AMPF)	Le compete ordenar y conducir los actos de investigación de un hecho con apariencia de delito, que pueda derivar en una investigación por encontrarse relacionada con recursos financieros, para lo cual se coordinará con la Policía y Peritos, para la investigación de un hecho que la ley señala como delito.
Unidad Especializada (UEAF)	Colaborar con AMPF de las unidades administrativas para determinar el inicio una carpeta de investigación, derivada de la presentación de una querella por parte de la Secretaría de Hacienda y Crédito Público

Cuadro 2: Elaboración propia

6.1.7 DESCRIPCIÓN DETALLADA DEL PROCESO

La investigación financiera y fiscal inicia cuando la Secretaría de Hacienda y Crédito Público presenta una querella por el delito de defraudación fiscal y existen indicios fundados de que la conducta se realizó mediante el empleo de criptomonedas

1. La/el AMPF inicia los actos de investigación financiera y fiscal.
2. La/el AMPF ordena a quien corresponda, la ejecución de actos de investigación financiera y fiscal.

   Nota: Ver anexo único. Diligencias en investigaciones financieras paralelas.
3. La PFM y/o Peritos, realizan actos de investigación y envían resultados a la/el AMPF.
4. La/el AMPF recibe resultados de los actos de investigación.

5. La/el AMPF solicita al Juez de Control la autorización para acceder a la información financiera en bancos y en general a cualquier Institución Financiera e Institución de Tecnología Financiera, justificando la necesidad de la medida.

6. De obtenerse la autorización judicial, la/el AMPF solicita informes a las Instituciones Financieras e Instituciones de Tecnología Financieras respecto de los hechos o personas relacionadas con la investigación primordial.

   Nota: Solicita a las unidades especializadas informen si cuentan con una investigación abierta o existen antecedentes respecto de los hechos o personas relacionadas con la investigación primordial.

7. La/el AMPF analiza los resultados y realiza una síntesis de los hechos denunciados.

   Nota: La/el AMPF analiza los actos de investigación, a efecto de determinar si de los mismos, existen indicios suficientes e idóneos para establecer vínculos que sean susceptibles de la posible comisión de un hecho que la ley señala como delito de defraudación fiscal.

8. La/el AMPF solicita los dictámenes periciales siguientes.

   - Dictamen pericial en sistemas de cómputo para establecer el empleo de criptomonedas y la tecnología en la cual se sustentó.
   - Dictamen pericial en valuación para establecer el valor de las criptomonedas al momento de la realización de los actos o actividades civiles y mercantiles que dieron lugar a la causación de las contribuciones
   - Dictamen Pericial en Contabilidad para determinar el monto del daño o perjuicio a la Hacienda Pública

6.1.8 GLOSARIO

Acrónimos / Siglas	Definición
AMPF	Agente del Ministerio Público Federal

CNPP	Código Nacional de Procedimientos Penales
UEAF	Unidad Especializada en Análisis Financiero

Cuadro 3: Elaboración propia

6.1.9 ANEXO. DILIGENCIAS EN INVESTIGACIONES FINANCIERAS Y FISCALES

La siguiente lista de actos de investigación se establece de manera enunciativa, más no limitativa con la finalidad de encontrar indicios constitutivos de un hecho que la ley señale como delito.

6.1.9.1 INFORMACIÓN PERSONAL

1. Solicitud de investigación a la Policía Federal Ministerial (todas sus bases de datos),
2. Consulta al Registro Nacional de Población e Identificación Personal.
3. Solicitud de información al Registro Civil del Estado donde guarden relación los hechos investigados
4. Solicitud de información a la Secretaría de Relaciones Exteriores.
5. Solicitud de información al Instituto Nacional de Migración.
6. Solicitud de información a la Fiscalía General del Estado donde guarden relación los hechos investigados.
7. Solicitud de información al Centro Nacional de Planeación Análisis e Información para el Combate a la Delincuencia. (CENAPI).
8. Consultar información en Plataforma México.
9. Solicitud de información al Centro de Investigación y Seguridad Nacional (CISEN).

La información que se obtenga respecto de lo anterior, permite conocer la identidad de las personas investigadas, modos vivendi, status social, si cuentan con antecedentes penales a nivel estatal o bien federal.

6.1.9.2 INFORMACIÓN FINANCIERA

1. Solicitud de información a la Comisión Nacional Bancaria y de Valores

2. Solicitud de información a la Comisión Nacional de Seguros y Fianzas
3. Solicitud de información a la Comisión Nacional del Sistema de Ahorro para el Retiro
4. Solicitud de información a American Express Company, México, S.A. de C.V.
5. Solicitud de información a la Secretaría de la Función Pública, en el caso de que los imputados tengan carácter de funcionarios públicos.
6. Solicitud de información al Banco de México.
7. Asistencia Jurídica Internacional (a través de las agregadurías y de la Coordinación de Asuntos Jurídicos Internacionales.

La información que se obtenga de lo anterior, permitirá conocer las diversas transacciones efectuadas por las personas investigadas mediante el empleo de criptomoneda, relacionadas con los hechos expuestos en la querella, el monto de las operaciones, el tipo de ahorro con el que cuentan, así como el monto del mismo, el incremento patrimonial de acuerdo a los activos que manejen.

Esta información debe obtenerse siempre que se hubiera obtenido autorización por parte del Juez de Control.

6.1.9.3 INFORMACIÓN FISCAL

1. Solicitud información al Servicio de Administración Tributaria, adicional a la ya suministrada por la autoridad fiscal en la querella correspondiente de ser necesario.
2. Solicitud de Información a la Secretaría de Finanzas de los Estados donde guarden relación los hechos investigados, adicional a la ya suministrada por la autoridad fiscal en la querella correspondiente de ser necesario.

Tal información permitirá conocer las actividades comerciales que se tienen registradas, así como saber si las personas sujetas a investigación se encuentran al corriente de los diversos impuestos que por sus actividades tengan que reportar.

6.1.9.4 INFORMACIÓN EMPRESARIAL

1. Solicitud de información a la Secretaría de Economía.

2. Solicitud de información a la Corredurías Públicas.
3. Solicitud de información a los Notarios Públicos como al Archivo General de Notarías.
4. Solicitud de información a las Cámaras de Comercio del ramo respectivo.
5. Solicitud de información al Instituto Mexicano del Seguro Social.

Esta información permitirá conocer si las personas investigadas tienen registrado a su nombre alguna empresa y de qué tipo, así como sus actividades, actos de comercio y el estado que guardan respecto a la misma.

Conclusiones

Conclusiones

1.- Tomando en cuenta que las características de la tecnología *Blockchain* sobre la que descansa la criptomoneda son publicidad, inmutabilidad, descentralización, distribución, consenso, seguridad y carácter abierto, se considera que es una tecnología confiable, pues tiene un alto grado de seguridad.

2.- La criptomoneda, no es dinero electrónico ni moneda digital; su naturaleza jurídica es la de ser un medio de pago, tiene como característica que se registra, transfiere electrónicamente y no es reconocida ni respaldada por el Banco de México; no tienen poder liberatorio para el cumplimiento de obligaciones, como en cambio, sí lo tiene el peso de nuestro país y divisas extranjeras, razón por la cual, desde un punto de vista estrictamente legal, ni siquiera puede llamársele "moneda".

4.- Con el empleo de la criptomoneda se permite la falta de identificación del usuario, por lo que es perfectamente posible que los recursos para su adquisición permanezcan ocultos y con ello se transformen en dinero y/o se adquieran bienes o servicios, de ahí que exista un riesgo importante en materia de prevención de operaciones con recursos de procedencia ilícita (lavado de dinero) y financiamiento al terrorismo, debido a la facilidad para transferir los activos virtuales a distintos países, así como la ausencia de controles y medidas de prevención homogéneos a nivel global.

5.- La Ley del Impuesto sobre la Renta no prevé mecánica o procedimiento alguno sobre la manera de calcular el impuesto correspondiente tratándose de la compraventa de criptomoneda y no es posible aplicar analógicamente las disposiciones, relacionadas con la ganancia o pérdida en la compra y venta de divisa extranjera, pues ésta no es divisa. Es necesario reformar la ley de la materia, para establecer un procedimiento para determinar la base gravable del Impuesto sobre la Renta, máxime cuando a diferencia de las divisas extranjeras, no hay parámetros ciertos de su valor, pues no existe una publicación oficial al respecto.

6.- Con las criptomonedas pueden cometerse múltiples delitos ya que con ellas se puede desarrollar una conducta típica, pues al representar de facto un valor económico, se usan como medio para obtener el pago en ilícitos como fraudes,

extorsiones, robo, secuestro, etcétera; por tanto, éstas son las herramientas con las que los sujetos se han valido para la realización de actividades con contenido económico y reprochables desde el punto de vista legal.

7.- En el tipo de defraudación fiscal, el engaño es el medio comisivo previsto por la ley para la realización del delito y puede realizarse con criptomonedas, puesto aun cuando no es dinero, al servir como instrumento de pago en las transacciones económicas o como instrumento de inversión, es sumamente complicado su fiscalización y proclive a la omisión de pago de impuesto.

8.- Al emplearse la criptomoneda como medio de pago, no existe una forma en que las autoridades fiscales tengan conocimiento de la operación y el monto de la misma de lo que depende la cuantificación de los impuestos y; como instrumento de inversión, en el supuesto de que ésta incremente su valor frente al peso mexicano, las autoridades mexicanas tampoco tendrán conocimiento de las ganancias devengadas por ello.

9.- En los delitos cometidos mediante el uso de criptomonedas la información bancaria y financiera es esencial, pues es necesario conocer los movimientos de cargo y abono tanto en los monederos virtuales como en los centros de intercambio entre la moneda nacional y las criptomonedas, sin embargo, esta información se encuentra protegida por el artículo 16, primer párrafo, constitucional y por el derecho de los particulares al secreto financiero y bancario que se traduce en que las instituciones bancarias no puedan divulgarla a terceros distintos de los propios usuarios.

10.- La solicitud de información financiera que realice el Ministerio Público Federal o el de las entidades federativas, además de realizarse a través del Fiscal General o el servidor público en quien delegue esa facultad, debe ser objeto de control judicial previo a que las instituciones financieras e instituciones de tecnología financiera otorguen la información, siempre que se justifique la necesidad de la medida.

11.- Si el Ministerio Público en su actuación no obtiene la autorización del Juez de Control para la obtención de la información financiera, estos datos de

prueba en la investigación, se habrán obtenido con violación a derechos fundamentales y deben ser excluidos por el Juez de Control en la etapa intermedia y no podrán ser valorados ni tomados en cuenta en el procedimiento penal.

12.- La determinación del daño a la hacienda pública, como la valuación de la criptomoneda y el empleo de la tecnología *blockchain* sólo pueden comprobarse mediante dictámenes periciales en los que de manera técnica y con profesionistas calificados se determinen tales aspectos, mismos que no están sujetos a control judicial previo, pues por sí mismos no inciden en los derechos fundamentales del contribuyente, sin embargo, para la determinación del daño a la hacienda pública, la valuación de la criptomoneda y el empleo de la tecnología *blockchain*, es necesaria la información financiera que previamente debió ser sujeta a control judicial, pues de no ser así, los datos de prueba serán ilícitos, así como también los dictámenes periciales que se realicen con base en esa información.

13.- Para la investigación del delito de defraudación fiscal mediante el empleo de criptomonedas, es necesario que se elabore un protocolo de actuación ministerial para que como una guía y, en cumplimiento a los principios constitucionales, sea utilizado por el Ministerio Público para establecer la existencia del delito y la probabilidad de que el imputado haya intervenido en su realización.

La Propuesta de Protocolo de Actuación Ministerial se presenta en el capítulo 6 del presente trabajo.

Bibliografía

AMBROSIO HIGUERA, Michel, *Derecho Penal Fiscal*, México, Porrúa, 2012.

AMEZCUA, Amezcua, Luis, "Algunos puntos relevantes sobre la dignidad humana en la jurisprudencia de la Corte Interamericana de Derechos Humanos", *Revista Iberoamericana de Derecho Procesal Constitucional*, México, No. 8. Porrúa, 2007, http://www. corteidh.or.cr/tablas/r24334.pdf>.

BIT2ME ACADEMY, "*¿Cómo funciona el Blockchain-Cadena de Bloques?"*, https://academy.bit2me.com/como-funciona-blockchain-cadena-de-bloques/.

CARRASCO IRIARTE, Hugo, Diccionario de Derecho Fiscal, México, Oxford, 2008.

CENTENO, Danya, *México y Convenio de Budapest: Posibles Incompatibilidades*, Red de Defensa de los Derechos Digitales, México, Junio 2018, *https://www.derechosdigitales.org/wp-content/uploads/minuta_r3d.pdf*.

CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS.

CONVENIO DE BUDAPEST.

CÓDIGO NACIONAL DE PROCEDIMIENTOS PENALES.

CÓDIGO FISCAL DE LA FEDERACIÓN.

CÓDIGO PENAL FEDERAL.

CÓDIGO PENAL PARA LA CIUDAD DE MÉXICO.

CÓDIGO PENAL DE JALISCO.

CÓDIGO PENAL DE SINALOA.

DEFINICION DE, Definicion De, "Cibernética" *https://definicion.de/cibernetica/*.

DONNA, Donna, Edgardo Alberto, "Precisiones sobre el principio de legalidad", *Estudios en Homenaje a Héctor Fix-Zamudio*, México, UNAM, Instituto de Investigaciones Jurídicas, 2009.

ECURED, "Informática", https://www.ecured.cu/Informática.

ELOY MORALES BRAND, José Luis, *Proceso Penal Acusatorio y Litigación Oral,* México, Rechtikal, 2014.

FLORES JUÁREZ, Othon, "¿Se pueden comprar inmuebles con criptomonedas?", *El Mundo del Abogado*, *1 de febrero de 2018,* http://elmundodelabogado.com/revista/posiciones/item/se-pueden-comprar-inmuebles-con-criptomonedas, consultado el 15 de diciembre del 2018.

GARCÍA MATA, Iñigo, "Criptografía básica para entender la tecnología blockchain", *Medium.com*, https://medium.com/@igmata/criptograf%C3%ADa-b%C3%A1sica-para-entender-la-tecnolog%C3%ADa-blockchain-eb94cdd64158.

GARCÍA MEXIA, Pablo, *Criptoderecho. La Regulación de Blockchain,* España, La Ley, 2018.

GARCÍA RICCI, Diego *Artículo 16 constitucional. Derecho a la Privacidad*, México, Suprema Corte de Justicia de la Nación, 2014, p.1, *https://archivos.juridicas.unam.mx/www/bjv/libros/8/3567/39.pdf.*

GÓMEZ BENÍTEZ, José Manuel, *Teoría Jurídica Del Delito, Derecho Penal Parte General, Madrid,* Civitas, 1984.

GONZÁLEZ QUINTANILLA, José Arturo, *Derecho Penal Mexicano,* México, Porrúa, 1991.

HERNÁNDEZ, Hernández, Aura, "Piden a México en Convenio de Budapest, ser más que un observador", *El Excelsior*, 7 de diciembre de 2016, *https://www.excelsior.com.mx/hacker/2016/12/07/1132670*.

HERRÁN AGUIRRE, Herrán Aguirre, Alejandro Francisco y Victorio López, Antonio de Jesús, "*Blockchain y confianza: Un estudio desde el Derecho*", *Revista Iberoamericana de Producción Académica y Gestión Educativa*, vol.5, núm. 10, julio – diciembre 2018, *http://pag.org.mx/index.php/PAG/article/view/754*.

LEY MONETARIA DE LOS ESTADOS UNIDOS MEXICANOS.

LEY PARA REGULAR LAS INSTITUCIONES DE TECNOLOGÍA FINANCIERA.

LEY FEDERAL PARA LA PREVENCIÓN E IDENTIFICACIÓN DE OPERACIONES CON RECURSOS DE PROCEDENCIA ILÍCITA.

LEY DE FIRMA ELECTRÓNICA AVANZADA.

LEY DEL IMPUESTO SOBRE LA RENTA.

LEY DE SEGURIDAD NACIONAL.

LEY DEL SEGURO SOCIAL.

LEY DEL INSTITUTO NACIONAL DEL FONDO NACIONAL DE LA VIVIENDA PARA LOS TRABAJADORES.

LEY DEL IMPUESTO AL VALOR AGREGADO.

LEY DE INSTITUCIONES DE CRÉDITO.

LEY PARA REGULAR LAS SOCIEDADES DE INFORMACIÓN CREDITICIA.

LIMA DE LA LUZ, María, “Delitos Electrónicos”, *Criminalia*, Academia Mexicana de Ciencias Penales, México, Porrúa, no. 1 - 6, año L, enero - junio 1984.

LIRA ARTEAGA, Óscar Manuel, *Cibercriminalidad. Fundamentos de Investigación en México,* 3a. ed., México, Ubijus, 2018

LÓPEZ LOZANO, López Lozano, Eduardo, “Investigaciones Financieras Paralelas”, Colegio de Contadores Públicos de México, 16 de julio de 2018, https://veritasonline.com.mx/investigaciones-financieras-paralelas/.

LÓPEZ MONROY, José de Jesús, *Diccionario Jurídico*, Instituto de Investigaciones Jurídicas de la Universidad Nacional Autónoma de México, México, Porrúa, 2004, Tomo III, p. 2353.

MIR PUIG, Santiago, *Derecho Penal, Parte General,* Barcelona, B de F; 2011.

------, *El Derecho Penal en el Estado Social y Democrático de Derecho,* Barcelona, Ariel, 1994, p. 159.

MIR PUIG, S. y Muñoz Conde F.; *Tratado de Derecho Penal, Parte General I;* Barcelona, Bosch, 1981.

MORENO GARCÍA, Alfonso, *Efectos Penales de la Discrepancia Fiscal de las Personas Físicas*, Tesis de Maestría, Universidad Panamericana, 2018, p. 72.

MUÑOZCANO ETERNOD, Antonio, *El derecho a la intimidad frente al derecho a la información*, México, Porrúa, 2010, p. 3.

NADER KURI, Jorge; *La investigación en el Código Nacional de Procedimientos Penales en el Código Nacional de Procedimientos Penales. Estudios*, México, Instituto de Investigaciones Jurídicas de la Universidad Nacional Autónoma de México, https://archivos.juridicas.unam.mx/www/bjv/libros/9/4032/8.pdf.

NAVA GARCÉS, Alberto Enrique, *Delitos Informáticos*, 3ª. Ed., México, Porrúa, 2016.

OJEDA VELÁZQUEZ, Ojeda Velázquez, Jorge, *Derecho constitucional Penal*, México, Porrúa, 2011, t. III.

ORCUTT, Mike, "Riesgos y ventajas de que los gobiernos lancen criptomonedas públicas" trad. de Ana Milutinovic, *MIT Technology Review, 2019*, *https://www.technologyreview.es/s/10815/riesgos-y-ventajas-de-que-los-gobiernos-lancen-criptomonedas-publicas*.

ORGANIZACIÓN PARA LA COOPERACIÓN Y EL DESARROLLO ECONÓMICO, *Computer related criminality: analysis of legal policy in the OECD Area*[98], ICCP, 1984.

ORO Y FINANZAS, Oro y Finanzas, *¿Qué son los contratos inteligentes o Smart contracts? Bitcoin y Ethereum o el dinero programable*, 17 de noviembre de 2015, *https://www.oroyfinanzas.com/2015/11/que-son-contratos-inteligentes-smart-contracts/*.

[98] Criminalidad relacionada con la informática: Análisis de la política legal en el área de la OCDE.

OROZCO ENRÍQUEZ, J. Jesús, *Diccionario Jurídico*, Instituto de Investigaciones Jurídicas de la Universidad Nacional Autónoma de México, México, Porrúa, 2004, Tomo III, p. 2353.

OROZCO-FELGUERES LOYA, Carlos, *Efectos Fiscales en Materia de Prevención de Lavado de Dinero,* Dofiscal Thomson Reuter, México 2013.

OSSORIO, Manuel, *Diccionario de Ciencias Jurídicas, Políticas y Sociales*, 27a. ed., Buenos Aires, Heliasta, 2000, p. 822.

PADILLA SANABRIA, Lizbeth Xóchitl, "Lavado de dinero y corrupción desde la perspectiva virtual", *El Heraldo de Puebla* del 10 de febrero de 2018, (*www.elheraldodepuebla.mx/archivos/28530).*

PASTORINO, Cecilia, "Convenio de Budapest: Beneficios e implicaciones para la seguridad informática", *We Live Security*, ESET Enjoy Safer Tecnology, 6 diciembre 2017, https://www.welivesecurity.com/la-es/2017/12/06/convenio-budapest-beneficios-implicaciones-seguridad-informatica.

PAVÓN VASCONCELOS, Francisco; *Diccionario de Derecho Penal, México,* Porrúa, 1997.

------, *Derecho Penal Mexicano*, Parte General, México, Porrúa, 2000.

PONCE RIVERA, Alejandro, *Nueva Responsabilidad fiscal penal*, México, Ediciones Fiscales ISEF, México 2000.

PORTE PETIT CANDAUDAP, Celestino, *Apuntamientos De La Parte General De Derecho Penal,* México, Porrúa, 1969.

REAL ACADEMIA ESPAÑOLA, "Criptograma", *http://buscon.rae.es/draeI/*.

------, "Información", *http://buscon.rae.es/draeI/*.

------, "consignar", *http://buscon.rae.es/draeI/*.

REYNOSO DÁVILA, Roberto, *Delitos patrimoniales*, México, Porrúa, 2001, p. 1.

RODRÍGUEZ, Darinka, "Criptomonedas no son de uso legal en México: Banxico", *El Financiero*, 10 marzo 2014,

http://www.elfinanciero.com.mx/economia/criptomonedas-no-son-de-uso-legal-en-mexico-banxico.html.

ROSEMBUJ, Tulio, *Bitcoin,* 1a. ed., Barcelona, el Fisco – G.L.E.T.S.L., 2015.

SANTIVAÑEZ, Juan José, "*Algunas Consideraciones sobre la Ley de Régimen Disciplinario del personal Policial*.", *Asociación Peruana de Derecho Policial*, 26 de septiembre de 2019 https://juanjosesantivanez.blogspot.com/2009/09/algunas-consideraciones-sobre-la-ley-n.html.

SARZANA, Carlo, "Criminalità E Tecnologia en Computers" *Crime, Rassagna Penitenziaria e Criminologia*[99], año 1, Roma, 1979, p.5, http://www.rassegnapenitenziaria.it/.

SEMANARIO JUDICIAL DE LA FEDERACIÓN Y SU GACETA, Novena Época, t. XXVII, mayo de 2008.

------, Novena Época, t. XXVIII, agosto de 2008.

------, Novena Época, t. XXX, diciembre de 2009.

------, Décima Época, Libro 33, t. II, agosto de 2016.

------, Décima Época, Libro 49, t. I, diciembre de 2017.

------, Décima Época, Libro 54, t. II, mayo de 2018, p. 1270.

------, Décima Época, Libro 55, t. II, junio de 2018.

------, Décima Época, Libro 66, t. II, mayo de 2019, p. 1270.

SOLÓRZANO DE LA BARREDA, Luis, *Punibilidad, Punición y Pena de los Sustitutivos Penales*, México, Porrúa, 2000, p. 70, *http://biblio.juridicas.unam.mx/libros/2/854/5.pdf*.

SOTO GAMA, Soto Gama, Daniel, *Principios Generales del derecho a la Información*, México, Instituto de Transparencia y Acceso a la Información Pública del Estado de México y Municipios, 2010,

[99] Criminalidad y tecnología en Computadoras. Revisión de prisiones y criminología.

ttp://www.infoem.org.mx/sipoem/ipo_capacitacionComunicacion/pdf/pet_tesis_003_2009.pdf.

TÉLLEZ VALDÉS, Téllez Valdés, Julio, *Derecho informático*, 3a. ed., México, McGraw-Hill, 2004.

TORRES LÓPEZ, Mario Alberto, *Teoría y Práctica de los delitos fiscales*, México, Porrúa, 2000.

URBINA NANDAYAPA., Arturo, *Los Delitos Fiscales en México, El cuerpo de los Delitos Fiscales en el Derecho Positivo*, México, PAC, 2012, t. II.

VON LISZT, Franz, *Tratado de Derecho Penal*, traducido de la 20a ed., trad. Luis Jiménez de Asúa, 4a. ed., Reus, Madrid, 1999, t. II. p. 4.

WIKIPEDIA, "*Electrónica*", https://es.wikipedia.org/wiki/Electr%C3%B3nica.

------, "*Dinero Fiduciario*", https://es.wikipedia.org/wiki/Dinero_fiduciario.