La Administración tributaria frente al anonimato de las criptomonedas: la seudonimia del Bitcoin[1]

BEGOÑA PÉREZ BERNABEU
Profesora Titular. Universidad de Alicante

1. Consideraciones previas. 2. El anonimato (relativo) del Bitcoin. 2.1. La criptografía de clave asimétrica o pública. 2.2. La seudonimia del sistema Bitcoin como elemento clave de su anonimato. 3. La información tributaria como elemento clave para asegurar el *tax compliance.* 3.1. Consideraciones previas. 3.2. Las distintas opciones legislativas de lucha contra el anonimato relativo de Bitcoin. 4 Reflexiones finales

RESUMEN. Dentro de la categoría de dinero electrónico no regulado, las criptomonedas –entre las que se incluye el Bitcoin– han adquirido un protagonismo inusitado en los últimos tiempos. Se trata de monedas basadas en tecnologías criptográficas avanzadas que permiten su emisión, validación y registro de manera descentralizada. A pesar de no ser una moneda de curso legal y de carecer de valor intrínseco, ha comenzado a ser utilizado para los intercambios comerciales. Consecuentemente, su adquisición, venta, uso o tenencia tienen una innegable trascendencia tributaria.

No obstante, una de las principales dificultades con las que se encuentra la Administración tributaria y que constituye el objeto principal de esta Comunicación, es, precisamente, el anonimato (relativo) que ofrece Bitcoin a sus usuarios, ya que la tecnología blockchain permite al usuario ocultar su identidad real bajo un seudónimo, gracias al sistema de doble clave (una pública y otra privada) sobre el que se basa.

El anonimato que brinda esta criptomoneda presenta un importante reto para la Administración tributaria que debe adaptar los tradicionales esquemas y recursos de los que hasta ahora se servía para emplearlos en su nueva lucha contra la ocultación y fraude tributario que tiene lugar en un ámbito que escapa a su control al desarrollarse toda la operativa sobre una red P2P (también denominada red de pares), es decir, entre usuarios particulares cuya identidad se desconoce y sin intervención de ninguna autoridad centralizada (como por ejemplo, el sistema bancario) sobre el que hacer recaer labores de control y suministro de información a la Administración tributaria. En la Comunicación, apuntamos algunas posibles vías de actuación de la Administración tributaria ante los desafíos que presenta el Bitcoin en particular y las criptomonedas en general.

[1] Este trabajo ha sido realizado en el marco del Proyecto de I+D (Convocatoria 2015) concedido por el Ministerio de Economía y Competitividad, bajo el título "La Seguridad Jurídica en el Ordenamiento Tributario", Referencia DER2015-68072-P (MINECO/FEDER), cuyos investigadores principales son el Profesor JORGE MARTÍN LÓPEZ y la Profesora BEGOÑA PÉREZ BERNABEU (Resolución de concesión de 6 de mayo de 2016).

Asimismo la autora pertenece al Grupo de Investigación que ha recibido las Ayudas para Grupos de Investigación de Excelencia del Programa PROMETEO 2016, "Los planes de acción contra la erosión de la base imponible y el traslado de beneficios y la seguridad jurídica en el ordenamiento europeo e internacional", (Resolución de concesión de 1 de septiembre de 2016, Expediente PROMETEO/2016/053), financiado por la Conselleria de Educación, Investigación, Cultura y Deporte, de la Generalitat Valenciana, con fecha de inicio 01/01/2016, con una duración de 4 años, cuya investigadora principal es AMPARO NAVARRO FAURE.

1. CONSIDERACIONES PREVIAS

Dentro de la categoría de dinero electrónico no regulado, las criptomonedas –entre las que se incluye el Bitcoin– han adquirido un protagonismo inusitado en los últimos tiempos. Se trata de monedas basadas en tecnologías criptográficas avanzadas que permiten su emisión, validación y registro de manera descentralizada que, a pesar de no ser una moneda de curso legal y de carecer de valor intrínseco, han alcanzado un elevado valor de capitalización en el mercado de criptodivisas –especialmente el Bitcoin– lo que ha provocado que haya comenzado a ser utilizado para los intercambios comerciales. En concreto, el Bitcoin es aceptado como medio de pago por comercios y negocios como Microsoft, Dell, PayPal, Expedia, Virgin Galactic, Steam, Chicago Sun-Times, Victoria's Secret, OkCupid o Subway, entre otros. Es decir, aunque no se trate de dinero desde un punto de vista legal, sí que es un bien económico con cualidades dinerarias puesto que es utilizado como medio de pago.

Bitcoin puede definirse como una moneda virtual no regulada de carácter bilateral basada en un complejo sistema de criptografía (de ahí deriva el término de criptomoneda) y de carácter descentralizado. Su abreviación para identificarla en los mercados es BTC. Además, el nombre de Bitcoin se aplica también al software libre diseñado por el mismo autor para la gestión en la red *Peer to Peer* o *P2P* en la que opera.

Esta criptodivisa apareció en 2008[2] cuando un autor (o grupo de ellos) desconocido publicó en Internet –bajo el seudónimo de Satoshi Nakamoto– un trabajo[3] que describía el sistema Bitcoin en el que se describía el sistema de funcionamiento de una moneda virtual basada en criptografía asimétrica de clave pública. El sistema entró en funcionamiento el enero de 2009 cuando su autor desconocido creó el primer bloque –denominado «bloque génesis»– de la *blockchain* y creó un monedero virtual o *e-wallet* de Bitcoin que permite operar con esta criptomoneda.

El funcionamiento del sistema Bitcoin está basado en un tipo de tecnología que se denomina *blockchain*. La *blockchain* es un registro, similar a un libro mayor de contabilidad, que contiene todas las operaciones realizadas con Bitcoins desde su inicio en enero de 2009 hasta la actualidad, lo que implica que su tamaño está creciendo constantemente. La *blockchain* es reproducida y almacenada libremente en los diferentes nodos de la red Bitcoin, por lo que se afirma que el sistema Bitcoin es un sistema completamente descentralizado, sin intervención de una autoridad centralizada.

Como la propia traducción literal de su nombre indica, *blockchain* es una secuencia de bloques. Cada bloque, a su vez, es una colección criptográficamente cerrada de todas las transacciones que han ocurrido en la red en los últimos diez minutos[4] (almacenadas en una estruc-

---

2 El documento se colgó el 31 de octubre de 2008 en una lista de correo.

3 https://bitcoin.org/en/bitcoin-paper, consultado por última vez el 29 de enero de 2018.

4 Las operaciones con Bitcoins no se recogen en la *blockchain* de manera fluida y continua, sino en intervalos de tiempo de aproximadamente 10 minutos que es el tiempo que se tarda en verificar cada bloque. Se trata de una medida de seguridad contra posibles atacantes del sistema.

tura llamada *MerkleTree*[5]) que, además, contiene un resumen criptográfico del bloque anterior (*hash)*.

Cada bloque se agrega a la *blockchain* de forma indexada y cada nuevo bloque contiene el *hash* del bloque previo, lo que asegura que la modificación de cualquier bloque por en medio de la cadena implicaría la modificación de todos los bloques de la cadena ubicados desde el que se modifica hasta el final de la misma al objeto de hacer coincidir todos los valores *hash*. Esto hace que sea prácticamente imposible modificar ningún bloque de la *blockchain*.

Para comenzar a utilizar el sistema *Bitcoin* y poder realizar transacciones no es necesario seguir ningún proceso de registro en la que deba facilitarse información de carácter personal, que pueda servir para identificar al usuario frente a terceros, ni tampoco se exige facilitar una dirección de *e-mail*[6], ni siquiera un nombre de usuario y contraseña. Para realizar transferencias con esta criptomoneda tan sólo se necesita instalar[7] en el ordenador, tableta o móvil algún tipo de monedero electrónico apto para operar con Bitcoin o bien utilizar los servicios de monedero electrónico o *e-wallet* de alguna plataforma on-line.

Una vez creado el monedero, se generan dos claves (una pública y otra privada, como veremos seguidamente) ambas claves están matemáticamente relacionadas, y de hecho, la clave pública deriva de la clave privada. A partir de esta clave pública, se genera la dirección Bitcoin, que es una cadena de números y letras que podríamos definir como la huella digital de la clave pública. Es un número identificador único[8] que se asigna a los usuarios de Bitcoin, si bien cada usuario de Bitcoin puede tener tantas direcciones de Bitcoin como desee asociadas al mismo monedero virtual.

La clave privada debe permanecer en secreto, puesto que permite la disposición de los Bitcoins, mientras que la dirección pública debe compartirse para poder realizar operaciones ya que será el destino de las adquisiciones de Bitcoin que realice el usuario.

2. EL ANONIMATO (RELATIVO) DEL BITCOIN

2.1. La criptografía de clave asimétrica o pública

Los sistemas de cifrado o criptográficos pueden ser clasificados, a grandes rasgos, en una doble tipología[9]: simétricos y asimétricos. En primer término, los sistemas de cifrado simétrico o de

---

5 Un árbol hash de Merkle (*Merkle Hash Tree*) o árbol de Merkle o árbol hash es una estructura de datos en árbol, binario o no, que permite que gran número de datos separados puedan ser ligados a un único valor de hash, el hash del nodo raíz del árbol. De esta forma proporciona un método de verificación segura y eficiente de los contenidos de grandes estructuras de datos, véase https://es.wikipedia.org/wiki/%C3%81rbol_de_Merkle, consultado por última vez el 17 de enero de 2018.

6 En ocasiones el usuario facilita de manera opcional una dirección de correo electrónico a los únicos efectos de verificar la identidad del usuario cuando quiera acceder a ella, así como una contraseña.

7 Debe descargarse desde bitcoin.org.

8 Por ejemplo: 15sa4MGQw8QR7qKENLNfgux8i8GAdT9DW8.

9 No obstante, herramientas como PGP, GnuPG, SSH o la capa de seguridad SSL para la jerarquía de protocolos TCP/IP utilizan una criptografía híbrida que usa tanto los sistemas de clave simétrico, como el de clave asimétrica.

clave privada son aquellos que utilizan la misma clave para cifrar y descifrar un documento, es decir, que tanto el emisor como el receptor deben utilizar la misma clave para cifrar y descifrar, respectivamente, el mensaje[10], siendo la principal ventaja de estos su velocidad, ya que es más rápida debido a que los métodos de cifrado y descifrado son más sencillos. No obstante, su talón de Aquiles viene representado por la necesidad de mantener secreta la clave y, por tanto, los problemas de distribución de dicha clave entre los usuarios.

Para superar estas desventajas se recurrió al sistema de clave asimétrica, el cual elimina el problema de transmisión de la clave secreta entre emisor y receptor, pues la única clave que se distribuye es la pública[11], manteniéndose la privada para el uso exclusivo del propietario, utilizándose la clave privada para descifrar y firmar los mensajes[12]. No obstante, presenta ciertas desventajas[13], pues para una misma longitud de clave y mensaje se necesita mayor tiempo de proceso, las claves deben ser de mayor tamaño que las simétricas (generalmente son cinco o más veces de mayor tamaño que las claves simétricas) y el mensaje cifrado ocupa más espacio que el original. Al objeto de salvar estos inconvenientes se han desarrollado nuevos sistemas de clave asimétrica basados en curvas elípticas. La criptografía de curva elíptica o *Elliptic Curve Digital Secure Algorithm* (*ECDSA*), la cual, además de ser extremadamente segura desde un punto de vista matemático, es más rápida y utiliza claves más pequeñas.

La criptografía de clave asimétrica o sistema de claves públicas anónimas asegura el anonimato en Bitcoin, pues aunque cada nodo[14] del sistema Bitcoin tiene acceso a la *blockchain* o cadena de bloques, ésta contiene información únicamente sobre la cuantía y el momento de realización de la operación, así como la clave pública de los intervinientes, sin recoger ningún tipo de información adicional de carácter personal.

Por tanto, el anonimato en el sistema Bitcoin radica en la imposibilidad de vincular cualquier clave pública con su usuario. Tan sólo podría llegar a conocerse la identidad del interviniente de la operación Bitcoin si, de alguna manera, se identifica a un determinado sujeto con una dirección o clave pública Bitcoin, en este caso resultaría sencillo rastrear en la *blockchain* todas las operaciones realizadas por este sujeto (es la situación que viene a denominarse *loss of transactional privacy*).

---

[10] Ejemplos de criptografía simétrica el cifrado César, también conocido como cifrado por desplazamiento, código de César o desplazamiento de César que es un tipo de cifrado por sustitución en el que una letra en el texto original es reemplazada por otra letra que se encuentra un número fijo de posiciones más adelante en el alfabeto o la autenticación de un móvil GSM: el número de teléfono es reconocido, aunque el usuario inserte la tarjeta SIM en otro teléfono.

[11] La clave pública puede ser utilizada por cualquier otro usuario que desee comunicarse con el usuario titular de dicha clave pública.

[12] Por tanto, se necesitarán sólo n pareces de claves por cada n personas que deseen comunicarse entre sí y cada una de las n personas tendrá su clave privada y n-1 claves públicas distintas si quiere enviar mensajes a todas las n-1 personas restantes.

[13] Véase https://es.wikipedia.org/wiki/Criptograf%C3%ADa_asim%C3%A9trica , consultada por última vez el 12 de enero de 2018.

[14] El sistema Bitcoin está compuesto por una red de ordenadores de particulares interconectados en los que está instalado el software de cliente de Bitcoin. Cada uno de estos ordenadores recibe el nombre de "nodo".

2.2. La seudonimia del sistema Bitcoin como elemento clave de su anonimato

En internet el anonimato puede entenderse de dos maneras distintas: de una manera literal, es decir, actuar sin ningún tipo de nombre o identidad, o bien de una manera relativa consistente operar mediante un pseudónimo o nombre falso. En el caso del Bitcoin, los usuarios operan dando a conocer una clave pública o dirección, es decir, no se conoce su identidad real, pero sí se recurre a un seudónimo. Es decir, el anonimato predicable del sistema Bitcoin no es absoluto, sino relativo.

Como hemos expuesto, la seudonimia no asegura *per se* el anonimato de los usuarios, ya que es posible, en algunos casos, establecer una relación entre la clave pública o dirección de Bitcoin y la identidad real del usuario. No obstante, el anonimato puede llegar a alcanzarse si a la seudonimia se une la propiedad de desvinculación (*unlinkability*) del sistema.

El término de desvinculación o *unlinkability*[15] hace referencia a la idea de que a cualquier usuario que acceda a la información contenida en la *blockchain* le resulta imposible obtener más información de la que está contenida en esos registros. En el fondo, se persigue proteger el anonimato de un usuario de Bitcoin del resto de usuarios del sistema. Gracias a la tecnología *blockchain*, antes descrita, la *unlinkability*es posible. Es por ello, que en el sistema Bitcoin es posible hablar de «trazabilidad» de las operaciones al quedar almacenadas en *blockchain*, pero se conserva el anonimato de los intervinientes en las distintas transacciones debido a la utilización de claves públicas o direcciones (que hacen las funciones de seudónimo).

A este anonimato intrínseco de la tecnología empleada en el sistema Bitcoin, debe sumarse la existencia de herramientas que permiten a los usuarios eliminar de forma intencionada la trazabilidad de las operaciones realizadas con Bitcoins. Algunos ejemplos de ello son el uso de varias cuentas (cada una de ellas con distinta clave pública) por el mismo usuario, el uso de software que mezcla múltiples direcciones de Bitcoins para dificultar o imposibilitar el rastreo del usuario que realizó la operación sujeta a gravamen (son los denominados *tumblers* o *mixers*, de los que TumbleBit es un ejemplo), o el cambio de Bitcoins por otras criptodivisas que permiten un anonimato absoluto (como es el caso de Monero, por ejemplo).

3. LA INFORMACIÓN TRIBUTARIA COMO ELEMENTO CLAVE PARA ASEGURAR EL *TAX COMPLIANCE*

3.1. Consideraciones previas

El tradicional sistema de obtención de información por parte de las Administraciones tributarias que asegura un grado satisfactorio de cumplimiento tributario (*tax compliance*) por parte de los obligados tributarios descansa sobre una estructura centralizada de intermediarios que suministran dicha información. Se trata de bancos, pagadores de rentas, notarios… sobre quienes reca-

[15] ANDROULAKI, E.; KARAME, G. O.; ROESCHLI,N M.; SCHERER, T., y CAPKUN ,S. (2013): "Evaluating User Privacy in Bitcoin" in *Financial Cryptography and Data Security*, SADEGHI, A. R. (ed.), Springer, Berlin, Heidelberg, págs. 34-51.

en obligaciones de obtención de información de los obligados tributarios y su posterior transmisión a la Administración tributaria, de manera que si el obligado tributario no procede de manera voluntaria al cumplimiento de sus obligaciones tributarias dentro de plazo, la Administración tributaria tiene la suficiente información para exigir su cumplimiento de manera coercitiva.

La aparición de las criptomonedas en general –y del Bitcoin en particular– como fenómeno con relevancia tributaria supone una quiebra de este esquema clásico del que se servía la Administración para asegurar el cumplimiento de las obligaciones tributarias por parte de los obligados tributarios.

Esta quiebra viene motivada, de un lado, por el carácter descentralizado de la tecnología subyacente a las criptomonedas cuya principal consecuencia es la inexistencia de una autoridad central, que asuma la condición de intermediario centralizado y sobre la que el legislador pueda hacer recaer obligaciones de suministro de información y, de otro lado, por el anonimato –absoluto o relativo, según los casos– que ofrecen estas criptomonedas a sus usuarios, lo que dificulta, cuando no imposibilita, a la Administración tributaria conocer la verdadera titularidad de estos usuarios, socavando de este modo los protocolos de obtención de información existentes y dejando a la Administración tributaria sin la herramienta más afectiva para asegurar el cumplimiento de las obligaciones tributarias por los obligados tributarios, ya se trate de un cumplimiento voluntario o coercitivo.

En el caso en concreto del Bitcoin, debido al carácter descentralizado de la tecnología *blockchain* sobre la que descansa su funcionamiento, unido a la seudonimia o anonimato relativo que proporciona el sistema Bitcoin, no es posible conocer la verdadera identidad del usuario que se esconde detrás de la clave pública. No obstante, dado que la todas las operaciones se encuentran recogidas en la *blockchain* de forma abierta, mediante el uso del oportuno software la Administración tributaria podría rastrear todas las operaciones realizadas con una determinada cuenta de Bitcoin identificando a ésta por su clave pública y, de esta manera, conocer el saldo de Bitcoins existentes en dicha cuenta, así como todas las transacciones realizadas con destino u origen en dicha cuenta.

3.2. Las distintas opciones legislativas de lucha contra el anonimato relativo de Bitcoin

Aunque la Administración tributaria tenga acceso a la información almacenada en la *blockchain*, todavía necesitaría poder vincular la clave pública con la identidad real de un obligado tributario para poder asegurar el cumplimiento de las obligaciones tributarias por parte de éste. Las posibles vías de actuación para conseguir este objetivo son dos, pues o bien la Administración consigue la necesaria información por sus propios medios, o bien pueden obtener esta información de otras Administraciones tributarias que ya posean esta información

Al objeto de identificar a los titulares de las cuentas de Bitcoin, las autoridades tributarias pueden recurrir a complejos métodos de análisis basados en técnicas de "desanonimización" de usuarios de Bitcoin mediante la agrupación de direcciones de Bitcoin que controla un mismo usuario (estas técnicas reciben el nombre de *deanonymizating techniques to cluster Bitcoin ad-*

dresses[16]), lo que permite llegar a identificar a este. No obstante, esta técnica no permite identificar a todos los usuarios de las cuentas sobre las que se trabaja, sino solo a un porcentaje de ellos, siendo más fácil identificar a los usuarios principales.

Otra posible vía de actuación para conseguir allegar a la Administración tributaria información con trascendencia tributaria sobre el uso de Bitcoin es ampliar el concepto de intermediario financiero[17], incluyendo dentro de éste a sujetos que tradicionalmente ha sido excluidos de esta categoría, como sería el caso de los *exchangers* o casas de cambio, intermediarios naturales del sistema Bitcoin.

La motivación de esta opción legislativa reside en el hecho de que el anonimato relativo que ofrece Bitcoin resulta fácil de mantener siempre que el usuario no salga del sistema, pero ya no se garantiza cuando el usuario salga de dicho sistema, por ejemplo, cuando desee materializar el valor atribuido a esta criptomoneda, convirtiendo sus Bitcoins a moneda de curso legal (euros, dólares…). Este cambio tiene lugar a través de casas de cambio o *exchangers* especializados en convertir esta criptomoneda en dinero de curso legal, por lo que la solución pasaría por la exigencia de facilitar información de carácter personal (que vaya más allá de la mera clave pública) a los usuarios que vayan a adquirir Bitcoins o que vayan a cambiarlos por moneda de curso legal como requisito imprescindible para realizar la operación deseada y la consecuente obligación del *exchanger* de suministrar dicha información a la Administración tributaria competente[18].

Esta ha sido la opción legislativa elegida por la Unión Europea (UE) y EEUU. En concreto EEUU se ha servido de la *Foreign Account Tax Compliance Act* (*FATCA*), aprobada en marzo de 2010 (que establecen un régimen de comunicación de información[19] para las instituciones financieras respecto de ciertas cuentas cuya titularidad corresponde a ciudadanos y residentes –personas físicas y entidades– estadounidenses), para obtener información sobre las cuentas de Bitcoin en el extranjero de sus nacionales, apoyándose en la amplia definición de *foreign financial institution*[20]

---

[16] De entre la abundante bibliografía existente sobre esta cuestión, véase MEIKLEJOHN, S.; POMAROLE, M.; JORDAN, G.; LEVCHENKO, K.; MCCOY, D.; VOELKER, G. M., y SAVAGE, S. (2013): "A fistful of Bitocins: characterizing payments among men with no names", en *Proceedings of the 2013 conference on Internet measurement conference,* ACM, págs. 127-140, y DOLL, A.; CHAGANI, S.; KRANCH, M., y MURTI, V. (2014): *Btctrackr: finding and displaying clusters in bitcoin,* Princeton University, USA, disponible en http://randomwalker.info/teaching/spring-2014-privacy-technologies/btctrackr.pdf, consultado por última vez el 30 de enero de 2018.

[17] Una obligación de suministro de información de este tipo también podría recaer sobre los establecimientos comerciales que aceptan el pago de sus productos o servicios con Bitcoin, si bien el reducido número de establecimientos que en la actualidad aceptan el pago en esta criptomoneda plantea dudas sobre la viabilidad de esta opción.

[18] Hay aún pocos requerimientos legales para las casas de cambio de bitcoin de identificar a sus usuarios, pero la mayoría –si no todas– requieren de forma preventiva algún tipo de identificación por parte de sus usuarios: facturas con nombre y dirección, documentos de identidad como pasaporte o carnet de conducir… Véase https://coineda.wordpress.com/2014/07/27/como-funciona-una-casa-de-cambio-de-criptodivisas/, consultada por última vez el 28 de enero de 2018.

[19] En virtud de esta norma, las instituciones financieras afectadas deben suministrar al IRS norteamericano en un archivo XML según el modelo de suministro de información fijado por FATCA el nombre de los inversores, dirección, número de identificación fiscal, número de cuenta, saldo de la cuenta y pagos realizados dentro del período establecido.

[20] "[a]ny foreign entity that: Accepts deposits in the ordinary course of banking or a similar business such as banks and credit unions. Holds financial assets for the account of others as a substantial portion of its business such as brokerages or custodians."

que contiene dicha norma que da cabida a la inclusión de los *exchangers* o casas de cambio y las plataformas que ofrecen el servicio de *e-wallets* o monederos virtuales. No obstante, la ambigüedad e imprecisión en los términos empleados por esta norma y la falta (parece ser que intencionada) de claridad sobre este aspecto del IRS está generando un clima de incertidumbre entre los contribuyentes norteamericanos, por lo que sería deseable la inclusión de referencias expresas a las criptodivisas, o los monederos virtuales en el texto de esta norma[21].

A falta de estos cambios legislativos, la aplicación de FATCA en su actual redacción al fenómeno Bitcoin significa no solo dotar a la figura del Bitcoin de una doble calificación jurídica (pues el IRS califica a los Bitcoin como *property*[22] a efectos de su legislación federal tributaria, pero los asimila a activos financieros para su posibilitar la aplicación de FATCA), sino forzar también la interpretación de algunas de las previsiones en ella contenidas, para incluir a las *e-wallets* donde los usuarios guardan sus Bitcoins dentro del concepto de instituciones de custodia o las instituciones de depósito[23] previstas en este instrumento jurídico, por ejemplo.

Por su parte, con una técnica legislativa más depurada, la UE en su propuesta[24] de Directiva COM (2016) 450 final 2016/0208 (COD) de modificación de la Directiva de Prevención de Blanqueo de Capitales (EU) 2015/849 (4AMLD), incluye dentro de su ámbito de aplicación a las plataformas de cambio de monedas virtuales (*exchangers*) y los proveedores de servicios de custodia de monederos electrónicos, que, una vez esta norma entre en vigor, tendrán que aplicar controles de diligencia debida con respecto al cliente, lo que pondrá fin al anonimato asociado a dichos intercambios.

Esta propuesta de Directiva es la primera iniciativa europea para llevar a la práctica el Plan de Acción de lucha contra la financiación del terrorismo de febrero de 2016, y en relación con la actividad del sector de las Monedas Virtuales podemos considerar que es la primera iniciativa legislativa Europea de regulación de dicho sector, siguiendo las recomendaciones Banco Central Europeo, que en su Informe de Febrero de 2015 relativo a la monedas virtuales establecía que las monedas virtuales no se encontraban reguladas, y que las autoridades nacionales y europeas debían utilizar los marcos legislativos existentes de regulación y supervisión para que los mismos fueran aplicables a las monedas virtuales a través de su modificación y adaptación.

Para ello, se procede a modificar tres preceptos de la Directiva de Prevención del Blanqueo de Capitales. En primer lugar, se incluye dentro del artículo 2 de la Directiva relativo a las entidades obligadas los apartados g) y h) para referirse a los proveedores de servicios que se dediquen

---

21 VALERIANE, E. (2016): "IRS, Will you spare some change? Defining virtual currency for the FATCA", *Valparios University Law Review*, n.º 863, págs. 903-910.

22 IRS Notice 2014-21.

23 Artículo 1, apartado 1, legras h) e i) del Acuerdo entre el Reino de España y los Estados Unidos de América para la mejora del cumplimiento fiscal internacional y la implementación de la Foreign Account Tax Complianc eAct, FATCA (Ley de cumplimiento tributario de cuentas extranjeras), hecho en Madrid el 14 de mayo de 2013, *BOE* núm. 159, de 1 de julio de 2014, páginas 50094 a 50122.

24 La propuesta fue presentada el 5 de julio de 2016, alcanzándose un acuerdo político sobre su contenido el 20 de diciembre de 2017 entre la Presidencia y el Parlamento Europeo. A continuación, el Parlamento y el Consejo deberán adoptar la propuesta de Directiva en primera lectura.

profesionalmente al cambio de monedas virtuales por monedas corrientes o divisas tradicionales y los proveedores de monederos electrónicos o *e-wallets* de monedas virtuales, que ofrezcan servicios de custodia de credenciales o claves necesarios para el acceso a las monedas virtuales, respectivamente.

En segundo lugar, se incluye dentro de las definiciones del artículo 3 a las monedas virtuales[25]. Y en tercer y último lugar, en el artículo 47 relativo a la supervisión y obligación de someter a licencia o registro a los establecimientos de cambio, las entidades de cobro de cheques y los proveedores de servicios a sociedades o fideicomisos, se incluyen a las plataformas de cambio y proveedores de monederos electrónicos o *e-wallets* de criptodivisas.

Si bien debido al período de transposición de esta norma (inicialmente previsto de 18 meses, según la propuesta de directiva) la definitiva adopción de esta norma puede retrasarse en los Estados miembros, en el caso de España, donde se ha presentado en el Senado una iniciativa legislativa[26] al objeto de considerar a los proveedores de servicios de cambio de moneda virtuales por monedas oficiales de algún Estado y a los prestadores de servicios de monederos virtuales entidades sujetas a la regulación de blanqueo de dinero quedando obligados a la identificación de sus clientes.

El principal inconveniente que plantea la opción legislativa de imponer a las casas de cambio y monederos virtuales obligaciones de suministro de información radica en el hecho de que las casas de cambio sólo ofrecen información cuando el usuario de Bitcoin "entra" o "sale" del sistema, mediante la compra o el cambio a otra divisa legal, permaneciendo el resto de operaciones realizadas dentro del sistema con carácter previo al cambio por divisa legal o posterior a la adquisición ignoradas por la Administración tributaria. Es por este motivo por el que a las casas de cambio o *exchangers* en este ámbito se les ha rebautizado con el expresivo término de *gatekeepers.*

El propio legislador europeo es consciente de que "la inclusión de las plataformas de intercambio virtual y de los proveedores de servicios de custodia de monederos electrónicos no resolverá totalmente la cuestión del anonimato asociado a las transacciones con monedas virtuales, al mantenerse el anonimato en gran parte del entorno de la moneda virtual, puesto que los usuarios pueden llevar a cabo transacciones al margen de las citadas plataformas o proveedores de servicios". Por este motivo y "para combatir los riesgos relacionados con ese anonimato, las Unidades de Información Financiera (UIF) nacionales deberían poder asociar las direcciones de las monedas virtuales a la identidad del propietario de esas monedas", añadiendo una tercera vía de actuación consistente en "la posibilidad de que los usuarios efectúen, con carácter voluntario, una autodeclaración a las autoridades designadas"[27].

---

25 Las cuales son definidas como "aquella representación digital de valor, no emitida por un Banco Central o Autoridad Pública y que no necesariamente se encuentre vinculada a monedas corrientes o divisas tradicionales, que sea aceptada por personas físicas y jurídicas como un medio de pago, y que pueda transferirse, almacenarse y comerciarse electrónicamente".

26 Presentada por el grupo popular en el Senado el pasado 23 de enero de 2018.

27 Considerando 7, propuesta de Directiva COM (2016) 450 final 2016/0208 (COD) de modificación de la Directiva de Prevención de Blanqueo de Capitales (EU) 2015/849 (4AMLD) Estrasburgo, 5.7.2016, COM(2016) 450 final.

Esta tercera opción parece ser una de las dos principales vías de actuación seguidas por EEUU, pues sobre los residentes en este país que sean titulares de cuentas de Bitcoin recaen obligaciones de información. En primer lugar, si se trata de supuestos de venta de Bitcoins o cambio de estos en dólares realizadas en EEUU, el contribuyente debe cumplimentar el formulario 8489[28] *Sales and Other Dispositions of Capital Assets*[29], en el cual deberá detallar cada una de las operaciones por separado.

Paralelamente, si se trata de cuentas de Bitcoin en el extranjero, la obligación de información tiene carácter doble[30]. Por un lado, si se superan ciertos límites, deben comunicar al *Financial Crimes Enforcement Network* (FinCEN) la tenencia de cuentas de Bitcoin mediante la cumplimentación de un formulario independiente denonimado*Form*114*Report of Foreign Bank and Financial Account*s (FBAR), dado que el FinCEN equipara[31] las cuentas de Bitcoin a las cuentas financieras (*financial account*).

Por otro lado, los contribuyentes usuarios de Bitcoin, cuyos activos superen un determinado valor, deben presentar al *Internal Revenue Service* (IRS), conjuntamente con su declaración anual de impuestos, el Form 8938, *Statement of Specified Foreign Financial*[32] suministrando información sobre las cuentas de Bitcoin de su titularidad.

El cumplimiento voluntario de estos deberes de suministro de información que recaen sobre los usuarios de Bitcoin se ve reforzada con un régimen de fuertes sanciones previsto a tal efecto, de manera que el incumplimiento de la obligación de informar al FinCEN mediante el Formulario 114 FBAR puede conllevar la imposición de sanciones civiles por cualquier tipo de comportamiento negligente e infracciones voluntarias e involuntarias. Estas multas ascenderán, para los casos más graves de incumplimientos voluntarios, en la mayor de las dos siguientes cuantías: o 100.000 dólares o el 50 por cien del balance de la contabilidad en el momento de comisión de la infracción. Mientras que en los supuestos de infracción por negligencia podrán reducirse hasta los 500 dólares.

Paralelamente, el incumplimiento del deber de cumplimentación y presentación del formulario 8938, el contribuyente se enfrenta a una multa por incumplimiento de su obligación de presentación cuya cuantía puede llegar hasta los 10.000 dólares, sanciones penales, y, si el incumplimiento de la obligación de presentación tiene como consecuencia una menor tributación del contribuyente, se enfrenta también a una sanción pecuniaria equivalente al 40 por ciento de la cantidad defraudada (*accuracy-related penalty*) y a una sanción por fraude equivalente al 75 por cien de la cantidad defraudada (*fraud penalty*).

---

28 Which is attached to Schedule D of a Form 1040.

29 Véase, https://www.irs.gov/pub/irs-pdf/f8949.pdf, consultado por última vez el 28 de enero de 2018.

30 Both forms are due by April 15, with the option to be extended until October 15.

31 Véase, FIN-2013-G001, "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies," March 18, 2013.

32 Véase www.irs.gov/Form8938 y también para consultar las instrucciones de cumplimentación de este formulario véase https://www.irs.gov/pub/irs-pdf/i8938.pdf, consultado por última vez el 28 de enero de 2018.

Sin embargo, aunque estas multas vienen a cumplir una innegable función de estímulo en el cumplimiento voluntario de las obligaciones tributarias (*tax compliance*) por parte de los usuarios de Bitcoin, su efectividad real queda en entredicho, ya que el IRS norteamericano desconoce de antemano los datos que el contribuyente debe declarar, al no existir la figura de un mediador centralizado en el sistema Bitcoin que suministra información con relevancia tributaria sobre las operaciones realizadas y la titularidad de las cuentas de Bitcoin. Es por ello que el IRS carece de herramientas para saber si sobre un determinado contribuyente recae la obligación de presentar el formulario 114 FBAR o el formulario 8938, por lo que desconoce si ese contribuyente ha incumplido sus obligaciones de información y, por tanto, debe ser sancionado.

De hecho, las sospechas que suscita un sistema de cumplimiento espontáneo de las obligaciones tributarias basado exclusivamente en la disposición de los obligados tributarios al cumplimiento voluntario de dichas obligaciones se vieron confirmadas por los datos aportados por el propio IRS relativos al reducido número de contribuyentes que cumplieron con dichas obligaciones, de manera que en 2013 únicamente 807 sujetos en todo EEUU informaron al IRS de la realización de alguna operación relativa a Bitcoins mediante la presentación del formulario 8949, número que ascendió a 893 en 2014 y 802 en el año 2015[33].

Es decir, la eficacia de un sistema de cumplimiento de obligaciones tributarias y de imposición de sanciones por su incumplimiento no puede descansar únicamente sobre la información declarada de forma unilateral por el contribuyente sin que la veracidad de esta información pueda ser contrastada por el IRS con la información suministrada por un tercero, pues difícilmente se puede sancionar a un sujeto que incumple su obligación de declarar, si la administración tributaria ignora incluso si sobre este sujeto recae la obligación de declarar.

Tal vez, el IRS ha querido contrarrestar esta ausencia de información mediante la realización de *fishing expeditions*[34] como la que tuvo lugar mediante la solicitud por parte del IRS estadounidense, en noviembre de 2016, de un *John Doesummons*[35], sobre todos los clientes de *Coinbase*, solicitando información[36] sobre el historial de transacciones, la dirección IP, entre otros datos desde 2013 a 2015.

---

[33] IRS Affidavit for Coinbase, Declaration of David Utzke in support of petition to enforce Internal Revenue Service Summons, Case 3:17-cv-01431-JSC, California Northern District Court.

[34] ELLIOTT, A. (2017): "Collection of cryptocurrency customer-information: tax enforcement mechanism or invasion of privacy?", *Duke Law & Technology Review*, vol. 16, n.º 1, pág. 12.

[35] Se trata de una citación para una persona no identificada, prevista en el *Internal Revenue Cod*, Section 7609(f). Se trata de una herramienta a disposición del IRS mediante una aprobación del sistema de la Corte Federal de los EEUU. El IRS utiliza la citación "John Doe" cuando lanza su amplia red para localizar los nombres de los contribuyentes estadounidenses que de otro modo serian desconocidos al IRS. Para poder obtener una citación "John Doe", el IRS debe de responder satisfactoriamente a la Corte Federal que la información que el IRS procura, no está disponible de otras fuentes regulares de información, y que existe una "base de causa razonable" para creer que el contribuyente estadounidense (o pluralidad de ellos) no ha cumplido con las leyes fiscales de EEUU.

[36] Si bien, debido a la presión ejercida por el Congreso de EEUU, la empresa *Coinbase* y los clientes de ésta, el 6 de julio de 2017 el Gobierno redujo el ámbito de la información solicitada.

En cuanto a la obtención de información mediante los oportunos procedimientos de intercambio de información, hasta la fecha destaca la intención de utilizar de esta vía por parte de EE.UU, quien pretende servirse de los Acuerdos Intergubernamentales para implementar FATCA ya existentes como mecanismo de obtención de información relativa al uso de Bitcoin que obre en poder de otras jurisdicciones tributarias. Si bien la terminología utilizada en estos Acuerdos no referida expresamente al fenómeno Bitcoin podría suponer un obstáculo a la efectividad de este instrumento, por lo que sería aconsejable modificar dichos acuerdos haciendo una referencia expresa al fenómeno Bitcoin introduciendo definiciones y previsiones a tal efecto[37].

4. REFLEXIONES FINALES

La tecnología *blockchain,* utilizada por la mayoría de criptomonedas y, en concreto, por el Bitcoin, supone un importante reto para la Administración tributaria que debe adaptar los tradicionales esquemas y recursos de los que hasta ahora se servía para emplearlos en su nueva lucha contra la ocultación y fraude tributario que tiene lugar en un ámbito que escapa a su control al desarrollarse toda la operativa sobre una red P2P descentralizada, es decir, entre usuarios particulares cuya identidad se desconoce y sin intervención de un intermediario centralizado (como pudiera ser el sistema bancario) que pudiera llevar a cabo labores de control y suministro de información a la Administración tributaria. Ante esta nueva realidad tecnológica, los mecanismos tradicionales de lucha contra la evasión fiscal mediante el intercambio de información no resultan efectivos para luchar contra la elusión fiscal en el ámbito de las criptomonedas, especialmente en el caso del Bitcoin.

La obtención de información por la Administración tributaria es la pieza fundamental del complejo rompecabezas que representa la lucha contra la evasión fiscal en el ámbito de Bitcoin propiciado por el anonimato relativo existente en el sistema de esta criptomoneda. Si bien, ante las dificultades que encuentra la Administración tributaria para obtener la información relativa a las verdaderas identidades de los usuarios de Bitcoin, resulta evidente que el sistema de información de Bitcoin no puede descansar exclusivamente sobre el cumplimiento voluntario de las obligaciones de información que recaen sobre los usuarios, ni siquiera, aunque pesen sobre estos la amenaza de importantes sanciones. Es por ello por lo que deben aprobarse nuevos instrumentos legales específicamente diseñados para luchar contra el fraude fiscal en el ámbito de esta novedosa tecnología, al mismo tiempo que los instrumentos existentes deben ser actualizados y adaptados a la misma.

Así pues, resulta claro que un sistema de información eficaz pasa por la obtención de información sobre la identidad de los titulares de las cuentas de Bitcoin sin necesidad de que los usuarios salgan del sistema Bitcoin para la obtención de dicha información. Ante esta necesidad, la lógica impone un sistema de obtención de información que vaya dirigido directamente contra los usuarios del sistema Bitcoin, ya que éstos son los únicos conocedores en todo momento del estado de sus cuentas y de las operaciones realizadas dentro del sistema.

---

[37] VALERIANE, E. (2016): "IRS, Will you spare some change? Defining virtual currency for the FATCA", *Valparios University Law Review*, n.º 863, 2016, págs. 903-910.

Para poder asegurar el cumplimiento forzoso de las obligaciones tributarias de los usuarios de Bitcoin, resulta imprescindible que la Administración tributaria pueda contrastar la información facilitada por el contribuyente con información que ya obra en su poder. En este sentido, es necesario complementar el sistema de obtención de información facilitada por el propio contribuyente con otros mecanismos de obtención de información a través de terceros sobre los que recaigan obligaciones de suministro de información, si bien esta vía complementaria de obtención de información con relevancia tributaria viene limitada por la condición de *gatekeepers* de estos intermediarios.

A todo ello hay que añadir que, dado el alto grado de deslocalización de las operaciones de Bitcoin, el intercambio de información a nivel internacional resulta una herramienta imprescindible. En este contexto, frente al uso de mecanismos bilaterales de intercambio de información tributaria como los Acuerdos Intergubernamentales del sistema FACTA o las disposiciones sobre intercambio de información previstas en los Convenios de Doble Imposición que presentan innegables limitaciones, los mecanismos multilaterales se presentan como la situación más adecuada. En este contexto, la Normativa CRS (Estándar Común de Reporte o *Common Reporting Standard*), elaborada por la OCDE junto con los países del G20 y la colaboración de la Unión Europea, aprobada por el Consejo de la OCDE el 15 de julio de 2014 –tras las oportunas modificaciones para adaptarla a las necesidades de obtención de información de los usuarios de criptodivisas– puede resultar una útil herramienta para el intercambio de información relativa a las criptodivisas y, en concreto, al fenómeno Bitcoin.

Mientras una iniciativa de este tipo llega a materializarse, la Administración tributaria española, consciente del desafío que suponen el uso de las nuevas tecnologías, como el *blockchain*, y la utilización de las criptomonedas, como el Bitcoin, por un lado, y la inaplazable necesidad de combatir el fraude fiscal en este ámbito, por otro lado, ha fijado como prioridad en su Plan de Control Tributario para 2018[38] potenciar "el uso por las unidades de investigación de la Agencia Tributaria de las nuevas tecnologías de recopilación y análisis de información en todo tipo de redes". Esta referencia prevista en el Plan de Control Tributario, parece referirse al hecho de que la AEAT se ha fijado como objetivo la obtención de datos relativos al uso de Bitcoin mediante el análisis de la *blockchain*, unido a la utilización de métodos de análisis dirigidos a la "desanonimización" al objeto de identificar a los titulares de las cuentas de Bitcoins.

[38] Resolución de 8 de enero de 2018, de la Dirección General de la Agencia Estatal de Administración Tributaria, por la que se aprueban las directrices generales del Plan Anual de Control Tributario y Aduanero de 2018, *BOE* 23 de febrero de 2018, n.º 20, págs. 8130-8153.