LAS CRIPTOMONEDAS: CONSIDERACIONES GENERALES Y EMPLEO DE LAS CRIPTOMONEDAS COMO INSTRUMENTO DE BLANQUEO DE CAPITALES EN LA UNIÓN EUROPEA Y EN ESPAÑA[1]

Xesús Pérez López

Universidad Rey Juan Carlos (Madrid)

Resumen: El trabajo, que se abre con un breve análisis introductorio del funcionamiento de las criptomonedas, afronta en su primera parte el análisis de las reacciones institucionales en la UE a los riesgos que éstas presentan desde el punto de vista de la ciberdelincuencia y de la delincuencia económica (incluyendo un análisis del proyecto de reforma de la Directiva (UE) 849, de blanqueo de capitales). La segunda parte del mismo presenta un panorama actualizado de la percepción social, reacciones institucionales y jurisprudenciales y práctica del uso de las criptomonedas en España, especialmente desde el punto de vista de su empleo criminal en el contexto del blanqueo de capitales.

Palabras clave: Criptomonedas, criptodivisas, *bitcoin*, blockhain, blanqueo de capitales, delincuencia económica, cibercrimen, ciberdelincuencia, Directiva (UE) 849/2015, estafa, ICOs

Abstract: The present work deals with the criminal uses of criptocurrencies in Europe and, in particular, Spain. In order to do so, it is preceded by a summary introduction to the economical and technical mechanics of the main virtual currencies. It studies then the institutional reactions

[1] El presente trabajo fue elaborado en el marco del proyecto de investigación «Ciberlaundry» (ref. DER2014-58257-R), financiado con cargo al Programa Estatal de I+D+i Orientada a los Retos de la Sociedad del MINECO y dirigido por C. Mallada Fernández y por D. Fernández Bermejo desde la Universidad a Distancia de Madrid (UDIMA), y está basado en la aportación del autor al Informe de Situación desarrollado por el equipo de dicho proyecto.

in the EU to the various risks underlying the use of criptocurrencies, both from a cybercrime and an economic crime point of view, with a particular interest put on the EU Money Laundering Directive reform project. Lastly, the particular situation of Spain is taken into consideration, scrutinizing the social perception of this phenomenon and the institutional reactions to it. The scarce case law on the subject is also analysed, as a means to review the related criminal practices.

Keywords: Criptocurrencies, *bitcoin*, blockchain, money laundering, economic criminality, cybercrime, Directive (EU) 849/2015, scam, ICOs

1. Introducción

Las criptomonedas siguen resultando un fenómeno esquivo y difícil de aprehender por un análisis objetivo, comenzando por la corrección de su misma denominación. Evidentemente, el nombre escogido por los promotores de la primera criptomoneda de uso generalizado y modelo de referencia de la mayor parte de las que han aparecido después, «*Bitcoin*», era en sí una afirmación del carácter de moneda en sentido propio de la misma[2], presentado así como un *fait accompli*.

Este carácter o no de moneda (*o currency*) en sentido propio de las criptomonedas ha sido objeto de cierta discusión. Hoy día, la posibilidad de considerarlas como dinero en sentido propio o legal parece haber quedado atrás[3], siendo ya pocos los defensores de tal idea fuera de los mismos promotores de éstas[4]. Una parte importante de los informes emitidos por autoridades supervisoras o grupos de trabajo evitan el uso de los términos «moneda» o «currency» para hacer referencia a las criptomonedas, o, de hacerlo, se apresuran a subrayar el sentido impropio de tal uso, llegando, en ocasiones, a negar expresamente su carácter de moneda. Tal ha sido desde un primer momento, por ejemplo, la postura del BCE[5], sin

[2] Como señala P. J. Pesch, *Cryptocoin-Schulden. Haftung und Risikoverteilung bei den Verschaffung von Bitcoins und Alt-Coins*, Múnich, C. H. Beck, 2017, pp. 70 s.: «Hinter Bitcoin steht also gewissermassen die Idee, das Konzept von Bargeld auf elektronische Zahlungen zu übertragen.»

[3] Al margen de los dictámenes del BCE y del BdE que mencionaremos a lo largo de este trabajo, v. ya, desde un punto de vista académico, Pesch, *Cryptocoin-Schulden,* cit., pp. 71 ss., cuyas consideraciones acerca de la naturaleza jurídica de las criptomonedas, aunque atinentes al derecho alemán, pueden aplicarse en gran medida, mutatis mutandis, a nuestro país.

[4] Ya muy raramente llegan a aceptarse los argumentos de los promotores de las criptomonedas, que apuntan a afirmar el carácter de moneda en sentido estricto de éstas: así T. Rosembuj, *Bitcoin*, Barcelona, El Fisco, 2015, p. 69, si bien, a nuestro entender, el autor se adhiere a dichos argumentos de manera tal vez un tanto acrítica (v. ult. op. cit., pp. 28 ss., 30 ss.).

[5] V., por ejemplo, Informe BCE *Virtual Currency Schemes – A Further Analysis*, febrero de 2015, p. 24.

que ello obste para que el TJUE haya afirmado de cierta criptomoneda (en particular, del *bitcoin*) que ésta «no tiene ninguna finalidad distinta de la de ser un medio de pago»[6] (pese a la posterior insistencia del BCE en la negación de tal carácter a las monedas virtuales, como veremos). Otros de estos estudios se muestran, por el contrario, más posibilistas al respecto, y califican a las criptomonedas como «dinero» o «moneda» desde el punto de vista de su función económica, aunque siempre introduciendo matices relevantes y diferenciándolas de la moneda de curso legal (*fiat currency*[7]).

En buena medida, se trata de una cuestión de punto de vista: de la posible idoneidad de las criptomonedas para cubrir potencialmente las funciones atribuidas tradicionalemente al dinero[8] no se sigue de manera necesaria que éstas deban ser reconocidas en cuanto tal por dichos ordenamientos jurídicos. Así, a pesar de que las criptomonedas no parecen presentar los riesgos de colapso de los sistemas financieros como tales (al menos, por el momento[9]) que llegaron a pesar sobre ellas (confirmándose, sin embargo, la existencia de otros a los que nos referiremos a los largo de este trabajo[10]), lo cierto es que a día de hoy ningún Estado ha reconocido a ninguna criptomoneda de uso corriente el status jurídico de moneda de curso legal[11]. Sin que por ello pretendamos sustraer nada a la importancia del aspecto económico de la cuestión, el presente traba-

---

[6] En la STJUE *Högsta förvaltningsdomstolen (cuestión prejudicial), asunto C-264/14, de 22 de octubre de 2015, y particularmente en su* § 24, sobre la cual volveremos más abajo.

[7] Así D. G. Baur, K. Hong y A. D. Lee, en *Virtual Currencies: Media of Exchange or Speculative Asset?*, SWIFT Institute Working Paper n.º 2014-007, publicado el 29 de junio de 2016, p. 10: (*Bitcoin*) «…can be defined as synthetic commodity money (Selgin, 2015) sharing features with both commodity monies such as gold and fiat monies (…) Bitcoin is a hybrid of commodity money and fiat money.»

[8] A. Ali, J. Barrdear, R. Clews y J. Southgate, «The economics of digital currencies», *Bank of England Quarterly Bulletin, Vol. 54, No. 3, 2014, pp. 276 ss. (disponible en* www.bankofengland.co.uk/publications/Documents/quarterlybulletin/2014/qb14q302.pdf), pp. 278 s., con su conclusión sobre este particular en p. 279: «In theory, digital currencies could serve as money for anybody with an internet-enabled computer or device. At present, however, digital currencies fulfil the roles of money only to some extent and only for a small number of people.»

[9] Así Ali *et al.*, «The economics of digital currencies», cit., pp. 283 s., pero también Baur, Hong y Lee, *Virtual Currencies: Media of Exchange or Speculative Asset?,* cit., p. 29, si bien señalando estos últimos, por el contrario de lo concluido por los especialistas del Bank of England, que la evolución de las criptomonedas en el futuro podría resultar eventualmente en una pérdida de relevancia de la política monetaria, con los riesgos que ello conllevaría.

[10] Al respecto v. p. ej. N. Vandezande, «Virtual Currencies Under EU Anti-Money Laundering Law», en *Computer Law and Security Review* 33, 2017, pp. 341 ss. y en particular pp. 342 s.

[11] Informe GAFI FATF *Virtual Currencies. Key Definitions and potential AML/CTF Risks,* Junio de 2014, p. 4. La criptomoneda auspiciada por el gobierno de Venezuela (el *petro*), además de presentar importantes peculiaridades con respecto a las criptomonedas al uso (siendo la más importante de ellas el no tratarse, en puridad, de una criptomoneda descentralizada), resulta aún una incógnita.

jo pretende analizar el impacto de las criptomonedas en la práctica del blanqueo de capitales, fenómeno eminentemente normativo. Así pues, consideraremos principalmente las criptomonedas desde el punto de vista de su consideración jurídica por los Estados y los organismos supranacionales, y por tanto no como monedas en sentido estricto (moneda de curso legal).

En cuanto a los principios técnicos que presiden el funcionamiento de las criptomonedas, y dado que no es esta la sede para entrar en una descripción en profundidad de los mismos[12], presupondremos un conocimiento básico de ellos por parte del lector. Tomando como referencia el caso del *bitcoin* (la criptomoneda de uso más extendido con dieferencia), nos limitaremos a resaltar una serie de características relevantes para nuestros propósitos que se deducen de la propia arquitectura técnica de su sistema de transacciones:

Primera, puesto que las transacciones son comprobadas y registradas por la comunidad de usuarios en su conjunto, no es técnicamente posible una supervisión centralizada.

Segunda, y a consecuencia del mismo principio de descentralización, las transacciones no requieren intermediarios (esto es, al menos desde un punto de vista estrictamente técnico: el funcionamiento económico del sistema, por el contrario, ha dado lugar al florecimiento de servicios análogos a los de intermediación financiera).

Tercera, dado que cada transacción puede (y suele) implicar a varias direcciones *bitcoin* que envían (pago) y varias direcciones que reciben (cobro), la misma arquitectura del sistema dificulta el relacionar una dirección de envío con los *bitcoin*s transferidos a una dirección de recepción determinada para una cierta transacción.

Cuarta, y por el mismo motivo, tampoco es posible atribuir números de serie a un *bitcoin* determinado, lo cual dificulta igualmente la trazabilidad de los movimientos de aquél dentro de la red *bitcoin*.

Quinta, los datos accesibles a los usuarios en el registro público (*ledger) no permiten conocer los límites de una cartera o wallet determinada, esto es, asociar un haz determinado de direcciones bitcoin a un usuario concreto*[13].

---

[12] Para una descripción en detalle de los principios técnicos y los aspectos prácticos del *bitcoin*, remitimos al lector a la monografía de F. Brezo Fernández y Y. Rubio Viñuela, *Bitcoin. La tecnología blockchain y su investigación,* Móstoles, ØxWord, 2017, y especialmente pp. 23 ss. (principios técnicos generales) y pp. 63 ss. (aspectos prácticos). Para una descripción abreviada, v. A. Badev y M. Chen, «Bitcoin. Technical Background and Data Analysis», Staff Working Paper 2014-104, *Finance and Economics Discussion Series (FEDS),* Federal Reserve Board, 7 de octubre de 2014, pp. 5 a 15.

[13] Badev y Chen, «Bitcoin. Technical Background and Data Analysis», cit., p. 11.

Sexta, las transferencias en *bitcoin*s no pueden ser revertidas una vez confirmadas. Por tanto, la devolución de un pago puede realizarse sólo mediante una transacción voluntaria *a posteriori* por parte del receptor del pago original.

Séptima, el que la pérdida de los tokens implique la pérdida del control sobre los bitcoins atribuidos a una dirección bitcoin determinada implica que la destrucción de los datos que conforman la cadena alfanumérica de que se trata equivale, en la práctica, a la destrucción de dichos bitcoins, mientras que el robo de dichos datos equivale al robo de los *bitcoins*[14].

Desde el punto de vista de su percepción social, las criptomonedas se debaten entre la actitud cautelosa de las autoridades de supervisión y el triunfalismo de sus promotores y de parte de sus comunidades de usuarios, que a menudo las identifican con la realización de un ideal anarcoliberal de liberación del individuo de la supervisión financiera estatal mediante la tecnología[15]. Pese a que esta última percepción pueda incluir una crítica legítima a las insuficiencias de la política monetaria clásica[16], lo cierto es que todo discurso que propugne la ausencia de cualquier control financiero (y fiscal) sobre las criptomonedas suscitará un cierto escepticismo, teniendo en cuenta la creciente profesionalización y corporativización del sector. Por lo demás, resulta discutible que una adopción generalizada de criptodivisas pueda servir, desde una perspectiva anarcoliberal, aún a largo plazo, para la eliminación de toda superestructura social que pese sobre la libertad económica individual[17].

---

[14] Ya en 2012, existía una corriente de *malware dedicado específicamente al robo de carteras gestinadas directamente desde los equipos de usuarios medios (v.* F. Brezo, «Aplicaciones ciberdelictivas de divisas como *Bitcoin*», Documento de Investigación sobre Seguridad Interior doc-ISIe n.º 04/2012, Instituto Universitario de Investigación sobre Seguridad Interior (IUISI), julio de 2012, p. 7). Tampoco el almacenamiento de los *tokens en sitios especialmente securizados garantiza por completo al usuario la protección de los bitcoins que en ellos deposita, como lo han demostrado los robos masivos de éstos, como el del sitio japonés Mt. Gox de 2014 o el de Bitfinex de agosto de 2016.*

[15] Acerca de la concepción tecno-utópica del *bitcoin* (esto es, como un *Deus ex machina tecnológico capaz de solucionar por sí solo los problemas planteados por la política monetaria) v.* N. Dodd, «The Social Life of *Bitcoin*», *Theory, Culture & Society*, publicado el 17 de diciembre de 2017 (obtenido mediante LSE Research Online), pp. 1 ss. y particularmente pp. 8 ss. Un ejemplo del discurso anarcoliberal en boga entre los promotores de las criptomonedas en V. E. Voorhees, «What is *Bitcoin*?», *yBitcoin Magazine*, vol. 2, iss. 2, Spring 2015, pp. 12 s. y particularmente p. 13: «With Bitcoin, there is no third party watching over the participants of economic activity, approving their conduct and charging a fee for doing so. With Bitcoin, one does not need permission to direct own's financial life.»

[16] J. Ekkenga, «*Bitcoin* und andere Digitalwährungen – Spielzeug für Spekulanten oder Systemveränderung durch Privatisierung der Zahlungssysteme?», en *Computer und Recht 11/2017, pp. 762 ss.*

[17] Puesto que tales superestructuras han surgido ya de manera espontánea; pueden compartirse a este respecto las conclusiones de Dodd, «The Social Life of *Bitcoin*», cit., p. 21: «*Bitcoin* itself seems not only to replicate but exacerbate the self-same inequities of wealth and power that can be found in the existing financial system.»

Por otro lado, la medición del impacto económico de las criptomonedas puede ser difícil. Hoy por hoy han sido implantadas en el mercado unas 500 criptomonedas diferentes, de las cuales buena parte son copias prácticamente idénticas del *bitcoin*[18], esto es: los principios técnicos y sistemáticos sobre los que están basadas, sus cauces de promoción y de expansión, su estrategia de comunicación y, en ocasiones, incluso su imagen de «marca» o logotipo imitan de cerca los de la *bitcoin*[19]. Esta multiplicidad de criptomonedas (a pesar de que la diversidad de las mismas pueda ser, en efecto, sólo relativa) dificulta la evaluación cuantitativa del impacto del fenómeno, tanto más cuanto que algunas de ellas tratan de competir con el *bitcoin* diferenciándose en puntos esenciales (este es, por ejemplo, el caso del *ether, con la posibilidad de conclusión de los llamados smart contracts*[20]*)*.

Prescindiendo del límite máximo de unidades de cuenta emisibles para cada tipo de criptomoneda[21], puede estarse de acuerdo con el supervisor europeo en que los factores clave de cara a medir el impacto de una criptomoneda concreta tendrían que ver con la aceptación y el uso de la misma por los usuarios (sean éstos particulares o empresas), así como con su conexión con la economía real, que podría medirse especialmente según su reconocimiento y empleo por entidades supervisadas por las autoridades bancarias[22].

Ahora bien, no resulta sencillo medir de modo inequívocamente significativo estos factores. En primer lugar, el uso de las criptomonedas para el pago de bienes y servicios a los minoristas que las aceptan parece ser, en la práctica, sumamente infrecuente[23]. Por el momento, y sobre

---

[18] Informe BCE *Virtual Currency Schemes – A Further Analysis*, cit., p. 32.

[19] Las definiciones del Informe GAFI FATF *Virtual Currencies. Key Definitions and potential AML/CTF Risks*, cit., pp. 5 s., diferencian entre «moneda virtual centralizada» (emitida por una autoridad administradora concreta y no convertible en dinero «real», como el «oro» del MMORPG *Warcraft*) y «moneda virtual descentralizada» (no emitida por una única autoridad administradora y convertible), de la que, a su vez, se distinguen dos categorías: el «*Bitcoin*» y las «*Altcoins*», englobando éstas «…math-based decentralised convertible virtual currency other than bitcoins, the original such currency…» (ult. *op. cit.*, p. 6). Las definiciones del informe no hacen referencia a ningún otro tipo de criptomonedas.

[20] Sobre los cuales v. Chr. G. Paulus y R. Matze, «Digitalisierung und private Rechtsdurchsetzung— Relativierung der Zwangsvollstreckung durch smarte IT-Lösungen?», en *Computer und Recht* 12, 2017, pp. 770 ss. y en particular pp. 771 s.

[21] Situado, para el *Bitcoin*, en 21 millones de unidades (si bien potencialmente fraccionables): Informe GAFI FATF *Virtual Currencies. Key Definitions and potential AML/CTF Risks*, cit., p. 6. Normalmente, las criptomonedas integran un límite de emisión total o anual.

[22] Informe BCE *Virtual Currency Schemes – A Further Analysis*, cit., p. 32.

[23] V. Badev y Chen, «Bitcoin. Technical Background and Data Analysis», cit., pp. 15 a 27, y particularmente su conclusión en la p. 27: «Our analysis of data from the *Bitcoin* system further suggests that Bitcoin is still barely used for payments for goods and services. In addition, the patterns of circulations of bitcions [sic] and the dynamics of

la base de los datos disponibles a partir del *ledger* público (el registro distribuido sobre el que se anotan todas las transacciones), es posible analizar, en cierta medida, la conducta de los usuarios; cruzándolos con otros datos, es posible tratar de estudiar la evolución del comportamiento de los actores del ecosistema de las criptomonedas (miners, exchangers, inversores, etc.). Los estudios que han venido adoptando este modelo de análisis han llegado, en general, a conclusiones similares: las bitcoins serían empleadas mayoritariamente como inversión y no como medio de cambio, frecuentemente con una finalidad meramente especulativa[24].

Primera parte: las criptomonedas en Europa

1. Las criptomonedas en el derecho europeo en general

Centrándonos ya en el ámbito jurídico, el encuadre regulatorio de las criptomonedas por parte de las instituciones europeas va experimentando tímidos avances, que se han concretado tanto en el ámbito de los procesos legislativos como en el jurisprudencial.

Tal y como habíamos apuntado más arriba, existe ya algún pronunciamiento del TJUE que concierne directamente las criptomonedas: dicha toma de postura se producía en su decisión sobre la aplicabilidad al *bitcoin* de una norma europea concerniente al IVA[25]. La sentencia resolvía una cuestión prejudicial elevada al TJUE por el Tribunal Supremo sueco, en el contexto de un recurso planteado por la administración tributaria nacional contra un dictamen de la Comisión de Derecho Fiscal sueca, por el cual ésta interpretaba, a petición de un particular, la norma de desarrollo en el derecho interno de la Directiva 2006/112/

---

the bitcoin exchange rate are consistent with low usage of Bitcoin for retail payment transactions.» V. en la misma dirección para el Reino Unido, sobre la base de las transacciones diarias operadas mediante MyWallet, Ali *et al.*, «The economics of digital currencies», cit., p. 280.

[24] Los investigadores del instituto SWIFT señalan expresamente la actividad especulativa como finalidad primordial de una parte sustancial de los inversores (Baur, Hong y Lee, *Virtual Currencies: Media of Exchange or Speculative Asset?*, cit., pp. 29, mientras que la investigación auspiciada por la Reserva Federal estadounidense, más prudente, se limita a afirmar la «falta de profundidad en los mercados de cambio» de *bitcoins (*Badev y Chen, «*Bitcoin*. Technical Background and Data Analysis», cit., pp. 26 s.). Por su parte, alcanzaba resultados más matizados L. Kristoufek, «What are the Main Drivers of the *Bitcoin* Price? Evidence from the Wavelet Coherence Analysis», en *PLOS One* 10(4), Abril 2015, pp. 1-15 y en particular p. 14: «Overall, the Bitcoin forms a unique asset possessing properties of both a standard financial asset and a speculative one.»

[25] STJUE *Högsta förvaltningsdomstolen* (cuestión prejudicial), asunto C-264/14, de 22 de octubre de 2015.

CE, de 28 de noviembre de 2006, en el sentido de declarar exenta del IVA la actividad consistente en el cambio de *bitcoin*s por moneda de curso legal[26].

En su cuestión prejudicial, el Tribunal Supremo sueco dirigía dos preguntas al TJUE, a saber: si en el sentido de la citada Directiva la actividad de cambio de *bitcoin*s por monedas de curso legal constituiría o no una prestación de servicios a título oneroso; y, en caso de respuesta afirmativa a la primera cuestión, si dicha actividad estaría exenta o no del IVA según el artículo 135.1 de la Directiva 2006/112/CE[27]. El Tribunal daba respuesta afirmativa a la primera pregunta y una respuesta afirmativa a la segunda que incluía ciertos matices, siguiendo en ello las conclusiones de la Abogado General Kokott[28].

Así, el TJUE resolvía la primera cuestión en el sentido de considerar la actividad de cambio como una prestación de servicios a título oneroso, cosa que, dada la naturaleza de los servicios ofrecidos (con el cómputo de un margen de beneficio para el cambista en los tipos de cambio ofrecidos), no ofrecía particulares problemas[29]. Para la segunda cuestión, el Tribunal distinguía en su respuesta entre las distintas causas de exención recogidas en el artículo 135.1 de la Directiva 2006/112/CE, concluyendo que los servicios de cambio de *bitcoin*s considerados en el litigio principal entrarían únicamente dentro de la exención prevista en el apartado e) del citado artículo, afirmando expresamente, por el contrario, la inaplicabilidad a dichos servicios de las exenciones previstas por sus apartados d) y f)[30].

El alcance de esta decisión del TJUE en lo que respecta a la construcción de un régimen jurídico para las criptomonedas debe ser valorado de manera realista. Por un lado, conviene no perder de vista el hecho de que la decisión, respondiendo a una cuestión prejudicial, se refiere a la aplicabilidad de una norma europea determinada. En

---

[26] El dictamen origen del litigio había sido emitido a petición del Sr. Hedqvist, un particular que deseaba convertirse en *exchanger de bitcoins: STJUE Högsta förvaltningsdomstolen* (cuestión prejudicial), cit., § 2, §§ 10 a 19.

[27] STJUE *Högsta förvaltningsdomstolen* (cuestión prejudicial), cit., § 21.

[28] Conclusiones de la AG J. Kokott sobre el asunto C-264/14, presentadas el 16 de julio de 2015, respectivamente §§ 12-18 (primera cuestión) y §§ 19 a 53 (segunda cuestión).

[29] STJUE *Högsta förvaltningsdomstolen* (cuestión prejudicial), cit., §§ 22 a 31.

[30] STJUE *Högsta förvaltningsdomstolen* (cuestión prejudicial), cit., §§ 38 a 43, que recogen la argumentación sobre la inaplicabilidad a los servicios en cuestión de la exención de IVA prevista en el art. 135.1 d) de la Directiva; §§ 44 a 53, que afirman la aplicabilidad a los servicios en cuestión de la exención contemplada en el art. 135.1 e) de la Directiva; y §§ 54 a 56, que establecen la inaplicabilidad a los servicios en cuestión de la exención contemplada en el art. 135.1 f) de la Directiva. Como hemos mencionado más arriba (y tal y como el propio TJUE indica en la sentencia), el Tribunal se ceñía a la argumentación propuesta por la AG Kokott en sus conclusiones: v. Conclusiones de la AG J. Kokott sobre el asunto C-264/14, cit., y, en particular, §§ 20 a 23, sobre el art. 135.1 f); §§ 24 a 45, acerca del art. 135.1 e); y §§ 46 a 53, sobre el art. 135.1 d).

sentido estricto, las conclusiones alcanzadas por el Tribunal en esta sentencia se limitan a la interpretación del artículo 135.1 de la Directiva 2006/112/CE, y no se refieren a los servicios de cambio de cualquier criptomoneda, sino únicamente a los servicios de cambio de *bitcoin*s[31]. En algún caso, incluso, la sentencia señala expresamente que alguna de sus valoraciones acerca de la naturaleza de las *bitcoin*s se ciñe estrictamente a las conclusiones alcanzadas en el litigio principal al respecto[32], o bien se basa en puntos de las conclusiones de la Abogado General fundados sobre tales conclusiones[33], lo cual viene a equivaler a una toma de distancia implícita del TJUE con respecto a tal valoración, al ligarla al criterio de la jurisdicción nacional sueca. Por ende, debe, al menos, dudarse razonablemente de la aplicabilidad a todas las criptomonedas (esto es, y no sólo a las *bitcoin*s) de las conclusiones alcanzadas en esta sentencia por el Tribunal. Por ello, y con mayor razón, consideramos desacertado el pretender extraer de esta decisión conclusiones sobre el criterio del Tribunal con respecto a otras aplicaciones potenciales de la *blockchain*[34].

Por otro lado, no cabe duda de que esta decisión será tenida en cuenta a nivel nacional por las jurisdicciones y los técnicos del Derecho en general, y ello más allá del carácter muy circunscrito del objeto de la decisión. En efecto, la ausencia de agarraderos regulatorios y jurisprudenciales sólidos[35] genera, inevitablemente, una suerte de voracidad exegética en los actores del tráfico jurídico, que tratarán de extraer del contenido de la sentencia hasta la menor gota de certeza que sea posible exprimir de ella. Como es lógico, la duración de este empeño dependerá de la rapidez con la que otros pronunciamientos de la jurisprudencia o del legislador contribuyan a colmar la laguna jurídica existente.

La preocupación de las instituciones europeas por las criptomonedas se ha traducido en la puesta en marcha de algunos procesos

---

[31] La propia sentencia pone buen cuidado en precisar, en múltiples ocasiones, que las valoraciones contenidas en la misma se circunscriben al caso del *bitcoin*: v. STJUE *Högsta förvaltningsdomstolen* (cuestión prejudicial), cit., §§ 24, 31, 52, 55 y 57.

[32] STJUE *Högsta förvaltningsdomstolen* (cuestión prejudicial), cit., § 52.

[33] STJUE *Högsta förvaltningsdomstolen* (cuestión prejudicial), cit., § 24, que remite, al considerar los *bitcoin*s como un «medio de pago puro», al § 17 de las conclusiones de la AG Kokott, cit.: «También los *bitcoin*s, según las apreciaciones del órgano jurisdiccional remitente, constituyen un medio de pago puro. […]»

[34] Sin embargo, ciertos autores parecen desconocer, a nuestro entender, estos límites del alcance de la sentencia: así J. Maupin «The ECJ's First Bitcoin Decision: Right Outcome, Wrong Reasons?», en *Völkerrecthsblog,* publicado el 19 de noviembre de 2015 (disponible online en: http://voelkerrechtsblog.org/the-ecjs-first-bitcoin-decision-right-outcome-wrong-reasons/).

[35] Para una suerte de «prehistoria» de la toma en cuenta de las criptomonedas por el derecho de la UE v. Vandezande, «Virtual Currencies Under EU Anti-Money Laundering Law», cit., pp. 343 a 349.

legislativos. Una perspectiva de conjunto de ellos nos la da la Resolución dirigida a la Comisión y al Consejo por el Parlamento europeo en 2016, en la que éste viene a establecer ciertos principios que deberían regir una futura actividad legislativa europea en materia de monedas virtuales[36]. Ciertamente, el Parlamento se toma en el texto el cuidado de subrayar los peligros de una regulación prematura[37]: una porción de la breve parte propiamente dispositiva de la Resolución (esto es, prescindiendo del encabezamiento y de los considerandos) se consagra a volver una vez más sobre los riesgos inherentes a las criptomonedas[38]. Sin embargo, el contenido de la resolución indica, aún con un tono de exquisita prudencia, la necesidad de efectuar acciones regulatorias en un futuro cercano no solamente en cuanto a las monedas virtuales, sino también con respecto a otras aplicaciones financieras de la tecnología de registros distribuidos (TRD) o *distributed ledger*[39] (principal bloque de construcción tecnológico de las criptomonedas). Lo que es más importante para nuestro objeto de estudio, el Parlamento apoyaba aquí la propuesta de la Comisión de reformar la Directiva 2015/849, de 20 de mayo, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, en el sentido de incluir en ella las plataformas de intercambio de monedas virtuales[40].

Cabe felicitarse por la toma en consideración específica, por parte del Parlamento europeo, de las aplicaciones de la TRD (y, por tanto, de la cadena de bloques o *blockchain*) más allá de su uso en las criptomonedas, lo cual refleja una mayor madurez en la reflexión del Parlamento europeo, que responde así al interés social que despiertan las aplicaciones ulteriores de la blockchain, tanto en el ámbito de la tecnología financiera en general *(fintech)* como más allá del mismo[41].

---

[36] Se trata de la Resolución del Parlamento Europeo, de 26 de mayo de 2016, sobre monedas virtuales, procedimiento n.º 2016/2007(INI), documento P8_TA(2016)0228.

[37] Resolución del Parlamento Europeo, de 26 de mayo de 2016, sobre monedas virtuales, cit., § 4, en que el Parlamento «…Señala, no obstante, que si se adopta una regulación de manera precoz, esta podría no estar adaptada a una realidad todavía en evolución y transmitir a la población un mensaje erróneo sobre las ventajas o la seguridad de las monedas virtuales».

[38] Resolución del Parlamento Europeo, de 26 de mayo de 2016, sobre monedas virtuales, cit., § 2.

[39] Resolución del Parlamento Europeo, de 26 de mayo de 2016, sobre monedas virtuales, cit., § 3: «…para abordar estos riesgos [los propios de las criptomonedas y las TRD] será necesario aumentar la capacidad reguladora, incluidos los conocimientos técnicos, así como desarrollar un marco jurídico sólido que esté a la altura de la innovación, garantizando una respuesta oportuna y proporcionada si, y en el momento en que, el uso de algunas aplicaciones de TRD se convierta en sistémicamente pertinente».

[40] Resolución del Parlamento Europeo, de 26 de mayo de 2016, sobre monedas virtuales, cit., § 19.

[41] Este interés social denota una percepción de la tecnología de cadena de bloques que presenta aspectos muy similares a la percepción social de las criptomonedas en

No obstante el acierto de la dirección tomada por el Parlamento europeo, los resultados materiales deberán esperar a la conclusión de un proceso legislativo que se encuentra aún en sus primeras fases. La Resolución mencionada autorizaba, por un lado, a la Comisión europea para la reforma de la Directiva 2015/849, de prevención del blanqueo de capitales; por otro lado, el Parlamento recomendaba a la Comisión (de considerarlo adecuado ésta tras un «balance exhaustivo de las monedas virtuales»), entre otras medidas concomitantes[42], la revisión de las Directivas sobre las cuentas de pago, sobre los servicios de pago y sobre el dinero electrónico[43].

2. *El uso ilegítimo de las criptomonedas en Europa: criptomonedas y blanqueo de capitales*

De las dos líneas de reforma legislativa aludidas, la que está experimentando avances más veloces es la relativa a la prevención de blanqueo de capitales, de la que nos ocuparemos más abajo. Tales avances no pueden extrañar si consideramos que una parte importante de las reservas formuladas en los últimos años con respecto a las criptomonedas tienen que ver con el uso de éstas en el contexto de las finanzas criminales, esto es, como medio de pago en contextos delictivos o en tanto que herramienta de blanqueo de capitales.

Por tomar un ejemplo, el informe que acompaña a la opinión de la European Banking Authority sobre las criptomonedas de 2014 señalaba

---

general: ciertos actores sociales bosquejan una perspectiva de futuro de las aplicaciones de la blockchain en términos tal vez en exceso optimistas, que no nos parecen lejanos de la argumentación comercial (es el caso de D. Tapscott y A. Tapscott, *Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Bussiness, and the World,* Londres, Penguin Books, 2016), mientras que los operadores financieros ya establecidos reconocen el gran potencial en términos de fintech de dicha tecnología desde una actitud más prudente (v. al respecto más abajo, en la sección dedicada a las criptomonedas en España).

[42] Resolución del Parlamento Europeo, de 26 de mayo de 2016, sobre monedas virtuales, cit., § 20. En cuanto a las medidas de acompañamiento, éstas se concretan en pedir la creación de un «grupo operativo horizontal» compuesto por expertos técnicos y reguladores dirigido por la Comisión (§ 22) y en la adopción por ésta de medidas encaminadas a garantizar que se brinde a los consumidores una información precisa sobre los productos y servicios basados en la TRD (§ 23).

[43] Esto es: la Directiva 2014/92/UE del Parlamento Europeo y del Consejo, de 23 de julio de 2014, sobre la comparabilidad de las comisiones conexas a las cuentas de pago, el traslado de cuentas de pago y el acceso a cuentas de pago básicas; la Directiva 2007/64/CE del Parlamento Europeo y del Consejo, de 13 de noviembre de 2007, sobre servicios de pago en el mercado interior; y la Directiva 2009/110/CE del Parlamento Europeo y del Consejo, de 16 de septiembre de 2009, sobre el acceso a la actividad de las entidades de dinero electrónico y su ejercicio, así como sobre la supervisión prudencial de dichas entidades.

una docena de riesgos asociados al uso de las mismas en el ámbito de la criminalidad (incluyendo la financiación del terrorismo), sobre un total de setenta[44]. Por su parte, los supervisores nacionales y europeos han mostrado su preocupación al respecto, sugiriendo la toma de medidas por el legislador en el sentido de encuadrar la extracción, el uso y, sobre todo, el cambio de *bitcoin*s por divisas de uso legal[45]. A nivel internacional, la incidencia del empleo de las criptomonedas con fines de blanqueo de capitales ha atraído la atención de la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC), que ha auspiciado la elaboración y publicación de un manual dirigido a mejorar las capacidades de prevención y lucha contra el blanqueo de capitales por medio de criptomonedas de las distintas agencias nacionales, con vistas a fortalecer la cooperación internacional al respecto[46].

Las reservas razonables formuladas por las autoridades de supervisión parecen ampliamente justificadas por el uso de las criptomonedas en las finanzas de la criminalidad. Si bien ningún producto o servicio financiero está a salvo de su uso malicioso en un contexto criminal (desde una simple cuenta corriente o una tarjeta de crédito hasta los productos financieros más complejos), en los últimos años las criptomonedas se han convertido en un medio de pago prevalente en el contexto de la criminalidad online[47].

Merece la pena, por tanto, que nos detengamos a repasar sumariamente los motivos más evidentes del atractivo de las criptomonedas para los ciberdelincuentes. Algunos de los más importantes los hemos ya mencionado al hilo de la discusión acerca de las características técnicas de las criptomonedas. De nuevo, las consideraciones que llevaremos a cabo aquí se basan en estudios que toman en cuenta principalmente el caso de las *bitcoin*s, si bien otras criptomonedas, como el ethereum, comienzan a ser objeto de atención por parte de las agencias interesadas en la prevención y la lucha contra el blanqueo de capitales[48].

1. En primer lugar, el principio de descentralización que informa el sistema implica la ausencia de mecanismos de supervisión de las transacciones por principio. Cierto, los intermediarios de distinto tipo que operan en el mercado de criptomonedas (especialmente,

---

[44] *EBA Opinion on Virtual Currencies*, cit., pp. 32 ss. (§§ 117 a 133).

[45] V. para una panorámica general de estas reacciones en Europa el Informe BCE *Virtual Currency Schemes – A Further Analysis,* cit., pp. 29 s.

[46] UNODC, *Basic Manual on the Detection And Investigation of the Laundering of Crime Proceeds Using Virtual Currencies,* publicado en junio de 2014 (disponible en: https://www.imolin.org/pdf/UNODC_VirtualCurrencies_final_EN_Print.pdf).

[47] EUROPOL, *Internet Organised Crime Threat Asessment (IOCTA)* 2017, pp. 60 ss.; *Internet Organised Crime Threat Asessment (IOCTA)* 2016, pp. 42 ss.; e *Internet Organised Crime Threat Asessment (IOCTA)* 2015, pp. 46 ss.

[48] EUROPOL, *Internet Organised Crime Threat Asessment (IOCTA)* 2016, p. 43, e *Internet Organised Crime Threat Asessment (IOCTA)* 2017, pp. 61 s.

los *exchangers* y los desarrolladores de aplicaciones) pueden desear aceptar voluntariamente mecanismos de supervisión, o verse constreñidos a ellos por los reguladores nacionales o supranacionales: de hecho, la línea regulatoria preconizada por EUROPOL con vistas a reducir el impacto del uso ilegítimo de las criptomonedas iba en 2015 en esta última dirección[49].

Opinamos, sin embargo, que a pesar de su necesidad para atajar el muy frecuente uso de las criptomonedas en contextos delictivos, la puesta en funcionamiento de mecanismos de control y supervisión sobre los intermediarios de las finanzas basadas en las criptomonedas no bastará por sí sola. Parece poco probable la aceptación sin más por parte de los actores legítimos de cualquier medida tendente a eliminar lo que es percibido como un rasgo inherente a las criptomonedas, esto es, la ausencia de supervisión centralizada. Lo que es más importante, la mecánica *peer-to-peer* y distribuida de éstas hace siempre posible operar directamente entre usuarios, prescindiendo de los intermediarios. Dado que podemos excluir de entrada la imposición de deberes de vigilancia a los mismos proveedores de servicios de conexión a internet (cosa problemática desde el punto de vista económico, pero sobre todo desde el punto de vista de la protección de los derechos fundamentales), las transacciones en criptomonedas, aún en caso de no pasar a través del empleo de productos y servicios financieros legítimos, pueden seguir siendo accesibles y eficaces desde el punto de vista de los costes para todos, incluidos los criminales.

2. En segundo lugar, y como consecuencia de la propia arquitectura del sistema de direcciones en el caso de las *bitcoin*s, las criptomonedas ofrecen un grado de privacidad de las transacciones elevado, dada la dificultad inherente al sistema para relacionar una transacción determinada con un usuario concreto y para trazar el camino seguido por una unidad de valor determinada que cambia de «propietario»[50]. Ciertamente, la red *bitcoin* no ofrece un anonimato perfecto: empleando métodos refinados y suficientes recursos, no es imposible seguir el rastro a las transacciones

[49] Informe BCE *Virtual Currency Schemes – A Further Analysis,* cit., p. 32. Pese a los palmarios intentos de desinformación con respecto a un posible cambio de dirección reciente en el punto de vista de EUROPOL al respecto, la agencia sigue considerando el uso de criptomonedas como un medio de blanqueo de capitales, hasta el punto de haber establecido recientemente un grupo de trabajo conjunto sobre la cuestión con INTERPOL y el Basel Institute of Governance: v. la nota de prensa de EUROPOL de 9 de septiembre de 2016, disponible en https://www.europol.europa.eu/newsroom/news/money-laundering-digital-currencies-working-group-established

[50] V. las características técnicas tercera a quinta de las *bitcoin*s que indicábamos en la sección anterior.

en *bitcoin*, dentro de ciertos límites[51]. En particular, la existencia de datos relacionables con el emisor y el receptor de cada pago (las direcciones *bitcoin*) hace que en sentido estricto, pueda hablarse más bien de «pseudonimia», y no de «anonimato», de la red *bitcoin*.

Ello no obsta para que una parte de la comunidad *bitcoin* promueva constantemente el refuerzo técnico de la privacidad de las transacciones en *bitcoin*s; por su parte, las nuevas criptodivisas ahora en desarrollo tratan precisamente de competir con el *bitcoin* ofreciendo un grado de privacidad superior, tendente hacia el resultado ideal de un anonimato técnicamente impenetrable (cuyos resultados serían potencialmente catastróficos para la capacidad de lucha contra el blanqueo de capitales de las fuerzas del orden)[52].

3. En tercer lugar, constituye un atractivo evidente la irreversibilidad de las transacciones en las criptomonedas más importantes[53], incluyendo las dos criptomonedas de uso más extendido, el *bitcoin* y el *ether*[54].

Esta irreversibilidad no solamente facilita los pagos de víctima a delincuente al hacer posible una transferencia de valor a distancia y no anulable *a posteriori*, sino que además dificulta la acción de las fuerzas del orden, que se ven reducidas a dos opciones para impedir que una transacción ilegítima se haga efectiva: injerirse directamente en las máquinas implicadas (con los inconvenientes que ello conlleva en términos de autorización de tales medidas de investigación, pero también en razón de la complejidad técnica y de la eficacia de las mismas), o confiar en la voluntad de colaboración de los intermediarios legítimos que

---

[51] Como quedó demostrado ya en 2013 por el estudio de un grupo de investigación de la University of California-San Diego: v. S. Meiklejohn, M. Pomarole, G. Jordan *et al.*, «A Fistful of *Bitcoin*s: Characterizing Payments Between Men with No Names», disponible en la web del Computer Science and Engineering Departement de dicha Universidad: https://cseweb.ucsd.edu/~smeiklejohn/files/imc13.pdf

[52] EUROPOL, *Internet Organised Crime Threat Asessment (IOCTA) 2016, pp. 43 s.*

[53] El manual de la UNODC, *Basic Manual on the Detection And Investigation of the Laundering of Crime Proceeds Using Virtual Currencies,* cit., pp. 39 ss., al considerar los riesgos específicos del uso de las criptomonedas con fines de blanqueo de capitales, colocaba a la cabeza la rapidez e irreversibilidad de las transacciones.

[54] Acerca del *bitcoin*, v. la información al respecto provista por los mismos promotores del mismo en https://bitcoin.org/en/you-need-to-know ; sobre el ethereum, v. las FAQs sobre el ether disponibles en el sitio del «Ethereum Project», https://www.ethereum.org/ether, que señalan: «Ethereum addresses don't have built-in checks on them yet. That means that if you mistype an address, your ether will be lost forever, without a secondary confirmation window.». Ahora bien, v., D. Z. Morris, «The Bizarre Fallout of Ethereum's Epic Fail», *Fortune*, publicado el 4 de septiembre de 2016 (disponible en http://fortune.com/2016/09/04/ethereum-fall-out/)

operan en el ecosistema de la moneda de que se trate (suponiendo que los delincuentes se sirvan de sus productos o servicios para gestionar los pagos, cosa que no siempre ocurrirá).

4. En cuarto lugar, en tanto que fenómenos exclusivamente digitales, las criptomonedas se amoldan perfectamente a las características clásicas de la ciberdelincuencia: instantaneidad (rapidez de las transacciones); distancia entre el infractor y el lugar de comisión de una parte sustancial del *iter* criminoso del delito; carácter transfronterizo, con la problemática jurídica asociada a la determinación de la jurisdicción competente para conocer de la infracción y a la cooperación internacional indispensable para perseguirla; inmaterialidad y, por tanto, facilidad de eliminación de las pruebas (esta última, sin embargo, reducida en alguna medida debido al carácter público del *ledger*).
5. En quinto lugar, y en relación con esta última característica, la criptomoneda ofrece el atractivo de una flexibilidad especial. Un *token* puede moverse instantáneamente por la Red; sin embargo, si las circunstancias lo exigen (por ejemplo, si se sospecha que la infraestructura digital de la organización está siendo objeto de medidas de vigilancia), el token puede «materializarse» al ser almacenado en un soporte físico portátil, y sortear los controles en el interior de un disco duro cuyo contenido podrá ser sólo revisado en caso de que se intercepte físicamente a su portador. Para el caso de un movimiento transfronterizo, parece poco probable que las autoridades de aduana revisen el contenido de un disco duro portado por un viajero a menos que estén específicamente sobre aviso.

Dadas las consideraciones llevadas a cabo hasta el momento, se entiende fácilmente que el uso de criptomonedas supone una ampliación importante de la panoplia de posibilidades a disposición de los delincuentes. Evidentemente, una de las opciones más interesantes para los blanqueadores y más disruptivas para su persecución (dada su sencillez, su eficacia en términos de costes en comparación con otros métodos y las dificultades técnicas asociadas a su trazado y evitación por las autoridades) es el mero envío de los *tokens* a paraísos fiscales para su cambio en moneda de curso legal por *exchangers* locales y su reintroducción en el sistema financiero internacional.

La misma minería de criptomoneda ofrece múltiples posibilidades de cara al blanqueo de los fondos obtenidos ilícitamente: la supervisión de la «producción» precisa de criptomonedas por parte de un minero determinado requiere de una vigilancia específica, pudiendo siempre declararse una producción menor de la realmente alcanzada a efectos de blanqueo o de evasión de impuestos; en ausencia de tal vigilancia, las criptomonedas obtenidas por otros medios pueden también disfrazarse como el producto de una instalación de minería de criptomoneda

determinada. Por añadidura, es posible emplear la capacidad de cálculo de una *botnet* de ordenadores infectados para la minería de criptomonedas[55], siguiendo así un método análogo al empleado para la realización de ataques distribuidos de denegación de servicio (DDoS): salvo que los investigadores consigan desentrañar el entramado de la *botnet*, el producto de esta minería «forzada» podría disfrazarse de nuevo como el de una instalación de minería de criptomoneda existente, en ausencia de una vigilancia específica.

Por lo demás, los pagos de víctima a criminal en el contexto de la cibercriminalidad se llevan a cabo mayoritariamente en criptomoneda (particularmente, en *bitcoins*), con las ventajas en cuanto a colocación y encubrimiento enormemente simplificados de las ganancias que ello conlleva para los criminales. Esta práctica está particularmente bien documentada para el caso del *ransomware,* que presenta un preocupante grado de automatización en términos de cobro de los rescates en criptomoneda y de colocación de los mismos mediante estructuras complejas de direcciones *bitcoin*[56]. Por motivos similares, la mayoría de los pagos de criminal a criminal en el marco de la ciberdelincuencia (por ejemplo, en el marco de la contratación de servicios de *CaaS*, pero no sólo) parecen llevarse a cabo hoy en criptomonedas[57].

Contempladas desde el punto de vista de la lucha del blanqueo de capitales, las ventajas de estas prácticas para los criminales pueden resumirse en una: éstas permiten cubrir de manera relativamente sencilla la primera fase del proceso de blanqueo de capitales, la colocación: precisamente aquélla en la que la acción de las autoridades puede resultar más eficaz.

Tal salto directo a la segunda fase del proceso de blanqueo depende de la privacidad de las transacciones que ofrecen las criptomonedas (entiéndase, de la dificultad de rastreo y de identificación de emisor y beneficiario). A pesar de la ausencia de una anonimidad total en tales transacciones (al menos, por el momento) a la que hemos ya aludido, las organizaciones cibercriminales logran dificultar extremadamente el rastreo de las mismas, bien mediante la redistribución de las ganancias en direcciones *bitcoin* diferentes mediante un proceso *batch* u *offline* autogestionado, o bien mediante el empleo de redes anónimas como TOR[58]. Esta última técnica es empleada de manera sistemática por las organizaciones dedicadas al cibercrimen, que encuentran en las redes P2P anóni-

[55] Brezo, «Aplicaciones ciberdelictivas de criptodivisas como *Bitcoin*», cit., pp. 7 s.

[56] V. al respecto el informe elaborado por IMPERVA, *The Secret Behind Cryptowall's Success, publicado en 2016 (disponible en* https://www.imperva.com/docs/IMPERVA_HII_CryptoWall_report.pdf).

[57] EUROPOL, *Internet Organised Crime Threat Asessment (IOCTA)* 2017, p. 61, e *Internet Organised Crime Threat Asessment (IOCTA)* 2015, pp. 46 ss.

[58] Brezo, «Aplicaciones ciberdelictivas de criptodivisas como *Bitcoin*», cit., p. 6.

mas un refugio seguro en el que poder desplegar sus actividades[59]: estas redes no solamente facilitan la comunicación entre los propios criminales, sino que los pagos de víctima a criminal pasan a través de ellas para tratar de garantizar que los criminales queden en el anonimato[60]. En resumen, el empleo de criptomonedas como medio de pago en contextos cibercriminales debe su generalización a «…las dificultades adicionales que conlleva el rastreo de las transacciones y el acceso a mercados de compraventa presentes en la *deep web*» [61].

3. *Las criptomonedas en el proyecto de reforma de la Directiva de prevención del blanqueo de capitales*

La preocupación de las instancias europeas por el uso de las criptomonedas en el contexto de las finanzas criminales en general y del blanqueo de capitales en particular (preocupación atestiguada por los informes citados de las instituciones europeas de supervisión bancaria y cooperación policial) ha suscitado la primera acción legislativa europea que afectará directamente a las criptomonedas, esto es: la reforma de la Directiva 2015/849, de prevención del blanqueo de capitales, que mencionábamos más arriba.

Conviene señalar preliminarmente que el alcance de esta reforma no se limita a la toma en cuenta de las criptomonedas. Si bien las disposiciones relativas al uso de criptomonedas son consecuencia directa del mandato dirigido por el Parlamento europeo a la Comisión europea sobre la necesidad de emprender acciones regulatorias al respecto mediante la Resolución que hemos ya mencionado[62], el proyecto de reforma (que tras su primera lectura ante el Parlamento[63] ha sido objeto

---

[59] V. al respecto F. Brezo Fernández y Y. Rubio Viñuela, «Herramientas de apoyo a la infraestructura tecnológica de los grupos organizados que operan en la Red», *Cuadernos de la Guardia Civil,* 50, 2015, pp. 27 ss. y concretamente pp. 37 s.

[60] IMPERVA, *The Secret Behind Cryptowall's Success,* cit., pp. 4 ss. Nótese además que para el caso de que la víctima tuviese «problemas» con las direcciones web creadas específicamente por los criminales para el pago del rescate, en la «nota de rescate» virtual se le conmina a instalarse un cliente TOR, a emplearlo para entrar en una dirección determinada y a seguir las instrucciones contenidas en ella.

[61] Brezo y Rubio, «Herramientas de apoyo a la infraestructura tecnológica de los grupos organizados que operan en la Red», cit., p. 41.

[62] Resolución del Parlamento Europeo, de 26 de mayo de 2016, sobre monedas virtuales, cit.

[63] Informe sobre la propuesta de Directiva del Parlamento Europeo y del Consejo por la que se modifica la Directiva (UE) 2015/849 relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, y por la que se modifica la Directiva 2009/101/CE (COM(2016)0450 – C8-0265/2016 – 2016/0208(COD)), Comisión de Asuntos Económicos y Monetarios y Comisión de Libertades Civiles, Justicia y Asuntos de Interior, 9 de marzo de 2017, documento de sesión A8-0056/2017.

de amplias discusiones[64]) va más allá, al introducir modificaciones en otras disposiciones ya existentes en la Directiva 849/2015 y al afectar también a la Directiva 2009/101, de 16 de septiembre, que establece determinadas obligaciones de transparencia para las sociedades comerciales[65].

En particular, tanto la proposición original de la Comisión europea como el texto enmendado incluido en el Informe sobre dicha proposición en primera lectura ante el Parlamento prevén un frente de reformas relativamente amplio, que contiene, además de disposiciones relativas a las monedas virtuales, restricciones a las tarjetas de prepago anónimas, un refuerzo de las competencias de acceso a la información de las Unidades de Inteligencia Financiera (en el caso de España, del SEPBLAC), una mejora en la colaboración con terceros países de riesgo y un robustecimiento de las normas relativas a la transparencia sobre la titularidad real de las sociedades anónimas y de responsabilidad limitada, así como de las entidades cuyo funcionamiento y estructura sean análogos al de los fideicomisos[66]. Estos cinco ejes fundamentales del proyecto de reforma aparecen recogidos en los considerandos que conforman la exposición de motivos del proyecto de reforma en su estado actual[67], reflejándose igualmente, como es lógico, en la parte dispositiva del mismo. Por lo

[64] Un texto de compromiso ha sido alcanzado en diciembre de 2017 tras las consultas al Banco Central Europeo, al Supervisor Europeo de Protección de Datos y a terceros países interesados, así como tras las negociaciones a tres bandas entre Parlamento, Comisión y Consejo: dicho texto aparece recogido en el Anexo de la Nota de la Presidencia del Consejo Europeo dirigida al Comité de Representantes Permanentes acerca de la propuesta de Directiva del Parlamento Europeo y del Consejo por la que se modifica la Directiva (UE) 2015/849 relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, y por la que se modifica la Directiva 2009/101/CE, 15849/17, de 21 de diciembre de 2017.

[65] Más exactamente, se trata de la Directiva 2009/101/CE del Parlamento y del Consejo de 16 de septiembre de 2009, tendente a coordinar, para hacerlas equivalentes, las garantías exigidas en los Estados miembros a las sociedades definidas en el artículo 48, párrafo segundo, del Tratado, para proteger los intereses de socios y terceros.

[66] En el estado actual del proceso legislativo (según éste resulta de la Nota de la Presidencia del Consejo Europeo de 21 de diciembre de 2017 (17/15849), cit.), la enmienda al párrafo 1. del artículo 31 del texto original establece expresamente la equivalencia, a los efectos de la regulación contemplada al respecto por la propuesta de Directiva, del *trust,* la *Treuhand,* la *fiducie* y el fideicomiso (este último término, en castellano en las versiones en otros idiomas del texto de compromiso).

[67] En particular, v. el texto enmendado por el Parlamento de la propuesta original de la Comisión, en el Informe sobre la propuesta de Directiva por la que se modifica la Directiva (UE) 2015/849 y la Directiva 2009/101/CE, cit., considerandos 5 *bis* a 8 para el caso de las monedas virtuales; considerandos 9 a 10 *sexies* para el caso de la cooperación con terceros países de alto riesgo; considerandos 11 y 12 para el caso de las tarjetas de prepago anónimas; considerandos 13 a 17 *ter*, para el caso de la ampliación de competencias en materia de acceso a la información de las UIF; y considerandos 18 a 36, para el caso de la información acerca de la titularidad real de sociedades anónimas, sociedades limitadas y entidades fideicomisarias (medida tomada según un razonamiento de equivalencia con los *trusts* anglosajones).

demás, alguna de las opiniones consultivas requeridas por las dos comisiones parlamentarias informantes estructura su valoración del proyecto de reforma según estos cinco ejes[68].

Las disposiciones del proyecto de reforma que interesan de manera más directa a nuestro objeto de estudio han sido objeto de una atención especial por parte del Supervisor Europeo de Protección de Datos y del Banco Central Europeo en los dictámenes consultivos que ambas instituciones han emitido en el marco del proceso legislativo[69]. Volveremos más adelante sobre las sugerencias formuladas por el Supervisor Europeo de Protección de Datos; en cuanto a las llevadas a cabo por el Banco Central Europeo, que en algún caso afectaban a puntos centrales del proyecto de reforma, éstas han tenido un peso importante en su evolución.

Pensamos, en particular, en el caso de la propia definición de las monedas virtuales incluida en el proyecto de reforma. Pese a una cierta indeterminación sobre su extensión a todas las monedas virtuales o solamente a las criptomonedas[70], el tenor original de la definición propuesta inicialmente por la Comisión, que empleaba la expresión «medio de pago» para referirse a las criptomonedas, había hecho concebir importantes esperanzas a los operadores del sector[71]. El Dictamen del Banco Central Europeo venía a enfriar tales expectativas, incidiendo específicamente en este particular de la definición propuesta por la Comisión en el sentido de propugnar su modificación.

Por un lado, el supervisor europeo dudaba de la aplicabilidad de la expresión «medio de pago» a las criptomonedas, en la medida en que éstas, de acuerdo con los informes ya citados emitidos anteriormente por el propio Banco Central Europeo, no serían «monedas» en sentido propio. Por otro lado, el Dictamen subrayaba la flexibilidad de la tecnología de registros distribuidos sobre la que se basan las criptomonedas, que per-

---

[68] V. la opinión de la Comisión de asuntos jurídicos (ponente: K. Chrysogonos), en el Informe sobre la propuesta de Directiva por la que se modifica la Directiva (UE) 2015/849 y la Directiva 2009/101/CE, cit., pp. 91 ss.

[69] Respectivamente, EDPS Opinion 1/2017, de 2 de febrero de 2017, on a Commission Proposal amending Directive (EU) 2015/849 and Directive 2009/101/EC – Access to beneficial ownership information and data protection implications; y Dictamen del Banco Central Europeo de 12 de octubre de 2016 sobre una propuesta de directiva del Parlamento Europeo y del Consejo por la que se modifica la Directiva (UE) 2015/849 relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, y por la que se modifica la Directiva 2009/101/CE (CON/2016/49) (2016/C 459/05).

[70] Sobre el particular v. VANDEZANDE, «Virtual Currencies Under EU Anti-Money Laundering Law», cit., p. 350, que propende (creemos que con razón) a estimar que el alcance la regulación propuesta se circuscribiría a las criptomonedas.

[71] Tal empleo dejaba espacio a los operadores del sector para la esperanza de una asimilación del régimen jurídico aplicable a las criptomonedas con el propio de las monedas de curso legal.

mite su uso para fines distintos del de pago, lo cual haría inevitable que su definición como «medio de pago» resultase en exceso circunscrita: como alternativa, el Banco Central Europeo proponía el uso de la expresión «medio de cambio»[72].

Las propuestas del Banco Central Europeo fueron acogidas por el Parlamento en su enmienda al texto de la Comisión: en efecto, en la definición de las «monedas virtuales» incluida en el texto enmendado por el Parlamento, la expresión «aceptada por personas físicas o jurídicas como medio de pago» fue sustuida por la de «aceptada por personas físicas o jurídicas como medio de cambio o para otros fines», añadiéndose así una alusión a la variedad de usos potenciales de las criptomonedas señalada por la autoridad de supervisión financiera europea en su Dictamen[73].

Ahora bien, con respecto a la definición propuesta por el Parlamento en primera lectura[74], la versión de la misma que aparece recogida en el texto de compromiso actual propuesto por la Presidencia de la Comisión[75] presenta dos enmiendas importantes.

En primer lugar, la definición propuesta por el Parlamento en primera lectura se cerraba con la aseveración de que «Las monedas virtuales no pueden ser anónimas», aseveración que ha sido eliminada del texto de compromiso. A nuestro entender, esta modificación ha de ser acogida de manera positiva. En efecto, la afirmación de que «las monedas virtuales no pueden ser anónimas» se antoja vaga: no solamente cabe dudar de si contendría una afirmación («es técnicamente imposible garantizar la total anonimidad de los usuarios de criptomonedas») o una disposición («quedarán excluidas de esta definición las

[72] Dictamen del Banco Central Europeo de 12 de octubre de 2016, cit., sección 1.1.3.

[73] V. la enmienda 26 al texto de la Comisión en el Informe sobre la propuesta de Directiva por la que se modifica la Directiva (UE) 2015/849 y la Directiva 2009/101/CE, cit., p. 109. El que la enmienda en cuestión quería acoger las observaciones del Banco Central Europeo lo afirma expresamente el Parlamento en la justificación que la acompaña: tras citar el Dictamen del Banco Central Europeo de 12 de octubre de 2016, el Parlamento se limita a afirmar lacónicamente que «La definición de moneda virtual debe mejorarse, tal y como sugiere el Banco Central Europeo.» (ult. loc. cit.).

[74] Ult. loc. cit., n. anterior: «18) 'monedas virtuales': representación digital de valor no emitida por un banco central ni por una autoridad pública, ni asociada a una moneda establecida legalmente que no posee el estatuto jurídico de moneda o dinero, pero aceptada por personas físicas o jurídicas como medio de cambio o para otros fines y que puede transferirse, almacenarse o negociarse por medios electrónicos. Las monedas virtuales no pueden ser anónimas.»

[75] Nota de la Presidencia del Consejo Europeo de 21 de diciembre de 2017 (17/15849), cit., Anexo, art. 1, (2) (c): «18) 'virtual currencies' means a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency, and does not possess a legal status of currency or money, but is accepted by natural or legal persons, as a means of exchange, and which can be transferred, stored and traded electronically.»

criptomonedas que sean anónimas»), sino que desde un punto de vista técnico se echa en falta una mayor precisión del grado de «anonimato» posible[76].

En segundo lugar, el texto de compromiso propuesto por la Comisión, en su versión más reciente, vuelve a hacer caer de la definición el añadido «o para otros fines» que el Parlamento había introducido en su enmienda en primera lectura de la misma en respuesta a las observaciones del Banco Central Europeo. Cabe interpretar la desaparición del añadido en el sentido de una toma de conciencia de que los «otros fines» distintos del empleo de las criptomonedas como medio de cambio que mencionaba el Dictamen del Banco Europeo[77] se encontrarían más allá del objeto del proyecto de reforma, que se circunscriben al ámbito de la prevención y lucha contra el blanqueo de capitales y la financiación del terrorismo.

Otro de los aspectos más interesantes para nuestros propósitos del proyecto de reforma ha sufrido una evolución importante desde la propuesta original de la Comisión: se trata de la precisión de los sujetos obligados por uno de los dos textos a modificar por la reforma prevista, la Directiva (UE) 2015/849 de 20 de mayo de 2015, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo. En efecto, desde un primer momento el proyecto de reforma preveía que las obligaciones especiales de diligencia debida y de información que vienen siendo atribuidas a los operadores financieros por la Directiva (UE) 2015/849 se hiciesen extensibles al sector de las criptomonedas. El alcance de tal extensión es uno de los puntos pacíficos del proyecto de reforma: tanto el proyecto de la Comisión como el texto enmendado en primera lectura como el Parlamento, así como la propuesta actual de texto de compromiso de la Presidencia de la Comisión, prevén la inclusión de ciertos actores del sector de las criptomonedas en el elenco de sujetos obligados por la Directiva (UE) 2015/849 presente en el actual artículo 2.1 de la misma, así como la exigencia a los Estados miembros de registro de dichos actores, prevista en el actual artículo 47.1 de la misma

---

[76] Esto es, dado que la «anonimidad» de los datos (o su «anonimización») presentan un alto grado de complejidad técnica, que requeriría un grado de concreción mayor que el contenido en la frase que analizamos y tal vez, incluso, una definición aparte de lo que sea la «anonimidad» de las criptomonedas a la que se alude: v. por todos el dictamen del Grupo de Trabajo del Artículo 29 sobre las técnicas de anonimización (A29WP Opinion 5/2014 on Anonymisation Techniques, de 10 de abril de 2014).

[77] En particular, se trataba del uso de las criptomonedas como «depósito de valor para ahorro o inversión», así como los usos mencionados en D. He, K. Habermeier *et al.*, IMF Staff Discussion Note SDN/16/03, «Virtual Currencies and Beyond: Initial Considerations», de enero de 2016, p. 7 (en donde sin embargo se apuntaba únicamente «VCs [*esto es, Virtual Currencies*] can be obtained, stored, accessed, and transacted electronically, and can be used for a variety of purposes, as long as the transacting parties agree to use them.»)

norma[78] (cuya concreción para el caso de los actores del sector de las criptomonedas podría, por lo demás, variar sustancialmente de un Estado miembro a otro en el estado actual del proyecto[79]).

Ahora bien, dado el carácter descentralizado de las criptomonedas, se planteaba (y sigue planteándose) la cuestión de a qué actores del sector en particular podrían imponerse tales obligaciones de diligencia debida y de información. Así, el texto original de la Comisión preveía únicamente la extensión de las obligaciones en cuestión a los *exchangers* y a los proveedores de servicios de administración de billeteros de criptomonedas (*e-wallets*). Sin embargo, el proyecto de reforma enmendado por el Parlamento en primera lectura operó una enorme extensión ulterior de dichas obligaciones, al imponerlas a «…las plataformas de cambio de monedas virtuales, los proveedores de servicios de custodia de monederos electrónicos de monedas virtuales, los emisores, administradores, intermediarios y distribuidores de monedas virtuales, así como los administradores y proveedores de sistemas de pago en línea.»[80]

Resulta aún difícil prever cómo se configurará la lista final de sujetos obligados relacionados con las criptomonedas, ya que el texto de compromiso propuesto por la Presidencia de la Comisión, en su versión actual, se conforma, en lo tocante a los sujetos obligados, a la propuesta original de la Comisión[81]: el desacuerdo del Parlamento y de la Comisión sobre este punto hace previsible así una prolongación de las negociaciones al respecto. Sea como fuere, la extensión de la lista de sujetos obligados relacionados con las criptomonedas propuesta por el Parlamento presenta, a nuestro entender, tres órdenes de problemas que la hacen cuestionable.

---

[78] V., por un lado, el Informe del Parlamento sobre la propuesta de Directiva por la que se modifica la Directiva (UE) 2015/849 y la Directiva 2009/101/CE, cit., pp. 106 s., enmiendas 20 y 21, al art. 1.1.1 del texto de la Comisión en el sentido de añadir las letras g) y h) bis al art. 2.1.3 de la Directiva (UE) 2015/849, y p. 127, enmienda 60, al art. 1.1.16 del texto de la Comisión, y en particular al texto enmendado del art. 47.1 de la Directiva (UE) 2015/849; y, por otro lado, Nota de la Presidencia del Consejo Europeo de 21 de diciembre de 2017 (17/15849), cit., Anexo, art. 1 (1). Estos textos fluctúan, en lo tocante a la reforma del art. 47.1 de la Directiva (UE) 2015/849, entre exigir a los Estados miembros el registro de los actores del sector de las criptomonedas, pero no su autorización (postura esta de la Comisión, que incluye a los actores del sector de las criptomonedas en la primera categoría de sujetos) y en exigir a los Estados miembros tanto el registro como la autorización de la actividad de dichos actores (postura del Parlamento).

[79] Sobre el particular v. VANDEZANDE, «Virtual Currencies Under EU Anti-Money Laundering Law», cit., p. 351.

[80] Informe del Parlamento sobre la propuesta de Directiva por la que se modifica la Directiva (UE) 2015/849 y la Directiva 2009/101/CE, cit., p. 96, enmienda al considerando 6 del texto de la Comisión.

[81] Nota de la Presidencia del Consejo Europeo de 21 de diciembre de 2017 (17/15849), cit., Anexo, art. 1 (1).

En primer lugar, la extensión de la lista de sujetos obligados supone, desde nuestro punto de vista, un aumento de la intensidad de la injerencia en los derechos individuales que supone la obligación de información impuesta por la norma, aumento este que podría poner en compromiso la proporcionalidad de esta medida con el fin legítimo buscado por la misma[82] (según el propio proyecto de reforma, la prevención y lucha contra la financiación del terrorismo[83]). Cabe recordar que no sería la primera vez que una medida restrictiva de estas características (deber impuesto a los operadores de un sector determinado de registrar por sistema y, en su caso, de facilitar a las autoridades datos personales de todos sus usuarios, de cara a la prevención y/o la represión de determinadas infracciones) sería censurada por los propios organos jurisdiccionales de la UE: fue el caso en la sentencia del TJUE que declaró la nulidad de la Directiva 2006/24/CE de de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones[84]. No es casual que el Supervisor Europeo de Protección de Datos haya aludido precisamente a esta sentencia en el Dictamen que emitió en el marco del proceso legislativo, al formular sus reservas acerca del respeto, en el articulaje del proyecto de reforma, del principio de proporcionalidad consagrado en el artículo 52 (1) de la Carta de Derechos Fundamentales de la UE[85].

Entendemos que la extrema amplitud del elenco de sujetos obligados en relación con los criptomonedas, tal y como éste aparece en el texto propuesto por el Parlamento en primera lectura, incrementa exponen-

---

[82] Empleamos aquí deliberadamente las expresiones utilizadas por la jurisprudencia del TEDH de cara a la evaluación de la proporcionalidad de las injerencias estatales en los derechos fundamentales consagrados en los arts. 8 a 11 del CEDH y, en particular, de cara a la evaluación de la aplicabilidad del art. 8.2 CEDH para la justificación de las injerencias estatales en el derecho a la vida privada y familiar, concretamente sobre la base de la «defensa del orden y la prevención de las infracciones penales»: v. p. ej. STEDH *Klass c. Alemania,* n.º 5029/71, de 6 de septiembre de 1978, §§ 42 ss.; STEDH *Malone c. Reino Unido*, n.º 8691/79, de 2 de agosto de 1984, §§ 65 a 89; STEDH *Rotaru c. Rumanía*, n.º 28341/95, de 4 de mayo de 2000, §§ 47 a 63; STEDH *Weber y Saravia c. Alemania*, n.º 54934/00, de 29 de junio de 2006, §§ 80 a 138; STEDH *Uzun c. Alemania*, n.º 35623/05, de 2 de septiembre de 2010, §§ 54 a 81; STEDH *M. K. c. Francia*, n.º 19522/09, de 18 de abril de 2013, §§ 30 a 47; etc.

[83] Informe del Parlamento sobre la propuesta de Directiva por la que se modifica la Directiva (UE) 2015/849 y la Directiva 2009/101/CE, cit., p. 96, enmienda al considerando 6 del texto de la Comisión. Ambos textos (el original de la Comisión y el enmendado por el Parlamento en primera lectura) aducen la lucha contra la financiación del terrorismo como único fin de la extensión a los actores del sector de las criptomonedas de las obligaciones previstas por la Directiva (UE) 2015/849 (esto es, sin mencionar el blanqueo de capitales).

[84] STJUE de 8 de abril de 2014, asuntos acumulados C293/12 y C594/12, *Digital Rights Ireland* y otros (cuestión prejudicial); la sentencia se refiere varias veces (en particular, en sus §§ 35, 47, 54 y 55) a la jurisprudencia pertinente del TEDH.

[85] EDPS Opinion 1/2017, de 2 de febrero de 2017, cit., §§ 44 ss.

cialmente la intensidad de la injerencia en el derecho a la protección de los datos personales de los individuos afectados (potencialmente, todo usuario de criptomonedas), cosa que podría poner en tela de juicio la proporcionalidad de la medida con respecto al fin legítimo perseguido por la misma.

En este mismo orden de consideraciones, y dada la diferencia entre el blanqueo de capitales y la financiación del terrorismo en términos de gravedad de ambos tipos de infracciones, se echa en falta también en ambas versiones del proyecto de reforma (la de la Comisión y la del Parlamento) una delimitación clara de las informaciones susceptibles de ser recogidas y empleadas por las autoridades nacionales y supranacionales para la prevención del blanqueo de capitales y aquéllas susceptibles de serlo para la prevención de la financiación del terrorismo[86].

Un segundo orden de problemas que presenta la extensión del elenco de sujetos obligados relacionados con las criptomonedas propuesta por el Parlamento reside en la imprecisión con la que dichos sujetos obligados aparecen designados. En particular, suscita dudas la expresión «los emisores, administradores, intermediarios y distribuidores de monedas virtuales», especialmente teniendo en cuenta que el elenco incluye ya a «las plataformas de cambio de monedas virtuales» y a «los proveedores de servicios de custodia de monederos electrónicos de monedas virtuales».

El proyecto de reforma incluye sendas definiciones de estas dos últimas categorías (definiciones que no están, sin embargo, exentas de problemas[87]). ¿Quiénes serán, en cambio, «los emisores, administradores, intermediarios y distribuidores de monedas virtuales»? Cuando nos refiramos a criptomonedas descentralizadas, y a falta de definiciones más precisas de estos términos, los prospectores (*miners*) podrían considerarse como «emisores» de criptomonedas, aunque la expresión

[86] A este respecto, cabe señalar que tanto la Comisión como el Parlamento coinciden en legitimar la extensión de las obligaciones de información impuestas a los actores del sector de las criptomonedas no sobre la base de la prevención del blanqueo de capitales, sino únicamente sobre la de la prevención de la financiación del terrorismo (sin duda, dada la mayor aceptación que suscita una restricción de los derechos individuales fundada en la lucha contra el terrorismo, fenómeno que despierta una mayor alarma social que el blanqueo de capitales en los países de la UE). A pesar de ello, resulta claro que es intención del legislador europeo la de fundar el empleo de los datos recogidos para la prevención de ambos tipos de infracciones y/o la lucha contra ambas, cosa que resulta, por motivos obvios, cuestionable. Por añadidura, el proyecto de reforma no establece diferencia alguna entre el uso en sede represiva de los datos personales de los usuarios de criptomonedas recabadas mediante los sujetos obligados y el uso de los mismos en sede preventiva, siendo así que la proporcionalidad de las medidas encaminadas a obtenerlos (esto es, en tanto que medidas limitadoras de derechos fundamentales) merecerá una valoración diferente según si éstos son empleados en una u otra sede.

[87] Al respecto VANDEZANDE, «Virtual Currencies Under EU Anti-Money Laundering LAW», cit., p. 350.

también podría referirse a los promotores originales de una criptomoneda determinada (con frecuencia, comunidades enteras de usuarios); cualquier usuario que mantenga en su ordenador una copia del registro distribuido (*distributed ledger*) y que aporte capacidad de computación a la anotación de nuevas transacciones en dicho registro (a saber: una gran mayoría de los particulares usuarios de criptomonedas) podría, por su parte, ser considerado como «administrador»; podría pensarse en los exchangers como «intermediarios», pero quedando éstos ya explícitamente indicados como sujetos obligados en la frase anterior del elenco, resulta difícil pensar en quiénes pudiesen ser tales «intermediarios»; por último, la expresión «distribuidores» de criptomonedas podría aplicarse, por ejemplo, a los operadores de servicios de telecomunicaciones, en la medida en que éstos contribuyen necesariamente a la «distribución» de las criptomonedas.

Evidentemente, cabe pensar que el legislador europeo tenga en mente acepciones más circunscritas de estos términos genéricos, y que éste deje al arbitrio del legislador nacional la concreción de las mismas mediante las correspondientes normas de transposición de las modificaciones de la Directiva (UE) 2015/849 de 20 de mayo de 2015 introducidas por la Directiva en proyecto, si bien ello conllevaría divergencias muy probables entre el status jurídico acordado a una misma actividad por distintos Estados miembros.

El tercer y último orden de problemas que suscita, según nuestro punto de vista, la extensión del elenco de sujetos obligados relacionados con las criptomonedas propuesta por el Parlamento tiene que ver con la eficacia de la norma jurídica. Ciertamente, parece factible el exigir legalmente el cumplimiento de las obligaciones de información previstas por la norma a algunos de los sujetos indicados en el elenco (en particular, a las plataformas de cambio de monedas virtuales y a los proveedores de servicios de custodia de monederos electrónicos), toda vez que éstos tengan una actividad en el territorio de un Estado miembro (en su caso, con los problemas habituales derivados del almacenamiento de datos fuera de la UE por parte de dichos sujetos).

Ahora bien, y debido al carácter descentralizado de las criptomonedas más importantes, resulta poco creíble que sea posible hacer cumplir tales exigencias en el caso de los «emisores, administradores, intermediarios y distribuidores de monedas virtuales». En muchos casos, tales sujetos (a falta de una definición más precisa de los mismos) equivaldrán a comunidades enteras de usuarios y/o administradores esparcidos a lo largo y ancho de la geografía mundial y, en muchos casos, sitos en terceros Estados poco interesados en establecer una cooperación encaminada a hacer cumplir ciertas obligaciones de información a los miembros de dichas comunidades. Teniendo además en cuenta la posibilidad de operar *peer-to-peer* de usuario de criptomonedas a usuario de criptomonedas, parece que, en muchos casos, y a pesar de la toma en cuenta por

el proyecto de reforma de la dimensión internacional que debería asumir todo mecanismo de control de las criptomonedas[88], la imposición de las obligaciones de información reguladas por la Directiva (UE) 2015/849 de 20 de mayo de 2015 a ciertos actores del sector se quedaría en un mero *desideratum*[89].

Para concluir esta sección con una valoración general de este proyecto de reforma, creemos pertinente volver a las consideraciones que hacíamos al abrirla: así, recordemos que las medidas tocantes a la regulación de las criptomonedas incluidas en dicho proyecto se limitan al ámbito estricto de la prevención del blanqueo de capitales y de la financiación del terrorismo, que se traducen en nuevas obligaciones de información justificadas (o, según el punto de vista que se adopte al respecto, tan sólo provistas de una apariencia de legitimidad) por las necesidades de la lucha contra la financiación del terrorismo. Una primera consecuencia que puede deducirse de todo ello es, obviamente, el carácter aspectual de las disposiciones relativas a las criptomonedas contenidas en el proyecto de reforma, que vienen a cubrir solamente ciertas facetas del uso y explotación comercial de aquéllas: quien espere una regulación europea de conjunto de las criptodivisas deberá aún conformarse con otear el horizonte legislativo.

La segunda consecuencia que creemos posible extraer de este breve análisis del proyecto de reforma tiene que ver, sin embargo, con sus fines estrictos. Pese a que hay que saludar la adopción en el proyecto de reforma de las obligaciones de información a cargo de los proveedores de productos y servicios basados en la TRD, que constituye, sin duda, un paso en la dirección correcta, dichas disposiciones no bastarán por sí solas para atajar el uso de las criptomonedas en el contexto del blanqueo de capitales, por los motivos que indicábamos ya en la sección anterior de este artículo.

---

[88] Esto es, dado que el proyecto de reforma contempla una serie de medidas encaminadas a establecer un mayor control de las transacciones que impliquen a «terceros países de alto riesgo»: v. arts. 2 *quinquies*) y 7 en el texto enmendado por el Parlamento en primera lectura (Informe del Parlamento sobre la propuesta de Directiva por la que se modifica la Directiva (UE) 2015/849 y la Directiva 2009/101/CE, cit., pp. 26 ss.) y, en la propuesta de texto de compromiso actual de la Presidencia de la Comisión, el art. 1, (2c) a (7) (Nota de la Presidencia del Consejo Europeo de 21 de diciembre de 2017 (17/15849), cit., Anexo, pp. 29 a 33). El proyecto prevé incluso el respaldo de tales medidas mediante mecanismos de presión política y económica, aunque esto último, sin embargo, únicamente en los considerandos del proyecto, y no en su parte dispositiva: v. al respecto el considerando 9 *in fine* de la versión del proyecto propuesta por el Parlamento en primera lectura, en Informe del Parlamento sobre la propuesta de Directiva por la que se modifica la Directiva (UE) 2015/849 y la Directiva 2009/101/CE, cit., pp. 9 s.

[89] A ello hay que añadir el impacto en la eficacia de la norma del segundo orden de problemas que acabamos de apuntar, esto es, el hecho de que la imprecisión con la que los sujetos obligados aparecen designados en la norma dificultará ya un control eficaz del cumplimiento de ésta.

Segunda parte: las criptomonedas en España

1. Percepción social en España

Aparte del carácter transfronterizo y (cuasi) instantáneo de las transacciones en criptomoneda o de la desmaterialización del *ledger* o de la actividad de cambio, el mismo anonimato y el propio carácter distribuido de las transacciones (a cuya anotación pueden contribuir usuarios de todo el mundo) contribuyen a hacer de las criptomonedas un fenómeno relativamente uniforme a nivel internacional. En ausencia de una regulación nacional o supranacional específica de las transacciones en criptomoneda, habrá que atender a otros factores susceptibles de generar peculiaridades a nivel nacional, tales como el grado de «digitalización» de la vida cotidiana y de cultura digital presentes en el país de que se trate.

Nuestro país no parece presentar un caso excéntrico (ni por exceso ni por defecto) en este sentido: la implantación del uso de internet en los hogares y la frecuencia de empleo de internet para usar servicios bancarios online, así como el nivel medio de competencias relacionadas con internet de los usuarios españoles, están esencialmente en la media europea[90]. No resulta, por ello, sorprendente que, en gran medida, las observaciones generales llevadas a cabo hasta el momento puedan trasladarse, *mutatis mutandis*, a la situación de las criptomonedas en nuestro país. En efecto, y si bien adoptando particularidades nacionales merecedoras de mención, las tendencias internas no se alejan en exceso de las que hemos señalado a nivel internacional.

Tal vez pueda señalarse como rasgo peculiar de la situación nacional la existencia de un interés patente en productos y servicios relacionados con las criptomonedas por parte de operadores de banca «tradicionales», como Barclays o el BBVA, interés que va desde la financiación de iniciativas empresariales relacionadas con las criptomonedas[91] hasta

---

[90] En cuanto a la implantación de internet en los hogares españoles el porcentaje de hogares con acceso a una conexión a internet en España se situaba en el 82%, por un 85% de media en la UE (2016). El porcentaje de individuos que emplean regularmente servicios bancarios online ascendería a un 43% en España, por un 49% de media en la UE (2013). Por último, los porcentajes de usuarios de internet con un nivel bajo, medio y alto de competencias corresponderían en España a un 28%, un 33% y un 14%, respectivamente, por un 30%, un 35% y un 12% en la UE (2013). Fuente: Eurostat, conjunto de estadísticas «Digital Economy and Society» (disponible en http://ec.europa.eu/eurostat/web/digital-economy-and-society/data/main-tables).

[91] V., respectivamente: Servimedia, «Bankinter invierte en coinffeine, una empresa española de tecnología *bitcoin*», diario *El Economista* de 17 de noviembre de 2014 (disponible en http://www.eleconomista.es/economia/noticias/6249235/11/14/Bankinter-invierte-en-coinffeine-una-empresa-espanola-de-tecnologia-bitcoin.html); y Europa Press, «BBVA apuesta por el *bitcoin*», diario *Expansión* de 20 de enero de 2015 (disponible en http://www.expansion.com/2015/01/20/empresas/banca/1421768862.html).

el patrocinio de congresos al respecto[92]. Sin embargo, es pronto para atribuir una significación relevante a las inversiones llevadas a cabo por estos operadores (esto es, más allá del indudable valor mediático de las mismas), en la medida en que —al menos, por el momento— se trataría de inversiones a veces relativamente modestas y llevadas a cabo a través de departamentos de *venture* o capital riesgo[93]. No contribuye tampoco a apreciar una madurez del mercado de criptomonedas a nivel nacional el hecho de que las organizaciones de consumidores y usuarios hayan tachado en su momento la inversión en criptomonedas de «inversión no recomendable», esencialmente a causa del desamparo del consumidor que conlleva el vacío regulatorio, pero también por motivo de otros factores, como la volatilidad de la cotización o las fallas de seguridad del sistema[94]. Las voces cautelosas encontrarán eco fácilmente si se tiene en cuenta la visibilidad mediática de la caída en picado de la cotización de las principales criptomonedas desde finales de 2017[95].

La cautela de nuestros actores económicos con respecto a la irrupción de las criptomonedas encuentra su reflejo —tal vez, *outre mesure*— en la actividad de los poderes públicos. Por el momento, las criptomonedas han merecido en contadas ocasiones un pronunciamiento específico por parte de estos últimos. Cuando de la atención de los poderes públicos sobre las criptomonedas se ha seguido una toma de postura, ésta ha afectado, en el mejor de los casos, a situaciones muy específicas y delimitadas. En buena medida, esta situación viene a reflejar la existente a nivel internacional y europeo, que se caracteriza por la actitud de espera de los legisladores ante un fenómeno complejo que podría aún sufrir cambios relevantes antes de alcanzar su madurez.

2. *Reacciones institucionales y jurisprudenciales en España*

Obviamente, de la ausencia de medidas legislativas o reglamentarias no se sigue necesariamente una ausencia de postura por parte del supervisor. Como hemos visto, las autoridades bancarias europeas y ciertas autoridades bancarias nacionales, prescindiendo de la inactividad de los respectivos legisladores, no se han abstenido de emitir informes que han contribuido a centrar la discusión en torno a la naturaleza de las criptomonedas.

---

[92] En particular, el BBVA patrocinó el Digital Currency Summit de 2015 (https://digitalcurrencysumm.it/madrid-2015/).

[93] V. al respecto Ú. O'Kuinghttons, «El resurgir de *bitcoin*», diario *El País*, 16 de junio de 2015.

[94] OCU, noticia «*Bitcoin*, la moneda virtual es un riesgo real», publicada en el sitio de la OCU el 21 de enero de 2014 (disponible online en: https://www.ocu.org/dinero/deposito-inversion/noticias/bitcoin-moneda-virtual-riesgo): «no recomendamos invertir en ellas».

[95] A. S. S., «El *bitcoin* pierde 100.000 millones de dólares en nueve días», diario *Expansión* de 6 de febrero de 2018 (disponible online en: http://www.expansion.com/mercados/divisas/2018/02/06/5a7975b2e5fdea2d658b45ec.html).

En el caso de nuestro Banco de España, disponemos de una nota informativa publicada en enero de 2014[96], en la que el supervisor señalaba una serie de riesgos o amenazas potenciales que afectarían al *bitcoin*, de distinta índole: uso potencial en el marco de las finanzas criminales, posibles efectos negativos sobre la reputación de otros medios de pago digitales, existencia de fallos en el sistema susceptibles de resultar en transacciones fraudulentas, eventuales impactos sobre la estabilidad de los precios y sobre la estabilidad financiera[97], e irreversibilidad de las transacciones. El enfoque del documento, centrado en los riesgos de las criptomonedas, no era sino el reflejo nacional en 2014 de la actitud de desconfianza de otros supervisores ante un fenómeno aún en evolución.

Por otro lado, el mismo supervisor ha emitido a principios de 2018 una nota conjunta con la CNMV sobre los riesgos de la inversión en criptomonedas (que hay que poner en relación con las fuertes variaciones de la cotización de las principales criptomonedas entre el comienzo de 2017 y la fecha de publicación de la nota conjunta) y, en particular, de la inversión en ICOs u ofertas iniciales de criptomonedas[98], a la que aludiremos más abajo (en la sección dedicada al uso criminal de las criptomonedas en España).

Por su parte, ni la Estrategia de Seguridad Nacional 2017 ni la Estrategia de Ciberseguridad Nacional se refieren específicamente a las criptomonedas. De nuevo, habrá de atribuirse tal omisión al enfoque amplio («estratégico») de ambos documentos, o puede que a la cautela de sus redactores[99]. A pesar de esta ausencia —tal vez a subsanar—, los informes de amenazas en materia de ciberseguridad del CCN-CERT han venido considerando regularmente el rol de las criptomonedas en los métodos y estructuras cibercriminales[100].

---

[96] S. Gorjón, «Divisas o monedas virtual [*sic*]: El caso de *Bitcoin*», Nota informativa del Banco de España de enero de 2014 (disponible online en: http://www.bde.es/f/webpcb/RCL/canales/home/menu-botonera/noticias/2014/Enero/pdf/Nota_informativa_*Bitcoin*_enero2014.pdf).

[97] La nota informativa parecía hacerse eco aquí de los riesgos detectados en el informe del Banco Central Europeo de 2012 (BCE *Virtual Currency Schemes*, cit., pp. 33 ss., 37 ss.).

[98] BdE y CNMV, *Comunicado conjunto de la CNMV y del Banco de España sobre «criptomonedas» y «ofertas iniciales de criptomonedas» (ICOs)*, de 8 de febrero de 2018.

[99] Si bien en el momento de publicación primera de ambos documentos estratégicos la presencia de las criptomonedas en la Red distaba ya de ser un fenómeno marginal, lo que es especialmente cierto para el caso de la Estrategia de Ciberseguridad Nacional, publicada en diciembre de 2013.

[100] Ver el Informe CCN-CERT IA 03/14, *Ciberamenazas 2013/Tendencias 2014*, publicado el 28 de marzo de 2014, pp. 42 ss., así como el Informe CCN-CERT IA-16/17, *Ciberamenazas y Tendencias 2017* (versión completa), en particular p. 32 (que apunta a las dificultades investigativas que implica el uso de criptomonedas por los grupos de ciberdelincuentes organizados) y, en general, con abundantes referencias al empleo de criptomonedas (en particular, de *bitcoins*) como medio de pago de víctima a criminal.

Dada la ausencia de un pronunciamiento del legislador acerca de la naturaleza jurídica de las criptomonedas, no resulta extraño que la cuestión haya venido siendo objeto de discusión. La sucinta nota informativa del Banco de España que hemos citado anteriormente no brindaba agarres sobre los que apoyarse para una definición. Por el contrario, el documento parecía evitar cuidadosamente una definición de las criptomonedas, limitándose a afirmar en sus primeras líneas que «Las divisas o monedas virtuales constituyen un conjunto heterogéneo de instrumentos de pago innovadores que, por definición, carecen de un soporte físico que los respalde.»[101]

A pesar de la ausencia de un acuerdo sobre la naturaleza jurídica de las criptomonedas entre los autores que se han ocupado de la cuestión, éstos parecen haber llegado a una conclusión común al delimitar negativamente su definición[102]: las criptomonedas no son «dinero electrónico» en el sentido de la Ley 21/2011, de 26 de julio, de dinero electrónico (norma de transposición a nuestro ordenamiento interno de la Directiva 2009/110/CE, de 16 de septiembre, sobre el acceso a la actividad de las entidades de dinero electrónico y su ejercicio, así como sobre la supervisión prudencial de dichas entidades[103]). En efecto, la definición de dinero electrónico ofrecida por la Ley 21/2011 presuponía un «valor monetario almacenado por medios electrónicos o magnéticos que represente un crédito sobre el emisor […] y que sea aceptado por una persona física o jurídica distinta del emisor de dinero electrónico»[104].

Nuestra norma nacional reproducía así, prácticamente palabra por palabra, el tenor literal de la definición contenida en la Directiva que transponía[105], norma europea que, a su vez, había sido promulgada

---

[101] Gorjón, «Divisas o monedas virtuales», cit., p. 1. Esta definición se ha visto superada por la evolución del fenómeno, así como por la de la percepción institucional del mismo: como hemos visto, el propio BCE negó a posteriori a las criptomonedas el carácter de medios de pago.

[102] V. al respecto D. Lisón, «Dinero electrónico vs. *Bitcoin*», blog personal del autor, publicado el 4 de febrero de 2015 (disponible online en: http://daniellison.es/dinero-electronico-vs-*bitcoin*/); y F. M.ª Ramos, «La prevención del blanqueo de capitales y el *bitcoin*», actualidad jurídica del sitio del Consejo General de la Abogacía Española, publicado el 26 de octubre de 2015 (disponible online en: http://www.abogacia.es/2015/10/26/la-prevencion-del-blanqueo-de-capitales-y-el-bitcoin/).

[103] Cuyo objeto fue desarrollado ulteriormente por el Real Decreto 778/2012, de 4 de mayo, de régimen jurídico de las entidades de dinero electrónico.

[104] Art. 1.2 de la Ley 21/2011, de 26 de julio: «Se entiende por dinero electrónico todo valor monetario almacenado por medios electrónicos o magnéticos que represente un crédito sobre el emisor, que se emita al recibo de fondos con el propósito de efectuar operaciones de pago según se definen en el artículo 2.5 de la Ley 16/2009, de 13 de noviembre, de servicios de pago, y que sea aceptado por una persona física o jurídica distinta del emisor de dinero electrónico.»

[105] Art. 2 2) de la Directiva 2009/110/CE, de 16 de septiembre: «"dinero electrónico": todo valor monetario almacenado por medios electrónicos o magnéticos que representa un crédito sobre el emisor, se emite al recibo de fondos con el propósito de efectuar ope-

cuando el *bitcoin* aún estaba naciendo y que, por ende, no pretendía ni podía pretender el tomar en consideración las criptomonedas a la hora de delinear los contornos de dicha definición. De los considerandos que introducen la norma resulta clara la voluntad del legislador europeo de presuponer un prepago con moneda de curso legal a favor de la entidad emisora de dinero electrónico[106], a pesar del empleo poco claro del término genérico «fondos» en el texto de la parte dispositiva de la Directiva.

Por su parte, el legislador nacional aclaraba que «la definición legal de dinero electrónico […] se basa en tres criterios, de manera que todo aquel producto que reúna esas tres características podrá calificarse como dinero electrónico»[107], siendo los tres criterios: que el valor monetario almacenado por medios electrónicos represente un crédito contra el emisor; que se emita al recibo de fondos con el propósito de efectuar operaciones de pago; y que sea aceptado (a efectos de pago) por una persona física o jurídica distinta del emisor. Prescindiendo del modo en que haya de entenderse la expresión «valor monetario» (esto es, si éste «valor monetario» hace referencia a una moneda de curso legal o no), debe estarse de acuerdo[108] en que las criptomonedas no parecen satisfacer los dos primeros criterios de la definición. En efecto, las criptomonedas no responden al esquema monetario clásico al no representar un título de valor respaldado por un emisor, y no son emitidas al recibo de «fondos», especialmente si entendemos que este término, en la línea marcada por nuestra interpretación de los considerandos de la Directiva 2009/110/CE, podría hacer referencia a moneda de curso legal.

Si bien la delimitación negativa del contorno de la definición jurídica de las criptomonedas con respecto al dinero electrónico resulta así clara, no puede decirse lo mismo de la delimitación positiva de su contenido. En ausencia de normativa específica, debe estarse a los escasos pronunciamientos por parte de las autoridades de supervisión y la jurisprudencia; ahora bien, estos pronunciamientos no permiten alzar un régimen jurídico estructurado a partir de ellos, ya que conciernen

---

raciones de pago, según se definen en el artículo 4, punto 5, de la Directiva 2007/64/CE, y que es aceptado por una persona física o jurídica distinta del emisor de dinero electrónico;».

[106] Directiva 2009/110/CE, de 16 de septiembre, considerando 7: «Resulta adecuado introducir una definición clara de dinero electrónico para que este concepto sea técnicamente neutro. Dicha definición debe cubrir todas las situaciones en las que el proveedor de servicios de pago emita un instrumento de valor almacenado y prepagado a cambio de fondos, y el cual pueda utilizarse como modo de pago porque la tercera persona lo acepta como tal.» V. igualmente el considerando 8 de la misma Directiva 2009/110/CE.

[107] Ley 21/2011, de 26 de julio, sección II del Preámbulo.

[108] Lisón, «Dinero electrónico vs. *Bitcoin*», cit.; y Ramos, «La prevención del blanqueo de capitales y el *bitcoin*», cit., que limitaba la argumentación al primer criterio: «Ante la falta en el *bitcoin* del respaldo de un crédito contra el emisor, debemos considerar que el *Bitcoin* no es dinero electrónico por la sencilla razón de que ese emisor no existe.»

mayoritariamente cuestiones relativas al ámbito de la fiscalidad de las criptomonedas.

Cierto es que una de las pocas excepciones a esta prevalencia del ámbito fiscal nos la brinda la jurisprudencia nacional y, en particular, la única sentencia relevante de la que disponemos por el momento, publicada por la Audiencia Provincial de Oviedo el 6 de febrero de 2015[109]. Esta decisión, que ha sido ya objeto de una cierta atención desde el punto de vista de la actualidad jurídica[110], venía a ser un reflejo jurisprudencial de la actitud de cautela de los supervisores nacional y europeo, ya mencionada. La Audiencia Provincial estimaba el recurso presentado contra la decisión en primera instancia favorable a la demandante, una compañía local de informática, por la demandada, una entidad bancaria, la cual había sido condenada por incumplir el contrato de afiliación a los sistemas de pago Visa y Mastercard, que incluía la instalación de una terminal de punto de venta (TPV)[111].

En su argumentación del recurso, la demandada aducía que la decisión de resolver el contrato había obedecido a la declaración inexacta por parte de la misma en el momento de conclusión del contrato de la finalidad para la que sería usado el TPV, ya que existiría una divergencia entre la actividad declarada originalmente por la demandante (facilitar el software para la adquisición de *bitcoin*s), y el servicio para el que realmente se emplearía la terminal (la compra directa de *bitcoin*s por medio del terminal). En apariencia, la demandante habría pretendido emplear los sistemas de pago citados para canalizar una actividad de *exchanger* de criptomonedas; la demandada había así decidido resolver el contrato por considerarla una actividad de alto riesgo y con posibilidades de servir de medio para el blanqueo de capitales[112].

La Audiencia Provincial daba la razón a la demandada, al considerar aplicable a la situación el texto de la Ley 10/2010 de 28 de abril, que impone a los sujetos obligados, cuando no puedan aplicar las medidas de diligencia impuestas por la propia Ley, el poner fin a las operaciones si la imposibilidad es apreciada sólo una vez en curso la relación de negocios[113]. Al fundar la aplicabilidad de dicha norma a la situación de autos,

---

[109] Audiencia Provincial de Oviedo, Sección Cuarta, n.º de recurso 37/2015, de 6 de febrero de 2015 (disponible online en la página web del CENDOJ/CGPJ).

[110] O. Martínez, «*Bitcoin*s y prevención del blanqueo de capitales», entrada publicada el 26 de mayo de 2015 en el blog del despacho de abogados Applicalia (disponible online en: http://www.applicalia.com/blog-entry/*bitcoin*s-prevencion-blanqueo-capitales); de la misma autora, «*Bitcoin*s y prevención del blanqueo de capitales», diario *Expansión* de 29 de septiembre de 2016 (disponible online en: http://www.expansion.com/juridico/opinion/2016/09/29/57ed56ff468aebfe2d8b4629.html)

[111] Sent. AP Oviedo, n.º 37/2015, cit., Antecedentes de hecho.

[112] Sent. AP Oviedo, n.º 37/2015, cit., FJ 2.

[113] Art. 7. 3 de la Ley 10/2010 de 28 de abril, de prevención de blanqueo de capitales y de la financiación del terrorismo: «Los sujetos obligados no establecerán relaciones de

la Audiencia Provincial se apoyaba no solamente en los indicios de especial riesgo de las actividades de la demandante que se desprendían de los mismos hechos, sino también en el especial riesgo de las criptomonedas desde el punto de vista del blanqueo de capitales que se desprendería de las conclusiones alcanzadas por el GAFI[114].

La mención de un informe emitido por un organismo internacional de estandarización como fundamento de la afirmación de los riesgos inherentes a los productos y servicios relacionados con las criptomonedas nos parece sintomática: en ausencia de un recorrido suficiente de las criptomonedas como para que su desarrollo se estabilice, parece inevitable que los primeros pronunciamientos de la jurisprudencia y de la legislación se vuelvan hacia los informes que hemos venido citando a lo largo de este trabajo, haciéndose eco de la cautela que los preside.

Más allá de esta sentencia, disponemos de ocho dictámenes vinculantes de la Dirección General de Tributos en materia de *bitcoin*s, de los cuales seis fueron formulados en respuesta a otras tantas cuestiones relativas a la fiscalidad de estas criptomonedas, en lo tocante al régimen de las actividades de minería y *exchanging* de bitcoins en relación con el Impuesto de Sociedades, con el Impuesto sobre el Valor Añadido (IVA) y con el Impuesto de Actividades Económicas (IAE)[115].

De estos seis dictámenes, los más relevantes nos parecen el primero desde el punto de vista cronológico, de 8 de julio de 2013[116], dado su carácter pionero (pese a que las líneas de interpretación marcadas en él por la DGT hayan sido superadas en algunos aspectos), y el segundo, de 3 de marzo de 2015[117], ya que en él la Dirección General de Tributos fijaba ya una línea de interpretación que sería seguida, en sus líneas esenciales, por los dictámenes posteriores.

El primero de los dos suponía la primera consulta respondida por la Dirección General de Tributos en relación con la fiscalidad de las criptomonedas en general, siendo planteada por un particular que deseaba iniciar una actividad de *exchanger*, así como de venta de

---

negocio ni ejecutarán operaciones cuando no puedan aplicar las medidas de diligencia debida previstas en esta Ley. Cuando se aprecie la imposibilidad en el curso de la relación de negocios, los sujetos obligados pondrán fin a la misma, procediendo a realizar el examen especial a que se refiere el artículo 17.»

[114] Sent. AP Oviedo, n.º 37/2015, cit., FJ 3. Aunque la sentencia se limita a citar las «conclusiones del GAFI» (aludiendo, además, al hecho de que las Recomendaciones del mismo organismo son mencionadas en la exposición de motivos de la Ley 10/2010), según el contexto de la mención estas «conclusiones» son, muy probablemente, las alcanzadas en el Informe GAFI FATF *Virtual Currencies. Key Definitions and potential AML/CTF Risks,* cit., p. 11.

[115] Examinaremos los dos restantes más adelante, en la sección dedicada al empleo de criptomonedas en el contexto del blanqueo de capitales en España.

[116] Consulta vinculante DGT n.º V2228-13, de 8 de julio de 2013.

[117] Consulta vinculante DGT n.º V1028-15, de 3 de marzo de 2015.

«tarjetas de crédito virtuales», en España. El particular deseaba una respuesta en cuanto a la forma de tributación de dichas actividades en el Impuesto sobre Sociedades y en el IVA. En cuanto al primero de los dos impuestos, la DGT respondía en el sentido de declarar que formarían parte de la base imponible del Impuesto sobre Sociedades los ingresos obtenidos por la empresa en concepto de comisión por cada una de ambas actividades[118]. Más ardua tarea suponía el responder a la cuestión atinente al IVA. A falta de todo asidero normativo sólido, la DGT se agarraba entonces a la normativa en materia de dinero electrónico (en particular, a la Ley 21/2011, de 26 de julio, de dinero electrónico), si bien lo hacía (a nuestro entender, con buen juicio) de manera tentativa, expresando sus reservas y evitando dar una respuesta concluyente[119]. La misma evolución social, institucional y jurisprudencial del fenómeno en los últimos años ha hecho que quede atrás la interpretación analógica bosquejada entonces por la DGT sobre el particular[120]: resulta prácticamente pacífico a día de hoy, según hemos visto ya, que las criptomonedas no son «monedas» *strictu sensu* (esto es, moneda de curso legal), motivo por el cual el supervisor financiero europeo ha negado a las criptomonedas el carácter de «medio de pago» en sentido propio[121].

Algo menos de dos años después, sin embargo, la DGT tuvo ocasión de aquilatar su doctrina en lo atinente a la tributación en el IVA de las actividades relacionadas con las criptomonedas: como hemos apuntado, una línea de interpretación ulterior fue abierta por un dictamen de la DGT de 2 de marzo de 2015[122]. En este caso, la actividad del consultante se dedicaba a facilitar la compraventa de *bitcoin*s a través de máquinas de *vending* y cajeros (esto es, se trataba de un exchanger). La DGT res-

[118] Consulta vinculante DGT n.º V2228-13, de 8 de julio de 2013: «formarán parte de la base imponible del Impuesto sobre sociedades, los ingresos devengados en cada período impositivo derivados de los servicios prestados por la consultante en concepto de comisión, tanto en las operaciones de compraventa de moneda virtual como en las operaciones de recarga de tarjetas de crédito virtuales.»

[119] Consulta vinculante DGT n.º V2228-13, de 8 de julio de 2013, al cierre de las consideraciones acerca de la tributación en el IVA de las actividades objeto de consulta: «Ahora bien, para ello sería necesario que la moneda electrónica objeto de adquisición y transmisión por el consultante cumpla los criterios definitorios establecidos en la citada Ley 21/2011, de dinero electrónico, cuestión que no es posible evaluar por parte de este Centro Directivo, dado que no se aporta información suficiente sobre las características de dicho medio de pago o moneda electrónica a efectos de realizar tal valoración.»

[120] La DGT apuntaba entonces la posibilidad de considerar aplicable a las criptomonedas la exención prevista en el art. 20.1 18º j) de la Ley Ley 37/1992, sobre la base de su carácter de «moneda», por considerarlas como «dinero electrónico» en el sentido de la Ley 21/2011 y, por tanto, como «sustituto electrónico de las monedas y los billetes de banco» en cuanto que medio de pago.

[121] V. Dictamen del Banco Central Europeo de 12 de octubre de 2016, cit., sección 1.1.3.

[122] Consulta vinculante DGT n.º V1028-15, de 3 de marzo de 2015.

pondía a la consulta: afirmando la aplicabilidad de la Ley 37/1992, de 28 de diciembre, del Impuesto sobre el Valor Añadido, a la actividad del consultante en cuanto que entrega de bienes o prestación de servicios por empresarios en el desarrollo de su actividad empresarial[123]; declarando que tal actividad estaría sujeta al impuesto en cuestión, pero exenta de éste[124] (y relevando al consultante, en consecuencia, de la obligación de realizar las declaraciones-liquidaciones exigidas por el Reglamento del Impuesto, en la medida en que sólo llevase a cabo dicha actividad declarada exenta del mismo[125]); y estimando la actividad del consultante como sujeta al IAE[126].

De los argumentos en los que se funda la contestación, tal vez conciten mayor interés los atinentes a la sujeción de la actividad de *exchanging* de *bitcoins* al IVA (y exención de dicho impuesto). La DGT se basaba en la interpretación del artículo 20.1 de la Ley 37/1992, el cual es la norma de transposición a nuestro ordenamiento nacional del artículo 135.1 de la Directiva 2006/112/CE, de 28 de noviembre. El dictamen de la DGT venía a considerar así la misma norma que poco más de siete meses después sería interpretada por el TJUE en un asunto similar, ya citado[127] (cuestión acerca de la aplicabilidad de la normativa sobre el IVA a la actividad de *exchanging* de *bitcoins*), para alcanzar la misma conclusión que alcanzaría el Tribunal en su decisión (sujeción de la actividad al impuesto, estando, sin embargo, exenta del mismo[128]).

Pese a estas similitudes, existía una divergencia notable entre la interpretación por parte de la DGT y del TJUE de la misma lista de exenciones. La exención del pago del IVA en la actividad de *exchanging* de *bitcoins* era fundada por la DGT en las letras h) e i) del artículo 20.1 de la Ley 37/1992, que constituyen, como indicaba la propia contestación, la transposición del apartado d) del artículo 135.1 de la Directiva 2006/112/CE[129]. Ahora

---

[123] Mediante la interpretación de los arts. 4.1 y 5.1 de la Ley en cuestión: Consulta vinculante DGT n.º V1028-15, cit., § 1 de la contestación.

[124] Consulta vinculante DGT n.º V1028-15, cit., § 2 de la contestación.

[125] Consulta vinculante DGT n.º V1028-15, cit., § 3 de la contestación.

[126] Siéndole aplicable la tarifa prevista en el epígrafe 969.7 de la sección primera del Real Decreto Legislativo 1175/1990, de 28 de septiembre: Consulta vinculante DGT n.º V1028-15, cit., § 4 de la contestación.

[127] STJUE *Högsta förvaltningsdomstolen* (cuestión prejudicial), cit.

[128] STJUE *Högsta förvaltningsdomstolen* (cuestión prejudicial), cit., §§ 38 a 43.

[129] Incluso, y en consonancia con la naturaleza de transposición de una norma de derecho europeo derivado del art. 20.1 h) e i) de la Ley 37/1992, la DGT (Consulta vinculante DGT n.º V1028-15, cit., § 2 de la contestación) invocaba de cara a la interpretación de la misma las conclusiones de la AG Kokott en un asunto planteado ante el mismo TJUE acerca de la interpretación del art. 135.1 d) de la Directiva 2006/112/CE (Conclusiones de la AG J. Kokott sobre el asunto C-461/12 *Granton Advertising BV c./ Inspecteur van de Belastingdienst Haaglanden/kantoor Den Haag*, presentadas el 24 de octubre de 2013), a las que la misma AG reenviaba en sus propias Conclusiones sobre el asunto C-264/14, *Högsta förvaltningsdomstolen* (cuestión prejudicial), cit., n. 24.

bien, por el contrario, el TJUE excluía expresamente la aplicabilidad del apartado d) del artículo 135.1 de dicha Directiva como base para la exención del impuesto de la actividad de cambio de *bitcoin*s, indicando, por el contrario, el apartado e) de dicho artículo 135.1 como única causa de exención pertinente de las contenidas en la lista[130].

Tal contradicción entre la interpretación de la DGT y aquélla del TJUE resulta tanto más notable cuanto que la misma argumentación de la DGT, basando la exención del IVA de la actividad de cambio de *bitcoin*s en la norma de transposición del artículo 135.1 d) de la Directiva 2006/112/CE, ha sido reproducida, prácticamente palabra por palabra, en otros tres dictámenes del mismo órgano que contestaban a consultas vinculantes sobre cuestiones similares (dictámenes que datan, respectivamente, del 3 de marzo de 2015, del 1 de octubre de 2015 y del 31 de agosto de 2016[131]). Por lo demás, dichos dictámenes no han dejado de ir introduciendo matizaciones en la interpretación de la normativa fiscal aplicable a las actividades relacionadas con la obtención y comercialización de *bitcoin*s, pero siempre en relación estricta con el IVA y el IAE. Más allá de señalar la declaración de la minería o extracción de *bitcoin*s como actividad no sujeta al IVA y la de la no deducibilidad de la cuota del IVA soportada por el consultante de las actividades de minado y de venta de *bitcoin*s por uno de ellos[132] (refiriéndose otro a la clasificación de la actividad de exchanging en la Tarifa del IAE[133]), no nos detendremos aquí sobre dichas

[130] V. STJUE *Högsta förvaltningsdomstolen (cuestión prejudicial), cit.*, §§ 38 a 43 y 54 a 56 (inaplicabilidad a los servicios en cuestión de la exención de IVA prevista en el art. 135.1 d) de la Directiva, así como en la letra f) del mismo art., respectivamente); y misma decisión, §§ 44 a 53 (aplicabilidad a los servicios en cuestión de la exención contemplada en el art. 135.1 e) de la Directiva)

[131] Consulta vinculante DGT n.º V1029-15, de 3 de marzo de 2015, y, en particular, su § 2; Consulta vinculante DGT n.º V2846-15, de 1 de octubre de 2015, § 2; y Consulta vinculante DGT n.º V3625-16, de 8 de agosto de 2016, § 3.

[132] Consulta vinculante DGT n.º V3625-16, de 8 de agosto de 2016, § 2, en lo tocante a la no sujección de la extracción de *bitcoin*s al IVA: de nuevo, la DGT acudía a la jurisprudencia del TJUE para la interpretación de la normativa de transposición de la Directiva 2006/112/CE (en particular, a la STJUE *Tolsma c./ Inspecteur der Omzetbelasting Leeuwarden*, asunto C-16/93, de 3 de marzo de 1994), para concluir que «la [*sic*] falta de una relación directa entre el servicio prestado y la contraprestación recibida en los términos señalados los servicios de minado objeto de consulta no estarán sujetos al Impuesto sobre el Valor Añadido». Sobre la base del art. 74.1 1.º a) de la Ley 37/1992, de 28 de diciembre, del Impuesto sobre el Valor Añadido (según el cual son deducibles «las entregas de bienes y prestaciones de servicios sujetas y no exentas del Impuesto sobre el Valor Añadido»), el mismo dictamen, en su § 4, negaba la deducibilidad de la cuotas del IVA soportadas por el solicitante de las actividades de minado (en cuanto que actividad no sujeta al impuesto) y de venta de *bitcoin*s (en cuanto que actividad sujeta, pero exenta).

[133] Consulta vinculante DGT n.º V-2908/17, de 18 de noviembre de 2017, § 3 de la respuesta.

matizaciones, debido al interés circunscrito que presentan de cara al tratamiento de nuestro objeto de estudio.

Como conclusión de esta sección, podemos constatar que la situación general de las criptomonedas en España es equiparable a la que constatábamos para el resto de los países desarrollados en general y de Europa en particular: reacciones sociales diversas, actitud cautelosa de las instituciones concernidas, tímida concreción de algunos rasgos aspectuales de su régimen jurídico por vía tributaria. Si debe apuntarse una peculiaridad, ésta podría ser el mayor interés de ciertos operadores españoles de banca tradicional por la inversión en criptomonedas y, en general, por la tecnología financiera (*fintech)* basada en la cadena de bloques, aunque sea todavía pronto para prever el impacto a largo plazo de esta apertura en nuestro sector financiero.

3. *Uso criminal de las criptomonedas y blanqueo de capitales en España*

Hemos apuntado ya que el uso de las criptomonedas en el contexto de las finanzas criminales no sólo prevalece en el ámbito de la criminalidad online, sino que además se amolda perfectamente a las características clásicas de la ciberdelincuencia. Dado el carácter desmaterializado y transfronterizo de este tipo de delincuencia, no resulta sorprendente que el uso de las criptomonedas en el contexto de las finanzas criminales con el que tienen que ver nuestras autoridades hasta el momento presente perfiles muy similares a los encontrados en otros países europeos.

A falta de informes específicos que traten de cuantificar (por fuerza, aproximativamente) el impacto específico del uso de las criptomonedas en el contexto de las finanzas criminales en España, la visibilidad de esta forma de delincuencia se reduce a su mención como fenómeno más o menos frecuente en los informes ya mencionados, a la presencia mediática de la actividad de nuestras Fuerzas y Cuerpos de Seguridad del Estado y a algunas decisiones judiciales.

Parte del uso criminal de las criptomonedas en España que así aflora es indirecto. Con alguna frecuencia, las criptomonedas no son empleadas como medio financiero por los criminales, sino que sirven más como cebo o reclamo en la organización de delitos de estafa para engañar a víctimas poco conocedoras del funcionamiento de las criptomonedas de tal modo que transfieran fondos a los delincuentes. La captación de estos fondos se produce so pretexto de participar en un fondo de inversión en criptomonedas o en una oferta inicial de criptomone-

das (*Initial Coin Offering* o *ICO*[134]), siendo tales inversiones o ICOs, en realidad, inexistentes, y asumiendo con la estafa así, con frecuencia, una organización de tipo esquema Ponzi o estafa piramidal, de cara a asegurar un flujo constante de dinero hacia los criminales durante un cierto período de tiempo. En particular, el empleo de ICOs fraudulentas es un riesgo bien conocido a nivel internacional, que ha sido señalado por los actores del sector[135] y que ha suscitado la reacción de las autoridades de supervisión de países como EE.UU. (donde la regulación del uso de las criptomonedas se encuentra en un estado avanzado) o China (donde las actividades económicas relacionadas con las criptomonedas tienen un peso económico especialmente notorio)[136]. A nivel europeo, la Autoridad Europea de Valores y Mercados (ESMA) ha publicado dos comunicados a finales de 2017 en los que advierte a los inversores de los riesgos de las ICOs[137] y recuerda a las empresas interesadas en lan-

---

[134] Modo de financiación de criptomonedas incipientes que funciona, en cierto modo, de manera similar al *crowdfunding*, puesto que consiste en la oferta al público (en particular a potenciales microinversores, aunque no sólo), por un precio determinado, de una cantidad de unidades de una criptomoneda en curso de creación, de cara a la creación de una base inicial de titulares de las criptomonedas, al respaldo del valor percibido de la misma por la comunidad (puesto que el valor percibido de cada unidad, al menos en un primer momento, ascenderá al menos a la cantidad que cada microinversor haya pagado por ella) y a la financiación de los gastos derivados de la misma creación de la criptomoneda de que se trate. Este esquema de financiación se empleó, por ejemplo, para el lanzamiento del ether, si bien en ese caso los desarrolladores del proyecto marcaron un precio fijo en *bitcoins* de los ethers ofrecidos en la preventa, que tuvo lugar en julio de 2014: v. T. Gerry, «Cut and Try: Building a Dream», entrada en el blog oficial del proyecto Ethereum, de 2 de febrero de 2016, disponible online en: https://blog.ethereum.org/2016/02/09/cut-and-try-building-a-dream/ (consultado el 6 de febrero de 2018).

[135] V. p. ej. B. McAllan, «Wolf of Wall Street warns of impending criptocurrencies scam», diario *Financial Times*, artículo de 22 de octubre de 2017 (disponible online en: https://www.ft.com/content/739f8954-b61a-11e7-a398-73d59db9e399, consultado el 6 de febrero de 2018).

[136] Así, la U.S. Security Exchanges Commission, «Investor Bulletins: Initial Coin Offerings», boletín de 25 de julio de 2017 (disponible online en: https://www.sec.gov/oiea/investor-alerts-and-bulletins/ib_coinofferings, consultado el 6 de febrero de 2018) ofrece una serie de consejos a los inversores interesados en invertir en una ICO para evaluar el riesgo de fraude que ésta pueda presentar, habiendo advertido a los inversores ya en 2013 del riesgo de las ICOs fraudulentas que encubren esquemas de Ponzi (U.S. Security Exchanges Commission, «Investor Alerts: Ponzi Schemes Using Virtual Currencies», de julio de 2013 (disponible online en: https://www.sec.gov/servlet/sec/investor/alerts/ia_virtualcurrencies.pdf, consultado el 6 de febrero de 2018). Por su parte, el Banco Popular de China (supervisor financiero en la República Popular de China) prohibió a finales de 2017 las ICOs por considerar que éstas presentaban un alto riesgo de fraude, imponiendo el reembolso de las cantidades ya pagadas a los inversores y prohibiendo a los exchangers el cambio de las criptomonedas procedentes de ICOs en marcha: v. p. ej. al respecto «*Bitcoin*: China prohíbe las colocaciones de criptodivisas», diario Cinco Días, artículo de 7 de septiembre de 2017 (disponible online en: https://cincodias.elpais.com/cincodias/2017/09/04/mercados/1504518523_957352.html, consultado el 6 de febrero de 2018).

[137] Statement ESMA50-157-829, *ESMA alerts investors to the high risks of Initial Coin Offerings (ICOs), de 13 de noviembre de 2017.*

zar ICOs la normativa europea aplicable a este tipo de operaciones[138], respectivamente. Recientemente, el Banco de España y la Comisión Nacional del Mercado de Valores han emitido una nota conjunta en la que advierten, entre otras cosas, del alto riesgo de fraude en las ICOs, subrayando la situación de posible indefensión del inversor perjudicado en este tipo de operaciones ante la ausencia de regulación de las criptomonedas a nivel europeo y nacional[139].

Una presunta estafa que responde a esta última tipología ha recibido gran atención mediática y social en los últimos años. Los presuntos organizadores de la estafa, basados en España, habrían recabado, entre 2013 y 2015, dinero de una multitud de víctimas repartidas por todo el mundo (que se estiman en unas 50.000), prometiéndoles unos retornos de inversión muy elevados. Tales retornos debían ser devengados en una criptomoneda creada por los presuntos organizadores de la estafa, criptomoneda a cuyo lanzamiento estarían ayudando las víctimas con sus aportaciones y que era, en realidad, inexistente. La continuidad en el tiempo del flujo de aportaciones de cada víctima se aseguraba mediante el uso de un esquema Ponzi[140].

En definitiva, se trataría de un caso que se acomodaría perfectamente a las ICOs fraudulentas que acabamos de mencionar. Lógicamente, el desconocimiento por parte de las presuntas víctimas (la mayoría de las cuales residen en Italia y España) de la mecánica de las criptomonedas en general y del funcionamiento de las ICOs en particular (operaciones, por lo demás, que, aún en ausencia de intención dolosa por sus promotores, conllevan un riesgo elevado para el inversor[141]) habría jugado un papel esencial en el éxito del esquema fraudulento.

Este desconocimiento viene a aflorar en las dos consultas vinculantes de la Dirección General de Tributos que restan del grupo de siete

---

[138] Statement ESMA50-157-828, *ESMA alerts firms involved in Initial Coin Offerings (ICOs) to the need to meet relevant regulatory requirements*, de 13 de noviembre de 2017.

[139] BdE y CNMV, *Comunicado conjunto de la CNMV y del Banco de España sobre «criptomonedas» y «ofertas iniciales de criptomonedas» (ICOs)*, de 8 de febrero de 2018.

[140] Se trata del célebre caso de la criptodivisa «Unete», que ha dado lugar a un complicado proceso judicial aún en curso: v. p. ej. R. Rincón y J. Gil, «Prisión para los dos fundadores de unete, la estafa de la moneda virtual», diario *El País*, 26 de octubre de 2015 (disponible online en: https://politica.elpais.com/politica/2017/01/06/actualidad/1483715726_394377.html, consultado el 6 de febrero de 2018); J. Gil, «La estafa de la moneda virtual española alcanza a 78 países», diario *El País*, 8 de enero de 2017 (disponible online en: https://politica.elpais.com/politica/2017/01/06/actualidad/1483715726_394377.html, consultado el 6 de febrero de 2018); y J. Gil, «El negocio oculto de los creadores de la moneda virtual española», diario *El País,* de 31 de enero de 2018 (disponible online en: https://politica.elpais.com/politica/2018/01/30/actualidad/1517341003_110594.html, consultado el 6 de febrero de 2018).

[141] Tal y como señalan el BdE y la CNMV, *Comunicado conjunto de la CNMV y del Banco de España sobre «criptomonedas» y «ofertas iniciales de criptomonedas» (ICOs)*, de 8 de febrero de 2018, en especial pp. 3 s.

que anticipábamos en la sección anterior. Ambas consultas vienen a ejemplificar los riesgos para el inversor nacional que presenta el carácter transfronterizo de la inversión en criptomonedas y, en especial, para el inversor particular que opera mediante intermediarios no situados en España.

En lo que más nos interesa ahora, la primera de ellas era planteada por la posible víctima de una estafa piramidal en la que el reclamo era, de nuevo, la inversión en criptomonedas[142]. Más que la respuesta de la DGT en sí[143], lo interesante en este caso era la descripción de los hechos que acompañaba la cuestión planteada por el consultante, en la medida en que ésta contiene un resumen que describe el esquema de la posible estafa. Según lo declarado por el consultante, éste habría invertido sus ahorros (cabe pensar, por tanto, que se tratase de un microinversor particular) en la compra de *bitcoin*s a través de distintos sitios de *exchanging*. En 2013 había depositado los *bitcoins* adquiridos (habrá que pensar que se trata aquí de los *tokens*) en un sitio que desarrollaría una suerte de actividad bancaria, al prestar el saldo en *bitcoins* a diferentes mutuatarios, debiendo llevarse el consultante una comisión por tales préstamos.

En un cierto momento, el administrador del sitio web (cuyo nombre real desconocía el consultante, por conocer únicamente su dirección de correo, su pseudónimo y una clave de *hash* pública del mismo) declaró haber sido víctima de un robo de *bitcoins* y no poder devolver los bitcoins a sus depositarios. Pese a serle ofrecida una transacción por el administrador del sitio (consistente en la renuncia al ejercicio de toda acción legal contra el administrador a cambio de la devlución de una porción mínima de los *bitcoins* originalmente depositados), el consultante decidió denunciar al administrador a las autoridades del país del administrador (hay que pensar que se trataría aquí de las autoridades del país en el que estuviese albergado el sitio web), que se inhibieron por considerar que la jurisdicción sobre el asunto correspondería al país de residencia del denunciante[144].

A falta de corroboración de la veracidad de los hechos aducidos por el consultante, lo cierto es que éstos encajan a la perfección con los ras-

---

[142] Consulta vinculante DGT n.º V1979-15, de 25 de junio de 2015.

[143] Que respondía a la consulta elevada en el sentido de considerar que el consultante tendría un derecho de crédito frente a un tercero (según el consultante, el presunto organizador de la posible estafa), debiendo ser éste judicialmente incobrable para que fuese posible computarlo como pérdida patrimonial a efectos de cálculo de la base imponible del IRPF y aludiendo al entonces reciente añadido de una letra k) al apartado 2 del artículo 14 de la LIRPF, según la cual pueden computarse como pérdidas patrimoniales los créditos vencidos y no cobrados en el período impositivo en que incurriesen ciertas circunstancias (alguna de las cuales, en particular la recogida en el supuesto descrito en el art. 14.2 k) 3.º IRPF, podía darse en el caso descrito por el consultante).

[144] Consulta vinculante DGT n.º V1979-15, de 25 de junio de 2015, descripción de los hechos.

gos habituales del tipo de estafas a las que venimos haciendo referencia. Concurrían, por un lado, el uso de modelos de negocio innovadores, poco conocidos y pretendidamente lucrativos[145] como reclamo, resultando, en este caso, digno de mención que el consultante y posible víctima de la estafa no era totalmente lego en materia de criptomonedas, habiendo llevado a cabo compras de *bitcoin*s en varios sitios de *exchanging*. Por otro lado, el posible estafador se prevalía de las características de las criptomonedas (posibilidad de transferencia internacional de la titularidad de las mismas al cambiar de manos los *tokens* correspondientes mediante la Red), así como de las ventajas clásicas de la criminalidad online (en este caso, anonimato y carácter transfronterizo). Por añadidura, cabe destacar la verosimilitud del motivo aducido por el administrador del sitio para el impago: robo de criptomonedas, si bien de un sitio mantenido por el mismo administrador, pero distinto de aquél en el que el consultante había hecho su depósito, lo cual, junto con el tipo de acuerdo al que trataba de llegar con el consultante, hace concebir serias dudas sobre la buena fe de aquél. La verosimilitud del motivo aducido y la consiguiente dificultad de la probable víctima para deslindar el engaño de la verdad viene de la misma mecánica de la criptomoneda en cuestión (posibilidad de «robar» *bitcoins* mediante un robo de datos que afecte a los *tokens* correspondientes). Dicho de otro modo, es difícil para el (micro) inversor distinguir entre una quiebra fraudulenta por robo (ficticio) de bitcoins y una quiebra legítima por robo (real) de *bitcoins*, ya que estas últimas no sólo son posibles, sino que se han dado en la práctica, y de manera notoria.

Sirva como ejemplo un caso en todo similar al que acabamos de presentar, pero en el que un robo real de *bitcoins* había causado una quiebra auténtica del deudor del interesado. Los hechos que fundaban otra consulta elevada a la DGT[146] (la última de nuestro grupo de siete) estaban relacionados también con una pérdida patrimonial del consultante por un impago de un tercero que habría quebrado por haber sido víctima de un robo de criptomonedas. La respuesta de la DGT era muy similar a la que ésta daba a la consulta que acabamos de tratar[147],

---

[145] La U.S. Security Exchanges Commission, ya en «Investor Alerts: Ponzi Schemes Using Virtual Currencies», de julio de 2013, cit., señalaba: «We are concerned that the rising use of virtual currencies in the global marketplace may entice fraudsters to lure investors into Ponzi and other schemes in which these currencies are used to facilitate fraudulent, or simply fabricated, investments or transactions. The fraud may also involve an unregistered offering or trading platform. These schemes often promise high returns for getting in on the ground floor of a growing Internet phenomenon.»

[146] Consulta vinculante DGT n.º V2603-15, de 8 de septiembre de 2015.

[147] En el sentido de que la DGT reitera su doctrina acerca de la posibilidad de computar el impago de un crédito contra un tercero como pérdida patrimonial deducible de la base imponible del IRPF sólo cuando el crédito sea judicialmente incobrable, añadiendo la misma consideración acerca del art. 12.4 k) de la LIRPF que llevaba a cabo en la Consulta vinculante DGT n.º V1979-15, de 25 de junio de 2015.

mientras que es, de nuevo, la descripción de los hechos la que concita nuestro interés. En ella, el consultante decía haber ingresado dos sumas de dinero con una diferencia de cinco días (el 21 y el 25 de febrero de 2014) en un banco polaco, con el encargo de que éste las transfiriese a un sitio japonés de *exchanging* y *storing* de criptomonedas. Al día siguiente de la fecha del último ingreso en dicho banco (es decir, el 26 de febrero de 2014), el consultante habría entrado en su cuenta del sitio japonés en cuestión para consultar su saldo en bitcoins, para encontrarse con que éste se había declarado en quiebra a causa de un robo masivo de *bitcoins*. Las fechas, así como el carácter aparentemente respetable del intermediario usado para la transacción (el banco polaco), nos hacen pensar que el sitio japonés en cuestión no era otro que Mt. Gox, que cerró su web el 25 de febrero de 2014 para acogerse a la ley de quiebras japonesa a causa de un robo masivo de *bitcoins*[148], como ya hemos apuntado más arriba. El banco polaco declinó toda responsabilidad en la pérdida del dinero y se negó a devolver al consultante los ingresos que había efectuado. Nótese cómo los hechos son, en parte, idénticos a los presentados en el caso anterior, variando únicamente el carácter legítimo de la quiebra causante del impago en este caso[149].

Al margen del uso de las criptomonedas como reclamo en delitos de estafa, éstas son empleadas por los criminales activos en nuestro país para el blanqueo de capitales. El que se trata de un uso frecuente resulta del informe sobre ciberamenazas del CCN-CERT de 2017, que para el ámbito específico de la ciberdelincuencia apunta el fuerte incremento de la dificultad de las investigaciones que éste supone[150]. Por lo demás, no se trata de un fenómeno novísimo. Un caso notorio por el número de víctimas en España de los delitos que generaron el dinero a blanquear y por el carácter pionero de la actuación policial y

[148] V. el artículo de agencias «La casa de *bitcoin*s Mt.Gox se acoge a la ley japonesa de quiebras», diario *El País, artículo de 28 de febrero de 2014 (disponible online en:* https://elpais.com/tecnologia/2014/02/28/actualidad/1393581588_264841.html, consultado el 6 de febrero de 2018).

[149] La descripción de los hechos en este último caso no precisa la posible participación del consultante en el concurso de acreedores de Mt. Gox.

[150] Informe CCN-CERT IA-16/17, *Ciberamenazas y Tendencias 2017* (versión completa), p. 32: «…los procedimientos de identificación de los autores siguen siendo manifiestamente insuficientes. El uso de técnicas de anonimización dificultan [*sic*] extraordinariamente las labores investigadoras (empleo de proxies y redes Tor). Todo ello, unido al anonimato que se deriva del uso de criptomonedas, dificulta el seguimiento y la identificación de los autores. Además, se han detectado sistemas de cambio ilegal de Bitcoin, totalmente anónimos, que, pese al porcentaje que exigen de cada cambio (entre el 8 y el 12%, frente al 0,5% de los legales) están teniendo un notable éxito.»

judicial fue el de la instrucción contra la red responsable del llamado «virus de la Policía»[151], en la llamada «Operación Ransom» u «Operación Ransomware»[152].

El elevado número de víctimas en España (a pesar de que éstas se encontraron en hasta 22 países[153]) contribuyó al impacto social del caso. Las infecciones comenzaron en 2011; la Policía recibió 1.222 denuncias relacionadas con el mismo sólo en el año 2012, mientras que el entonces INTECO (actual INCIBE) recibió 784.415 consultas al sitio dedicado al *malware* en cuestión y 26.028 llamadas a su teléfono de asistencia en el mismo año. Los delincuentes simultanearon varios medios de blanqueo de los beneficios obtenidos, que variaban en función del país de procedencia de los mismos. Mediante el mismo *ransomware*, obtenían en Europa códigos de prepago de *Ukash* o de *PaySafeCard* (proveedores británico y austríaco, respectivamente, de dinero electrónico), y, en los EE.UU., de *MoneyPak* (proveedor estadounidense de tarjetas de crédito Visa y Mastercard prepagadas), adquiridos por las propias víctimas[154]. Muchos de los códigos eran vendidos en foros rusos, siendo a su vez el producto de la venta ya ingresado en servicios de pago online mediante el empleo de documentación falsa o robada, ya blanqueado a través de casinos online, ya convertido en criptomonedas (en particular, en *bitcoin*s). Las tarjetas *Moneypak* estadounidenses eran obtenidas en los EE.UU., enviadas por paquetería a nuestro país y activadas en España (la cúpula de la red estaba basada en la Costa del Sol) mediante una llamada desde los Estados Unidos (fingida mediante un ordenador dedicado, sito en España), retirándose después el dinero en cajeros por parte de una red de «mulas» dedicada a tal efecto. El

---

[151] Se trataba de un *ransomware* con elementos de *phishing* aparecido en 2011, que bloqueaba el ordenador de sus víctimas, mostrando una página diseñada de tal modo que éstas creyesen que el bloqueo era consecuencia de una supuesta acción punitiva de los cuerpos de seguridad, a su vez resultado de un supuesto delito cometido por la víctima por medios informáticos. La página en cuestión no sólo estaba disfrazada de tal modo que pareciese proceder de los cuerpos de seguridad del país de residencia de cada una de las víctimas, sino que también mostraba la IP y la localización aproximada del ordenador de la víctima (cosas que se conseguían mediante la inclusión de una carpeta de geolocalización por IP en el código del *ransomware* en cuestión: v. «Detenido el creador del famoso Virus de la Policía» en el sitio *SecurityNull,* https://www.securitynull.net/detenido-el-creador-del-famoso-virus-de-la-policia/, consultado el 6 de febrero de 2018).

[152] Algunos de los particulares que siguen fueron participados por Daniel Campos, Fiscal de la Audiencia Nacional, a los asistentes al Primer Workshop CyberLaundry, celebrado en la sede de la UDIMA en Villalba el 13 de diciembre de 2016.

[153] En los EE.UU., el FBI alertaba de la existencia del «virus de la Policía» en su sitio web a mediados de 2012 (v. «New Internet Scam. Ransomware Locks Computers, Demands Payment», disponible online en: https://www.fbi.gov/news/stories/new-internet-scam, consultado el 6 de febrero de 2018).

[154] Siendo un error importante de los delincuentes el no facilitar el desbloqueo de los ordenadores una vez pagado el rescate: ello facilitó enormemente la detección de los casos de infección, al acudir las víctimas a la Policía para quejarse de que el ordenador no se desbloquease tras el pago de la «multa».

dinero en efectivo podía ser entonces reintroducido en el circuito del dinero electrónico en sentido propio, para seguir siendo convertido en diferentes medios de pago, a fin de dificultar su trazabilidad y ofuscar su procedencia.

Una gran parte de los beneficios de la organización terminaba su ciclo de conversiones siendo cambiado en *bitcoin*s, que eran gestionados directamente por el cerebro de la operación en persona, siendo una de las dificultades principales afrontadas por los investigadores la de acceder a las cuentas-monedero (*wallets*) de éste a falta de los códigos necesarios. Esta dificultad se resolvió, en buena medida, mediante la captura *in fraganti* del mismo cuando tenía gran parte de sus cuentas-monedero abiertas en su ordenador, lo que permitió la incautación del saldo en bitcoins de las mismas mediante una orden judicial específica, sobre cuya base la Policía Nacional convirtió en moneda de curso legal los *bitcoins* en cuestión y transfirió el producto a la cuenta bancaria de consignaciones judiciales correspondiente[155].

La sentencia de la Audiencia Nacional que coronó el proceso subsiguiente[156] impuso a los acusados condenas por delitos de estafa (en concurso medial con el delito de daños informáticos), de blanqueo de capitales, de falsedad en documento mercantil, de pertenencia a organización criminal y contra la intimidad[157]. Las penas quedaron mitigadas por la concurrencia en todos los acusados de las circunstancias modificativas de la responsabilidad penal de reparación del daño (en la medida en que los acusados ingresaron las responsabilidades civiles interesadas por las acusaciones) y de confesión tardía (al haber reconocido los hechos durante el juicio)[158], debiendo ello atribuirse, a nuestro entender, al perfil criminológico propio de los ciberdelincuentes. Aunque su cúpula organizativa estuviese basada en España, el caso en sí respondía al carácter transfronterizo y global de la cibercriminalidad, en la medida en que la red de delincuentes operaba en multitud de países por medios informáticos, tanto en lo que a la difusión, control y explotación de *malware* se refiere como en lo tocante al blanqueo de los beneficios procedentes de tales actividades. Ciertamente, no yerran quienes consideran el uso criminal de las criptomonedas como un fenómeno esencialmente internacional, que no puede ser reducido al territorio de un único país[159].

---

[155] La prensa se hizo eco de estas incautaciones, siendo de las primeras de *bitcoin*s realizadas en el mundo: v. p. ej. P. Romero, «Así se incauta la Policía de *Bitcoin*s», diario *El Mundo,* artículo de 1 de noviembre de 2013 (disponible online en: http://www.elmundo.es/tecnologia/2013/11/01/5270d45363fd3da7618b4576.html, consultado el 6 de febrero de 2018).

[156] Sentencia AN, Sec. IV, n.º 14/2016, de 3 de marzo de 2016.

[157] Sentencia AN, Sec. IV, n.º 14/2016, de 3 de marzo de 2016, FF. DD., primero.

[158] Sentencia AN, Sec. IV, n.º 14/2016, de 3 de marzo de 2016, FF. DD., segundo.

[159] Brezo y Rubio, *Bitcoin. La tecnología blockchain y su investigación*, cit., pp. 113 ss.

Por lo demás, y a pesar de que la red desarticulada en la «Operación Ransom» gozaba de un alto grado de competencia técnica, lo cierto es que ciertos usos criminales de las criptomonedas son técnicamente asequibles, de manera que éstos no sólo están al alcance de grandes redes internacionales especializadas en ciberdelitos. Un ejemplo de ello a nivel nacional nos lo provee el caso de una red que distribuía fraudulentamente contenidos televisivos de pago, en el contexto del cual se han producido igualmente incautaciones de *bitcoin*s[160]. Si bien el método mediante el cual se cometía la infracción principal se caracterizaba por su alto grado de complejidad técnica, la técnica de blanqueo de los beneficios así obtenidos era relativamente sencilla: adquisición de equipos dedicados a la extracción de *bitcoin*s, creación de «granjas» de servidores a tal efecto y cambio de la producción en *bitcoin*s de dichas granjas por moneda de curso legal, para su reintegración directa en el sistema financiero o la adquisición de vehículos de lujo o de inmuebles.

Del proceso contra la red, que aún está en marcha, constan ya tres autos de la Audiencia Provincial de Pontevedra, que resuelven otros tantos recursos interpuestos por la defensa de algunos de los encausados contra los autos del Juzgado de 1.ª Instancia e Instrucción de Redondela en los que se ordenaban diversas medidas de investigación contra ellos o se rechazaba la cesación de las mismas solicitadas en recursos previos: en dos casos se trataba de peticiones de información a la AEAT y al Interlocutor con el Servicio Ejecutivo de la Comisión Nacional para la Prevención del Blanqueo de un banco nacional (estimándose parcialmente ambos recursos, en el sentido de restringir el período para el cual se solicitaban las informaciones de las cuentas de los imputados)[161], mientras que en el tercero se trataba de la incautación de equipos de extracción de *bitcoin*s (desestimándose el recurso)[162].

De los autos en cuestión se deducen varios detalles reveladores. Por un lado, los encausados habrían estado robando fluido eléctrico a fin de mantener los servidores en funcionamiento. El objeto de estos robos no sería solamente el de ahorrar el coste en electricidad (potencialmente elevado) que conlleva el funcionamiento continuo de equipos de extracción, sino que desde nuestro punto de vista debe entenderse, sobre todo, en términos de encubrimiento del método empleado para el blanqueo.

Se deduce de la información disponible que los equipos en cuestión habrían sido adquiridos con el producto de la actividad de distribución

---

[160] Agencia Efe, «Descubren el mayor productor ilegal de *bitcoin* para blanquear un fraude de TV», artículo de 25 de mayo de 2016 (disponible online en: https://www.efe.com/efe/espana/sociedad/descubren-el-mayor-productor-ilegal-de-bitcoin-para-blanquear-un-fraude-tv/10004-2935598, consultado el 6 de febrero de 2018).

[161] Auto AP Pontevedra, Sec. 5, n.º 208/2017, de 23 de marzo de 2017, y Auto AP Pontevedra, Sec. 5, n.º 515/2017, de 7 de julio de 2017.

[162] Auto AP Pontevedra, Sec. 5, n.º 483/2017, de 30 de agosto de 2017.

fraudulenta de contenidos televisivos de pago, de manera que no podría justificarse la procedencia del dinero empleado para su adquisición. Nos parece más bien así que el robo de fluido eléctrico tendría por objeto el mantener en la sombra la existencia de las granjas de minería (lógicamente, a condición de que tal robo no fuese detectado, como, por el contrario, lo fue), existencia de la que sería reveladora un alto consumo de electricidad.

Dicho de otro modo, se habría planteado una disyuntiva a los presuntos delincuentes: o bien justificar el alto consumo de energía mediante alguna otra actividad lícita, asumiendo su coste normalmente, o bien robar el fluido eléctrico necesario, confiando en no ser detectados. La primera opción habría requerido, a su vez, el montaje de un negocio pantalla y la justificación del dinero empleado para adquirir el material que debería justificar el alto consumo de energía. Esta resultaba factible, aunque habría requerido una cierta capacidad organizativa: podría pensarse en la adquisición de material de coste comparativamente bajo necesario para la actividad aparente del negocio pantalla y que consumiese también grandes cantidades de energía, permitiendo el coste menor del material en cuestión su compra con dinero «limpio», esto es, de procedencia justificable.

Otro detalle interesante es la reintegración directa de los fondos adquiridos tras el cambio de las *bitcoin*s extraídas por los presuntos defraudadores en el sistema financiero o su uso para la adquisición de bienes de lujo o bienes raíces sitos, aparentemente, en territorio nacional (estos últimos, aparentemente, mediante sociedades pantalla[163]). Habría aquí, por lo tanto, una combinación de medios «tradicionales» de blanqueo de capitales (empleo de sociedades pantalla, instrumentalización de la inversión inmobiliaria) y medios más novedosos (actividad de minería no declarada y *exchanging* de *bitcoins*). Sin embargo, en comparación con el sofisticado andamiaje de ofuscación de los movimientos del producto de la actividad criminal en el caso del «virus de la Policía», la reinversión directa en territorio nacional del producto del cambio de las criptomonedas (al menos, según consta de la información de que disponemos hasta ahora) se antoja relativamente simple: contra lo que cabría esperar, el empleo de las criptomonedas como medio de blanqueo de capitales habría sido (también) un flanco vulnerable en la estructura de la organización.

[163] En particular, los autos se refieren a la detección de diversos documentos de cesiones de créditos entre la sociedad que gestionaría un sitio web, una empresa inmobiliaria y una empresa de reformas, las tres vinculadas de un modo u otro a la presunta red criminal (Auto AP Pontevedra, Sec. 5, n.º 515/2017, de 7 de julio de 2017, FF. JJ., tercero; Auto AP Pontevedra, Sec. 5, n.º 483/2017, de 30 de agosto de 2017, FF. JJ., tercero; y Auto AP Pontevedra, Sec. 5, n.º 208/2017, de 7 de julio de 2017, FF. JJ., tercero).

Síntesis

Las incertidumbres que persisten sobre el posible recorrido económico y social de las criptomonedas en los años por venir determinan en parte la actitud cautelosa de supervisores y legislador frente a las mismas. La punta de lanza jurisprudencial sobre la materia concierne, ante todo, la fiscalidad de las actividades relacionadas con las criptomonedas. Por su parte, los primeros proyectos legislativos constituyen una reacción ante las posibilidades de las mismas como medio de blanqueo de capitales, que se concreta en un alza de su uso a tal fin (aunque no sólo) por parte de los criminales, especializados o no. La reforma regulatoria europea en marcha por el momento quiere abordar principalmente una faceta de las criptomonedas, esto es, su potencial uso en el marco de las finanzas criminales. Prescindiendo de los problemas técnico-jurídicos de los que tal reforma pueda adolecer, el carácter descentralizado de las principales criptomonedas hace difícil que ésta pueda bastar por sí sola para atajar el problema.