Utilización de las nuevas tecnologías en la comisión del blanqueo de dinero

Prof. Dr. Diego José Gómez Iniesta
Facultad de Derecho de Albacete
Universidad de Castilla-La Mancha

1. Introducción

Las causas que favorecen la existencia del blanqueo de dinero son múltiples; la primera de ellas es, evidentemente, la propia existencia de delitos que son la fuente del dinero que luego se blanquea, a la que habría de añadirse la conexión del blanqueo con otros delitos, la corrupción, así como la globalización del sistema económico y financiero y, por supuesto, las nuevas tecnologías e Internet[1].

Las tecnologías de la información y comunicación son desarrollos de tipo tecnológico, tanto de los procesos como del diseño, que se centran fundamentalmente en la comunicación y el intercambio de la información. Las nuevas tecnologías ocupan un lugar importantísimo en nuestras vidas y en la forma en que funciona la sociedad; y es que en el ámbito de las telecomunicaciones, además de la informática y el video, esta revolución está produciendo cambios importantes, porque sus efectos superan el ámbito de la información y el conocimiento, y están provocando alteraciones en las estructuras políticas, sociales, económicas, educativas, laborales y jurídicas, debido a que la información se convierte, almacena, administra, manipula y se transmite con gran rapidez, y afecta igualmente a la forma de interactuar de los individuos, la de estos con las máquinas y con las empresas y la administración. Más específicamente, este entorno ha creado un caldo de cultivo para la aparición de nuevos métodos de pago, alternativos a los ofrecidos por los servicios financieros tradicionales, con los que se vienen a cubrir necesidades de tipo mercantil, para ofrecer otros nuevos frente a los clásicos y satisfacer las necesidades de sus clientes y las necesidades de aquellos otros que tienen una mala calificación crediticia o que viven en zonas con escasa oferta bancaria; entre otros, las tarjetas prepago, el pago con teléfonos móviles, los servicios de pago por internet, las monedas virtuales, con los que se satisfacen las necesidades de los consumidores[2].

En efecto, el avance de los medios de pago electrónicos está teniendo una extensión cada vez mayor y desplazando a los pagos con dinero en efectivo. Baste recordar como las propias entidades financieras prestan diversos servicios financieros de forma electrónica, desde la posibilidad de acceder a la información bancaria y consultar el saldo, banca móvil para realizar diversas operaciones (como transferencias, solicitud de créditos, pago de facturas, etc.), pasando por ofrecer a los clientes, como alternativa al dinero en efectivo, monederos móviles, para usar el valor como método de pago en establecimientos. A su vez, ese mismo entorno, junto al tipo de servicios ofrecidos, más ágiles y anónimos, crean enormes oportunidades para la comisión de delitos, como la financiación de sus actividades o la realización de operaciones propias de blanqueo que buscan escapar del control, dificultando a investigación y su persecución[3]. Se exige entonces al legislador

1 DE LA CUESTA, J.L., "Principales lineamientos político criminales de la AIDP en un mundo globalizado", en *I Conferencia mundial de Derecho penal. El Derecho penal del siglo XXI*, Guadalajara (México), Noviembre 2007, ReAIDP, 2008, págs. 1 y ss. ANDREAS, P., "Illicit Globalisation: Myths and Misconceptions", en *Globalisation, Criminal Law and Criminal Justice: Theorertical, Comparative and Transnational Perspectives*, Mitsilegas/Alldridge/Cheliotis (ed.), Hart Publishing, 2015, págs. 55 y ss.

2 Cfr. LESLIE, D.A., "Introduction, Money Laundering and Cyber crime", en *Legal Principles for Combatting Cyberlaundering*, AA.VV., Springer, Suiza, 2014, págs. 1-54.

3 Como dice NUTZ, M.S., el avance en el campo de las TIC ha cambiado todos los aspectos de la sociedad, pero también del delito, con lo que crecen las oportunidades para la comisión de delitos y con ello la tasa de la

un continuo proceso de adaptación y actualización de la normativa, tanto de la penal como de la preventiva, que preserve la confianza en el sistema financiero.

2. Nuevos métodos de pago
    1. 1. Tarjetas prepago, pago con teléfono móvil y compra en línea

La demanda de las tarjetas prepago, que surgieron en los años 90 como alternativa a las tarjetas de crédito y al dinero en efectivo, ha aumentado rápidamente al garantizar el anonimato del cliente y no estar asociadas a una cuenta bancaria, y con un grado de funcionalidad que depende de si se trata de una tarjeta de ciclo cerrado o no. Con relación a las de ciclo cerrado, que son aquellas que solo pueden emplearse para adquirir bienes o servicios en los establecimientos del emisor o dentro de una red limitada de proveedores de servicios o para adquirir una gama limitada de productos (por ejemplo, las tarjetas regalo, las tarjetas de transporte, etc.), son anónimas, pero suelen reducirse a un ámbito concreto y no permiten extraer efectivo ni realizar otras operaciones; por ejemplo, cuando los servicios de telefonía permiten las recargas mediante tarjetas prepago existe la obligación de llevar un registro, en el que constará la identidad del cliente, mediante documentos acreditativos, que adquiera la tarjeta, así como la obligación de información sobre la existencia de dicho registro y los derechos que le asisten. Pues bien, en el caso de estas tarjetas no se advierte un gran riesgo. No ocurre lo mismo cuando se trata de una tarjeta de prepagado de ciclo abierto, que abarcan tanto a personas que disponen de una cuenta bancaria, como a las que no la tienen. Son estas últimas las que más preocupan desde el punto de vista de la lucha contra el blanqueo de dinero, ya que al tener una mayor funcionalidad y alcance, por ejemplo, porque si son anónimas o si no hay límite de valor o si permiten comprar en línea o recargarlas desde un dispositivo electrónico con conexión a internet o extraer dinero de un cajero automático, el riesgo que representa es mayor. Por tanto, no cabe duda de las ventajas que presentan estas tarjetas, como ha sido subrayado constantemente, ya que permiten la inclusión financiera de personas no bancarizadas y con las que muchos gobiernos han puesto en prácticas algunas de sus políticas sociales (inclusión financiera y social), pero al instante, la experiencia demuestra que su utilización para la financiación terrorista, como para el blanqueo de dinero, es relativamente fácil, en algunos casos porque no están involucradas las instituciones financieras, se realizan transferencias, se retira efectivo, se realizan pagos, por lo que las oportunidades de cometerlos aumentan[4].

Por lo que se refiere a los servicios de pago a través del teléfono móvil, su uso para realizar compras por Internet es cada vez mayor. Se estima que en el 31% de las ellas se utilizaron un teléfono inteligente en 2016[5]. Al igual que sucede con las tarjetas prepago, su extensión se debe a que permite a una buena parte de la población que no está bancarizada el acceso a todo tipo de servicios que existe en Internet. Es por ello por lo que este método de pago también ha estado en el punto de mira de las autoridades por los riesgos de la transmisión de valor a través de Internet, tanto para la adquisición de bienes y servicios, como para la realización de transferencias o pago de facturas, cuando la experiencia demuestra que en algunos supuestos puede blanquearse el dinero. Los

---

criminalidad ("Taking advantage of new technologies: For and against crime", *en Computer Law & Security Review*, vol. 24, 2008, págs. 437-446). Sobre las dificultades para la persecución del delito en el entorno de Internet, cooperación y asistencia judicial mutua, vid. JOOSTEN, J., *Combating cyber money laundering: selected jurisdictional issues*, Faculty of Law, University of The Western Cape, octubre, 2010 (disponible en: http://etd.uwc.ac.za/xmlui/bitstream/handle/11394/3041/Joosten_LLM_2010.pdf?sequence=1&isAllowed=y). Vid. también ABEL SOUTO, M., "Money laudering, new technologies, FAFT and Spanish penal reform"; en *Journal of Money Laundering Control*, vol. 16, núm. 3, 2013, págs. 266-268, y bibliografia allí cit.

4 Ampliamente, ABEL SOUTO, M., "Blanqueo, innovaciones tecnológicas, amnistía fiscal de 2012 y Reforma Penal", en *Revista electrónica de Ciencia penal y Criminología*, 14-14 (2012), págs. 1-5.

5 Observatorio Cetelem, "El comercio electrónico en España: tendencias y comportamientos", 2015, disponible en: http://www.elobservatoriocetelem.es/wp-content/uploads/2015/12/observatorio-cetelem-ecommerce-2015.pdf. Vid. igualmente el Informe de Mastercard sobre "Barómetro de tarjetas 2016", disponible en: https://newsroom.mastercard.com/eu/es/press-releases/el-676-de-los-espanoles-ya-tiene-una-tarjeta-de-debito-el-mayor-porcentaje-de-la-serie-historica-del-estudio-de-mastercard/.

proveedores de estos servicios, pueden ser una entidad bancaria, pero este producto también lo han desarrollado los operadores de red móvil, que ofrecen servicios de pago con el teléfono móvil u ofrecen cuentas prepago o pospago. Pues bien, en la medida en que forman parte del sistema financiero formal (también los operadores de red móvil tienen que entrar en contacto con una entidad financiera para ofrecer su servicio de dinero móvil), están sometidos a la normativa antiblanqueo.

2.2. Monedas virtuales

Más recientemente, la atención se ha centrado en las monedas virtuales. En la actualidad hay más de mil monedas virtuales en circulación. No estamos hablando de futuro, sino una realidad que está cambiando la realidad financiera, pero también la comercial, la jurídica y la social.

Si nos centramos en el análisis de la moneda virtual descentralizada y convertible más conocida, el Bitcoin, se comprueba como las transacciones son directas, sin intermediación alguna, sin un emisor central, permitiendo la transferencia de valor de persona a persona; utiliza un sistema de verificación por el que se certifican y registran las operaciones, con lo que se evita el doble gasto[6]. Además, el valor de la misma no depende del precio del oro ni está basado en una moneda de curso legal, sino que se fija en función de la oferta y la demanda, y si se ha generalizado su uso, al ser aceptado como medio de pago y depósito de valor, es por la confianza que provoca entre el público y en la dificultad para falsificarlo, a diferencia de otras transacciones que se realizan en Internet que son más fáciles de descifrar[7].

Su mayor atractivo es su protocolo que está basado en la *blockchain* o cadena de bloques, formada por un código alfanumérico que permite la transferencia de valor de persona a persona, en el que se registra y verifica cualquier acto pasado o presente, cualquier transacción que hay tenido lugar, en una base datos digital, actualizada y pública, con lo que se elimina la posibilidad del doble gasto, si bien no se detallan aspectos concretos de dichos actos, como los relativos a los participantes.

Claro que las monedas virtuales pueden utilizarse para fines ilegítimos[8] y existe una idea difundida por la que se identifica, posiblemente por la influencia de los medios de comunicación, a las monedas virtuales con uso delictivo, principalmente por el que llevan acabo las organizaciones criminales: el Bitcoin y las demás monedas virtuales se está usando activamente como medio para ocultar dinero, blanquearlo, usarlo en actividades ilícitas con malware (como el Ransomeware CryptoLocker con pago en Bitcoins) y hacer pagos a grupos terroristas, entre otros delitos[9]. Bien es

6 CHAUM, D., "Achieving Electronic Privacy", en *Scientific American*, agosto de 1992, págs. 96-101.

7 Extensamente, CAPITÁN LÓPEZ, S., "Los bitcoines y su utilización como dinero descentralizado y anónimo", en *Cuadernos de Formación*, Colaboración 3/15, vol. 19/2915, págs. 33 y ss.

8 El caso paradigmático es *Silk Road*, creado en 2011, se trataba de un mercado que intermediaba en transacciones anónimas aceptando bitcoins para la venta y adquisición de bienes y servicios ilícitos, y que utilizaba el sistema de navegación Tor (*The Onion Router*), que al redirigir la conexión entre diferentes países y garantizar el anonimato en la navegación, junto al anonimato del bitcoin, dificultaba la identidad de los consumidores; o el caso *Liberty reserve*, un mercado centralizado de moneda digital, que garantizaba el anonimato es otro caso que ha avivado las sospechosas sobre la moneda, cuando las autoridades norteamericanas les acusar de blanquear dinero procedente de diversas actividades delictivas. Su atractivo residía en la garantía de transacciones financieras anónimas, aunque exigía identificación, no había comprobación de la identidad, cobrando una pequeña cantidad por cada transacción que se realizaba. Vid. Departamento del Tesoro EE.UU., *National Money Laundering Risk Assessment*, 2015, págs. 57, 58 y 62, en el que se identifican los riesgos de blanqueo de dinero que son prioritarios para EEUU (disponible en: https://idusr9594usfrip1o442l1bj-wpengine.netdna-ssl.com/wp-content/uploads/2015/06/National-Money-Laundering-Risk-Assessment-–-06-12-2015.pdf). Igualmente, GRZYWOTZ, J./KÖHLER, O.M./RUCKERT, C., "Cybercrime mit Bitcoins – Straftaten mit virtuellen Währungen, deren Verfolgung und Prävention", en *Strafverteidiger*, vol. 36, núm. 11 (noviembre, 2016), págs. 753-759.

9 Sobre el aumento de ataques Ransomware y Ddos, que son software malicioso diseñado específicamente para encriptar datos y para cuyo descifrado se exige el pago en Bitcoin o tarjetas de prepago, vid. BundesKriminalAmt, *Cibercrime*, Austria, 2015, (disponible en: http://www.bmi.gv.at/cms/bk/publikationen/files/30102016_cybercrime_2015.pdf).

cierto que cada vez más sabemos de su funcionamiento y se han puesto de relieve los riesgos, debido al alto grado de anonimato, a diferencia de las clásicas transferencias financieras, y es aquí donde reside su atractivo: es un medio para ocultar dinero, blanquearlo, pagar a grupos terroristas y organizaciones criminales, etc., al no requerir identificación y verificación de los participantes ni existir una autoridad central. Sin embargo, incluso en dicho protocolo es muy complicado garantizar el anonimato absoluto, porque de hecho cuando se produce una operación entre dos claves públicas, quedan registradas la hora, la cantidad y otros datos en la cadena en bloque, y la misma está a disposición publica. El problema es que esas claves no están vinculadas a ninguna identidad y las dificultades aumentan cuando se utiliza la red Tor o cualquier *software* que garantice el anonimato para enmascarar las conexiones, con lo cual se pierde la dirección del protocolo de Internet.

Bien es cierto que el uso de programas de cifrado es extraordinariamente útil para los ciudadanos y también para la empresa y los Estados, porque es una manera de proteger sus datos, impidiendo a la delincuencia que accedan a los mismos. Sin embargo, el uso de cifrado por los delincuentes para proteger de igual manera sus datos forma parte de la ciberdelincuencia. De esta manera, se emplea *software* de cifrado, tipo *Tryecrypt* o *Bitlocker*, y ello se ha extendido también a los teléfonos móviles, se usa toda clase de técnicas que buscan el anonimato a través de programas de encriptación, proxis anónimos o anonimizadores web o servicios de correo anónimo, programas maliciosos para controlar remotamente los equipos o programas de encriptación para esconder contenidos, o diversas técnicas de ingeniería que permiten ocultar la identidad o suplantarla, capturando los nombres de usuario y contraseñas, y todo ello se ha extendido también a los teléfonos móviles. Sin embargo, el control aunque complicado no es del todo imposible[10], tomando en cuenta que muchas de las operaciones al generar registros electrónicos suministran información a las autoridades; y es que las ventajas que presenta la tecnología para los delincuentes son las mismas que para las autoridades de control: en muchos supuestos la realización de las operaciones dejan rastros a través del IP, lugar de realización y tipo de operación, esto es, los mismos medios informáticos también sirven a las autoridades para el seguimiento de las operaciones y la identidad y localización del autor (a través de la SIM o en el supuesto de que se conozca el IP del ordenador desde el que opera), pero las dificultades continúan cuando existen programas para garantizar el anonimato del IP, ocultándolo o falseándolo, utilizando proxies, o se ofrecen servicios de mensajería que no requieren identificación o se utilizan zonas Wifi públicas.

A pesar de ello, como quiera que el Bitcoin está en el centro de atención, la ciberdelincuencia está buscando el amparo de otras monedas virtuales que garanticen mucho mejor el anonimato, algo que el Bitcoin no es capaz de garantizar[11].

La expansión de su uso ha tenido como resultado que haya dejado de tener como principal función la criminal. Hay que tener en cuenta que este tecnología no solo sirve para alojar unidades monetarias, sino también puede contener contratos, actos judiciales, etc., dando lugar a plataformas jurídicas. Debe destacarse su papel en la financiación de *start ups* y que muchos establecimientos amplíen su oferta admitiendo el pago mediante este tipo de monedas. Efectivamente, es una realidad que algunos modelos de negocio, tanto en línea como físicos, están aceptando estas monedas virtuales junto a otros medios de pago, desde los tradicionales hasta los más novedosos, como las

10 VASSILAKI, I., *Computer- und Internet Strafrecht*, Berufsbegleitender Masterstudiengang, Informationsrecht, Center für lebenslanges Lernen, Carl von Ossietzky Universität Oldenburg, 2015, págs. 6-46; GOMEZ, E. /ESPINOZA, H., "Cómo responder a un delito informático", en *Revista Ciencia UNEMI*, junio 2014, págs. 43 y ss.; HERNÁNDEZ QUINTERO, H.A., "Informática y delito de lavado de activos", en *Derecho penal y Criminología* 47 (2007), págs. 47 y ss.

11 Por ejemplo, Monero es presentada como una moneda digital privada que utiliza el protocolo *Cryptonote*, con el que no se revela la identidad de ningún participante ni la cantidad de la transacción, y en el que las transacciones están firmadas por varias personas a la vez, además de utilizar el software I2P, con el que las direcciones IP de los usuarios también están ocultas.

tarjetas de crédito o pago móvil. Y es que cuando las empresas aceptan como medio de pago las virtuales, reducen costos en las transacciones al no existir emisores ni intermediarios y surgen proveedores de servicios de pago, tipo Bitpay, que ante la volatilidad de la moneda virtual la convierten inmediatamente en cualquier divisa. Además, esta tecnología está revolucionando el mundo empresarial y de las finanzas, debiéndose destacar la inversión de importantes empresas en proyectos TIC, basados en la tecnología *blockchain*, con el fin de desarrollar soluciones de seguridad de nueva generación y detectar amenazas en las infraestructuras o prevenir la piratería informática[12]. Algo parecido a lo que están haciendo algunos grandes bancos que están promoviendo el uso del dinero virtual investigando en dicha tecnología para permitir transacciones con monedas fiduciarias.

3. Las nuevas tecnologías ante el Derecho penal: el ciberblanqueo

No es de extrañar que la delincuencia se adapte a un entorno que facilita la comisión de ilícitos y que las transformaciones conlleven, entretanto, nuevas formas de delinquir, o mejor, nuevas formas de cometer el delito, que son una adaptación de conductas delictivas más o menos clásicas pero que se aprovechan de las enormes oportunidades que ofrece Internet debido a sus características, aquellas que lo constituyen como un factor criminógeno de primer orden[13]. Como observa Miró Llinares, se trata de un ámbito de especial oportunidad delictiva, en el que el espacio y tiempo se ven modificados, porque aquí los sujetos tienen menos restricciones espaciales y temporales para sus actos y las consecuencias de los mismos, que quedan plasmadas en unas coordenadas espacio/temporales determinadas, ofreciendo menos información que en el espacio físico (sus características intrínsecas en cuanto al espacio y tiempo). A ello habría que sumarle las características extrínsecas: su neutralidad, transnacionalidad, descentralización (universal y abierto), un espacio entendido como universal, global, colectivo, lo que le otorga una gran dimensión. En consecuencia, "el ciberespacio no cambia los caracteres esenciales que hacen que a determinados eventos se les pueda seguir denominando crímenes, pero sí modifica los parámetros espacio/tiempo en los que el crimen tiene lugar, por lo que es lógico que ello exija un replanteamiento, no tanto de las teorías criminológicas que tratan el crimen como evento, pero sí del propio evento y de los elementos del mismo con especial atención al contexto espacial y temporal en el que éste se produce"[14].

Y es que desde el momento en que la actividad delictiva genera dinero, se diseñan técnicas más o menos complejas para realizar de manera eficaz y evitar que se descubra su procedencia ilícita[15]. Los métodos de blanqueo de dinero son variados y en continua evolución; de hecho, junto a las técnicas tradicionales de blanqueo, como la adquisición de un inmueble o un artículo de lujo, como decíamos más arriba, han ido apareciendo otras que recurren a ámbitos económicos más vulnerables basados en las nuevas tecnologías de la información y comunicación[16].

---

12 Vid. la noticia en: http://www.koreaherald.com/view.php?ud=20160714000151.

13 La Secretaría de Estado de Seguridad en su *Estudio sobre la cibercriminalidad en España*, 2016 (disponible en: http://www.interior.gob.es/documents/10180/5791067/Estudio+Cibercriminalidad+2016.pdf/456576b2-9ce8-4f3c-bbcc-ca0dbf3bb3cf) subraya que en el periodo comprendido entre 2013 a 2016, como hecho irrefutable extraído de los resultados registrados por las Fuerzas y Cuerpos de Seguridad, ha habido un aumento de los delitos informáticos. De esta forma, podemos apreciar que, en 2016, se ha conocido un total de 66.586 hechos, lo que supone un 10,7% más con respecto al año anterior. De este montante final, el 68,9% corresponde a fraudes informáticos y el 17,2% a amenazas y coacciones. Vid. DE LA MATA BARRANCO, N.J., "Delitos vinculados al ámbito informático", en *Derecho penal informático*, de la Mata Barranco (coord.), Cuesta Arzamendi (dir.), 2010, págs.. 15-30.

14 MIRÓ LLINARES, F., "La oportunidad criminal en el ciberespacio. Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen", *RECPC* 13-07 (2011), págs. 13- 19.

15 BURMBERGER, C., *Geldwäsche im Internet. Methoden, Gefahren für die internationale Wirtschart und Bekämpfungsmöglichkeiten*, München, GRIN Verlag, 2015, págs. 3 y ss.

16 LEVI, M., "Crime of Globalisation: Some Measurement Issues", *New tipes of crime. Procedings of the International Seminar held in connection with HEUNI´s thirtieth anniversary*, Joutsen (ed.), Helsinki, 2012, págs. 107-115. Como dice, GONZÁLEZ RUS, J.J., "Precisiones conceptuales y político-criminales sobre la intervención penal en

Todas las conductas delictivas que tienen lugar en el entorno de Internet se agrupan bajo una amplia categoría, la del delito informático, cada vez más en desuso y a favor de otras como cibercrimen, ciberdelito o delito cibernético, que tienen el mismo significado al referirse a delitos relacionados con las TIC, que se realizan en la distancia, de comisión instantánea, con un importante elemento de internacionalización y que afecta a una pluralidad de bienes jurídicos[17]. El mejor ejemplo de la evolución de la criminalidad en la sociedad del riesgo, como dice Silva Sánchez, es la criminalidad asociada a los medios informáticos y a Internet, y los rasgos que la definen se corresponden con los destacados por la dogmática funcionalista[18]; a saber, su anonimato y su carácter transnacional, o mejor dicho, su carácter global gracias a Internet, que es el paradigma de la globalización total[19], que permite realizar operaciones con carácter transfronterizo y de consumación instantánea[20]. En el mismo sentido, señala Anarte Borrallo que esta categoría forma parte de la sociedad global del riesgo y frente a ello, se demanda seguridad, para reducir el riesgo, controlarlo y llevar a cabo intervenciones preventivas. El problema es que al mismo tiempo se provoca inseguridad jurídica, ya que el Derecho penal de la sociedad de la información no es partícipe de los principios garantistas que han sido formulados con relación a una forma de delinquir básicamente individual y marginal, si no que participa de los principios que inspiran el Derecho penal en la sociedad del riesgo, distante del modelo clásico de imputación. Se demanda al legislador penal, por ello, la creación de nuevos tipos penales o que se creen subtipos relacionados con otros existentes o la ampliación del tipo objetivo o subjetivo de otros también existentes para conseguir las condiciones de seguridad adecuadas ante los daños materiales e inmateriales que produce este tipo de delincuencia[21].

Junto a lo anterior, estas modificaciones pueden observarse en cuanto a las técnicas de tipificación, recurriendo a las típicas de peligro abstracto y en lo que se refiere a la imputación se hace depender de las posibilidades de la tecnología y de los nuevos instrumentos que puedan ir apareciendo[22]. Lo cierto es que la elaboración del tipo penal de blanqueo de dinero ha tenido un largo recorrido hasta su redacción actual, desde la tipificación penal aplicable exclusivamente al dinero del blanqueo relacionado con el tráfico de drogas, para pasar a ser a partir de 1995 un comportamiento delictivo diferente de la receptación, a través de los artículos 301 y siguientes, y aplicable al dinero procedente de cualquier actividad delictiva, adaptándose a la perfección a los diferentes métodos de comisión. Hasta el día de hoy, la intervención penal se ha intensificado, lo cual es fiel reflejo de la

---

Internet", en *Delito e informática: algunos aspectos*, AA.VV., Cuadernos penal José María Lidón, núm. 4, Universidad de Deusto, Bilbao, 2007, págs. 13-40, especialmente, págs. 29 y ss., el medio a través del que se produce un hecho no tiene que suponer una transformación de las necesidades y posibilidades de tutela, con la aparición de nuevas formas de agresión sin que ello suponga de forma automática un contenido nuevo del bien jurídico.

17 Sobre el concepto de "crimen virtual", para hacer referencia a todo lo que envuelve la tecnología, especialmente a lo relacionado con Internet, LASTOWKA, F.G./HUNTER, D., "Virtual Crimes", en *New York Law School Law Review*, núm. 49, pág. 294. Con relación a la adaptación del crimen organizado al contexto transnacional y las posibilidades que brinda el ciberespacio, vid. CARPINTERO SANTAMARÍA, N./OTERO, M.P. "Cyberspace: A Plataform for Organized Cirme", en *Cyberspace. Risks and Benefits for Society, Security and Development*, AA.VV., Martin y García Segura ed., Springer International Publishing AG, 2017, págs. 121-140.

18 SILVA SÁNCHEZ, J.M., *La expansión del Derecho penal*, Madrid, Civitas, 2001, pág. 28.

19 ABEL SOUTO, M., *Normativa internacional sobre el blanqueo de dinero y su recepción en el ordenamiento penal español*, Universidad de Santiago de Compostela, 2001, págs. 45 y ss. y bibliografía allí cit.

20 DEL CID GÓMEZ, J.M., "El uso de las nuevas tecnologías en el blanqueo de capitales: los nuevos métodos de pago", en *Actas III Jornadas de Estudios de Seguridad*, Requena ed., Instituto Universitario General Gutiérrez Mellado-UNED, Madrid, 2011, págs. 411-421; DE CEVALLOS Y TORRES, J.F., *Blanqueo de capitales y principio de lesividad*, Tesis Doctoral, Facultad de Derecho, Salamanca, 2013, págs. 148 y ss. (disponible en: https://gredos.usal.es/jspui/bitstream/10366/122959/1/DDPG_FernandezdeCevallosyTorres_Blanqueo_CapitalesPrincipio_Lesividad.pdf).

21 ANARTE BORRALLO, E., "Incidencia de las nuevas tecnología en el sistema penal. Aproximación al Derecho en la Sociedad de la Información", en *Derecho y conocimiento*, vol. 1, 2001, págs. 195 y 196.

22 O incluso tipos agravados por la disposición de medios tecnológicos avanzados (vid. VIDALES RODRÍGUEZ, C., "Delincuencia organizada y medios tecnológicos avanzados: el subtipo agravado previsto en relación con organizaciones criminales y grupos criminales", en *Revista penal*, núm. 30, julio 2012, págs. 158 y ss.).

política criminal que se ha apuntado más arriba, por ejemplo, con la previsión de conductas típicas que van más allá de las comunes de adquirir, convertir y transmitir, y extendiéndose a otras, como la posesión y la utilización. La falta de concisión y exactitud es tal que es capaz de comprender cualquier comportamiento, por lo que no es de extrañar que el TS en su archiconocida sentencia 265/2015, abril de 2015, llevara a cabo una interpretación restrictiva por la que en el tipo penal no hay dos grupos de conductas: por un lado, la adquisición, conversión, posesión, utilización y transmisión sabiendo que los bienes proceden de un delito y, de otro, la tipificación indeterminada de cualquier otro acto sobre dichos bienes para ocultar o encubrir o ayudar[23].

Además, como pone de relieve Anarte Borrallo, se recurre a cláusulas atemporales, tales como "u otro artificio semejante" en relación con la estafa informática o en el blanqueo de dinero, cuando el artículo 301 CP dice literalmente "o de cualquier otro modo", con las que se trata de asegurar la perfecta adaptación de la norma a las cambiantes formas de vida, y pretender dar respuesta a los constantes y acelerados cambios sociales y comprender todos los métodos posibles para blanquear, pero al precio de ambigüedad e inexactitud[24].

La idea de seguridad preside la intervención penal, también la administrativa, en la regulación de la cibercriminalidad, y en lo que nos ocupa, el ciberblanqueo. Todo esto aparece con los rasgos propios de la ampliación del Derecho penal, su flexibilización, que afortunadamente, no ve la necesidad de intervenir necesaria y exclusivamente recurriendo al mismo, pues junto a él, aparece una incisiva intervención administrativa de carácter preventiva. Esa idea, además, hace que las garantías penales se limiten, sin que conozca ningún límite político criminal, bajo el argumento de que es necesario luchar contra el blanqueo al poner en juego los fundamentos del sistema financiero y su confianza, así como el correcto funcionamiento del sistema de pagos. Más aún con el reforzamiento de formas de imputación extraordinarias, a través de la responsabilidad penal de los sujetos obligados por blanqueo imprudente, considerando que existen determinadas "profesiones peligrosas" y que en el ejercicio de su profesión deben tener bien presente que sobre ellas pesa constantemente la amenaza penal, y a los que se impone deberes a partir de los cuales deriva la responsabilidad penal, debido a la especial cercanía con el bien jurídico. Ciertamente, las normas penales se acompañan de un arsenal de normas que atribuyen más competencia a las instancias de control o ampliando el círculo de sujetos obligados precisamente invocando los peligros que ocasiona para la sociedad, con lo que se intenta disminuir las dificultades en la persecución del ilícito. De hecho, es la legislación la que fija los deberes de identificación, análisis, control, colaboración con las autoridades frente al tipo de operaciones que realizan, es decir, se trata de deberes específicos a partir de los cuales se deduce su responsabilidad, también penal, en caso de incumplimiento. A la vista de lo anterior, con la intervención penal, así como la preventiva, se limita esos efectos criminógenos, generándose las necesarias condiciones que dificultan la comisión de ilícitos.

Pues bien, el ciberblanqueo es un ejemplo más de dicha evolución, de la adaptación de las formas de comisión delictiva al contexto de la Sociedad de la Información, que recurre a ámbitos vulnerables y, en este momento, Internet sigue siendo muy vulnerable por sus especiales características, con lo que las posibilidades para realizar blanqueo de dinero, financiación del terrorismo y fraude fiscal, aumentan[25].

---

23 Vid. la noticia en http://www.poderjudicial.es/cgpj/es/Poder-Judicial/Noticias-Judiciales/El-Tribunal-Supremo-dictamina-que-existe-blanqueo-si-hay-finalidad-de-encubrir-los-bienes.

24 ANARTE BORRALLO, E., ob. cit. , págs. 197 y 198.

25 MÜNCH, H., "Tatort Internet – Neue Herausforderungen, neue Aufgaben", en *Sicherheit in einer digitalen Welt*, Patrick Ernst Sensburg ed., Nomos, 2017, págs. 9-22. FERRÉ OLIVÉ, J.C. "Tecnologías de información y comunicación, comercio electrónico, precios de transparencia y fraude fiscal", en *Nuevas amenazas a la seguridad nacional. Terrorismo, criminalidad organizada y tecnologías de las información y la comunicación*, González Cussac/ Cuerda Arnau (dir.), Fernández Hernández (coord.), Tirant lo Blanch, Valencia, 2013, especialmente págs.. 157 y ss. págs. 193-203.

Teniendo en cuenta que en la actualidad es suficiente con disponer de una conexión a la red para que se pueda realizar cualquier transacción en Internet, también a nivel internacional, la alta negociabilidad, la utilidad de los fondos y la rapidez con la que se realizan las transacciones con relaciones de negocio no presenciales, con el enorme atractivo del anonimato, se favorece la existencia de testaferros, el uso de identidades falsas o el robo de la identidad real de un cliente[26]. Por ejemplo, en este ámbito, uno de los temas que más preocupan y que causan desconfianza en cuanto a la comisión de ilícitos es el fraude en la banca electrónica, más conocido como *phising*[27], toda vez que en una operación es posible el engaño por parte de uno de los intervinientes en la operación. Con relación a la calificación jurídica del *phising*, por la que se sustrae la identidad del cliente de un banco para acceder a sus cuentas, es unánime su tipificación según lo establecido en el art. 248.2 CP, porque no se engaña al titular, sino que la transferencia es inconsentida a partir de una manipulación informática, con la que se obtienen los datos reales necesarias para ingresar al sistema informático bancario y llevar a cabo la transferencia[28]. Pero el tema que más discusión ha producido es la intervención del tercero, del que pone a disposición de la organización su cuenta bancaria, donde se depositarán las sumas de las transferencias inconsentidas, que tras detraer la correspondiente comisión, hará la transferencia, y en estos casos, las defensas suelen alegar que su patrocinado desconocía el fraude. Un sector doctrinal considera que esta figura se adapta perfectamente en la receptación del 298 CP, sin embargo, no tiene en cuenta que la participación del mulero bancario no es *a posteriori*, una vez que se ha agotado la estafa informática, sino que su colaboración en la estafa es esencial al haber facilitado su cuenta bancaria, aceptado el cobro de una comisión y la posterior transmisión del dinero, entra en el ámbito de la cooperación necesaria, integrándose en el injusto de otro, sabiendo que se organiza de forma delictiva, aun cuando desconozca el papel que juega en el hecho, si bien sabe que lo juega; por tanto, con su participación se consuma la estafa informática. En el caso de que la estafa se hubiera consumado o que no se pueda probar la cooperación en ella, queda abierta la posibilidad de castigar por blanqueo, pero entonces se llegaría a un exceso punitivo, al absurdo de castigar con una pena de hasta 6 años, o bien recurrir al blanqueo imprudente[29], con lo que entonces nos plantearíamos sobre las consecuencias penales de un tipo que es aplicable a todo ciudadano por falta de cuidado socialmetne exigible para evitar la lesión del bien jurídico (STS 1034/2005, 14 de septiembre y SAN 40/2010, 31 de mayo) o solo a los que están sometidos a especiales deberes de cuidado, con grave dejación de los más elementales deberes de diligencia que son exigibles legalmente (STS 924/2005, 17 de junio)[30].

---

26 Sobre el problema del cibercrimen en el sector bancario y su impacto en sus finanzas, vid. RAGHAVAN, A.R./PARTHIBAN, L., "The effect of cybercrime on a Bank´s finances", en *International Journal of Current Research and Academic Review*, vol. 2, febrero 2014, págs. 173-178. En el informe de EUROPOL, *Internet Organised Crime Threat Assessment*, IOCTA 2016, pág. 17 se señala como los métodos se han perfeccionado y ahora también se recurre a aplicaciones maliciosas para teléfonos inteligentes, sobre todo en la plataforma de Android, que recopilan credenciales y otras informaciones privadas de e-banca y aplicaciones de monedero de bitcoin (pág. 17). De la misma manera, las campañas de *crowdfunding* de Internet son cada vez más populares método de recaudación de fondos para el desarrollo de nuevos productos o tecnologías. Los delincuentes también han aprovechado este no solo como un medio de blanqueo de capitales fondos, invirtiéndolos en el proyecto, pero adicionalmente posteriormente defraudando a los inversores que creen que están financiando proyectos legítimos (pág. 44).

27 Entre otros, PELKA, P., *Phising. Welche Strafverfolgungs- und Präventionsmöglichkeiten stehen der Polizei zur Verfügung?*, Bachelorarbeit, Grin, 2016, *passim*. OXMAN, N., "Estafas informáticas a través de Internet: acerca de la imputación penal del "phising" y el "pharming", en *Revista de Derecho de la Pontificia Universidad Católica de Valparaíso*, XLI, Chile, 2013, págs. 211-262.

28 Vid. MORENO VERDEJO, J., "Algunas cuestiones acerca de la estafa informática y uso de tarjetas (Incidencia del Anteproyecto de 2006 de reforma del Código penal)", en *Delito e informática: algunos aspectos*, AA.VV., Cuadernos penal José María Lidón, núm. 4, Universidad de Deusto, Bilbao, 2007, págs. 173 y ss.

29 Por todos, FABIÁN CAPARRÓS, E.A., "Oportunidad político-criminal y viabilidad dogmática del delito imprudente de blanqueo de capitales", en *Estudios sobre la corrupción, una reflexión hispano brasileña*, BERDUGO GÓMEZ DE LA TORRE / LIBERATORE S. BECHARA (coords.), Centro de Estudios Brasileños / Universidad de Salamanca, España, 2013, págs. 353-385.

30 Vid., por todos, GÓMEZ INIESTA, D.J., "Estafa y blanqueo de dinero a través de Internet", en *La ley penal: revista*

4. Nuevas tecnologías y prevención del blanqueo de dinero: una aproximación en el contexto internacional y europeo

4.1. Las directrices de GAFI sobre métodos de pago y monedas virtuales

Las nuevas tecnologías han facilitado el surgimiento de métodos de pago y su expansión ha sido vertiginosa debido a su gran aceptación, por ejemplo, a través de aplicaciones de terceros se pueden realizar muchas operaciones bancarias fuera de ese entorno como otras no bancarias.

Ya en 1996, cuando el GAFI revisó las Recomendaciones para reflejar las crecientes tendencias e ir más allá del dinero procedente de las drogas, mostró igualmente una enorme preocupación en su Informe anual del mismo año por las nuevas tecnologías y el peligro que estas tenían para el blanqueo de dinero, a cuyo tenor "La aparición de nuevas tecnologías ofrece riesgos potenciales de blanqueo de dinero. Estas nuevas tecnologías pueden posibilitar la conducción de transacciones a gran escala de forma instantánea, remota y anónima, y pueden permitir que tales transacciones se efectúen sin implicar a las instituciones financieras tradicionales. Aunque no existe actualmente evidencia que indique esas nuevas tecnologías estén siendo utilizadas abusivamente de este modo, el GAFI ha decidido afrontar activamente el problema instando a los países a tomar nota de la amenaza potencial plateada por las nuevas tecnologías y a adoptar las soluciones apropiadas para minimizar dicha amenaza"[31].

Hay que esperar a 2006 para que el GAFI presentara un nuevo Informe sobre los peligros latentes que estas nuevas tecnologías suponían, al facilitar la realización de operaciones sin tener que identificarse[32]. Incidiendo y como actualización del anterior, en 2010 se distribuyó un Informe, sobre los nuevos métodos de pago, comparando y constatando con más evidencias, a través de casos y tipologías, los riesgos que ya se apuntaron. De esta manera se subrayó que, junto a supuestos de blanqueo en los que se compran con tarjetas prepago en el mercado ilegal, debería prestarse más atención a los servicios de pago por Internet y su utilización para el ciberblanqueo y la financiación del terrorismo: su propagación se ha debido fundamentalmente a que en muchos casos no están involucradas las instituciones financieras, porque permiten realizar todo tipo de operaciones bancarias, fuera de dicho entorno, como transferencias o pagos, o porque permiten, incluso sin necesidad de identificarse y sin disponer de una cuenta bancaria o tarjeta de crédito, extraer efectivo de cajeros automáticos[33].

Posteriormente, en 2013 se dieron las Directrices para un Enfoque basado en Riesgo a las Tarjetas Prepagados, Pagos móviles y Servicios de Pagos en Internet (Informe de NPPS de junio de 2013) y otro más en junio de 2014, sobre Monedas Virtuales Definiciones Clave y Riesgos Potenciales de blanqueo y financiación del terrorismo[34], en el que se constata como su surgimiento ha atraído inversión en infraestructura de pagos basado en los protocolos de *software* y con los que se intenta proporcionar un nuevo método para la transmisión de valor a través de Internet.

En 2015, GAFI presentó sus Directrices para un enfoque basado en el riesgo de monedas virtuales, de junio de 2015[35], que es continuación del Informe sobre monedas virtuales, definiciones clave y riesgos potenciales de junio de 2014 que, , se basa en las directrices para un enfoque basado en el

de derecho penal, procesal y penitenciario, núm. 105, 2013, págs. 4 y ss.

31 FATF, *Annual Report 1995-1996* (28 junio 1996).

32 FAFT, *Report on new payment methods*, 2006.

33 FAFT, *Money laundering and terrorism financing: Vulnerabilities of commercial websites and internet payment systems* (2010) y *Money laundering using new payment methods* (2010).

34 Informe GAFI, *Monedas virtuales. Definiciones clave y riesgos potenciales de LA/FT*, junio 2014, disponible en: http://www.gafilat.org/UserFiles/Biblioteca/Doc%20Interes/tipologias%20gafi/MonedasVirtuales(ESP).pdf.

35 Disponible en: http://www.fatf-gafi.org/media/fatf/documents/Directrices-para-enfoque-basada-en-riesgo-Monedas-virtuales.pdf.

riesgo de las tarjetas prepagados, pagos móviles y servicios de pago en Internet. Así, cuando la Recomendación 1 requiere que los países identifiquen, comprendan y evalúen los riesgos, lo que está diciendo es que se creen las condiciones que los mitiguen y, como resultado, si hay riesgos asociados a las monedas virtuales y el uso de nuevas tecnologías, entonces deriva una obligación de intervenir legalmente. Junto a lo dicho antes, lo más relevante de estas directrices es que GAFI trata de encontrar los "puntos de intersección" que ofrecen las fuentes del sistema financiero, haciendo especial referencia a los cambiadores de moneda virtual convertible. De ahí que sus Recomendaciones 14, 15 y 16 deberían aplicarse a dichos sujetos económicos, así como a cualquier otra institución cuyas actividades con moneda virtual convertible se cruzan con el sistema financiero regulado. Debe recordarse que la Recomendación 14 establece que los países deben tomar medidas para asegurar que tanto personas físicas como jurídicas, que prestan servicios de transferencia de dinero o valores, tengan licencia o estén registradas y que estén sujetos a sistemas de monitorización para asegurar el cumplimiento de las recomendaciones de GAFI. Además, deben tomar medidas para identificar las personas físicas y jurídicas que no cuenten con las correspondientes licencias o autorizaciones, y la obligación de aquellas de mantener una lista actualizada de sus agentes. Por tanto, los cambiadores de moneda virtual convertible cuando transfieren valor digitalmente a través de Internet, en los países de origen deberían exigirles requisitos internos para otorgar licencia o registro. Más concretamente, la recomendación 15ª se refiere a la obligación de identificación y evaluación de riesgos de nuevos productos y prácticas comerciales, incluyendo los mecanismos de envío, así como el uso de nuevas tecnologías en desarrollo de productos existentes como nuevos. Por tanto, también es de aplicación a los cambiadores esta Recomendación al referirse a las nuevas tecnologías, nuevos productos y prácticas de negocio, así como el uso de nuevas tecnologías en desarrollo de nuevos productos o ya existentes. Por último, la recomendación 16ª, por la que se obliga a las instituciones financieras a que incluyan información sobre el ordenante y el beneficiario de una transferencia electrónica. Además, deben monitorizarse todas ellas con el fin de detectar aquellas que carezcan de la información requerida. En consecuencia, cuando se refiere a las transferencias electrónicas, por extensión sería aplicable cuando los cambiadores realizan transferencias, por lo que deberían incluir la información exigida y monitorizar las transferencias para la detección de aquellas que no incluyan la requerida[36].

En definitiva, conforme a las directrices de GAFI, se trata de someter las actividades de los cambiadores de moneda virtual, así como otros posibles negocios, que tengan por negocio realizar transferencias de dinero o valor, aceptar depósitos y otros fondos, emisión y gestión de medios de pago y el comercio en moneda extranjera o valores negociable, a la normativa antiblanqueo[37]. Es por ello por lo que busca los puntos de intersección que proporcionan fuentes al sistema financiero regulado, especialmente cuando un proveedor realiza una actividad que cae bajo la definición de institución financiera, y aquí cabe incluir a los cambiadores de moneda virtual convertible en el contexto de los nuevos métodos de pago y, de esta manera, poder identificar las recomendaciones aplicables a la prevención del blanqueo y financiación terrorista. Todo lo último se inscribe en la línea de fortalecimiento del control de este tipo de delincuencia, mediante la incorporación de

36 Igualmente la Recomendación 26 requiere que los países aseguren que los cambiadores de moneda virtual convertible que actúan como nodos cuando las actividades de moneda virtual cruzan con el sistema financiero regulado de moneda ffiduciaria están sujetas a una reglamentación y supervisión adecuada, con lo que los países, en la medida de lo posible, deberían considerar la modificación de marcos legales heredados. Por último, la Recomendación 32 insta a los países a que garanticen que sus autoridades obstaculicen o restrinjan el movimiento de efectivo potencialmente relacionado con el blanqueo de dinero (FATF, 2012, págs. 25 y 99-102) y el artículo 14.2 de la Convención de las Naciones Unidas contra la corrupción "Los Estados Partes considerarán la posibilidad de aplicar medidas viables para detectar y controlar la circulación de efectivo e instrumentos negociables apropiados a través de sus fronteras", pero "sin obstaculizar en modo alguno el movimiento del capital legítimo" (habitualmente se ha dicho que el dinero en efectivo es el medio común de intercambio en las transacciones criminales, vid. JURADO, N./GARCÍA, R., "El blanqueo de capitales", en *El enriquecimiento ilícito*, Avilés Gómez (coord.), ed. Club Universitario, Alicante, 2011, págs. 159-192.

37 ABEL SOUTO, M., "Blanqueo…", cit., págs. 5-9.

políticas con las que se tiene la intención de mitigar el riesgo en actividades y profesiones no financieras, como ya ha hecho en otras ocasiones, por ejemplo, cuando incorporó los juegos de azar, estableciendo dentro de la gran categoría de "actividades y profesiones no financieras designadas" a los casinos, además de los casinos por internet, por lo que este sector debía cumplir con los procedimientos de debida diligencia del cliente y conservación de los registros establecidos[38].

4.2. La propuesta de Directiva del Parlamento europeo y del Consejo, relativa a monedas virtuales

Una vez que ha finalizado el plazo para que los Estados miembros notifiquen la transposición de la cuarta Directiva en materia de blanqueo, se ha abierto el debate sobre la necesidad de introducir medidas adicionales ante la rapidez con la que evolucionan los riesgos, los avances tecnológicos y las comunicaciones; más concretamente, los atentados terroristas de París y Bruselas precipitaron la agenda de la Comisión europea, para presentar en julio de 2016 la propuesta de Directiva del Parlamento europeo y del Consejo, a la luz del Informe de 2015 del Banco Central Europeo, relativo a monedas virtuales, por la que se modifica la Directiva (UE) 2015/849 relativa a la prevención del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, y por la que se modifica la Directiva 2009/101/CE, así como el Reglamento (UE) 2015/847, relativo a la información que acompaña a las transferencias de fondos y que entraron en vigor el 26 de junio 2017. Su objetivo es claro: con el fin de mejorar la detección de las transacciones sospechosas se pondrá toda la atención en los pagos en efectivo, las tarjetas prepago y las plataformas de intercambio de monedas virtuales y proveedores de monederos electrónicos, porque en la actualidad no pesa sobre ellos ningún tipo de obligación de detectar las operaciones sospechosas.

Así es, no había entrado aún en vigor la Directiva (UE) 2015/849 contra el blanqueo cuando se aspira a actualizar las normas, en el sentido de reforzar las obligaciones de proceder a una evaluación de riesgos, los requisitos de transparencia sobre la titularidad real, a través de un registro central, y políticas coherentes con países que disponen de una legislación deficiente en materia de blanqueo mediante el control de los flujos procedentes de países de alto riesgo. Resumidamente, lo que se propone entonces es ir más allá de la cuarta Directiva para impedir que el terrorismo, y por extensión al blanqueo de dinero, disponga de medios financieros a través del dinero en efectivo, el tráfico de bienes culturales, las monedas virtuales y las tarjetas prepago anónimas, contando con que las normas aplicables a las transacciones sospechosas en las que están implicados países de alto riesgo, como las realizas con monedas virtuales, así como la utilización de instrumentos prepago anónimos, son consideradas insuficientes o inexistentes.

Más específicamente, con relación al importe de pagos en efectivo, se prevé reducir el comercio de bienes de 15000 euros a 10000 euros, lo cual ya fue implantado en España al reducir los pagos en efectivo a 2500 euros, cuando una de las partes actúe en calidad de empresario o profesional[39]. La propuesta también se fija en los proveedores de juego a los que se les aplicará medidas de diligencia

38 Sobre la aplicación de las Recomendaciones a instituciones no financieras, vid. ABEL SOUTO, M, "Blanqueo…", cit., págs. 12-16. Id., "Money laundering…", cit., pág. 269 y ss.

39 Artículo 7 de la Ley 7/2012, de modificación de la normativa tributaria y presupuestaria y adecuación de la normativa financiera en la prevención y lucha contra el fraude. Artículo 7. 5. Esta limitación no resultará aplicable a los pagos e ingresos realizados en entidades de crédito ni, cuando estén sujetos a la supervisión del Banco de España y a la normativa de blanqueo de capitales, a las operaciones de cambio de moneda en efectivo realizadas por los establecimientos de cambio de moneda a los que se refiere el Real Decreto 2660/1998, de 14 de diciembre, sobre el cambio de moneda extranjera en establecimientos abiertos al público distintos de las entidades de crédito y a las operaciones a que se refiere éste artículo realizadas a través de las entidades de pago reguladas en la Ley 16/2009, de 13 de noviembre, de servicios de pago (redactado por el apartado uno de la disposición final quinta de la Ley 34/2015, de 21 de septiembre, de modificación parcial de la Ley 58/2003, de 17 de diciembre, General Tributaria (B.O.E. 22 septiembre).

debida en transacciones por valor económico igual o superior a 2000 euros, si bien la Ley 10/2010 solo prevé la identificación del cliente cuando compre o venda por valor igual o superior a 2000 euros.

Por otra parte, y con relación a las tarjetas de prepago anónimas, recargables o no, todos los organismos internacionales, también en el ámbito europeo, asumen el papel que cumplen en cuanto a que se trata de un instrumento fundamental a través del cual los Estados llevan a cabo determinados fines sociales, mostrando una gran sensibilidad por un instrumento que tiene un gran valor social, pues, como decíamos más arriba, permiten a las personas económicamente más vulnerables y a los excluidos del sistema financiero disponer de un medio para adquirir bienes y servicios en Internet o fuera de él. Además, tampoco debe obviarse el uso que le dan personas bancarizadas para limitar el riesgo de fraude en Internet[40]. El problema con el que se encuentra la UE es cómo proteger la privacidad y los enormes beneficios que dichos instrumentos tienen cuando se utilizan legítimamente, y, de otro lado, cuáles son las medidas más adecuadas que pueden adoptarse en la lucha contra operaciones de blanqueo de dinero y financiación del terrorismo, que se aprovechan y benefician de ese anonimato, sin afectar a su uso legítimo. Pues bien, la respuesta más adecuada para la propuesta europea de entre las varias opciones barajadas es la de una combinación de medios con los que se ambiciona impedir las operaciones anónimas empleando tarjetas prepago con fines delictivos. Para ello, se propone legalmente, tomando en consideración las prácticas habituales de operaciones que no caen bajo sospecha efectuada con métodos de pago anónimos y, por tanto, sin menoscabar los intereses particulares, la supresión del anonimato del uso en línea de las tarjetas prepago recargables y no recargables, esto es, la exención de la diligencia debida, obligando a la identificación y verificación de la identidad del titular de la tarjeta, y que en el caso de operaciones *in situ* se reduzca el umbral actual de 250 euros para las tarjetas prepago anónimas a 150 euros[41]. En resumen, se considera que es una medida proporcionada por debajo de la cual no existe riesgo que haga necesario el ejercicio de la diligencia debida con respecto al cliente, con lo cual no se perjudican los intereses legítimos de los usuarios, y someterá a normas más rigurosas el uso de estas tarjetas para pagar a través de internet de forma que no sea posible su uso anónimo; todo ello, teniendo en consideración lo dispuesto en el artículo 4 de la Directiva, por el que cualquier Estado puede permitir a las entidades obligadas no aplicar determinadas medidas de diligencia debida con respecto al cliente cuando se trate de dinero electrónico, cuando se den ciertas condiciones (por debajo de este umbral se autoriza a los sujetos obligados a que no se apliquen algunas de las medidas de diligencia debida con respecto al cliente). También, y relacionado con lo precedente, teniendo en cuenta que la mayor parte de las tarjetas de prepago que se emiten en la UE se circunscriben al territorio europeo, no siempre sucede lo mismo cuando se trata de tarjetas prepago emitidas fuera de la UE, en cuyo caso, se restringirá su uso a aquellas que cumplen con los requisitos de la directiva. Esta es la propuesta europea, que al limitar el anonimato, incentivará a que solo puedan ser utilizadas con fines legítimos y dificulte su atractivo para fines terroristas y de blanqueo.

La propuesta no se olvida de las monedas virtuales. Lo primero que hace la propuesta es dar una definición de las mismas, siguiendo lo dispuesto en el Dictamen del Banco Central Europeo[42], del siguiente tenor: "representación digital de valor no emitida por un banco central ni por autoridad pública ni necesariamente asociada a una moneda fiduciaria, pero aceptada por personas físicas y

40 Los riesgos son apuntados en el Plan de Acción de la Comisión para intensificar la lucha contra la financiación del terrorismo COM/2016/050 final (disponible en: http://eur-lex.europa.eu/resource.html?uri=cellar:e6e0de37-ca7c-11e5-a4b5-01aa75ed71a1.0016.02/DOC_1&format=PDF).

41 En nuestra legislación, el RD 304/2014, prevé en el artículo 16, relativo a los productos u operaciones susceptibles de aplicación de medidas simplificadas de diligencia debida, en su apartado e), que se aplique al dinero electrónico "cuando no pueda recargarse y el importe almacenado no exceda de 250 euros.

42 Disponible en: https://www.ecb.europa.eu/ecb/legal/pdf/celex_52014ab0050_es_txt.pdf. Sobre el concepto de moneda virtual, vid. NAVAS NAVARRO, S., "Un mercado financiero floreciente: el del dinero virtual no regulado", en *Revista CESCO de Derecho de Consumo*, núm. 13/2015, págs. 79 y ss., especialmente, 86 y ss.

jurídicas como medio de pago y que puede transferirse, almacenarse o negociarse por medios electrónicos" (punto 18, del artículo 3 de la Directiva). De las opciones que se barajan para detectar las transacciones sospechosas con monedas virtuales dentro de las redes descentralizadas de moneda virtual convertibles que no son actividades de intercambio, sino transferencias de persona a persona, se decide por incluir en el ámbito de la Directiva a las plataformas de cambio de monedas virtuales y a los proveedores de monederos electrónicos, ya que desde el momento en que los clientes pueden hacer o recibir pagos, dichas entidades deberían pasar a ser entidades obligadas sometidas a las normas de diligencia debida, sobre todo cuando se trate de personas físicas y jurídicas ubicadas en países de alto riesgo. En este sentido, ya en la Comunicación de la Comisión al Parlamento europeo y al Consejo sobre un Plan de Acción de la Comisión para reforzar la lucha contra la financiación del terrorismo[43] seguía la misma dirección al hacer hincapié en su nota a pie número nueve, que las Plataformas de cambio de monedas virtuales "pueden considerarse agencias de cambio «electrónicas» que intercambian monedas virtuales por monedas fiduciarias. Los proveedores de monederos electrónicos de monedas virtuales mantienen cuentas en moneda virtual en nombre de sus clientes. En el mundo del dinero virtual, son el equivalente de un banco que ofrece una cuenta corriente en la que puede depositarse dinero fiduciario. Almacenan monedas virtuales y permiten su transferencia a otros monederos o cuentas de monedas virtuales". Es por ello por lo que el riesgo de que las transferencias de monedas virtuales puedan ser utilizadas por las organizaciones terroristas para encubrir transferencias, ya que las transacciones con monedas virtuales se registran, pero no existe ningún mecanismo de información equivalente al que existe en el sistema bancario convencional para detectar actividades sospechosas[44]. Por su parte, el Informe de la Comisión europea de 2016, indicaba que las monedas virtuales no están reguladas actualmente a escala de la UE. Como primer paso, sugería someter las operaciones anónimas de cambio de divisas al control de las autoridades competentes mediante la ampliación del ámbito de aplicación de la Directiva contra el blanqueo de capitales para incluir a las plataformas de cambio de monedas virtuales y someterlas a supervisión con arreglo a la legislación contra el blanqueo de capitales y la financiación del terrorismo a nivel nacional. Además, consideró que debe estudiarse más a fondo la aplicación de las normas sobre licencias y supervisión de la Directiva sobre servicios de pago a las plataformas de cambio de monedas virtuales favorecerían un mejor control y comprensión del mercado, así como la posibilidad de incluir a los «proveedores de monederos electrónicos» de monedas virtuales. Pues bien, a la luz de este Informe y siguiendo la senda marcada por el GAFI, se propone someter a licencia y registro e incluir en la categoría de sujetos obligados a las plataformas de cambio de moneda virtual y a los proveedores de monederos o *wallets* de monedas virtuales, que ofrecen servicios de custodia de credenciales y claves[45]. En consecuencia, para combatir los riesgos inherentes al uso de estas monedas virtuales, y a sabiendas de que en la actualidad, conforme a los conocimientos técnicos disponibles, es prácticamente imposible eliminar el anonimato, que seguirá manteniéndose en gran parte del entorno de las monedas virtuales, con el fin de combatir los riesgos relacionados con él, dice la propuesta, "las Unidades de Información Financiera (UIF) nacionales deberían poder asociar las direcciones de monedas virtuales a la identidad del propietario de esas monedas. Además, debería analizarse más a fondo la posibilidad de que los usuarios efectúen, con carácter voluntario, una autodeclaración a las autoridades designadas" con lo cual se ampliará desde el punto de vista de los sujetos obligados el artículo 2 de la Directiva vigente.

A partir de la propuesta de la Directiva, merece destacarse el Dictamen de la autoridad bancaria europea en el que aplaude la inclusión de los proveedores en su ámbito de aplicación. Con anterioridad, en julio de 2014, la autoridad Bancaria Europea difundió entre los Estados de la UE un

43 *Plan de Acción del Consejo para intensificar la lucha contra la financiación del terrorismo* (COM (2016) 50 final, de 2 de febrero de 2016 (disponible en: http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1455113825366&uri=CELEX:52016DC0050).

44 Dictamen del Banco Central Europeo sobre las monedas virtuales, 4 de julio de 2014, disponible en: https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf.

45 Informe de la Comisión de asuntos económicos y monetarios, de 3 de mayo de 2016. Ponente: Jakob von Welzsäcker.

informe sobre las monedas virtuales[46], donde ya advertía del riesgo en operaciones de compra, tenencia o venta, considera entidades obligadas a aquellas que realizan servicios de cambio de moneda de curso legal a moneda virtual[47]. Ahora, vuelve a enunciar que "en este contexto, el BCE entiende además que las monedas digitales no tienen que cambiarse necesariamente por monedas legalmente establecidas, sino que pueden también utilizarse para adquirir bienes y servicios sin necesidad de cambiarse por monedas legalmente establecidas o recurrir a un proveedor de servicios de custodia de monederos electrónicos. Esas operaciones no estarían comprendidas en ninguna de las medidas de control establecidas en la directiva propuesta y podrían ser un medio de financiación de actividades ilícitas". A lo anterior añade su inquietud por el hecho de que desde la UE pueda impulsarse este tipo de monedas digitales con carácter privado, puesto que estos medios de pago alternativos ni son monedas de curso legal emitidos por bancos centrales y otros poderes públicos. Por ello, no está de acuerdo en admitir el concepto de moneda virtual, en el sentido de que debe aclararse expresamente que no lo son y, en consecuencia, no definirlas solo como medio de pago, sino como medio de cambio (algunas de ellas más recientes aparecen con una tecnología más compleja y se aplican más allá de los pagos, por ejemplo, aplicaciones de casino en línea)[48]. Por razones evidentes, el Banco central europeo mantiene una postura conservadora de su política monetaria en el dictamen, rechazando que la moneda virtual pertenezca al ámbito del dinero o de las divisas, al no cumplir con las funciones del dinero: medio de pago, reserva de valor y unidad de cuenta, lo que dificulta su equiparación debido a su limitada aceptación como medio de pago entre el público y su alta volatilidad. En realidad, se trata de una revolución tecnológica que está cuestionando su existencia, y parece mirar a otro lado cuando algunos entidades bancarias están empezando a utilizar la tecnología *blockchain* para crear monedas "oficiales" o cuando la propia Comisión europea está instando al sin embargo, los acontecimientos se precipitan, por ejemplo cuando algunos bancos empiezan a usar la tecnología *blockchain* para crear monedas "oficiales", y que incluso la Comisión europea está instando al Banco central para que experimente con un euro virtual, una especie de divisa comunitaria en línea, que unificaría la supervisión financiera, centrada en la transparencia de los riesgos y la protección de los consumidores, simplificando y reduciendo las cargas administrativas.

Por su parte, el Proyecto de Informe de la Comisión de Asuntos Económicos y Monetarios, de 23 de febrero de 2016, sobre monedas virtuales[49], las valora positivamente, al estar basadas en las tecnologías de registros distribuidos contribuyen al desarrollo económico porque reduce los costes de las transacciones de pagos y transferencias de fondos y el coste de acceso a la financiación, aun sin una cuenta bancaria, aumenta la celeridad de los pagos, alto nivel de privacidad aunque no total por lo que es posible el rastreo de las operaciones, al permitir unificar los diversos sistemas de pagos tanto los tradicionales como los más innovadores, observa que debe regularse con extrema

46 Ibidem.

47 Sobre el dinero como medio generalmente aceptado y la futura protección de las monedas virtuales, vid. GLESS S./KUGLER, P./ STAGNO D., "Was is Geld? Warum schützt man es? Zum strafrechtlichen Schutz von virtuellen Währungen am Beispiel von Bitcoins", en *Recht* 2 (2015), págs. 1 y ss. HAENE, C., "Ist Bitcoin eine disruptive Innovation für unser Geldsystem?", München, GRIN Verlag, 2015 (Disponible en: http://www.grin.com/de/e-book/317983/ist-bitcoin-eine-disruptive-innovation-fuer-unser-geldsystem);
HUNGERLAND, F. et al., Die Zukunft des Geldes – das Geld der Zukunft, en *Strategie* 2030 – Vermögen und Leben in der nächsten Generation, núm. 24, pags. 47 y ss. (disponbile en: https://www.econstor.eu/bitstream/10419/162390/1/890366063.pdf).

48 Banco Central Europeo, Dictamen 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 (DOCE 9 diciembre 2016) (disponible en: https://www.ecb.europa.eu/ecb/legal/pdf/celex_52016ab0049_es_txt.pdf).

49 Disponible en: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2F%2FEP%2F%2FNONSGML%2BCOMPARL%2BPE-575.277%2B01%2BDOC%2BPDF%2BV0%2F%2FES. Sobre el juego en internet en EE.UU y Reino Unido, vid. HUGEL, P./KELLY, J., "Internet grambling, credit cards and money laundering", en *Journal of Money Laundering Control*, vol. 6, 1, 1997, págs.. 57-65.

precaución, ya que el riesgo de blanqueo y financiación del terrorismo y fraude fiscal pueden aprovecharse de la pseudonimia y la trazabilidad es menor, así como la falta de estructuras de gobernanza flexibles y fiables, y las dificultades de los reguladores para garantizar un funcionamiento correcto cuando aparecen nuevas monedas, cuando pasan a ser sistémicas, como cuando crecen. Esta línea es también la seguida por Europol en su informe de 2016 cuando sugiere sus aspectos positivos, en el sentido de que la tecnología *blockchain* está atrayendo considerablemente el interés de la industria y de la academia y apunta sus aspectos positivos, ya que "tiene aplicaciones potenciales para muchos actividades transaccionales tales como votación, gestión de identidad, activos digitales y acciones, contratos inteligentes, almacenamiento de archivos y registro manteniendo, para nombrar sólo unos pocos". De la misma forma manifiesta que esa misma tecnología está siendo una de las preferidas del cibercrimen, porque van apareciendo casos en los que la cadena de bloques se está usando para fines criminales, por ejemplo, para almacenar imágenes de abuso infantil[50]. En esta misma dirección, el Parlamento europeo en su Informe sobre monedas virtuales destaca destacar las enormes posibilidades de las monedas virtuales tanto en el desarrollo económico como financiero, debido a la reducción de costes de las operaciones y funcionamiento de pagos, principalmente en el caso de las transferencias transfronterizas, su contribución a la inclusión financiera, la rapidez de pago, el desarrollo de sistemas seguros de micropagos en línea y el anonimato. Lentamente, los prejuicios iniciales hacia las monedas virtuales están despareciendo y están ganando las finalidades legítimas. Como dice Turpin, a pesar de que el Bitcoin se sigue utilizando para fines ilegítimos, no pueden menospreciarse las importantes ventajas económicas que tiene sobre las monedas de curso legal y otros métodos de transacción en línea, por lo que es necesario que los Estados regulen su utilización sin frenar su crecimiento[51].

A la vista de lo anterior, en este momento se tiene un conocimiento más profundo sobre el funcionamiento de las monedas virtuales, fundamentalmente, con relación a los proveedores de servicio de cambio de monedas virtuales por monedas de uso legal, y qué duda cabe que, a diferencia de las transacciones con monedas fiduciarias que gozan de un alto grado de control que disminuye su anonimato, no ocurre lo mismo cuando se trata de operaciones con monedas virtuales.

En fin, los riesgos de que están sean utilizadas para la comisión de ilícitos, especialmente de hechos terroristas como de blanqueo, cuando se intenta ocultar la identidad de los titulares, es muy alto. Hemos de recordar que los riesgos están relacionados con la irreversibilidad de las operaciones, las dificultades para luchar contra las fraudulentas, su naturaleza anónima y la complejidad tecnológica, junto a la ausencia de una regulación, favorecen su extensión. Como quiera que las nuevas tecnologías ofrecen la posibilidad de seguir el rastro de las transacciones, se impone a los proveedores de servicio una serie de obligaciones específicas, como la monitorear las operaciones, la conservación de la información, etc., asimismo, se refuerzan las posibilidades de que las unidades de vigilancia financiera, encargadas del control e investigación, puedan recurrir a las intervenciones tecnológicas, legitimándose un control de las transacciones casi constante que puede incidir tanto en sujetos no sospechosos como en operaciones no anómalas. Esta tarea dista de ser sencilla, como sucede con las monedas virtuales, porque aunque se intenta mejorar la detección de operaciones sospechosas incluyendo a las plataformas de cambio y a los proveedores de monederos electrónicos como sujetos obligados, el anonimato asociado a las transacciones con monedas virtuales seguirá produciéndose al existir otras muchas que se realizan al margen de esos sujetos (por ejemplo, la creación de desarrolladores o mezcladores dirigidos a usuarios con fínes ilícitos, mediante la creación de productos diseñados para evitar el control de las autoridades aplicadoras de la ley).

De nuevo, en el ámbito europeo se apela a los sujetos que por su especial cercanía con el bien

50 EUROPOL, *Internet Organised Crime Threat Assessment*, IOCTA 2016, págs. 8 y ss., 33 y 44.

51 TURPIN, J.B., "Bitcoin: The Economic Case for a Global, Virtual Currency Operating in an Unexplored Legal Framework", en *Indiana Journal of Glogal Legal Studies*, vol. 21, 1, 2014, págs. 335-368.

jurídico protegido, como ya lo están las instituciones financieras, están en condiciones de atender adecuadamente a aquellos riesgos, con una normativa que les incluye en la categoría de sujetos obligados. Y es que, precisamente gracias a los avances tecnológicos, como dice la exposición de la propuesta de Directiva, "la distribución electrónica de efecto digital presenta eficiencias potenciales y, a diferencia del efectivo físico, lleva consigo un registro de transacciones que no existe en el caso del efectivo físico (…) y reconoce el hecho de que las monedas virtuales han apuntado a métodos innovadores para que los gobiernos reduzcan el fraude, la corrupción, los errores y los costes de procesos que generan y consumen un alto volumen de papel". Además, es consciente que las medidas planteadas son necesarias, aunque no suficientes, porque dejan al margen un importante número de operaciones que se realizan al margen de estos sujetos. Conforme a lo anterior, en el caso de que la propuesta fuera aprobada y en el momento de su entrada en vigor, como expone Ramos Suárez, las plataformas de cambio europeas estarán obligadas a fijar procedimientos o políticas contra el blanqueo y la financiación terrorista, más concretamente: medidas de control interno, relativas al estudio y análisis del riesgo, con los correspondientes manuales de prevención sobre la política de admisión de clientes, la relación detallada de hechos u operaciones que, por su naturaleza, puedan estar relacionados con el blanqueo y la financiación del terrorismo, así como, un procedimiento interno de detección de hechos u operaciones sujetas a especial examen, órganos de control interno, formación de personal y examen externo de especialistas; identificación formal y del titular real, obligaciones de información y comunicación ante el SEPBLAC con relación a operaciones susceptibles de estar relacionadas con el blanqueo de dinero o la financiación del terrorismo. Junto a ello, continúa diciendo muy acertadamente, habrían de añadirse otras basadas en el control tecnológico y las limitaciones del sector de cambio de moneda virtual por otra de uso legal, tales como: registro y almacenamiento de direcciones IP/fecha/hora de conexión, códigos de doble autenticación a través del teléfono móvil, limitación de aquellas conexiones encriptadas usando Tor o similares, limitación del número de operaciones, la monitorización del comportamiento del usuario en la cadena cuando se tengan sospechas, el almacenamiento de las direcciones públicas de los monederos virtuales a los que se transfieren o desde el que se reciben las monedas virtuales, etc.[52]

Como puede comprobarse, las medidas, de aprobarse, son muy exigentes en cuanto al conocimiento del cliente y de las personas que no son siempre los clientes, titulares reales, así como la valoración del riesgo. Entran en juego intereses generales, como garantizar la eficiencia del mercado financiero, junto a otros intereses particulares, ya que se ha de recoger, procesar y registrar datos personales y comunicarlos, en su caso, a las autoridades competentes. Se trata, entonces, de buscar un equilibrio entre la efectividad de la normativa, que garantice el correcto funcionamiento del sistema de pagos y de los mercados financieros y los derechos y libertades individuales, entre otros, la protección de datos y la libertad de empresa; entre el derecho a la privacidad y la protección de datos de carácter personal, ya que las obligaciones previstas exigen que se conozca al cliente, así como el ejercicio de la actividad empresarial, las obligaciones no suponen restricción algunas desde el punto de vista de su ejercicio, aunque a partir de la directiva sí que tendrá que aplicar las medidas de debida diligencia con relación a sus clientes.

En efecto, la UE es consciente de las medidas que plantea son el mejor remedio para garantizar una respuesta adecuada a los riesgos de delitos financieros y a la continua amenaza terrorista, además de la transparencia. Es por ello por lo que recalca que si bien el objeto es el de proteger el sistema financiero aspira a la salvaguarda de los derechos fundamentales relacionados con la protección de datos y las libertades económicas, que pueden verse afectados por disposiciones como las previstas, en contrapeso a la necesidad de reforzar la seguridad; entre otros, el derecho a la vida privada y

52 RAMOS SUÁREZ, F.M., "La UE regula la actividad del bitcoin y otras monedas virtuales a través de la normativa de blanqueo de capitales, en *Abogacía Española, Consejo General*, 29 noviembre 2016 (disponible en: http://www.abogacia.es/2016/11/29/la-ue-regula-la-actividad-del-bitcoin-y-otras-monedas-virtuales-a-traves-de-la-normativa-de-blanqueo-de-capitales/

familiar (previsto en el artículo 7 de la Carta de los Derechos Fundamentales), la protección de datos de carácter personal, al imponer a estas entidades la obligación de procesar datos personales, recogida y tratamiento de datos financieros personales en línea, y la libertad de empresa (artículos 8 y 16 del mismo cuerpo legal, respectivamente)[53]. Y es que en la medida en que la regulación anteriormente descrita afecta a las plataformas de cambio de monedas virtuales, incluyéndolas en la categoría de entidades obligadas, la concreta en materia de blanqueo y financiación terrorista exige a dichos sujetos el conocimiento del cliente, e igualmente a los titulares reales, evaluando los riesgos. Es por ello por lo que se dispone la obligación de recoger, procesar y registrar datos personales, y su comunicación a las autoridades competentes, con lo cual esto tendrá repercusiones para los particulares. De otro lado, se toma en consideración a la liberta de empresa, ya que las medidas propuestas tendrán un evidente impacto en los agentes económicos, que hasta este momento no tienen obligación de aplicar medidas de diligencia debida respecto a los clientes. En mi opinión, las soluciones propuestas tienen en cuenta la defensa de los intereses colectivos, como es la prevención de actividades delictivas, que se valoran por encima de la intimidad personal, como interés individual, que quedaría salvaguardado en el supuesto de que se arbitre un oportuno sistema de protección de datos personales, con la correspondiente sanción en caso de incumplimiento, y lo mismo valdría para la protección de datos de carácter personal, que no es absoluta, sino que permite cesiones siempre y cuando exista justificación legítima[54].

Finalmente, esta responsabilidad aplicable a los proveedores de acceso a determinados servicios dimana del diseño por la legislación de una serie de deberes de evitación, control, supervisión y colaboración con las autoridades por el tipo de operaciones que desempeñan los sujetos obligados, porque se ve la necesidad de intervención administrativa, y no únicamente al Derecho penal, para el cumplimiento de aquellos objetivos, superando las dificultades de persecución. Efectivamente, la regulación preventiva tiene como objetivos principales: por un lado, asegurar la identificación o diligencia debida con relación al cliente, y de otro, proporcionar instrumentos jurídicos para la investigación y persecución del blanqueo. Es por ello por lo que dicha regulación está en constante proceso de adaptación a los estándares internacionales y su implementación al derecho interno, apareciendo como ineludible la adecuación de la regulación preventiva a los tiempos cambiantes, de forma rápida y efectiva, frente a formas técnicamente avanzadas de blanqueo, eliminando en lo posible o mitigando el riesgo de las fuentes anónimas. No está de mas recordar que esa adaptación se ve favorecida por el hecho de que las medidas preventivas aplicables al blanqueo se corresponden con las relativas a la financiación del terrorismo, y en este sentido, ante una amenaza terrorista que se ha extendido y presenta una clara evolución usando los avances tecnológicos y las comunicaciones, como dice la exposición de motivos de la Propuesta de Directiva de 2016, se intenta cubrir las lagunas existentes ante los variados métodos empleados por los terroristas "que van desde el dinero en efectivo hasta el comercio de bienes culturales, pasando por las monedas virtuales y las tarjetas prepago anónimas", en un marco de actuación mucho más amplio que se refiere a la creación de un mercado único de pagos y digital, la protección del consumidor y la inclusión financiera y de datos, el comercio electrónico, etc.

53 Con relación a la protección de datos, vid. PESCH, P./ BÖHME, R., "Datenschutz trotz öffentlicher Blockchain? Chancen und Risiken bei der Verfolgung und Prävention Bitcoin-bezogener Straftaten", en *DuD (Datenschutz und Datensicherheit*, 2(2017), págs. 93 y ss.

54 En el ámbito fiscal, LUCAS DURÁN, M., "La eliminación del dinero en efectivo y su sustitución por divisa electrónica como vía más eficaz para combatir el fraude y la elusión fiscales", en Instituto de Estudios Fiscales, DOC núm. 12/2016 (disponible en: http://www.ief.es/documentos/recursos/publicaciones/documentos_trabajo/2016_12.pdf) menciona como referente la STC 110/1984, de 26 de noviembre, "en la se indicó que los requerimientos de información a los bancos por parte de la Administración tributaria no pueden entenderse contrario al derecho a la intimidad (…) De manera que cuando resulte proporcionada la interferencia en la vida privada de los individuos para lograr determinados fines de lucha contra actividades ilícitas o criminales, no podrá entenderse violación alguna del derecho a la intimidad. Y ello tiene la fuerza de un principio general en relación con los derechos fundamentales, de manera que resulta aplicable no sólo en el ámbito de la protección constitucional de los derechos fundamentales y otros intereses tutelados por la Carta Magna en el ámbito interno, sino también en el europeo e internacional".

5. Conclusión final.

El nacimiento y desarrollo de nuevos métodos de pago con el fin de atender las necesidades de los clientes, tanto de aquellos no bancarizados como de los que forman parte del sistema bancario y financiero, los hace especialmente atractivos para el ciberdelito, sobre todo, en un principio, cuando surgieron por falta de regulación y, en consecuencia, escasa vigencia de la diligencia debida, por garantizar el anonimato del titular de la operación.

En este sentido, basta con revisar los estándares internacionales, los informes emitidos por organismos internacionales y la política europea en la lucha contra el blanqueo y financiación del terrorismo para advertir que se propugna un sistema de protección que haga frente a los diversos peligros derivados del uso de nuevos métodos para el blanqueo y proporcione seguridad al sistema financiero. Para ello, se establece la necesidad de identificar los riesgos y la aplicación estricta de la normativa en cuanto a la obligación de identificación de los clientes, con especial atención a las operaciones sospechosas y, debido al carácter internacional de muchas operaciones, atender al riesgo que aumenta precisamente porque los proveedores de servicios se encuentran en jurisdicciones con una escasa regulación antiblanqueo; más concretamente, de lo que se trata es de reducir el anonimato, tener el control de los riesgos y una decidida intervención preventiva.

Son muchos los desafíos legales que plantea el mundo digital, pero debemos estar a la altura de los retos que igualmente suscita el ciberblanqueo. La evolución permanente de las nuevas tecnologías ofrecen la posibilidad de realizar operaciones transfronterizas, de realización rápida y con anonimato, relativo en algunos casos, total en otros, dificulta la eficacia de las normas. Es necesario adecuar la regulación a los nuevos tiempos, absolutamente cambiantes, con rapidez y efectividad, en una continua actualización, así como los conocimientos técnicos dentro de un marco jurídico que esté atento a la innovación tecnológica, sin incidir negativamente en derechos individuales y libertades (privacidad, secreto de las comunicaciones, libertad de empresa, etc.). En este sentido, la característica del modelo político criminal de la sociedad del riesgo informatizada se expresa claramente en la especial persecución del blanqueo, para evitar lagunas de punibilidad. Además, hay otras características de la sociedad del riesgo que se ven claramente en la especial persecución respecto a las ganancias procedentes de la actividad delictiva, como son la cooperación internacional de los agentes implicados y la coordinación en Europa, entre las instituciones de la Unión y los Estados, o la extensión de la jurisdicción (aunque el delito antecedente o los hechos de blanqueo hayan tenido lugar, total o parcialmente, en el extranjero).

Ligado a ello, se sigue dando primacía a las estrategias de tipo preventivo, de aquella que incrementan las competencias de las autoridades de inteligencia financiera y ampliación del círculo de sujetos obligados. En este sentido, la normativa preventiva surge de sistemas de control supranacional que toma las decisiones que luego han de adaptar las legislaciones nacionales y tiene como misión fundamental garantizar el correcto funcionamiento del sistema de pagos y de los mercados financieros. Para ello se ha eliminar el riesgo de las fuentes anónimas, sometiendo a las monedas virtuales a las mismas normas reguladoras antiblanqueo, aplicables a otros métodos de pago, permitiendo únicamente aquellas que apliquen con eficacia medidas de identificación y verificación de la identidad del cliente y el control de las operaciones, que en el caso que consideramos debería añadir los propios controles tecnológicos (por ejemplo, almacenamiento de direcciones públicas de los monederos) para garantizar la eficacia de los controles y la protección de los intereses en juego.

BIBLIOGRAFÍA

ABEL SOUTO, M., *Normativa internacional sobre el blanqueo de dinero y su recepción en el*

ordenamiento penal español, Universidad de Santiago de Compostela, 2001.

- "Blanqueo, innovaciones tecnológicas, amnistía fiscal de 2012 y Reforma Penal", en *Revista electrónica de Ciencia penal y Criminología*, 14-14 (2012).
- "Money laundering, new technologies, FAFT and Spanish penal reform"; en *Journal of Money Laundering Control*, vol. 16, núm. 3, 2013, págs. 266-284.

ANARTE BORRALLO, E., "Incidencia de las nuevas tecnología en el sistema penal. Aproximación al Derecho en la Sociedad de la Información", en *Derecho y conocimiento,* vol. 1, 2001, págs. 191-257.

ANDREAS, P., "Illicit Globalisation: Myths and Misconceptions", en *Globalisation, Criminal Law and Criminal Justice: Theorertical, Comparative and Transnational Perspectives*, Mitsilegas/Alldridge/Cheliotis (ed.), Hart Publishing, 2015, págs. 55 y ss.

Banco Central Europeo, *Dictamen sobre las monedas virtuales*, 4 de julio de 2014.

Banco Central Europeo, *Dictamen sobre una propuesta de directiva del Parlamento Europeo y del Consejo por la que se modifica la Directiva (UE) 2015/849, relativa ala 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*, de 12 de octubre de 2016.

CAPITÁN LÓPEZ, S., "Los bitcoines y su utilización como dinero descentralizado y anónimo", en *Cuadernos de Formación*, Colaboración 3/15, vol. 19/2915, págs. 33 y ss.

CARPINTERO SANTAMARÍA, N./OTERO, M.P. "Cyberspace: A Plataform for Organized Crime", en *Cyberspace. Risks and Benefits for Society, Security and Development*, AA.VV., Martin y García Segura ed., Springer International Publishing AG, 2017, págs. 121-140.

CHAUM, D., "Achieving Electronic Privacy", en *Scientific American*, agosto de 1992, págs. 96-101.

DE CEVALLOS Y TORRES, J.F., *Blanqueo de capitales y principio de lesividad*, Tesis Doctoral, Facultad de Derecho, Salamanca, 2013, págs. 148 y ss.

DE LA CUESTA, J.L., "Principales lineamientos político criminales de la AIDP en un mundo globalizado", en *I Conferencia mundial de Derecho penal. El Derecho penal del siglo XXI*, Guadalajara (México), Noviembre 2007, *ReAIDP*, 2008, págs. 1 y ss.

DE LA MATA BARRANCO, N.J., "Delitos vinculados al ámbito informático", en *Derecho penal informático*, de la Mata Barranco (coord.), Cuesta Arzamendi (dir.), 2010, págs.. 15-30.

DEL CID GÓMEZ, J.M., "El uso de las nuevas tecnologías en el blanqueo de capitales: los nuevos métodos de pago", en *Actas III Jornadas de Estudios de Seguridad*, Requena ed., Instituto Universitario General Gutiérrez Mellado-UNED, Madrid, 2011, págs. 411-421.

EUROPOL, *Internet Organised Crime Threat Assessment*, IOCTA 2016.

FABIÁN CAPARRÓS, E.A., "Oportunidad político-criminal y viabilidad dogmática del delito imprudente de blanqueo de capitales", en *Estudios sobre la corrupción, una reflexión hispano brasileña*, BERDUGO GÓMEZ DE LA TORRE / LIBERATORE S. BECHARA (coords.), Centro de Estudios Brasileños / Universidad de Salamanca, España, 2013, págs. 353-385.

FERRÉ OLIVÉ, J.C. "Tecnologías de información y comunicación, comercio electrónico, precios de transparencia y fraude fiscal", en *Nuevas amenazas a la seguridad nacional. Terrorismo, criminalidad organizada y tecnologías de las información y la comunicación*, González Cussac/ Cuerda Arnau (dir.), Fernández Hernández (coord.), Tirant lo Blanch, Valencia, 2013, especialmente págs.. 157 y ss. págs. 193-203.

GOMEZ, E. /ESPINOZA, H., "Cómo responder a un delito informático", en *Revista Ciencia UNEMI*, junio 2014, págs. 43 y ss.

GÓMEZ INIESTA, D.J., "Estafa y blanqueo de dinero a través de Internet", en *La ley penal: revista de derecho penal, procesal y penitenciario*, núm. 105, 2013, págs. 4 y ss.

GONZÁLEZ RUS, J.J., "Precisiones conceptuales y político-criminales sobre la intervención penal en Internet", en *Delito e informática: algunos aspectos*, AA.VV., Cuadernos penal José María Lidón, núm. 4, Universidad de Deusto, Bilbao, 2007, págs. 13-40, especialmente, págs. 29 y ss., el medio a través del que se produce un hecho no tiene que suponer una transformación de las necesidades y posibilidades de tutela, con la aparición de nuevas formas de agresión sin que ello

suponga de forma automática un contenido nuevo del bien jurídico.
GLESS S./KUGLER, P./ STAGNO D., "Was is Geld? Warum schützt man es? Zum strafrechtlichen Schutz von virtuellen Währungen am Beispiel von Bitcoins", en *Recht* 2 (2015), págs. 1 y ss.
GRZYWOTZ, J./KÖHLER, O.M./RUCKERT, C., "Cybercrime mit Bitcoins – Straftaten mit virtuellen Währungen, deren Verfolgung und Prävention", en *Strafverteidiger*, vol. 36, núm. 11 (noviembre, 2016), págs. 753-759.
HERNÁNDEZ QUINTERO, H.A., "Informática y delito de lavado de activos", en *Derecho penal y Criminología* 47 (2007), págs. 47 y ss.
HUGEL, P./KELLY, J., "Internet grambling, credit cards and money laundering", en *Journal of Money Laundering Control*, vol. 6, 1, 1997, págs. 57-65
HUNGERLAND, F. et al., Die Zukunft des Geldes – das Geld der Zukunft, en *Strategie* 2030 – Vermögen und Leben in der nächsten Generation, núm. 24, pags. 47 y ss.
JOOSTEN, J., *Combating cyber money laundering: selected jurisdictional issues*, Faculty of Law, University of The Western Cape, octubre, 2010.
JURADO, N./GARCÍA, R., "El blanqueo de capitales", en *El enriquecimiento ilícito*, Avilés Gómez (coord.), ed. Club Universitario, Alicante, 2011, págs. 159-192.
LESLIE, D.A., "Introduction, Money Laundering and Cyber crime", en *Legal Principles for Combatting Cyberlaundering*, AA.VV., Springer, Suiza, 2014, págs. 1-54.
LASTOWKA, F.G./HUNTER, D., "Virtual Crimes", en *New York Law School Law Review*, núm. 49, pág. 294.
LEVI, M., "Crime of Globalisation: Some Measurement Issues", *New tipes of crime. Procedings of the International Seminar held in connection with HEUNI´s thirtieth anniversary*, Joutsen (ed.), Helsinki, 2012, págs. 107-115.
LUCAS DURÁN, M., "La eliminación del dinero en efectivo y su sustitución por divisa electrónica como vía más eficaz para combatir el fraude y la elusión fiscales", en *Instituto de Estudios Fiscales*, DOC núm. 12/2016.
MIRÓ LLINARES, F., "La oportunidad criminal en el ciberespacio. Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen", *RECPC* 13-07 (2011), págs. 13- 19.
MORENO VERDEJO, J., "Algunas cuestiones acerca de la estafa informática y uso de tarjetas (Incidencia del Anteproyecto de 2006 de reforma del Código penal)", en *Delito e informática: algunos aspectos*, AA.VV., Cuadernos penal José María Lidón, núm. 4, Universidad de Deusto, Bilbao, 2007, págs. 173 y ss.
MÜNCH, H., "Tatort Internet – Neue Herausforderungen, neue Aufgaben", en *Sicherheit in einer digitalen Welt*, Patrick Ernst Sensburg ed., Nomos, 2017, págs. 9-22.
NAVAS NAVARRO, S., "Un mercado financiero floreciente: el del dinero virtual no regulado", en *Revista CESCO de Derecho de Consumo*, núm. 13/2015, págs. 79 y ss., especialmente, 86 y ss.
NUTZ, M.S., "Taking advantage of new technologies: For and against crime", *en Computer Law & Security Review*, vol. 24, 2008, págs. 437-446.
Observatorio Cetelem, *El comercio electrónico en España: tendencias y comportamientos*, 2015.
OXMAN, N., "Estafas informáticas a través de Internet: acerca de la imputación penal del "phising" y el "pharming", en *Revista de Derecho de la Pontificia Universidad Católica de Valparaíso*, XLI, Chile, 2013, págs. 211-262.
PELKA, P., *Phising. Welche Strafverfolgungs- und Präventionsmöglichkeiten stehen der Polizei zur Verfügung?*, Bachelorarbeit, Grin, 2016, *passim*.
PESCH, P./ BÖHME, R., "Datenschutz trotz öffentlicher Blockchain? Chancen und Risiken bei der Verfolgung und Prävention Bitcoin-bezogener Straftaten", en *DuD (Datenschutz und Datensicherheit*, 2(2017), págs. 93 y ss.
RAGHAVAN, A.R./PARTHIBAN, L., "The effect of cybercrime on a Bank´s finances", en *International Journal of Current Research and Academic Review*, vol. 2, febrero 2014, págs. 173-178.

RAMOS SUÁREZ, F.M., "La UE regula la actividad del bitcoin y otras monedas virtuales a través de la normativa de blanqueo de capitales, en *Abogacía Española, Consejo General*, 29 noviembre 2016.

Secretaría de Estado de Seguridad, *Estudio sobre la cibercriminalidad en España*, 2016.

SILVA SÁNCHEZ, J.M., *La expansión del Derecho penal*, Madrid, Civitas, 2001.

TURPIN, J.B., "Bitcoin: The Economic Case for a Global, Virtual Currency Operating in an Unexplored Legal Framework", en *Indiana Journal of Glogal Legal Studies*, vol. 21, 1, 2014, págs. 335-368.

VASSILAKI, I., *Computer- und Internet Strafrecht*, Berufsbegleitender Masterstudiengang, Informationsrecht, Center für lebenslanges Lernen, Carl von Ossietzky Universität Oldenburg, 2015, págs. 6-46

VIDALES RODRÍGUEZ, C., "Delincuencia organizada y medios tecnológicos avanzados: el subtipo agravado previsto en relación con organizaciones criminales y grupos criminales", en *Revista penal*, núm. 30, julio 2012, págs. 158 y ss.