

COVID-19 y comisión del delito de blanqueo de dinero mediante las nuevas tecnologías *

Miguel Abel Souto

Universidad de Santiago de Compostela

ABEL SOUTO, MIGUEL. COVID-19 y comisión del delito de blanqueo de dinero mediante las nuevas tecnologías. *Revista Electrónica de Ciencia Penal y Criminología*. 2022, núm. 24-28, pp. 1-31.
<http://criminet.ugr.es/recpc/24/recpc24-28.pdf>

RESUMEN: La economía mundial se ha visto muy afectada por la COVID-19 y el blanqueo sin duda lesiona o pone en peligro el orden socioeconómico estatal e internacional. Tanto el blanqueo como la COVID-19 son fenómenos globales, por lo que las iniciativas estatales aisladas están condenadas al fracaso. Como en la COVID-19 es preferible evitar el contagio, también es mejor prevenir el blanqueo que castigarlo. La COVID-19 ha incrementado la cibercriminalidad, especialmente los fraudes de productos médicos necesarios para combatirla u otros fraudes *online*. La mayor parte de las ganancias de estos delitos se blanquean. También aumentaron con la COVID-19 las ofertas de trabajo a potenciales blanqueadores a través de correos electrónicos. Además, la Directiva 2018/1673 obliga a los estados miembros a garantizar que los nuevos riesgos de las monedas virtuales se aborden adecuadamente. Las Directivas 2015/849 y 2018/843 exigen continuas adaptaciones del marco legal para responder a las amenazas del uso de las nuevas tecnologías en el blanqueo. Sin duda, los nuevos sistemas de pago facilitan la actividad criminal de los blanqueadores, pero con la COVID-19 se evita el uso de efectivo y se da preferencia a los medios de pago electrónicos. En el mismo sentido, incluso se pretende eliminar el efectivo para evitar el blanqueo. La COVID-19 también ha afectado al control total de la población a través de los teléfonos móviles, un control total que también se pretende utilizar en las investigaciones de blanqueo. Sin embargo, el control total puede llevarnos al mundo de las telepantallas orwellianas.

PALABRAS CLAVE: Blanqueo de dinero, COVID-19, cibercriminalidad, nuevas tecnologías, dinero electrónico y monedas virtuales.

TITLE: COVID-19 and money laundering through new technologies

ABSTRACT: The world economy has been seriously altered by COVID-19 and money laundering unquestionably damages or endangers the state and international socio-economic order. Both money laundering and COVID-19 are global phenomena, so isolated state initiatives are doomed to failure. As in COVID-19 it is preferable to avoid contagion, so it is also better to prevent money laundering than to punish it. COVID-19 has increased cybercrime, especially frauds of medical products needed to combat it or other online frauds. Most of the profits from these crimes are laundered. Also increased with COVID-19 job offers to potential money launderers through emails. In addition, Directive 2018/1673 obliges member states to ensure that new risks of virtual currencies are addressed appropriately. Directives 2015/849 and 2018/843 require continuous adaptations of the legal framework to respond to threats of the use of new technologies in money laundering. Undoubtedly, the new payment systems facilitate money launderers' criminal activity, but with COVID-19 the use of cash is avoided and electronic means of payment are preferred. In the same sense, it is even intended to eliminate cash to prevent money laundering. COVID-19 has also affected the total control of the population through mobile phones, a total control that is also intended to be used in money laundering investigations. However, total control can lead us to the world of Orwellian telescreens.

KEYWORDS: Money laundering, COVID-19, cybercrime, new technologies, electronic money and virtual currencies.

Fecha de recepción: 15 septiembre 2022

Fecha de publicación en RECPC: 11 diciembre 2022

Contacto: miguel.abel@usc.es

SUMARIO: I. COVID-19 y criminalidad. II. Dos pandemias: blanqueo de dinero y COVID-19. III. Blanqueo de dinero y nuevas tecnologías. IV. Conclusiones. V. Reflexión final. Bibliografía

* Este artículo se integra en el proyecto PID2021-126422OB-I00 (AEI/FEDER, UE), financiado por la Agencia Estatal de Investigación (Ministerio de Ciencia e Innovación) y la Unión Europea: Blanqueo de dinero, mundo digital, reformas de 2021 y la posibilidad de un Derecho penal europeo.

I. COVID-19 y criminalidad

La pandemia, además de afectar a la vida e integridad de miles de millones de personas en todo el mundo¹, también generó evidentes “manifestaciones de tipo económico”², amén de complejos problemas para atribuir responsabilidad penal por contagio³, desobediencia, delito de odio, desórdenes públicos⁴ o por infracción de las normas sobre prevención de riesgos laborales⁵, ponderaciones entre derechos fundamentales y seguridad, como la libertad de expresión respecto a las *fake news*⁶, cuya desinformación amenaza la seguridad y el Estado de Derecho⁷, una reducción en la tasa de feminicidios⁸, discutibles declaraciones de inconstitucionalidad⁹ y múltiples cuestiones jurídicas¹⁰.

Igualmente, el elevado uso de las nuevas tecnologías motivado por la COVID-19¹¹ propició un “notable aumento de los cibercrímenes”¹², que entre 2016 y 2019 ya se habían duplicado pero que la pandemia incrementó considerablemente¹³, y del blanqueo de dinero¹⁴ utilizando como medio “una red de ordenadores en cualquier fase de la comisión”¹⁵, pues el cierre de empresas, bancos y sucursales de la *Western Union* durante el confinamiento dificultó el blanqueo por las vías tradicionales y fomentó el uso de nuevas fórmulas, aunque después los rescates gubernamentales a las

¹ Cfr. GONZÁLEZ CUSSAC/VELÁSQUEZ VELÁSQUEZ, 2022, p. 12.

² *Ibidem*.

³ Vid. CANCIO MELIÁ/PANTALEÓN DÍAZ, 2022, pp. 489-502.

⁴ Vid. JERICÓ OJER, 2020, pp. 461-483.

⁵ Vid. RODRÍGUEZ VÁZQUEZ, 2021, pp. 415-491.

⁶ Cfr. NIETO MARTÍN, 2020, p. 6.

⁷ Cfr. GONZÁLEZ CUSSAC, 2022, p. 13.

⁸ Cfr. FERNÁNDEZ TERUELO, 2022, p. 182.

⁹ Vid. FERNÁNDEZ HERNÁNDEZ, 2022, pp. 79-115. Por el objeto de estudio de este artículo no se analizarán las sentencias del TC sobre la pandemia. Tampoco se cita jurisprudencia relativa a la COVID-19 y el blanqueo porque los casos todavía no han llegado al TS.

¹⁰ Vid. CERDEIRA BRAVO DE MANSILLA, 2021.

¹¹ Aunque el acrónimo de *COronaVirus Disease* y 2019 se utilice normalmente en masculino por influjo del género de *coronavirus*, usaré el femenino la COVID-19 por ser la enfermedad (*disease*) el núcleo del acrónimo, como pone de manifiesto la Real Academia de la Lengua en “¿Es «el COVID-19» o «la COVID-19»?”, <http://www.rae.es> (septiembre de 2022).

¹² GONZÁLEZ CUSSAC, 2022, p. 13.

¹³ Cfr. ABADÍAS SELMA/FERNÁNDEZ ALBESA/LEAL RUIZ, 2021, pp. 13 y 41.

¹⁴ Cfr. POSADA MAYA, 2022, p. 70.

¹⁵ LLEDÓ BENITO, 2022, p. 17.

pequeñas empresas aumentaron la actividad financiera y las oportunidades para los blanqueadores¹⁶.

II. Dos pandemias: blanqueo de dinero y COVID-19

Según el diccionario de la Real Academia de la Lengua Española “epidemia” es un “mal o daño que se expande” y el diccionario académico define “pandemia” como una epidemia “que se extiende a muchos países”¹⁷, por lo que puede afirmarse que el blanqueo, al igual que la COVID-19, constituye una pandemia, una lacra que afecta a todo el mundo y que sin duda debe ser combatida.

De otro lado, la economía mundial se ha visto muy afectada por la COVID-19, que genera una gran destrucción de empleo y una enorme disminución de los intercambios de productos, bienes y servicios, los cuales nos han llevado a una profunda crisis económica. En el mismo sentido el blanqueo de dinero indiscutiblemente lesiona o pone en peligro el orden socioeconómico estatal e internacional¹⁸. Concretamente, en la Unión Europea la COVID-19 “causó divergencias económicas notables”¹⁹ y hasta se constató que en Italia la mafia a través del blanqueo financia y controla empresas en crisis²⁰. Respecto a España, ha sido una de las grandes economías más afectadas, con una reducción del PIB de 10,8% en 2020, una fuerte caída de la rentabilidad empresarial y un aumento del endeudamiento, el cual ha convertido en vulnerables a las PYMES que concentran el 48% del empleo²¹.

Asimismo, tanto el blanqueo de dinero como la COVID-19 son fenómenos mundiales, por lo que exigen respuestas globales, de manera que las iniciativas estatales aisladas están condenadas al fracaso²².

Además, al igual que en la COVID-19 resulta preferible evitar el contagio a curar la enfermedad, así también es mejor prevenir el blanqueo que castigarlo, por ello los diversos estados aprueban, junto a las normas penales, medidas administrativas de prevención²³ de conformidad con la consideración del Derecho penal como *ultima ratio*.

Obviamente es necesario sancionar el blanqueo de dinero. Sin embargo, en su persecución y castigo se está incurriendo en diversos excesos²⁴, como veremos, que deben ser denunciados.

En este sentido la Asociación Internacional de Criminología formuló, el 1 de abril

¹⁶ Cfr. DOUGLAS HEAVEN, 2020, pp. 1 y 3.

¹⁷ REAL ACADEMIA ESPAÑOLA (2020), *Diccionario de la lengua española*, en <http://dle.rae.es>, voces “epidemia” y “pandemia” (septiembre de 2022).

¹⁸ Vid. ABEL SOUTO, 2005, pp. 56-89, y 2014a, pp. 11-65.

¹⁹ HERNÁNDEZ DE COS, 2022, p. 2.

²⁰ Cfr. NIETO MARTÍN, 2020, p. 6.

²¹ Cfr. BLANCO/MAYORDOMO/MENÉNDEZ/MULINO, 2021, pp. 5, 8 y 17.

²² Vid. ABEL SOUTO, 2002 y 2020.

²³ Vid. MORÓN PENDÁS, 2021, pp. 347-367, 921 y 922.

²⁴ Vid. ABEL SOUTO, 2021a, pp. 27-39 y 2021b, pp. 401-412.

de 2020, una solicitud urgente a los gobiernos para que redujesen la masificación en las prisiones, por el riesgo inminente de infección, sobre todo teniendo en cuenta que un alto porcentaje de los internos no han sido todavía condenados²⁵, dato muy importante en relación con el blanqueo de dinero por la evidente desproporción, mayor que en otros delitos, entre los detenidos o presos provisionales y los que acaban siendo condenados²⁶. Con todo, aunque en algún país se hable de un “estado inconstitucional”²⁷ de las cárceles, en España la incidencia de la COVID-19 en prisión fue bastante menor que en la población no reclusa, pese a que no se han explorado todas las posibilidades para generar durante la pandemia una menor perturbación en la vida y resocialización de los presos²⁸.

III. Blanqueo de dinero y nuevas tecnologías

Es necesario evitar los peligros que implica la utilización de las nuevas tecnologías en la comisión del delito de blanqueo, los cuales exigen una actualización constante de las investigaciones. En este sentido la Directiva 2018/1673, sobre el combate contra el blanqueo mediante el Derecho penal²⁹, advierte de que “el uso de monedas virtuales presenta nuevos riesgos y desafíos desde la perspectiva de lucha contra el blanqueo”³⁰, pero ya unos años antes la Directiva 2015/849, o cuarta Directiva³¹, exigía “adaptaciones rápidas y continuas del marco jurídico”³² para responder a las amenazas del uso de las nuevas tecnologías en el blanqueo y también la Directiva 2018/843³³, o quinta Directiva³⁴, insiste en la “necesidad de adaptarse a las nuevas amenazas”³⁵ y de modificar la Directiva de 2015. En la misma línea el informe que la Comisión debía presentar como muy tarde el 11 de enero de 2022 sobre aplicación de la Directiva 2018/843 tenía que incidir en los problemas emergentes y nuevas

²⁵ Cfr. VIANO, 2020, p. 1.

²⁶ Vid. ABEL SOUTO, 2013, pp. 1-33, 2014b, pp. 137-201 y 309-317.

²⁷ VELÁSQUEZ VELÁSQUEZ, 2022, p. 195.

²⁸ Cfr. LEÓN ALAPONT, 2022a, pp. 139 y 170.

²⁹ Vid. *Directiva (UE) 2018/1673 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativa a la lucha contra el blanqueo de capitales mediante el Derecho penal*, en *Diario Oficial de la Unión Europea*, L 284, 12 de noviembre de 2018, pp. 22-30.

³⁰ Considerando 6.

³¹ Vid. *Directiva (UE) 2015/849 del Parlamento Europeo y del Consejo, de 20 de mayo de 2015, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo y por la que se modifica el Reglamento (UE) n° 648/2012 del Parlamento Europeo y del Consejo y se derogan la Directiva 2005/60/CE del Parlamento Europeo y del Consejo y la Directiva 2006/70/CE de la Comisión*, en *Diario Oficial de la Unión Europea*, L 141, 5 de junio de 2015, pp. 73-117.

³² Considerando 28.

³³ Vid. *Directiva (UE) 2018/843 del Parlamento Europeo y del Consejo, de 30 de mayo de 2018, 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 modifican las Directivas 2009/138/CE y 2013/36/UE*, en *Diario Oficial de la Unión Europea*, L 156, 19 de junio de 2018, pp. 43-74.

³⁴ Sobre las dos directivas de 2018 vid. ABEL SOUTO, 2021c, pp. 41-75. En torno a la responsabilidad penal de las personas jurídicas vid. ABEL SOUTO, 2021d, pp. 1-62.

³⁵ Considerando 6.

tendencias e incluir propuestas sobre monedas virtuales, la creación de una base de datos central para las identidades y direcciones de monedero electrónico de los usuarios accesibles para las Unidades de Inteligencia Financiera y los formularios de autodeclaración de los usuarios de monedas virtuales³⁶. Sin embargo, la Comisión no se limitó simplemente a informar sino que el 20 de julio de 2021 presentó “un ambicioso paquete de propuestas legislativas”³⁷ contra el blanqueo que tiene en cuenta “los retos nuevos y emergentes relacionados con la innovación tecnológica”³⁸, como las monedas virtuales.

Concretamente se trata de cuatro propuestas legislativas: un reglamento que crea la nueva autoridad de la Unión Europea en materia de lucha contra el blanqueo³⁹, el cual también “ayudará a las unidades de información financiera a mejorar su capacidad analítica sobre los flujos y a convertir la inteligencia financiera en una fuente clave para las fuerzas de seguridad”⁴⁰; otro reglamento contra el blanqueo con normas directamente aplicables; una sexta Directiva que sustituya la Directiva 2015/849 vigente o cuarta Directiva, ya modificada por la quinta, y una revisión del Reglamento 2015/847 sobre transferencias de fondos para rastrear las de criptoactivos. Hasta ahora únicamente algunos proveedores de servicios de criptoactivos se incluían en la normativa de prevención comunitaria contra el blanqueo, pero la reforma abarcará todo el sector criptográfico, obligará a cualquier proveedor de servicios a aplicar la diligencia debida a sus clientes, se garantizará la plena trazabilidad de las transferencias con criptoactivos, como el *bitcoin*, se permitirá prevenir y detectar su uso para el blanqueo y se prohibirán los monederos anónimos de activos criptográficos⁴¹.

No obstante, el supervisor europeo de protección de datos denunció que el paquete de propuestas legislativas de la Comisión necesitaba “un nivel mayor de detalles y aclaraciones”⁴² para garantizar el cumplimiento de los principios necesidad, proporcionalidad y seguridad jurídica⁴³.

Por el momento la propuesta más avanzada es la relativa a la nueva autoridad central contra el blanqueo, que surge ante los “muchos agujeros”⁴⁴ que dejaban las

³⁶ Cfr. art. 65, modificado.

³⁷ COMISIÓN EUROPEA, 2021, p. 1.

³⁸ *Ibidem*.

³⁹ *Vid. Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se crea la autoridad de lucha contra el blanqueo de capitales y la financiación del terrorismo y se modifican los Reglamentos (UE), n° 1093/2010, (UE) n° 1094/2010 y (UE) n° 1095/2010, COM (2021) 421 final, 20 de julio de 2021, pp. 1-126.*

⁴⁰ COMISIÓN EUROPEA, 2021, p. 2.

⁴¹ *Ibidem*.

⁴² SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS, 2021, pp. 1-6.

⁴³ *Ibidem*.

⁴⁴ “Europa quiere una autoridad central contra el lavado de dinero”, en <https://www.worldcomplianceassociation.com>, p. 1 (septiembre de 2022).

autoridades nacionales en la batalla transnacional y ningún supervisor quería “meterse en la taifa del vecino”⁴⁵. Así, el 29 de junio de 2022 el Consejo acordó su posición sobre la propuesta de la Comisión⁴⁶ y añadió competencias a la autoridad para que supervisase directamente a determinadas “entidades financieras y de crédito, entre ellas a los proveedores de servicios de criptoactivos en caso de que se consideren un riesgo”⁴⁷.

En suma, las nuevas tecnologías precisan “la presencia de un permanente y detallado soporte jurídico”⁴⁸. A estas innovaciones “el legislador europeo ha estado muy atento”⁴⁹, las normativas internas han sido obligadas a un “constante proceso de adaptación a los estándares internacionales”⁵⁰ y la Unión Europea continuará en los próximos años, según su agenda estratégica, protegiendo “a nuestras sociedades contra las ciberactividades malintencionadas”⁵¹.

En este marco entran en juego las *Fintech*⁵², acrónimo de las palabras *Finance* y *Technology* con el que se alude a las empresas que utilizan en los negocios financieros las nuevas tecnologías, como las aplicaciones de teléfonos móviles o los sistemas *big data* de manera que gestionan riesgos, seguros, transacciones o criptomonedas, conceden préstamos o llevan a cabo *crowdfunding* y hasta elaboran programas de *compliance*⁵³.

El blanqueo de dinero constituye un “delito de globalización”⁵⁴, cuya importancia en la actualidad resulta trascendental debido a la profunda crisis económica que padecemos, agravada por la COVID-19⁵⁵, pues el blanqueo lesiona o pone en peligro, además de la Administración de Justicia, el tráfico legal económico y financiero⁵⁶, y las organizaciones criminales, caracterizadas por una creciente naturaleza transnacional, con sus actividades ilegales cada vez debilitan más la economía⁵⁷ y penetran en el sistema financiero, las haciendas públicas⁵⁸ o servicios aduaneros a causa de su vulnerabilidad⁵⁹. Ya hace más de dos décadas que PIETH reconoció que las innovaciones tecnológicas facilitan de un modo decisivo la internacionalización, entre las

⁴⁵ *Ibidem*.

⁴⁶ *Vid. Proposal for a Regulation of the European Parliament and of the Council establishing the authority for anti-money laundering and countering the financing of terrorism and amending Regulations, (EU) n° 1093/2010, (EU) 1094/2010, (EU) 1095/2010, 2021/0240 (COD), 29 de junio de 2022, pp. 1-192.*

⁴⁷ CONSEJO EUROPEO, 2022, p. 2.

⁴⁸ FERNÁNDEZ TERUELO, 2020, p. 27.

⁴⁹ GÓMEZ INIESTA, 2020, p. 325.

⁵⁰ *Ibidem*.

⁵¹ CONSEJO EUROPEO, 2019, p. 3.

⁵² *Vid. DONNA, 2021, pp. 197-238.*

⁵³ *Cfr. <http://www.epitoch-it.es>; <http://www.iebschool.com> (septiembre de 2022).*

⁵⁴ LEVI, 2012, p. 107. En el mismo sentido se ha pronunciado recientemente FERNÁNDEZ GARCÍA, 2021, p. 150.

⁵⁵ *Vid. ABEL SOUTO, 2021e, pp. 23-50.*

⁵⁶ *Vid. ABEL SOUTO, 2005, pp. 21-89.*

⁵⁷ *Vid. FINKLEA, 2009, pp. 9-40.*

⁵⁸ *Vid. FERRÉ OLIVÉ, 2018.*

⁵⁹ *Vid. FISHER, 2012, pp. 153-161.*

que tienen especial interés las nuevas posibilidades de comunicación y con ellas la intensificación de los flujos financieros e informativos⁶⁰. Las relaciones sociales y jurídicas han sido transformadas mediante la informática y las telecomunicaciones⁶¹ en la denominada “sociedad de la información”. Asimismo, los cambios se suceden a una “velocidad vertiginosa”⁶² en el mundo de las tecnologías de la información y la comunicación, lo que genera una “obsolescencia fugacísima”⁶³, y el ciberespacio se encuentra en una permanente revolución que incrementa el ámbito de oportunidades delictivas⁶⁴. Si a ello se le une la “globalización de mercados y economías”⁶⁵ resulta que “la internacionalización del sector financiero no solo ha traído las ventajas de la celeridad y de la seguridad en las transacciones financieras, sino que desgraciadamente también ha mejorado las modalidades y la expansión del blanqueo de dinero”⁶⁶, porque la movilidad, informatización y *desregulación* han abierto un campo ideal de actuación para los delincuentes económicos en general, sobre todo mientras el Derecho penal siga organizándose nacionalmente⁶⁷.

En efecto, se ha señalado que “uno de los delitos que más se ha beneficiado de *internet* es el blanqueo”⁶⁸, “generalizado y radicalizado”⁶⁹ por los nuevos medios electrónicos, con un desarrollo “espectacular”⁷⁰ gracias al potencial ejecutivo que le ofrecen *internet* y las transferencias electrónicas⁷¹, vertiginosa transformación tecnológica que genera “la percepción de un Derecho siempre superado por la realidad”⁷², “la errónea imagen de ineficacia e inutilidad”⁷³ del Derecho penal. El creciente uso de los nuevos métodos de pago ha producido, con sus transacciones y movimientos de fondos, un incremento en la detección de casos de blanqueo cometidos utilizando medios telemáticos⁷⁴, ya que el atractivo que presentan las nuevas tecnologías para los blanqueadores surge, principalmente, del anonimato⁷⁵, “la eficiencia”⁷⁶, la alta negociabilidad y utilidad de los fondos así como del acceso global por la red de cajeros automáticos⁷⁷, factores a los que habría que añadir los problemas

⁶⁰ Cfr. PIETH, 1997, p. 756.

⁶¹ Cfr. PÉREZ ESTRADA, 2010, p. 305.

⁶² GAMERO CASADO, 2012, p. 48.

⁶³ *Ibidem*.

⁶⁴ Cfr. MIRÓ LLINARES, 2011, pp. 13 y 38.

⁶⁵ MATA BARRANCO, 2010, p. 21.

⁶⁶ PONTE, 1996, p. 242.

⁶⁷ Cfr. PIETH, 1997, p. 757.

⁶⁸ VELASCO SAN MARTÍN, 2012, p. 75.

⁶⁹ SANDYWELL, 2010, p. 46.

⁷⁰ PÉREZ ESTRADA, 2010, p. 306.

⁷¹ Cfr. FERNÁNDEZ TERUELO, 2007, pp. 155 y 158, 2011, pp. 231 y 234.

⁷² GONZÁLEZ CUSSAC, 2022, p. 14.

⁷³ *Ibidem*.

⁷⁴ Cfr. FATF, 2010, p. 7, §1 y p. 9, §18.

⁷⁵ Cfr. FERNÁNDEZ TERUELO, 2007, p. 158 y 2011, p. 234; MATA BARRANCO, 2010, p. 19; MIRÓ LLINARES, 2011, pp. 12, 13, 25 y 26; VELASCO SAN MARTÍN, 2012, p. 75.

⁷⁶ GÓMEZ INIESTA, 2021, p. 651.

⁷⁷ Cfr. FATF, 2010, p. 7, §5.

de persecución⁷⁸ y prueba, por falta de competencia, medios y hasta capacitación, dificultades de detección, lugar comisivo, prescripción, ley aplicable, distanciamiento geográfico, cooperación policial y judicial⁷⁹, ante los que la Administración de Justicia no puede “fossilizarse como un paquidermo pleistocénico”⁸⁰ y que requieren nuevos métodos de investigación que mantengan un delicado equilibrio entre seguridad y derechos fundamentales⁸¹.

En este sentido la Ley orgánica 9/2022, de 28 de julio⁸², que transpone la Directiva 2019/1153⁸³, en la medida en que “resulta crucial reforzar la seguridad, mejorar el enjuiciamiento de los delitos financieros, luchar contra el blanqueo de capitales y la financiación del terrorismo, así como prevenir los delitos fiscales”⁸⁴, contempla un “acceso directo de las autoridades competentes”⁸⁵ al Fichero de Titularidades Financieras, sin previa autorización judicial o del ministerio fiscal que exigía antes la Ley de prevención del blanqueo de dinero, supresión que suscita gran “polémica”⁸⁶, pero se advierte del necesario “equilibrio entre la eficiencia y la protección de datos personales”⁸⁷, aunque lamentablemente también se aprovechó la reforma para modificar el apartado segundo del artículo 234 del Código penal, elevando a delito tres antiguas faltas de hurto, hoy delitos leves, ante la negativa del Tribunal Supremo de aplicar en estos casos, por desproporcionada, la agravante séptima del artículo 235.1 de multirreincidencia, milagrosa conversión de tres granos de trigo en un pan que recuerda la aplicación de la regla del béisbol a la política criminal estadounidense con el *three strikes and you are out*.

En cualquier caso, para evitar el abuso por la criminalidad organizada de las insuficiencias legales en las nuevas tecnologías⁸⁸, *internet* no puede ser un “ámbito ajeno al derecho”⁸⁹, sino que debe ser regulado⁹⁰.

Ciertamente los nuevos sistemas de pago facilitan a los blanqueadores su actividad

⁷⁸ Vid. GLESS, 2012, pp. 3-22.

⁷⁹ Cfr. MATA BARRANCO, 2010, pp. 19, 20, 26 y 28.

⁸⁰ GAMERO CASADO, 2012, p. 50.

⁸¹ Vid. PÉREZ ESTRADA, 2010, pp. 307, 309 y 311-317.

⁸² Vid. Ley orgánica 9/2022, de 28 de julio, por la que se establecen normas que faciliten el uso de información financiera y de otro tipo para la prevención, detección, investigación o enjuiciamiento de infracciones penales, de modificación de la Ley orgánica 8/1980, de 22 de septiembre, de financiación de las comunidades autónomas y otras disposiciones conexas y de modificación de la Ley orgánica 10/1995, de 23 de noviembre, del Código penal, BOE nº 181, de 29 de julio de 2022, pp. 1-27.

⁸³ Vid. Directiva (UE) 2019/1153 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, por la que se establecen normas destinadas a facilitar el uso de información financiera y de otro tipo para la prevención, detección, investigación o enjuiciamiento de infracciones penales y por la que se deroga la Decisión 2000/642/JAI del Consejo, en Diario Oficial de la Unión Europea, L 186, 11 de julio de 2019, pp. 122-137.

⁸⁴ Preámbulo, III, párrafo 7.

⁸⁵ Preámbulo, III, párrafo 6.

⁸⁶ LEÓN ALAPONT, 2022b, p. 13.

⁸⁷ Preámbulo, III, párrafo 9.

⁸⁸ Vid. ANGELINI/GIBSON, 2007, pp. 65-73.

⁸⁹ GLESS, 2012, p. 22.

⁹⁰ Cfr. GÓMEZ TOMILLO, 2006, p. 189.

criminal, pues son mejores que el dinero en efectivo para trasladar grandes cantidades pecuniarias; la velocidad de las transacciones dificulta el control de los bienes o su posible congelación; las relaciones de negocios no presenciales favorecen la utilización de testaferreros e identidades falsas y la ausencia de riesgo crediticio, al existir normalmente un prepago, desincentiva que los proveedores de servicios obtengan una completa y precisa información sobre los clientes o la naturaleza de las relaciones comerciales⁹¹, proveedores que suelen utilizar una “débil tecnología”⁹².

No obstante, el desarrollo de las tecnologías, entre ellas *internet*, ha implicado incuestionables ventajas⁹³, “un auténtico cambio en los modos de relación administrativa, educativa, laboral o social”⁹⁴, la seguridad criptográfica, la trazabilidad de la cadena de bloques, la elaboración de perfiles de usuarios⁹⁵ y hasta facilita⁹⁶, mediante recursos *online*, la verificación de la identidad u otros deberes de diligencia para la prevención del blanqueo⁹⁷, como en las empresas *Fintech* mediante sistemas *big data* y aplicaciones informáticas⁹⁸, incluso se habla de *Regtech* o gestión tecnológica del cumplimiento con la regulación⁹⁹ con “la visualización de datos, la cadena en bloques y la inteligencia artificial”¹⁰⁰, pues las herramientas de aprendizaje automático, como los algoritmos, se adaptan para ayudar a detectar actividades anormales o sospechosas y generan alertas mediante la inteligencia artificial¹⁰¹, que contribuye a “anticipar y neutralizar amenazas o gestionar incidencias de ciberseguridad”¹⁰² más rápida y eficazmente al analizar grandes cantidades de datos sin intervención humana especializada¹⁰³. Así, la Directiva 2018/843 pone de manifiesto que “los últimos avances técnicos en la digitalización de las transacciones y los pagos permiten una identificación remota o electrónica segura”¹⁰⁴. Los nuevos métodos de pago, además de una respuesta reciente al fraude en *internet* y al mantenimiento en la privacidad de las compras¹⁰⁵, son fruto de la necesidad mercantil de ofrecer alternativas a los servicios financieros tradicionales, de no excluir a nadie del sistema por mala calificación crediticia, edad o residencia en zonas de escasa oferta bancaria y pueden tener un efecto positivo sobre la economía, dada su eficiencia en términos de rapidez de

⁹¹ Cfr. FATF, 2010, p. 21, §§58 y 61.

⁹² GÓMEZ INIESTA, 2021, p. 656.

⁹³ Cfr. MATA BARRANCO, 2010, p. 16.

⁹⁴ *Ibidem*.

⁹⁵ Cfr. GÓMEZ INIESTA, 2021, pp. 652 y 663.

⁹⁶ Vid. MARTÍNEZ ARRIBAS, 2019, pp. 125-142.

⁹⁷ Vid. *The money laundering officer's practical handbook 2011, Compliance training products limited, Cambridge*, pp. 37-39 y 54.

⁹⁸ Cfr. <http://www.iebschool.com> (septiembre de 2022).

⁹⁹ Cfr. <http://www.ciberseguridad.com> (septiembre de 2022).

¹⁰⁰ GÓMEZ INIESTA, 2020, p. 304, nota 24.

¹⁰¹ Cfr. DOUGLAS HEAVEN, 2020, pp. 1, 3 y 4.

¹⁰² LLEDÓ BENITO, 2022, p. 23.

¹⁰³ *Ibidem*.

¹⁰⁴ Considerando 22.

¹⁰⁵ Cfr. GÓMEZ INIESTA, 2020, pp. 296 y 319.

las transacciones, seguridad tecnológica, bajos costes comparados con los instrumentos de pago basados en el papel y accesibilidad, especialmente de las tarjetas prepago y los servicios de pago con teléfonos móviles, identificados como una posible herramienta para integrar a los excluidos por razones de pobreza¹⁰⁶, “un método de inclusión financiera y social para personas con dificultades para bancarizarse”¹⁰⁷, especialmente en un momento de incremento de comisiones por mantenimiento de cuentas¹⁰⁸, una forma de “acercar a todos”¹⁰⁹ los servicios financieros, métodos alternativos que suponen “una relevante mejora”¹¹⁰ de las condiciones de vida cuya regulación debe evitar limitaciones desproporcionadas en “perjuicio de los grupos sociales más vulnerables”¹¹¹.

A modo de ejemplo, Estados Unidos “distribuyó 137.000.000.000 dólares mediante tarjetas de prepago en 2018”¹¹², sobre todo en programas de asistencia alimentaria, pagos de la seguridad social, desempleo y asistencia juvenil¹¹³, incrementando un uso no nuevo, pues ya hace más de una década que se enfrentó al problema de cuatro millones de personas que recibían subsidios de la seguridad social y carecían de cuentas bancarias; para reducir su dependencia respecto a los cheques, que obligaba a los menos favorecidos a gastar entre 50 y 60 dólares mensuales en el cambio de cheques, pago de facturas o envío de dinero a familiares, se les suministraron las prestaciones mediante tarjetas de prepago con las que podían comprar bienes u obtener dinero en efectivo. Por otra parte, en Pakistán la guerra desplazó, en 2009, a más de un millón de personas y su gobierno distribuyó tarjetas de prepago con un valor máximo de 25.000 rupias, unos 300 dólares, de manera que proporcionó asistencia inmediata a casi 300.000 familias. Igualmente, en Afganistán se pagó a la policía mediante teléfonos móviles con el fin de evitar tanto el abandono del puesto de trabajo para cobrar el salario como la corrupción y el cohecho¹¹⁴.

En el mismo sentido la Directiva 2018/843 reconoce la “indiscutible utilidad”¹¹⁵ de las tarjetas de prepago de uso múltiple al contribuir “a la inclusión social y financiera”¹¹⁶, pero advierte de los peligros de las tarjetas de prepago anónimas¹¹⁷.

Frente a los clientes anónimos incluso los nuevos métodos de pago ofrecen a las autoridades más pistas que el dinero en efectivo, porque siempre generan un registro

¹⁰⁶ Cfr. FATF, 2010, p. 12, §29 y notas 7 y 8.

¹⁰⁷ FERNÁNDEZ GARCÍA, 2021, p. 152.

¹⁰⁸ *Ibidem*.

¹⁰⁹ GÓMEZ INIESTA, 2021, p. 652.

¹¹⁰ FERNÁNDEZ GARCÍA, 2021, p. 169.

¹¹¹ *Ibidem*.

¹¹² BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM, 2019, p. 1.

¹¹³ Cfr. GÓMEZ INIESTA, 2020, p. 300.

¹¹⁴ Cfr. FATF, 2010, pp. 12 y 13, cuadro 1, p. 15, nota 17 y p. 20, cuadro 5.

¹¹⁵ LORENZO SALGADO, 2020, p. 461.

¹¹⁶ Considerando 4.

¹¹⁷ *Ibidem*.

electrónico que puede suministrar la dirección de IP¹¹⁸, los lugares de pago, transferencia o retirada de fondos y hasta la localización e identificación del sospechoso de blanqueo mediante cámaras de vigilancia ubicadas en el sitio en el que se utilizó el producto¹¹⁹, aunque sigue siendo más compleja la identificación en el mundo digital que en el real¹²⁰ debido a “diversas técnicas de ingeniería informática que permiten ocultar la identidad o suplantarla”¹²¹, y se ha cuestionado la utilidad de las huellas electrónicas en la medida en que la dirección de IP puede falsificarse, llevar a zonas problemáticas o cibercafés en que la videovigilancia no existe¹²², hay *tumblers* o mezcladores de múltiples direcciones que garantizan el anonimato¹²³, las redes *wifi* permiten accesos desde sitios abiertos, hay proveedores de servicios gratuitos que no exigen identificación, sistemas que admiten el envío de correos electrónicos anónimos y robots que impiden reconocer al usuario¹²⁴, con lo que “el ciberespacio puede seguir siendo un ámbito para la intercomunicación anónima”¹²⁵ gracias a mecanismos de navegación del tipo TOR o *The Onion Router*¹²⁶.

El GAFI ya en 1996 se preocupó por las nuevas tecnologías en la 13^a de sus recomendaciones, porque suponen un peligro para el blanqueo¹²⁷ al permitir la realización de enormes transacciones instantáneamente, desde lugares remotos, guardando el anonimato y sin la implicación de instituciones financieras tradicionales¹²⁸. La ausencia de intermediación financiera dificulta la identificación de clientes y el registro de información¹²⁹. Además, las técnicas de investigación tradicionales devienen poco efectivas u obsoletas ante las nuevas tecnologías: el problema que presentaba para los blanqueadores el volumen físico del dinero —hasta el punto de abandonar el papel moneda porque no podían moverlo con suficiente rapidez— se minimiza con el “dinero electrónico”; su rápida movilidad, especialmente en *internet*, dificulta seguir el rastro de los fondos transferidos y el desacostumbrado volumen de datos a analizar casi imposibilita la detección de actividades sospechosas¹³⁰.

Téngase en cuenta que hace 40 años *internet* no existía¹³¹. Sin embargo, década y

¹¹⁸ Cfr. FATF, 2010, p. 20, §57 y nota 33.

¹¹⁹ Sobre los problemas relativos a la detección de ordenadores desde los que se accede a *internet* vid. PALOMO DEL ARCO, 2011, pp. 281-286.

¹²⁰ Cfr. MATA BARRANCO, 2010, p. 19, nota 10.

¹²¹ GÓMEZ INIESTA, 2021, p. 653.

¹²² Cfr. FATF, 2010, pp. 20 y 21, nota 34.

¹²³ Cfr. GÓMEZ INIESTA, 2021, p. 660.

¹²⁴ Cfr. MIRÓ LLINARES, F., 2011, p. 13.

¹²⁵ *Ibidem*.

¹²⁶ Vid. GÓMEZ INIESTA, 2021, p. 662, nota 25.

¹²⁷ Cfr. recomendación 13^a, FATF-VII, 1996, anexo 1.

¹²⁸ Cfr. FATF-VII, 1996, *Reviewing money laundering methods and counter-measures*, p. 8, §24.

¹²⁹ Vid. FATF-VIII, 1997, *Annex 1, Issues concerning new payment technologies*, pp. 25-27, §§17-19 y 21-29.

¹³⁰ Cfr. FATF-VIII, 1997, *Issues concerning new payment technologies*, pp. 28, 29 y 31, §§31, 32, 34, 36, 37 y 45.

¹³¹ Cfr. “Frequently asked questions: the new european cybercrime centre”, en <http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/12/221>, Bruselas, 28 de marzo de 2012, p. 1.

media más tarde se acordó el cierre en Antigua del *European Union Bank*¹³², famoso por ser el primer banco que operaba a través de *internet*¹³³, cuya publicidad en la *web* se destinaba a los defraudadores fiscales y a los blanqueadores de dinero¹³⁴. En 2012 casi tres cuartas partes de los hogares de la Unión Europea contaban con acceso a *internet*, más de un tercio de la población realizaba operaciones bancarias en línea¹³⁵ y en el mundo se habían alcanzado 2.267 millones de usuarios de *internet*¹³⁶, cifra que en la actualidad ya se ha duplicado debido a la COVID-19¹³⁷ hasta llegar a los 4.600 millones, el 59'5% de la población mundial¹³⁸ en 2021 y a 5.000 millones, el 63% de la humanidad, en 2022¹³⁹.

Precisamente por ello el GAFI elaboró, el 13 de octubre de 2006, un informe sobre nuevos métodos de pago, entre cuyas conclusiones figuraba la necesidad de su actualización en dos años¹⁴⁰, y otro documento, el 18 de junio de 2008, relativo a las vulnerabilidades de las *webs* comerciales y los sistemas de pago en *internet* contra el blanqueo y la financiación del terrorismo¹⁴¹. Posteriormente, en octubre de 2010, se redactó otro informe¹⁴² sobre el uso de los nuevos métodos de pago para el blanqueo de dinero¹⁴³ en el que se estudiaron, primeramente, las tarjetas de prepago, reguladas y supervisadas en todas las jurisdicciones que contestaron al cuestionario que se les presentó, con proveedores de servicios, en 34 de los 37 países analizados, en los que el número de usuarios pasó, desde 2004 hasta 2008, de 107'6 a 275'28 millones y utilizadas por el 17% de los estadounidenses que, según las estimaciones, se harían con el 53% del mercado mundial en 2017¹⁴⁴ y respecto a las que en 2018 su uso en Estados Unidos se incrementó un 9'6% sobre el año anterior¹⁴⁵. Entre los casos detectados figuraban supuestos de blanqueo de productos obtenidos mediante la venta ilegal en línea de esteroides, pagados con tarjetas de prepago, asuntos relacionados con el juego ilícito, narcotráfico, financiación del terrorismo¹⁴⁶ y otras actividades

¹³² Vid. SCHUDELARO, 2006, pp. 47-72.

¹³³ Cfr. FATF-LX, 1998, pp. 4 y 16, §§11 y 72.

¹³⁴ Vid. BLUM./LEVI/NAYLOR/WILLIAMS, 1999, pp. 52-57, con reproducción de los anuncios que el "Banco de la Unión Europea" incluyó en *internet*; MARTIN, 1997, pp. 38 y 39.

¹³⁵ Cfr. "Bruselas propone crear un centro europeo contra la ciberdelincuencia", en *Gaceta Informativa, Lex Nova*, nº 436, 28 de marzo de 2012, <http://www.lexdiario.es/noticias/119713/bruselas->, p. 1; COMISIÓN EUROPEA, "Un centro europeo contra la delincuencia informática para luchar contra los delincuentes en línea y proteger a los consumidores que utilizan *internet*", en <http://europa.eu/rapid/pressReleasesAction.do?reference=IP/12/317>, p. 1; "Frequently...", *cit.*, p. 1.

¹³⁶ Cfr. FUNDACIÓN ORANGE, 2012, p. 9.

¹³⁷ Cfr. ABEL SOUTO, 2021e, p. 39.

¹³⁸ Cfr. GALEANO, 2021.

¹³⁹ Cfr. "El 63% de la población mundial es usuaria de *internet*", en <https://www.ituser.es> (septiembre de 2022).

¹⁴⁰ Cfr. FATF, 2006, p. 25.

¹⁴¹ Vid. FATF, 2008, pp. 1-39.

¹⁴² Vid. FATF, 2010, pp. 1-117.

¹⁴³ Vid. BALDWIN/FLETCHER, 2004, pp. 125-158.

¹⁴⁴ Cfr. FATF, 2010, pp. 8, 10, 15 y 16, §§9, 23, 36 y 37.

¹⁴⁵ Cfr. GÓMEZ INIESTA, 2020, p. 299.

¹⁴⁶ Vid. FATF, 2010, pp. 37 y 38, casos 1 a 5.

delictivas¹⁴⁷. Hoy en día el uso de las tarjetas de prepago para el blanqueo “es una tendencia en alza”¹⁴⁸, con ofertas en *internet* de tarjetas de prepago anónimas de ciclo abierto sin límites de carga, microblanqueos a través de cientos de pequeñas transacciones, mulas de tarjetas, su adquisición masiva y posterior venta u ofertas de tarjetas de prepago de la banca *offshore* para extraer después los fondos en cajeros de cualquier país¹⁴⁹.

La Directiva 2018/843 advierte de que las tarjetas de prepago anónimas facilitan la financiación del terrorismo¹⁵⁰, por lo que rebaja los importes para autorizar a las entidades obligadas “a no aplicar alguna de las medidas de diligencia debida”¹⁵¹ de 250 a 150 euros en los instrumentos de pago que tienen “un límite máximo mensual para transacciones”¹⁵² o un “máximo almacenado electrónicamente”¹⁵³ y de 100 a 50 euros en los reembolsos o retirada en efectivo, a los que se añaden las operaciones remotas de pago según el artículo 4.6 de la Directiva 2015/2366¹⁵⁴. Estos umbrales y medidas no solo afectan a la “libertad de empresa”¹⁵⁵ por el “impacto en los agentes económicos”¹⁵⁶, sino que resultan desproporcionados¹⁵⁷ al implicar un procesamiento invasivo de datos personales de los consumidores, aceptable en la lucha contra el terrorismo pero no en la prevención del blanqueo, que puede excluir a los más desfavorecidos del sistema financiero formal y conducirlos a alternativas más baratas, de confianza y culturalmente próximas, aunque carentes de sistemas adecuados de control¹⁵⁸. Igualmente, la Directiva 2018/843 exige que las tarjetas de prepago anónimas emitidas fuera de la Unión Europea únicamente puedan utilizarse en ella si “cumplen requisitos equivalentes a los establecidos en el Derecho de la Unión”¹⁵⁹, obligación de trasponer el artículo 12.3 de la Directiva que fue cumplida por el legislador español con el Real decreto-ley 7/2021, lo que supuso la primera mención expresa a las tarjetas de prepago, mas con elipsis de la preposición “de”, en Ley 10/2010 sobre prevención del blanqueo¹⁶⁰: “Las entidades financieras que actúen como adquirentes solo aceptarán pagos efectuados con tarjetas prepago anónimas emitidas en países fuera de España cuando esas tarjetas cumplan con los umbrales y

¹⁴⁷ Vid. FATF, 2010, pp. 41 y 42, casos 16 a 24, p. 44, casos 28 y 29, pp. 46 y 47.

¹⁴⁸ GÓMEZ INIESTA, 2020, p. 303.

¹⁴⁹ Cfr. GÓMEZ INIESTA, 2020, pp. 304 y 305.

¹⁵⁰ Cfr. considerando 14.

¹⁵¹ *Ibidem*.

¹⁵² Art. 12.1, letra a).

¹⁵³ Art. 12.1, letra b).

¹⁵⁴ Cfr. art. 12.2.

¹⁵⁵ GÓMEZ INIESTA, 2020, p. 329.

¹⁵⁶ *Ibidem*.

¹⁵⁷ Cfr. PEREIRA MENAUT, 2019, p. 117.

¹⁵⁸ Cfr. GÓMEZ INIESTA, 2020, pp. 326, 328 y 330.

¹⁵⁹ Considerando 15.

¹⁶⁰ Cfr. FERNÁNDEZ GARCÍA, 2021, p. 153.

requisitos establecidos en el artículo 12 de la Directiva (UE) 2015/849¹⁶¹. La exigencia de que las tarjetas de prepago anónimas no europeas cumplan con los mismos requisitos de la Directiva para poder ser utilizadas en la Unión deriva de “la globalización económica”¹⁶², pues el dinero y las tarjetas cruzan las fronteras y “no se limitan a un área geográfica determinanda”¹⁶³.

En segundo término, el citado informe del GAFI de 2010 analizó los servicios de pago en *internet*¹⁶⁴, de crecimiento constante¹⁶⁵, y su empleo abusivo para la ejecución del denominado “ciberblanqueo”¹⁶⁶, también vinculado a la financiación del terrorismo¹⁶⁷. El pago por *internet* se encontraba regulado y sometido a supervisión en la mayoría de las jurisdicciones, aunque no en todas, y 17 de los 37 países que contestaron al cuestionario del estudio contaban entonces con proveedores de este servicio¹⁶⁸, los cuales desempeñan un papel fundamental para prevenir el blanqueo¹⁶⁹. En los últimos años el cibercrimen se ha desarrollado rápidamente gracias a los mercados *online*, en los que prolifera el robo de credenciales (*phishing*), vendidas en línea, por delincuentes especializados que no serán los usuarios finales¹⁷⁰, y tanto la suplantación de identidad¹⁷¹ como su falsificación constituyen una de las principales fórmulas utilizadas para blanquear dinero a través de *internet*¹⁷². De hecho, se ha evolucionado desde la “carta nigeriana”, así llamada porque correos electrónicos no solicitados procedentes de África se originaron mayoritariamente en Nigeria, consistente en un mero envío de un mensaje electrónico, hasta las más sofisticadas actividades criminales por medio de *internet* basadas en la falsificación de documentos, el robo de identidad y el blanqueo de dinero¹⁷³. Incluso algún *Land* alemán tuvo que paralizar las subvenciones durante la pandemia dado que “a través de delitos informáticos se estaban presentando solicitudes de ayuda suplantando la identidad de ciudadanos”¹⁷⁴. Así, se han detectado casos de utilización de los servicios de pago en *internet* para blanquear las ganancias de la propaganda racista prohibida, de la venta de cosas robadas en una *web* comercial, de la extorsión, de la venta *online* de productos falsificados, mediante vales de caja o bonos en efectivo, uso de una cuenta de moneda digital para recibir el producto de robos bancarios por *internet* de un socio

¹⁶¹ Art. 7, apartado 8.

¹⁶² GÓMEZ INIESTA, 2020, p. 325.

¹⁶³ *Ibidem*.

¹⁶⁴ *Vid.* PHILIPPSOHN, 2001a, pp. 485-490; PING, 2004, pp. 48-55; YAN/AI/TANG, 2011, pp. 93-101.

¹⁶⁵ *Cfr.* FATF, 2010, p. 17, §§44 y 47.

¹⁶⁶ *Vid.* FILIPKOWSKI, 2008, pp. 15-27.

¹⁶⁷ *Vid.* HUMMEL, 2008, pp. 117-130; SOUZA, 2012.

¹⁶⁸ *Cfr.* FATF, 2010, pp. 8 y 10, §§9 y 23.

¹⁶⁹ *Vid.* PHILIPPSOHN, 2001b, pp. 87-95.

¹⁷⁰ *Vid.* WATTERS, 2011, pp. 32-43.

¹⁷¹ *Vid.* MATA Y MARTÍN, 2010, pp. 199-220.

¹⁷² *Cfr.* FERNÁNDEZ TERUELO, 2007, p. 159 y 2011, p. 234; VELASCO SAN MARTÍN, 2012, p. 75.

¹⁷³ *Vid.* ATTA-ASAMOAH, 2009, pp. 106-114.

¹⁷⁴ NIETO MARTÍN, 2020, pp. 5 y 6.

extranjero o blanqueo de los beneficios derivados del tráfico prohibido de hormonas y esteroides¹⁷⁵, entre otros casos¹⁷⁶.

Recientemente, con la pandemia de la COVID-19 se han incrementado los “ciberdelitos”, especialmente las estafas de productos médicos necesarios para combatirla y otras estafas *online*¹⁷⁷, hasta se ha apreciado un aumento del 377% respecto a la suplantación de identidad digital en algún país¹⁷⁸, porque los criminales tienen que buscar a sus víctimas en el ciberespacio al no encontrarlas ya en la calle, y los gobiernos tienen que distribuir enormes sumas de dinero para hacer frente a la pandemia con procedimientos rápidos y flexibles “que implican un gran riesgo de corrupción”¹⁷⁹, aunque fuese necesario relajar los controles para gestionar miles de expedientes¹⁸⁰. La mayoría de los beneficios de estos delitos se blanquean¹⁸¹. Así, en abril de 2022 la fiscalía anticorrupción se querelló, por estafa, falsedad y blanqueo, contra el hermano del Duque de Feria y un amigo suyo por cobrar una comisión de casi seis millones de euros en la venta de material defectuoso (guantes, tests rápidos y mascarillas) al Ayuntamiento de Madrid, que gastaron en coches de lujo, un yate y un piso en Pozuelo¹⁸². También aumentaron con la COVID-19 las ofertas de trabajo a potenciales blanqueadores, dolosos o imprudentes, mediante correos electrónicos que prometen un fácil trabajo en casa facilitando una cuenta bancaria para hacer transferencias o ayudando a supuestas asociaciones filantrópicas, huérfanas de países del tercer mundo o desamparadas viudas millonarias a administrar su dinero¹⁸³.

En tercer lugar, el documento del GAFI de 2010 abordó los pagos con teléfonos móviles, también regulados y supervisados en la mayoría de las naciones, aunque no en todas, con proveedores en 16 de los 37 países analizados¹⁸⁴ en ese momento. Igualmente, los servicios de pagos con móviles estaban experimentando un incremento constante, de manera que en 2015 se preveía que 1.400 millones de personas utilizarían para enviar dinero sus teléfonos móviles¹⁸⁵, previsiones que en 2020 se habían duplicado¹⁸⁶. Sin embargo, hasta entonces únicamente se habían detectado en este sector tres casos que podrían estar relacionados con el blanqueo, dos en Filipinas, vinculados a estafas, y uno en las Islas Caimán, sobre venta de créditos telefónicos robados, bien sea debido a que el volumen y valor de las transacciones todavía era muy pequeño, o bien por los bajos límites máximos de operaciones admitidas o

¹⁷⁵ Cfr. FATF, 2010, pp. 38-40, casos 6 a 12.

¹⁷⁶ Vid. FATF, 2010, p. 43, casos 25 a 27, pp. 44 y 45, casos 30 a 33; SOUZA, 2012, pp. 78-87.

¹⁷⁷ Cfr. INTERPOL, 2020, pp. 14-16.

¹⁷⁸ Cfr. POSADA MAYA, 2022, p. 70.

¹⁷⁹ GAFILAT, 2020, p. 3.

¹⁸⁰ Cfr. NIETO MARTÍN, 2020, p. 5.

¹⁸¹ Cfr. ABEL SOUTO, 2021e, p. 24.

¹⁸² Cfr. PEINADO/VIEJO, 2022.

¹⁸³ Cfr. ABEL SOUTO, 2021e, p. 24.

¹⁸⁴ Cfr. FATF, 2010, pp. 8 y 10, §§9 y 23.

¹⁸⁵ Cfr. FATF, 2010, p. 18, §§51 y 52 y nota 29.

¹⁸⁶ Vid. <http://www.arketfinder.thinkwi-thgoogle.com> (septiembre de 2022).

tal vez porque los proveedores y las fuerzas del orden público no estaban familiarizados con la tecnología para descubrir sus empleos abusivos o por el poco éxito del negocio, en aquel momento, para los proveedores, dado su escaso margen de beneficios y las necesidades de conseguir un gran número de clientes para obtener ganancias y de superar tanto obstáculos tecnológicos como de seguridad con el fin de ganar su confianza o debido a las regulaciones prudenciales de la materia y las normativas antiblanqueo¹⁸⁷. Sin embargo, la COVID-19 ha afectado en muchos países al control total de la población mediante los teléfonos móviles para vigilar las prohibiciones de movimientos y aproximación, un control total que también pretende utilizarse en las investigaciones sobre blanqueo para lograr mayor eficacia. No obstante, el control total puede llevarnos al mundo de las telepantallas orwellianas, a un futuro que ORWELL describió en su obra *1984*, de “una bota aplastando, incesantemente, el rostro humano”¹⁸⁸.

Posteriormente, las nuevas recomendaciones revisadas del GAFI, que se presentaron el 16 de febrero de 2012, hicieron referencia, en la 15ª, a que los países y las entidades financieras deberían identificar y evaluar los riesgos que para el blanqueo de dinero entrañan las nuevas tecnologías y también se ocupaba, en la 16ª, de las transferencias electrónicas y la identificación tanto de sus ordenantes como beneficiarios¹⁸⁹, recomendación sobre la que existe una nota interpretativa en la que se admite la fijación por los países de umbrales mínimos no superiores a 1.000 euros para relajar las obligaciones informativas, que se incrementan en el caso de transferencias cualificadas al exceder tales límites¹⁹⁰. Precisamente, para atenuar las exigencias identificativas, durante la elaboración de recomendación 16ª, se había sustituido el término “plena”, que calificaba a la información, por “exigida” y en las transferencias cualificadas por su cuantía los requisitos relativos a la dirección del ordenante, el número nacional de identidad, el número de identificación del cliente y la fecha y lugar de nacimiento se habían transformado en alternativos mediante la conjunción disyuntiva “o”¹⁹¹.

Después, en junio de 2013 el GAFI presentó una guía con un enfoque basado en el riesgo para las tarjetas de prepago, los pagos con móviles y los servicios de pago en *internet*¹⁹², en junio de 2014 elaboró otro informe sobre monedas virtuales¹⁹³, en junio de 2015 publicó unas directrices para un enfoque basado en el riesgo respecto

¹⁸⁷ Cfr. FATF, 2010, p. 10, §23 y nota 5, p. 18, §52, p. 19, nota 31, p. 26, §80, p. 37, §123 y p. 40, casos 13 a 15.

¹⁸⁸ Cfr. ABEL SOUTO, 2021e, p. 41.

¹⁸⁹ Cfr. FATF, 2012, p. 17.

¹⁹⁰ Vid. FATF, 2012, pp. 71-76.

¹⁹¹ Cfr. “Las nuevas recomendaciones del GAFI: presentación”, en <http://www.controlcapital.net/noticia/991>, 27 de febrero de 2012, p. 2.

¹⁹² Vid. FATF (2013), *Guidance for a risk-based approach. Prepaid cards, mobile payments and internet-based payment services, june*, en <http://www.fatf.gafi.org> (septiembre de 2022).

¹⁹³ Vid. FATF (2014), *Report. Virtual currencies. Key definitions and potential AML/CTF risks, june*, en <http://www.fatf.gafi.org> (septiembre de 2022).

a las monedas virtuales¹⁹⁴, en octubre de 2018 modificó la recomendación 15^a para aclarar cómo se aplican sus estándares a las actividades u operaciones con activos virtuales¹⁹⁵ y en junio de 2019 aprobó una nota interpretativa a la recomendación 15^a¹⁹⁶, para que las empresas que operan con criptomonedas recopilen y compartan datos de sus clientes en las operaciones superiores a 1.000 euros o dólares, con lo que surgen preocupaciones sobre si la tecnología *blockchain*, calificada de “anónima, segura, sin intermediarios, transparente, accesible”¹⁹⁷ y descentralizada, al sustituir la autoridad central por una red de ordenadores¹⁹⁸, tendrá que reestructurarse o si se incrementarán los costes de las criptomonedas¹⁹⁹ con esta traslación de deberes públicos a los particulares²⁰⁰, la cual también se da en el uso de “alertadores”²⁰¹ o denunciadores. Finalmente, en junio de 2021 se actualizó la nota interpretativa a la recomendación 15^a para aclarar que las nuevas obligaciones sobre evaluación y mitigación de riesgos de blanqueo también se aplican a los proveedores de servicios activos virtuales²⁰².

En esta línea la Directiva 2018/843 amplía el ámbito de aplicación de la Directiva 2015/849 para detectar actividades sospechosas a los proveedores de servicios de cambio de monedas virtuales por monedas fiduciarias y a los proveedores de servicios de custodia de monederos electrónicos²⁰³, incorporación de “nuevos sujetos obligados”²⁰⁴ que constituye “una medida fundamental”²⁰⁵ para combatir el blanqueo de dinero y la financiación del terrorismo.

Tanto las monedas virtuales, entre las que destaca el *bitcoin*²⁰⁶ aunque existen más de 6.000²⁰⁷, como los proveedores de servicios de custodia de monederos electrónicos se definen en los nuevos apartados 18 y 19 del artículo 3 de la Directiva, la cual advierte de que no deben confundirse²⁰⁸ las monedas virtuales con el dinero electrónico, ni con las monedas de juegos, ni con las locales²⁰⁹.

Es relativamente fácil regular el intercambio de criptomonedas en los proveedores

¹⁹⁴ Vid. FATF (2015a), *Guidance for a risk-based approach virtual currencies, june*, en <http://www.fatf.gafi.org> (septiembre de 2022).

¹⁹⁵ Vid. GAFI (2018), “Regulación de activos virtuales”, París, en <http://www.fatf.gafi.org> (septiembre de 2022).

¹⁹⁶ Cfr. FATF, 2013, pp. 4, 55 y 56.

¹⁹⁷ LLEDÓ BENITO, 2022, p. 29.

¹⁹⁸ *Ibidem*.

¹⁹⁹ Cfr. HUILLET, 2019, p.1.

²⁰⁰ Vid. ABEL SOUTO, 2021e, p. 40.

²⁰¹ OLAIZOLA NOGALES, 2022, p. 270.

²⁰² Cfr. FATF, 2022, pp. 76 y 138.

²⁰³ Cfr. considerando 8 y nuevas letras g) y h) del art. 2.

²⁰⁴ LORENZO SALGADO, 2020, p. 460.

²⁰⁵ *Ibidem*.

²⁰⁶ Vid. ARÁNGUEZ SÁNCHEZ, 2020, pp. 75-103; OPPEL, 2022, pp. 75-104.

²⁰⁷ Cfr. GÓMEZ INIESTA, 2021, p. 658.

²⁰⁸ Cfr. considerandos 10 y 11.

²⁰⁹ Cfr. LORENZO SALGADO, 2020, p. 461, nota 64.

que cambian monedas de curso legal por digitales o viceversa²¹⁰ para controlar al cliente en la vuelta al mundo real o al intentar escaparse de él; sin embargo, en los proveedores de custodia de monederos electrónicos únicamente se tiene en cuenta la puesta a disposición de un servidor para alojar las claves del usuario y custodiar los fondos almacenados en el monedero electrónico o “billeteras calientes”, pero no las “frías” o “programas de *hardware* o *software*, que permiten al usuario almacenar sus claves fuera de línea o con aplicaciones descargables”²¹¹, con lo que los intercambios de virtual a virtual, que suponen un evidente riesgo para el blanqueo, quedan, de momento, al margen de la normativa europea²¹².

De otro lado, la Directiva no se aplica a los proveedores de activos virtuales, criptoactivos o *tokens*, que no son monedas virtuales²¹³, de manera que permite “nuevas oportunidades para el blanqueo de ganancias con posible financiación de actividades ilícitas”²¹⁴, por lo que debería ampliarse, según recomendó el GAFI, a los activos virtuales²¹⁵ para abarcar la participación y promoción de ofertas iniciales de moneda, los intercambios “entre activos virtuales y monedas nacionales como actividad del mercado primario”²¹⁶ y entre criptomonedas o *tokens* como actividad del mercado secundario y la transferencia, liquidación, custodia o administración de activos virtuales²¹⁷.

Ciertamente el legislador español podría haber ido más allá del mínimo exigido por la Directiva 2018/843 para alcanzar los *tokens* de utilidad, que permiten el acceso a un producto, o de inversión, que habilitan la propiedad²¹⁸, siguiendo al GAFI, en su noción de activos virtuales como “representación digital de valor que puede ser negociado o transferido digitalmente y que puede utilizarse como medio de pago o de inversión”²¹⁹, pero ha perdido su oportunidad al mostrarse secuaz del legislador europeo en la modificación de la Ley 10/2010 sobre prevención del blanqueo²²⁰ operada por el Real decreto-ley 7/2021, de 27 de abril²²¹, tanto en la definición de moneda virtual o “representación digital de valor no emitida ni garantizada por un banco

²¹⁰ Cfr. GÓMEZ INIESTA, 2021, p. 679.

²¹¹ *Ibidem*.

²¹² Cfr. GÓMEZ INIESTA, 2021, p. 679.

²¹³ Cfr. LORENZO SALGADO, 2020, p. 461.

²¹⁴ *Ibidem*.

²¹⁵ Vid. FATF (2019), *Guidance for a risk-based approach. Virtual assets and virtual asset service providers*, June, en <http://www.fatf-gafi.org>, pp. 1-57.

²¹⁶ GÓMEZ INIESTA, 2021, p. 683.

²¹⁷ *Ibidem*.

²¹⁸ GÓMEZ INIESTA, 2021, p. 674.

²¹⁹ GÓMEZ INIESTA, 2021, p. 675.

²²⁰ Vid. Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo, BOE nº 103, 29 de abril de 2010, pp. 37458-37499.

²²¹ Vid. Real decreto-ley 7/2021, de 27 de abril, de transposición de directivas de la Unión Europea en las materias de competencia, prevención del blanqueo de capitales, entidades de crédito, telecomunicaciones, medidas tributarias, prevención y reparación de daños medioambientales, desplazamiento de trabajadores en la prestación de servicios transnacionales y defensa de los consumidores, BOE nº 101, 28 de abril de 2021, apartado III, pp. 49752-49754, y art. 3, pp. 49788-49803.

central o autoridad pública, no necesariamente asociada a una moneda legalmente establecida y que no posee estatuto jurídico de moneda o dinero, pero que es aceptada como medio de cambio y puede ser transferida, almacenada o negociada electrónicamente”²²², como en el concepto de proveedores de servicios de custodia de monederos electrónicos o “personas físicas o entidades que prestan servicios de salvaguardia o custodia de claves criptográficas privadas en nombre de sus clientes para la tenencia, el almacenamiento o la transferencia de monedas virtuales”²²³, y entiende el cambio de moneda virtual por fiduciaria del siguiente modo: “la compra y venta de monedas virtuales mediante la entrega o recepción de euros o cualquier otra moneda extranjera de curso legal o dinero electrónico aceptado como medio de pago en el país en el que ha sido emitido”²²⁴.

También modifica el Real decreto-ley 7/2021, en el apartado 1 del artículo 2 de la Ley 10/2010 sobre prevención del blanqueo, las letras b), h), k), l), m) y r) y añade la z), que se refiere a “los proveedores de servicios de cambio de moneda virtual por moneda fiduciaria y de custodia de monederos electrónicos”, con lo que el legislador, además de reformar el apartado 4 del artículo 2, agota todas las letras del abecedario en el amplísimo catálogo de sujetos obligados, a los que al día siguiente, mediante la Ley orgánica 6/2021, de 28 de abril, convierte en sujetos activos de un nuevo tipo agravado²²⁵.

Por último, el Real decreto-ley 7/2021 incorpora una disposición adicional segunda a la Ley 10/2010, la cual “crea”²²⁶ el registro en el que deben inscribirse los proveedores de servicios de cambio de moneda virtual por moneda fiduciaria y de custodia de monederos electrónicos.

Con todo, la Directiva 2018/843 es consciente de su debilidad, pues “no evita el anonimato”²²⁷, al mantenerse “en gran parte del entorno de la moneda virtual”²²⁸, ya

²²² Apartado 5 del art. 1 de la Ley 10/2010, incorporado por el Real decreto-ley 7/2021, cuya redacción únicamente se diferencia del apartado 18 del art. 3 de la Directiva en el irrelevante singular “moneda virtual”, en el uso de la disyuntiva “o” antes de “autoridad”, la posición del adverbio “legalmente”, el añadido de una cópula y un artículo en “y que no posee el estatuto jurídico”, el cambio de “pero aceptada por personas físicas o jurídicas” por “que es aceptada”, la sustitución de tres infinitivos por participios y la utilización del adverbio “electrónicamente” en vez de la locución “por medios electrónicos”. Ninguno de estos cambios estilísticos, meramente formales, altera el contenido de la definición.

²²³ Apartado 7 del art. 1 de la Ley 10/2010, incorporado por el Real decreto-ley 7/2021. En este caso el legislador español, tal vez por aparentar que ha hecho algún trabajo en la transposición, cambia el singular “proveedor”, del apartado 19 del art. 3 de la Directiva, por el plural “proveedores”, con las obligadas concordancias del sustantivo “entidades”, a las que añade alternativamente las personas físicas, y el verbo “prestan”, suprime una coma y a la “salvaguardia” le añade “o custodia”.

²²⁴ Art. 1, apartado 7, de la Ley 10/2010, incorporado por el Real decreto-ley 7/2021.

²²⁵ Vid. ABEL SOUTO, 2022a, pp. 975-988, y 2022b, pp. 17-25.

²²⁶ FERNÁNDEZ TERUELO, 2021, p. 779.

²²⁷ LORENZO SALGADO, 2020, p. 460.

²²⁸ NAVARRO CARDOSO, 2019, p. 88.

que “los usuarios pueden llevar a cabo transacciones al margen”²²⁹ de los proveedores de servicios con intermediarios con servidores fuera de la Unión Europea²³⁰, por lo que las Unidades de Inteligencia Financiera, como el Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias²³¹ en el caso español²³², “deben poder obtener informaciones que les permitan asociar las direcciones de las monedas virtuales a la identidad del propietario de la moneda virtual”²³³ y tiene que analizarse la posibilidad de que, voluntariamente, los usuarios efectúen “una autodeclaración a las autoridades”²³⁴.

En cuanto a la detección y vigilancia de movimientos transfronterizos de dinero en efectivo²³⁵, pese a ser una de las más viejas técnicas de blanqueo, incluso continúa incrementando su volumen²³⁶ de forma significativa²³⁷. Así, en el estudio de un entramado mafioso los bienes delictivos llegaban a Italia mediante una gran red de individuos que viajaban desde Rusia con dinero en efectivo²³⁸. Aunque el transporte físico de bienes constituye un método tradicional de blanqueo²³⁹, que no necesita la intervención de terceros²⁴⁰, en el que el dinero en efectivo atraviesa las fronteras por avión, barco o coche destruyendo el vínculo entre la actividad criminal previa y la introducción de los fondos en el circuito financiero²⁴¹, también proliferan las nuevas “mulas” captadas por los blanqueadores a través de la red y que actúan en ella, a veces engañadas por falsas empresas que ofrecen altos ingresos a cambio de poco tiempo y esfuerzo; únicamente se les pide proporcionar los datos bancarios al contratante-blanqueador —que abonará en la cuenta dinero de origen delictivo con la autorización de la “mula”, porque retiene una comisión, generalmente en torno al 10% de la cantidad ingresada— y remitir el dinero a otra cuenta facilitada por el

²²⁹ Considerando 9.

²³⁰ FERNÁNDEZ GARCÍA, 2021, p. 161.

²³¹ Sobre el SEPBLAC y su máxima calificación internacional *vid.* LORENZO SALGADO, 2020, pp. 460 y 461, nota 63. *Vid.* también FATF, *Consolidated assessment ratings*, en <http://www.fatf-gafi.org> (febrero de 2021).

²³² En torno a la eficacia del sistema español de lucha contra el blanqueo *vid.* ABEL SOUTO, 2022c, pp. 241-266.

²³³ Considerando 9.

²³⁴ *Ibidem.*

²³⁵ *Cfr.* recomendación 23^a, FATF-I, p. 20; recomendación 22^a, FATF-VII, 1996, anexo 1; recomendación 32^a, FATF, 2012, p. 25.

²³⁶ *Cfr.* FATF (2015b), *Report. Money laundering through the physical transportation of cash, october*, en <http://www.fatf.gafi.org>, p. 3.

²³⁷ *Cfr.* FATF-VII, 1996, *annex 3, 1995-1996 Report on Money Laundering Typologies*, p. 5, §22. *Vid.* FATF-IX, 1998, *Report on Money Laundering Typologies*, p. 8, §33; *Annexes to the 1997-1998 FATF Report on Money Laundering Typologies, Selected cases of money laundering*, caso 3, pp. 21 y 22; FATF, 2010, pp. 46 y 47, §§132-136.

²³⁸ *Cfr.* VARESE, 2012, p. 242.

²³⁹ *Cfr.* BLANCO CORDERO, 2015, p. 73.

²⁴⁰ *Cfr.* CHINCHILLA, 2011, p. 149.

²⁴¹ *Cfr.* COLLADO MEDINA, 2010, p. 485; JURADO/GARCÍA, 2011, p. 167.

blanqueador²⁴². Estas “mulas de dinero”, reclutadas por correo electrónico con oportunidades de trabajo en casa, a veces el único pago que reciben es la persecución penal por blanqueo²⁴³, ofertas laborales que se han incrementado durante la pandemia de la COVID-19²⁴⁴.

Asimismo, el GAFI en su informe sobre uso de los nuevos métodos de pago relata el caso de dos acusados en Estados Unidos por blanqueo de dinero procedente de la droga que, ayudados de familiares y amigos, llegaron a abrir 380 cuentas en seis estados, realizaron múltiples depósitos entre 500 y 1.500 dólares e incluso ingresos de más de 100.000 dólares en 112 cuentas bancarias en un solo día. De cada cuenta obtuvieron dos tarjetas, una la guardaron y la otra fue remitida por correo a Colombia, país en el que los fondos fueron retirados a través de los cajeros automáticos²⁴⁵.

También el GAFI recomendó reducir las transferencias en efectivo mediante técnicas de gestión de fondos modernas y seguras, con inclusión de un aumento del uso de cheques, tarjetas de pago, domiciliación de nóminas y registro automático de operaciones con títulos²⁴⁶. Actualmente la recomendación 32^a exhorta a los países a asegurar que sus autoridades puedan impedir o restringir los movimientos de dinero en efectivo ante sospechas de blanqueo²⁴⁷ y la Convención de Naciones Unidas contra la corrupción dispone que los “Estados Parte considerarán la posibilidad de aplicar medidas viables para detectar y vigilar el movimiento transfronterizo de efectivo”²⁴⁸, pero “sin restringir en modo alguno la circulación de capitales lícitos”²⁴⁹. También la Directiva 2018/843 advierte de que “las medidas tomadas deben ser proporcionales a los riesgos²⁵⁰ y en el informe que la Comisión debía presentar como muy tarde el 11 de enero de 2022 se requería una evaluación del respeto a los derechos y principios fundamentales de la Carta de Derechos Fundamentales en la aplicación de la Directiva 2018/843²⁵¹.

En esta línea se ha dicho que el dinero en efectivo es el medio común de intercambio en las transacciones criminales²⁵² y en sentido similar el gobierno español, aunque pensando más en finalidades recaudatorias, aprobó en el consejo de ministros de 22 de junio de 2012 un proyecto de ley de lucha contra el fraude fiscal que, teniendo en cuenta la experiencia legislativa de otros países comunitarios, limitó a 2.500 euros

²⁴² Cfr. CHINCHILLA, 2011, pp. 139, 153 y 154.

²⁴³ Cfr. CLOUGH, 2010, pp. 187 y 188.

²⁴⁴ Cfr. ABEL SOUTO, 2021e, p. 24.

²⁴⁵ Cfr. FATF, 2010, p. 46, §132.

²⁴⁶ Cfr. recomendación 25^a, FATF-I, p. 21; recomendación 24^a, FATF-VII, 1996, anexo 1.

²⁴⁷ Cfr. FATF, 2012, p. 25 y nota interpretativa a la recomendación 32^a, pp. 99-102.

²⁴⁸ *Instrumento de ratificación de la Convención de las Naciones Unidas contra la corrupción, hecha en Nueva York el 31 de octubre de 2003*, en BOE, nº 171, de 19 de julio de 2006, p. 27137, art. 14.2.

²⁴⁹ *Ibidem*.

²⁵⁰ Considerando 2.

²⁵¹ Cfr. letra g) del art. 65.1.

²⁵² Cfr. JURADO/GARCÍA, 2011, p. 172.

los pagos en efectivo cuando en las operaciones participen empresarios o profesionales²⁵³, que se sumó al plan de control de billetes de alta denominación, de 500 y 200 euros²⁵⁴. Sobre estas limitaciones de pagos en efectivo el Consejo General del Poder Judicial puso el acento en su trasfondo tributario²⁵⁵. En julio de 2021 en España se modificó el art. 7 de la Ley 7/2012 para reducir el límite de pagos en efectivo a 1.000 euros²⁵⁶, como en Francia y en Italia, y en la India el gobierno prohibió en 2016 los billetes de 500 y 1.000 rupias. También con la COVID-19 el uso de dinero en efectivo es evitado y se prefieren los medios de pago electrónicos, para reducir el posible contagio por el contacto físico con el dinero²⁵⁷. Sin embargo, tras el aparente dogma del “carácter criminógeno del dinero en efectivo” se esconde un programa que supera la lucha contra la delincuencia, permite el control del ámbito privado y margina todavía más a los que ganan menos²⁵⁸. Amén de que, al huir de la Caribdis del papel moneda nos toparemos con la Escila del “dinero electrónico”, pues las nuevas tecnologías de pago, según se ha visto, no se hallan exentas de riesgos que pueden frustrar la prevención y represión del blanqueo de dinero.

IV. Conclusiones

En la medida en que se define "epidemia" como un "mal o daño que se propaga" y en tanto que "pandemia" es una epidemia "que se extiende a muchos países", por ello el blanqueo de dinero y la COVID-19 son dos pandemias. La economía mundial se ha visto muy afectada por la COVID-19, que genera una gran destrucción de puestos de trabajo y una enorme disminución en el intercambio de productos, bienes y servicios, desembocando en una profunda crisis económica. En el mismo sentido, el blanqueo de dinero incuestionablemente lesiona o pone en peligro el orden socioeconómico estatal e internacional. Tanto el blanqueo de dinero como la COVID-19 son fenómenos globales que requieren respuestas globales, por lo que las iniciativas estatales aisladas están condenadas al fracaso. Como en la COVID-19 es preferible evitar el contagio que curar la enfermedad, así también es mejor prevenir el blanqueo de dinero que sancionarlo, por lo que los distintos estados aprueban, además de normas penales, medidas administrativas de prevención. INTERPOL advierte que la pandemia de la COVID-19 ha incrementado la ciberdelincuencia, especialmente los

²⁵³ Cfr. “Aprobadas las medidas para la lucha contra el fraude fiscal”, en <http://www.lamoncloa.es/ConsejodeMinistros>, viernes, 22 de junio de 2012.

²⁵⁴ Cfr. BORE, 2012, p. 34.

²⁵⁵ Cfr. CGPJ, 2012, pp. 4 y 5.

²⁵⁶ Cfr. Ley 11/2021, de 9 de julio, de medidas de prevención y lucha contra el fraude fiscal, la transposición de la Directiva UE/2016/1164, del Consejo, de 12 de julio de 2016, por la que se establecen normas contra las prácticas de elusión fiscal que inciden directamente en el funcionamiento del mercado interior, de modificación de diversas normas tributarias y en materia de regulación del juego, en BOE nº 164, de 10 de julio de 2021, p. 82657, art. 18.

²⁵⁷ Cfr. ABEL SOUTO, 2021e, p. 41.

²⁵⁸ Cfr. PIETH, 1992, p. 27. Así también cfr. DIETZI, 1992, p. 90; HOLZINGER, 1994, pp. 19 y 20.

fraudes de productos médicos necesarios para combatirla u otros fraudes online, y según GAFILAT los gobiernos deben destinar grandes sumas de dinero para enfrentar la pandemia con procedimientos rápidos y flexibles “lo que se traduce en mayor riesgo de corrupción”. La mayoría de las ganancias de estos delitos se blanquea. También aumentaron con la COVID-19 las ofertas de trabajo a potenciales blanqueadores de dinero a través de correos electrónicos que prometen trabajo fácil en casa facilitando una cuenta bancaria para realizar transferencias o ayudando a supuestas asociaciones filantrópicas, huérfanos africanos o viudas millonarias a gestionar su patrimonio.

Evidentemente hay que sancionar el blanqueo de dinero. Sin embargo, en la persecución y castigo del blanqueo se está incurriendo en diversos excesos. En este sentido, la Asociación Internacional de Criminología hizo un llamamiento urgente a los gobiernos para que reduzcan el hacinamiento en las cárceles, debido al “riesgo inminente de contagio”, sobre todo teniendo en cuenta que un alto porcentaje de los presos todavía no han sido condenados, un dato muy importante en relación con el blanqueo por la evidente desproporción, mayor que en otros delitos, entre los presos provisionales y los que finalmente son condenados.

Por otra parte, la Directiva 2018/1673 obliga a los estados miembros a garantizar que los nuevos riesgos de las monedas virtuales se aborden adecuadamente. Las Directivas 2015/849 y 2018/843 sobre blanqueo de dinero exigen continuas adaptaciones del marco legal para responder a las amenazas del uso de nuevas tecnologías en el blanqueo, la Comisión presentó en 2021 un ambicioso paquete con cuatro propuestas legislativas contra el blanqueo que tiene en cuenta los nuevos retos relacionados con la innovación tecnológica y la Ley orgánica 9/2022, de 28 de julio, que traspone la Directiva 2019/1153, contempla un acceso directo de las autoridades competentes al Fichero de Titularidades Financieras sin autorización judicial ni del ministerio fiscal. La Directiva 2018/843 amplía el alcance de la Directiva 2015/849 a proveedores de servicios de cambio de monedas virtuales por monedas fiduciarias, así como a los proveedores de servicios de monederos electrónicos y el Real decreto-ley 7/2021, de 27 de abril, los convierte en sujetos obligados a los que, al día siguiente, mediante la Ley orgánica 6/2021, de 28 de abril, se eleva a sujetos activos de un nuevo tipo agravado.

V. Reflexión final

Sin duda, los nuevos sistemas de pago facilitan la actividad criminal de los blanqueadores. Estos sistemas son mejores que el dinero en efectivo para mover grandes sumas de dinero, las relaciones comerciales no presenciales favorecen el uso de testarferos y falsas identidades, la ausencia de riesgo crediticio, ya que suele haber un

prepago, desalienta a los proveedores de servicios a obtener una información completa y precisa del cliente, y la naturaleza de las relaciones comerciales y la velocidad de las transacciones dificultan el control de los bienes o su congelación. Sin embargo, el desarrollo de las tecnologías, incluido internet, conlleva indudables ventajas e incluso prevé, a través de recursos *online*, la verificación de la identidad o el cumplimiento de otros deberes de vigilancia para la prevención del blanqueo. También con la COVID-19 se evita el uso de efectivo y se da preferencia a los medios de pago electrónicos, para reducir el posible contagio a través del contacto físico con el dinero. En el mismo sentido, incluso se pretende eliminar el efectivo para evitar el blanqueo, pero detrás del aparente dogma del carácter criminógeno del efectivo se esconde un programa que excede la lucha contra el crimen, margina todavía más a quienes ganan menos y permite el control de la privacidad. Por último, pero no menos importante, la COVID-19 también ha afectado al control total de la población a través de los teléfonos móviles, para vigilar las prohibiciones de circulación o acercamiento, un control total que se pretende utilizar también en las investigaciones contra el blanqueo para lograr una mayor eficacia. Sin embargo, el control total puede llevarnos al mundo de las telepantallas orwellianas, a un futuro, que Orwell describió en su obra *1984*, de "una bota aplastando el rostro humano, incesantemente".

En definitiva, como se pone de manifiesto en la agenda estratégica de la Unión Europea²⁵⁹ hasta 2024, aunque en los años venideros “la transformación digital se seguirá acelerando y tendrá repercusiones de gran alcance”²⁶⁰, la política europea debe continuar reflejando los valores de nuestra sociedad, fomentando la inclusión y respetando la forma de vida europea²⁶¹.

Bibliografía

- ABADÍAS SELMA, A.; FERNÁNDEZ ALBESA, N.; LEAL RUIZ, R. (2021), *Ciberdelincuencia*, A Coruña.
- ABEL SOUTO, M. (2002), *El blanqueo de dinero en la normativa internacional: especial referencia a los aspectos penales*, Santiago de Compostela.
- ABEL SOUTO, M. (2005), *El blanqueo de dinero en el Código penal español*, Barcelona.
- ABEL SOUTO, M. (2013), “Volumen mundial del blanqueo de dinero, evolución del delito en España y jurisprudencia reciente sobre las últimas modificaciones del Código penal”, *Revista General de Derecho Penal*, nº 20, pp. 1-33.
- ABEL SOUTO, M. (2014a), “El blanqueo de dinero como innovador instrumento de control económico y social”, *Revista Cuatrimestral Europea sobre Prevención y Represión del Blanqueo de Dinero*, nº 1, pp. 11-65.

²⁵⁹ Sobre la construcción de un Derecho penal europeo *vid.* FERRÉ OLIVÉ, 2021, pp. 781-804 y 971-973; LENZO SALGADO, 2021, pp. 813-842, 977 y 978.

²⁶⁰ CONSEJO EUROPEO, 2019, p. 4.

²⁶¹ *Ibidem*.

- ABEL SOUTO, M. (2014b), “Jurisprudencia penal reciente sobre el blanqueo de dinero, volumen del fenómeno y evolución del delito en España”, en Abel Souto, M./Sánchez Stewart, N. (coords.): *IV congreso internacional sobre prevención y represión del blanqueo de dinero*, Valencia, pp. 137-201 y 309-317.
- ABEL SOUTO, M. (2020), *Normativa internacional sobre el blanqueo de dinero y su recepción en el Ordenamiento penal español*, Montevideo/Buenos Aires/Madrid.
- ABEL SOUTO, M. (2021a), “Tres décadas de expansión en el castigo del blanqueo de dinero”, en Abel Souto, M.; Brage Cendán, S.B.; Guinarte Cabada, G.; Martínez-Buján Pérez, C.; Vázquez-Portomeñe Seijas, F. (coords.): *Estudios penales en homenaje al profesor José Manuel Lorenzo Salgado*, Valencia, pp. 27-39.
- ABEL SOUTO, M. (2021b), “Los nuevos tipos agravados de blanqueo de dinero introducidos por la Ley orgánica 6/2021, de 28 de abril”, en Santana Vega, D.M.; Fernández Bautista, S.; Cardenal Montraveta, S.; Carpio Briz, D.I.; Castellví Monserrat, C. (dirs.): *Una perspectiva global del Derecho penal. Libro homenaje al profesor dr. Joan J. Queralt Jiménez*, Barcelona, pp. 401-412.
- ABEL SOUTO, M. (2021c), “Blanqueo de dinero, responsabilidad criminal de las personas jurídicas y directivas de 2018”, en Sanz Hermida, A.M. (dir.): *La justicia penal del siglo XXI ante el desafío del blanqueo de dinero. 21st century criminal justice facing the challenge of money laundering*, Valencia, pp. 41-75. Existe una versión inglesa de este artículo bajo el título “*Money laundering, criminal responsibility of legal persons and 2018 directives*”, en pp. 301-334 y en *Journal of Applied Business & Economics*, vol. 22, 2020, pp. 205-222.
- ABEL SOUTO, M. (2021d), “Algunas discordancias legislativas sobre la responsabilidad criminal de las personas jurídicas en el Código penal español”, *Revista General de Derecho Penal*, nº 35, pp. 1-62.
- ABEL SOUTO, M. (2021e), “*Money laundering, COVID-19 and new technologies*”, en Arlacchi, P.; Sidoti, F. (eds.): *Financial crime, money laundering and asset recovery. Global trends, theoretical issues and case studies, International Forum on Crime and Criminal Law*, Craiova, pp. 23-50.
- ABEL SOUTO, M. (2022a), “El nuevo tipo agravado de blanqueo en el ejercicio profesional de los obligados por la normativa de prevención, incorporado por la Ley orgánica 6/2021, y los proveedores de servicios de cambio de moneda virtual y de custodia de monederos electrónicos”, en Gómez Martín, V.; Bolea Bardon, C.; Gallego Soler, J.-I.; Hortal Ibarra, J.C.; Joshi Jubert, U. (dirs.): *Un modelo integral de Derecho penal. Libro homenaje a la profesora Mirentxu Corcoy Bidasolo*, Madrid, pp. 975-988, también en *Revista Penal México*, nº 20, 2022b, pp. 17-25.
- ABEL SOUTO, M. (2022c), “*FATF’s most compliant countries. Spain’s technical compliance and effectiveness: lessons for least compliant jurisdictions*”, *De Legibus*, pp. 241-266.
- ANGELINI, D.; GIBSON, S. (2007), “*Organized crime and technology*”, *Journal of Security Education*, vol. 2, nº 4, pp. 65-73.
- ARÁNGUEZ SÁNCHEZ, C. (2020), “El bitcoin como instrumento y objeto de delitos”, *Cuadernos de Política Criminal*, II, nº 131, septiembre, pp. 75-103.
- ATTA-ASAMOAH, A. (2009), “*Understanding the west african cyber crime process*”, *African Security Review*, vol. 18, nº 4, december, pp. 106-114.
- BALDWIN, Jr.; FLETCHER, N. (2004), “*The financing of terror in the age of the internet: wilful blindness, greed or a political statement?*”, *Journal of Money Laundering Control*, vol. 8, nº 2, diciembre, pp. 125-158.
- BLANCO, R.; MAYORDOMO, S.; MENÉNDEZ, A.; MULINO, M. (2021), “El impacto de la crisis del COVID-19 sobre la vulnerabilidad financiera de las empresas españolas”, *Documentos Ocasionales* nº 2119, Banco de España, pp. 1-43.
- BLANCO CORDERO, I. (2015), *El delito de blanqueo de capitales*, 4ª ed., Cizur Menor.

- BLUM, J.A.; LEVI, M.; NAYLOR, R.T.; WILLIAMS, P. (1999), *Refugios financieros, secreto bancario y blanqueo de dinero*, Naciones Unidas, Nueva York.
- BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM (2019), *Report to the Congress on Government-Administered, General-Use Prepaid Cards*, Washington.
- BORE, N. (2012), “El gobierno no aclara cómo controlará el pago en efectivo”, *La Voz de Galicia*, viernes, 13 de abril.
- CANCIO MELIÁ, M.; PANTALEÓN DÍAZ, M. (2022), “¿Responsabilidad penal por contagios individuales de coronavirus? Algunos problemas de imputación”, en Gómez Martín, V.; Bolea Bardon, C.; Gallego Soler, J.-I.; Hortal Ibarra, J.C.; Joshi Jubert, U. (dirs.): *Un modelo integral de Derecho penal. Libro homenaje a la profesora Mirentxu Corcoy Bidasolo*, Madrid, pp. 489-502.
- CERDEIRA BRAVO DE MANSILLA, G. (2021), *Aspectos jurídicos del coronavirus*, 2ª ed., Madrid.
- CLOUGH, J. (2010), *Principles of cybercrime*, Cambridge.
- COMISIÓN EUROPEA (2021), “Lucha contra los delitos financieros: la Comisión revisa las normas contra el blanqueo de capitales y la financiación del terrorismo”, Bruselas, 20 de julio, pp. 1-3.
- CONSEJO EUROPEO (2019), *Una nueva agenda estratégica 2019-2024*, Bruselas.
- CONSEJO EUROPEO (2022), “Nueva autoridad de la UE para la lucha contra el blanqueo de capitales: el Consejo acuerda su posición de negociación”, 29 de junio, en <https://www.consiliumeuropa.eu>.
- CONSEJO GENERAL DEL PODER JUDICIAL (2012), *Informe al anteproyecto de Ley de modificación de la normativa tributaria y presupuestaria y de adecuación de la normativa financiera para la intensificación de las actuaciones de prevención y lucha contra el fraude*, 31 de mayo, en <http://www.poderjudicial.es>.
- DIETZI, H. (1992), “*Der Bankangestellte als eidgenössisch konzessionierter Sherlock Holmes? Der Kampf gegen die Geldwäscherei aus der Optik des Ersten Rechtskonsulenten einer Grossbank*”, en Pieth, M., *Bekämpfung der Geldwäscherei...*, cit., pp. 67-96.
- Directiva (UE) 2015/849 del Parlamento Europeo y del Consejo, de 20 de mayo de 2015, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo y por la que se modifica el Reglamento (UE) nº 648/2012 del Parlamento Europeo y del Consejo y se derogan la Directiva 2005/60/CE del Parlamento Europeo y del Consejo y la Directiva 2006/70/CE de la Comisión, en Diario Oficial de la Unión Europea*, L 141, 5 de junio de 2015, pp. 73-117.
- Directiva (UE) 2018/843 del Parlamento Europeo y del Consejo, de 30 de mayo de 2018, 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 modifican las Directivas 2009/138/CE y 2013/36/UE, en Diario Oficial de la Unión Europea*, L 156, 19 de junio de 2018, pp. 43-74.
- Directiva (UE) 2018/1673 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativa a la lucha contra el blanqueo de capitales mediante el Derecho penal, en Diario Oficial de la Unión Europea*, L 284, 12 de noviembre de 2018, pp. 22-30.
- Directiva (UE) 2019/1153 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, por la que se establecen normas destinadas a facilitar el uso de información financiera y de otro tipo para la prevención, detección, investigación o enjuiciamiento de infracciones penales y por la que se deroga la Decisión 2000/642/JAI del Consejo, en Diario Oficial de la Unión Europea*, L 186, 11 de julio de 2019, pp. 122-137.
- DONNA, S.A. (2021), “*Fintech y responsabilidad penal del compliance officer por omisión*”, *Derecho Penal Económico, COVID y sus consecuencias jurídico-económicas I*, pp. 197-238.
- DOUGLAS HEAVEN, W. (2020), “IA para perseguir el blanqueo de capitales en tiempos de

- coronavirus”, en <https://technologyreview.es>, pp. 1-5.
- FERNÁNDEZ GARCÍA, G. (2021), “Los riesgos de las nuevas tecnologías para el blanqueo y el necesario mantenimiento de las ventajas de los avances tecnológicos en la financiación alternativa y el emprendimiento social”, en Abel Souto, M.; Lorenzo Salgado, J.M.; Sánchez Stewart, N. (coords.): *VIII congreso internacional sobre prevención y represión del blanqueo de dinero*, Valencia, pp. 149-171.
- FERNÁNDEZ HERNÁNDEZ, A. (2022), “Orden público y COVID. Efectos derivados de la sentencia del Tribunal Constitucional núm. 148/2021, de 14 de julio de 2021”, en González Cussac, J.L.; Velásquez Velásquez, F., *op. cit.*, pp. 79-115.
- FERNÁNDEZ TERUELO, J.G. (2007), *Cibercrimen. Los delitos cometidos a través de internet*, Oviedo.
- FERNÁNDEZ TERUELO, J.G. (2011), *Derecho penal e internet*, Valladolid.
- FERNÁNDEZ TERUELO, J.G. (2020), “Prólogo”, en Fernández Villazón, L.A. (coord.): *Derecho y nuevas tecnologías*, Cizur Menor, pp. 27 y 28.
- FERNÁNDEZ TERUELO, J.G. (2021), “Evolución del Derecho penal económico europeo”, en Abel Souto, M.; Lorenzo Salgado, J.M.; Sánchez Stewart, N., *VIII congreso..., cit.*, pp. 767-779, 969 y 970.
- FERNÁNDEZ TERUELO, J.G. (2022), “El feminicida de pareja como sujeto inasequible a la amenaza penal: muerte diádica y comportamiento postdelictual”, en Fernández Teruelo, J.G.; García Amez, J.; Fernández-Rivera González, P. (dirs.): *Nuevas formas de prevención y respuesta jurídico-social frente a la violencia de género*, Cizur Menor, pp. 181-190.
- FERRÉ OLIVÉ, J.C. (2018), *Tratado de los delitos contra la hacienda pública y contra la seguridad social*, Valencia.
- FERRÉ OLIVÉ, J.C. (2021), “El *Corpus Iuris* de normas penales para la tutela de los intereses financieros de la Unión Europea. Desde el proyecto europeo hasta la actualidad”, en Abel Souto, M.; Lorenzo Salgado, J.M.; Sánchez Stewart, N., *VIII congreso..., cit.*, pp. 781-804 y 971-973.
- FILIPKOWSKI, W. (2008), “*Cyber laundering: an analysis of typology and techniques*”, en *International Journal of Criminal Justice Sciences*, vol. 3, nº 1, pp. 15-27.
- Financial Action Task Force on Money Laundering (FATF), Annual Report 1995-1996 (FATF-VII)*, en <http://www.oecd.org/fatf/annual95.htm>, anexo 1.
- FATF, Annex 1 to the Financial Action Task Force on Money Laundering, Annual Report 1996-1997 (FATF-VIII)*, en <http://www.oecd.org/fatf/rep96-97.htm>, *Report on typologies-Issues concerning new payment technologies*.
- FATF 1997-1998 (FATF-IX) Report on money laundering typologies*, en <http://www.oecd.org/fatf/fatfix.htm>.
- FATF (2006), *Report on new payment methods, 13 october*, en <http://www.fatf-gafi.org>.
- FATF (2008), *Money laundering & terrorist financing vulnerabilities of commercial websites and internet payment system, 18 june*, en <http://www.fatf-gafi.org>, pp. 1-39.
- FATF Report (2010), *Money laundering using new payment methods, october*, en <http://www.fatf-gafi.org>.
- FATF (2012), *International standards on combating money laundering and the financing of terrorism & proliferation. The FATF recommendations, february*, en <http://www.fatf-gafi.org>.
- FATF (2013), *Guidance for a risk-based approach. Prepaid cards, mobile payments and internet-based payment services, june*, en <http://www.fatf.gafi.org>.
- FATF (2014), *Report. Virtual currencies. Key definitions and potential AML/CTF risks, june*, en <http://www.fatf.gafi.org>.
- FATF (2015a), *Guidance for a risk-based approach virtual currencies, june*, en <http://www.fatf.gafi.org>.

- FATF (2015b), *Report. Money laundering through the physical transportation of cash, october*, en <http://www.fatf.gafi.org>.
- FATF (2019), *Guidance for a risk-based approach. Virtual assets and virtual asset service providers, june*, en <http://www.fatf-gafi.org>, pp. 1-57.
- FATF (2021), *Consolidated assessment ratings*, en <http://www.fatf-gafi.org> (febrero de 2021).
- FATF (2022), *International standards on combating money laundering and the financing of terrorism & proliferation. The FATF Recommendations, Updated march*, en <http://www.fatf.gafi.org>.
- FINKLEA, K.M. (2009), “Organized crime in the United States: trends and issues for congress”, *Journal of Current Issues in Crime, Law & Law Enforcement*, vol. 2, nº 1, pp. 9-40.
- FISHER, J. (2012), “The vulnerability of her majesty’s revenue & customs to penetration by criminal actors”, *Journal of Money Laundering Control*, vol. 15, nº 2, pp. 153-161.
- FUNDACIÓN ORANGE (2012), *eEspaña. Informe anual 2012 sobre el desarrollo de la sociedad de la información en España*, en www.fundacionorange.es.
- GAFI (2018), “Regulación de activos virtuales”, París, en <http://www.fatf.gafi.org>.
- GAFILAT (2020), *Statement on COVID-19 and its associated ML and FT risk, 8 april*, en <http://www.gafilat.org>.
- GALEANO, S. (2021), “El número de usuarios de internet en el mundo crece un 7’3% y alcanza los 4.600 millones (2021)”, en <http://www.marketing4ecommerce.net>.
- GAMERO CASADO, E. (2012), “El objeto de la Ley 18/2011 y su posición entre las normas relativas a las tecnologías de la información”, en el mismo autor; Valero Torrijos, J. (coords.): *Las tecnologías de la información y la comunicación en la Administración de Justicia. Análisis sistemático de la Ley 18/2011, de 5 de julio*, Cizur Menor, pp. 45-88.
- GLESS, S. (2012), “Strafverfolgung im Internet”, *Schweizerische Zeitschrift für Strafrecht*, vol. 130, nº 1, pp. 3-22.
- GÓMEZ INIESTA, D.J. (2020), “El uso de las tarjetas de prepago para el blanqueo y la financiación terrorista y la Directiva 843/2018”, en Abel Souto, M.; Lorenzo Salgado, J.M.; Sánchez Stewart, N. (coords.): *VII congreso sobre prevención y represión del blanqueo de dinero*, Valencia, pp. 295-330 y 541-543.
- GÓMEZ INIESTA, D.J. (2021), “El uso de las monedas virtuales y el dinero electrónico en el delito de blanqueo y la directiva 843/2018”, en Abel Souto, M.; Lorenzo Salgado, J.M.; Sánchez Stewart, N., *VIII congreso...*, *cit.*, pp. 651-685 y 959-962.
- GÓMEZ TOMILLO, M. (2006), *Responsabilidad penal y civil por delitos cometidos a través de internet. Especial consideración del caso de los proveedores de contenidos, servicios, acceso y enlaces*, 2ª ed., Cizur Menor.
- GONZÁLEZ CUSSAC, J.L. (2022), “Pandemia, desinformación y verdad en Derecho penal”, en González Cussac, J.L.; Velásquez Velásquez, F., *op. cit.*, pp. 13-40.
- GONZÁLEZ CUSSAC, J.L.; VELÁSQUEZ VELÁSQUEZ, F. (2022), “Presentación”, en los mismos autores (eds.): *Derecho penal y coronavirus*, Bogotá, pp. 11 y 12.
- HERNÁNDEZ DE COS, P. (2022), *El impacto asimétrico de la pandemia en la UE: el papel de los recursos del NGUE*, Banco de España, Madrid.
- HOLZINGER, L. (1994), *Weissbuch Schwarzgeld. Geldwaschen in Österreich, Wien*.
- HUILLET, M. (2019), “El GAFI publicará nuevas reglas para el criptosector mundial que afectan a los exchanges, fondos y custodios”, en <http://www.es.coin-telegraph>.
- HUMMEL, M.L. (2008), “Internet terrorism”, en *Homeland. Security Review*, vol. 2, nº 2, summer, pp. 117-130.
- INTERPOL (2020), *COVID-19 pandemic. Guidelines for law enforcement, 26 march*, en <http://www.interpol.int>.
- JERICÓ OJER, L. (2020), “Responsabilidad penal en época de coronavirus: una reivindicación de las garantías penales ante el nuevo escenario de riesgo”, en Luquin Bergareche, R. (dir.):

- COVID-19: Conflictos jurídicos actuales y otros desafíos*, Madrid, pp. 461-483.
- LEÓN ALAPONT, J. (2022a), “Sistema penitenciario y COVID-19: breve análisis de los efectos en España”, en González Cussac, J.L.; Velásquez Velásquez, F., *op. cit.*, pp. 139-171.
- LEÓN ALAPONT, J. (2022b), “Un comentario de urgencia de la Ley orgánica 9/2022, de 28 de julio, por la que se establecen normas que faciliten el uso de información financiera y de otro tipo para la prevención, detección, investigación o enjuiciamiento de infracciones penales”, *Diario La Ley*, nº 10123, de 5 de septiembre, pp. 1-13.
- LEVI, M. (2012), “*Crimes of globalisation: some measurement issues*”, en Joutsen, M. (ed.): *New types of crime. Proceedings of the international seminar held in connection with HEUNI’s thirtieth anniversary Helsinki 20 October 2011*, Helsinki, pp. 107-115.
- Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo*, BOE nº 103, 29 de abril de 2010, pp. 37458-37499.
- Ley 11/2021, de 9 de julio, de medidas de prevención y lucha contra el fraude fiscal, la transposición de la Directiva UE/2016/1164, del Consejo, de 12 de julio de 2016, por la que se establecen normas contra las prácticas de elusión fiscal que inciden directamente en el funcionamiento del mercado interior, de modificación de diversas normas tributarias y en materia de regulación del juego*, en BOE nº 164, de 10 de julio de 2021, p. 82657, art. 18.
- Ley orgánica 9/2022, de 28 de julio, por la que se establecen normas que faciliten el uso de información financiera y de otro tipo para la prevención, detección, investigación o enjuiciamiento de infracciones penales, de modificación de la Ley orgánica 8/1980, de 22 de septiembre, de financiación de las comunidades autónomas y otras disposiciones conexas y de modificación de la Ley orgánica 10/1995, de 23 de noviembre, del Código penal*, BOE nº 181, de 29 de julio de 2022, pp. 1-27.
- LLEDÓ BENITO, I. (2022), *El Derecho penal, robots, IA y cibercriminalidad: desafíos éticos y jurídicos ¿Hacia una distopía?*, Madrid.
- LORENZO SALGADO, J.M. (2020), “El blanqueo de dinero procedente de los delitos descritos en los artículos 368 a 372 del CP y las nuevas tendencias de financiación del terrorismo advertidas por las directivas de 2018”, en Abel Souto, M.; Lorenzo Salgado, J.M.; Sánchez Stewart, N., *VII congreso...*, *cit.*, pp. 439-467 y 555-557.
- LORENZO SALGADO, J.M. (2021), “Consideraciones sobre el dogma legalista como principio básico en la construcción de un Derecho penal europeo”, en Abel Souto, M.; Lorenzo Salgado, J.M.; Sánchez Stewart, N., *VIII congreso...*, *cit.*, pp. 813-842, 977 y 978.
- MARTIN, D. (1997), *La criminalité informatique. Cyber-crime: sabotage, piratage, etc., évolution et répression*, Paris.
- MARTÍNEZ ARRIBAS, F. (2019), “El uso de la informática para la prevención del blanqueo según el Reglamento europeo 2015/847 y la eventual vulneración de principios y derechos reconocidos en la Constitución Española y la Carta de Derechos Fundamentales”, en Abel Souto, M.; Sánchez Stewart, N. (coords.): *VI congreso internacional sobre prevención y represión del blanqueo de dinero*, Valencia, pp. 125-142.
- MATA BARRANCO, N.J. DE LA (2010), “Ilícitos vinculados al ámbito informático: la respuesta penal”, en Cuesta Arzamendi, J.L. de la (dir.), *Derecho penal informático*, Cizur Menor, pp. 15-30.
- MATA Y MARTÍN, R. (2010), “El robo de identidad: ¿una figura necesaria?”, en Alamillo Domingo, I. y otros: *Robo de identidad y protección de datos*, Aranzadi, Cizur Menor, pp. 199-220.
- MIRÓ LLINARES, F. (2011), “La oportunidad criminal en el ciberespacio. Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen”, *Revista Electrónica de Ciencia Penal y Criminología*, nº 13-07, pp. 1-55.
- MORÓN PENDÁS, I. (2021), “La exposición a la corrupción como factor de riesgo en el sistema de prevención del blanqueo de dinero y la financiación del terrorismo”, en Abel Souto,

- M.; Lorenzo Salgado, J.M.; Sánchez Stewart, N. (coords.): *VIII congreso internacional sobre prevención y represión del blanqueo de dinero*, Valencia, pp. 347-367, 921 y 922.
- NAVARRO CARDOSO, F. (2019), “Criptomonedas (en especial, bitc in) y blanqueo de dinero”, *Revista Electr nica de Ciencia Penal y Criminolog a*, 21-14, pp. 1-45.
- NIETO MART N, A. (2020), “Derecho penal ante el coronavirus: entre el estado de emergencia y la gobernanza global”, en <https://almacenederecho.org>, pp. 1-10.
- OLAIZOLA NOGALES, I. (2022), “La Directiva (UE) 2019/1937 whistleblower: su eficacia contra la corrupci n”, en G mez Mart n, V.; Bolea Bardon, C.; Gallego Soler, J.-I.; Hortal Ibarra, J.C.; Joshi Jubert, U., *op. cit.*, pp. 269-278.
- OPPEL, S. (2022), “Bitcoin: herramientas de an lisis para abordar investigaciones penales que incluyan operaciones con esta criptomoneda”, *Revista de Derecho Penal y Criminolog a*, n  6, pp. 75-104.
- PALOMO DEL ARCO, A. (2011), “Delitos contra la propiedad intelectual: investigaci n a trav s de las nuevas tecnolog as”, en Mata y Mart n, R.M. (dir.): *La propiedad intelectual en la era digital. L mites e infracciones a los derechos de autor en internet*, Madrid, pp. 281-286.
- PEINADO, F.; VIEJO, M. (2022), “Anticorrupci n se querrela contra dos empresarios que cobraron una comisi n de casi seis millones en una compra sanitaria en Madrid”, *El Pa s*, 6 de abril.
- PEREIRA MENAUT, A.-C. (2019), “ Puede la lucha contra el blanqueo de dinero producir nihilismo jur dico?”, en Abel Souto, M.; S nchez Stewart, N., *VI congreso...*, *cit.*, pp. 103-124, 539 y 540.
- P REZ ESTRADA, M.J. (2010), “La investigaci n del delito a trav s de las nuevas tecnolog as. Nuevos medios de investigaci n en el proceso penal”, en Cuesta Arzamendi, J.L. de la (dir.): *Derecho penal inform tico*, Cizur Menor, pp. 305-319.
- PHILIPPSOHN, S. (2001a), “Money laundering on the internet”, *Computer & Security*, vol. 20, n  6, pp. 485-490.
- PHILIPPSOHN, S. (2001b), “The dangers of new technology - Laundering on the internet”, *Journal of Money Laundering Control*, vol. 5, n  1, pp. 87-95.
- PIETH, M. (1992), “Zur Einf hrung: Geldw scherei und ihre Bek mpfung in der Schweiz”, en el mismo autor (ed.): *Bek mpfung der Geldw scherei: Modellfall Schweiz?*, Basel, Frankfurt am Main und Stuttgart, pp. 1-27.
- PIETH, M. (1997), “Internationale Harmonisierung von Strafrecht als Antwort auf transnationale Wirtschaftskriminalit t”, *Zeitschrift f r die Gesamte Strafrechtswissenschaft*, n  4, pp. 756-776.
- PING, H. (2004), “New trends in money laundering - From the real world to cyberspace”, en *Journal of Money Laundering Control*, vol. 8, n  1, pp. 48-55.
- PONTE, C. DEL (1996), “L'impegno internazionali nell'applicazione della normativa antiriciclaggio nel settore finanziario”, en Palombi, E. (a cura di): *Il riciclaggio dei proventi illeciti. Tra politica criminale e diritto vigente*, Napoli, pp. 242-249.
- POSADA MAYA, R. (2022), “Principales manifestaciones criminales durante la pandemia del SARS-COV-2 en Colombia”, en Gonz lez Cussac, J.L.; Vel squez Vel squez, F., *op. cit.*, pp. 69-78.
- Proposal for a Regulation of the European Parliament and of the Council establishing the authority for anti-money laundering and countering the financing of terrorism and amending Regulations, (EU) n  1093/2010, (EU) 1094/2010, (EU) 1095/2010, 2021/0240 (COD)*, 29 de junio de 2022, pp. 1-192.
- Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se crea la autoridad de lucha contra el blanqueo de capitales y la financiaci n del terrorismo y se modifican los Reglamentos (UE), n  1093/2010, (UE) n  1094/2010 y (UE) n  1095/2010, COM (2021) 421*

- final, 20 de julio de 2021, pp. 1-126.
- Real decreto-ley 7/2021, de 27 de abril, de transposición de directivas de la Unión Europea en las materias de competencia, prevención del blanqueo de capitales, entidades de crédito, telecomunicaciones, medidas tributarias, prevención y reparación de daños medioambientales, desplazamiento de trabajadores en la prestación de servicios transnacionales y defensa de los consumidores*, BOE nº 101, 28 de abril de 2021, apartado III, pp. 49752-49754, y art. 3, pp. 49788-49803.
- RODRÍGUEZ VÁZQUEZ, V. (2021), “La protección penal de la vida, salud e integridad física de los trabajadores ante el SARS-COV-2 y la pandemia de COVID-19”, *Estudios Penales y Criminológicos*, vol. XLI, pp. 415-491.
- SANDYWELL, B. (2010), “*On the globalisation of crime: the internet and new criminality*”, en Jewkes, Y.; Yar, M.: *Handbook of internet crime*, Devon/Portland, pp. 38-66.
- SCHUDELARO, T. (2006), “*Electronic payment systems and money laundering: beyond the internet hype*”, *Global Journal on Crime & Criminal Law*, vol. 10, nº 1, pp. 47-72.
- SOUZA, J.D'. (2012), *Terrorist financing, money laundering, and tax evasion. Examining the performance of financial intelligence units*, Boca Raton.
- SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS (2021), *Resumen del dictamen del supervisor europeo de protección de datos sobre el paquete de propuestas legislativas sobre la lucha contra el blanqueo de capitales y la financiación del terrorismo (LBC/LFT)*, en *Diario Oficial de la Unión Europea*, C 524, 29 de diciembre, pp. 1-6.
- VARESE, F. (2012), “*How mafias take advantage of globalization. The russian mafia in Italy*”, *The British Journal of Criminology*, vol. 52, nº 2, marzo, pp. 235-253.
- VELASCO SAN MARTÍN, C. (2012), *La jurisdicción y competencia sobre delitos cometidos a través de sistemas de cómputo e internet*, Valencia.
- VELÁSQUEZ VELÁSQUEZ, F. (2022), “El coronavirus y las cárceles”, en González Cussac, J.L.; Velásquez Velásquez, F., *op. cit.*, pp. 194-218.
- VIANO, E. (2020), *The International Society of Criminology faced with the emergency posed by the Coronavirus pandemic*, International Society of Criminology, Washington.
- WATTERS, P.A. (2011), “*A methodology for analyzing the credential marketplace*”, *Journal of Money Laundering Control*, vol. 14, nº 1, pp. 32-43.
- YAN, L.; AI, L.; TANG, J. (2011), “*Risk-based AML regulation on internet payment services in China*”, *Journal of Money Laundering Control*, vol. 14, nº 1, pp. 93-101.