



# Diritto Penale Contemporaneo

RIVISTA TRIMESTRALE

---

REVISTA TRIMESTRAL DE DERECHO PENAL  
A QUARTERLY REVIEW FOR CRIMINAL JUSTICE



4/2020

#### EDITOR-IN-CHIEF

Gian Luigi Gatta

#### EDITORIAL BOARD

*Italy:* Antonio Gullo, Guglielmo Leo, Luca Luparia, Francesco Mucciarelli, Francesco Viganò

*Spain:* Jaime Alonso-Cuevillas, Sergi Cardenal Montraveta, David Carpio Briz,

Joan Queralt Jiménez

*Chile:* Jaime Couso Salas, Mauricio Duce Julio, Héctor Hernández Basualto,

Fernando Londoño Martínez

#### MANAGING EDITORS

Carlo Bray, Silvia Bernardi

#### EDITORIAL STAFF

Enrico Andolfatto, Enrico Basile, Emanuele Birritteri, Javier Escobar Veas,

Stefano Finocchiaro, Alessandra Galluccio, Elisabetta Pietrocarlo, Rossella Sabia,

Tommaso Trinchera, Maria Chiara Ubiali, Stefano Zirulia

#### EDITORIAL ADVISORY BOARD

Rafael Alcacer Guirao, Alberto Alessandri, Giuseppe Amarelli, Ennio Amodio,

Coral Arangüena Fanego, Lorena Bachmaier Winter, Roberto Bartoli, Fabio Basile,

Hervé Belluta, Alessandro Bernardi, Carolina Bolea Bardón, David Brunelli,

Silvia Buzzelli, Alberto Cadoppi, Pedro Caeiro, Michele Caianiello, Lucio Camaldo,

Stefano Canestrari, Francesco Caprioli, Claudia Cárdenas Aravena, Raúl Carnevali,

Marta Cartabia, Elena Maria Catalano, Mauro Catenacci, Massimo Ceresa Gastaldo,

Mario Chiavario, Mirentxu Corcoy Bidasolo, Roberto Cornelli, Cristiano Cupelli,

Norberto Javier De La Mata Barranco, Angela Della Bella, Cristina de Maglie,

Gian Paolo Demuro, Miguel Díaz y García Conlledo, Ombretta Di Giovine, Emilio Dolcini,

Jacobo Dopico Gomez Aller, Patricia Faraldo Cabana, Silvia Fernández Bautista,

Javier Gustavo Fernández Terruelo, Marcelo Ferrante, Giovanni Fiandaca, Gabriele Fornasari,

Novella Galantini, Percy García Caveró, Loredana Garlati, Mitja Gialuz, Glauco Giostra,

Víctor Gómez Martín, José Luis Guzmán Dalbora, Ciro Grandi, Giovanni Grasso,

Giulio Illuminati, Roberto E. Kostoris, Máximo Langer, Juan Antonio Lascurain Sánchez,

Maria Carmen López Peregrín, Sergio Lorusso, Ezequiel Malarino,

Francisco Maldonado Fuentes, Stefano Manacorda, Juan Pablo Mañalich Raffo,

Vittorio Manes, Grazia Mannozi, Teresa Manso Porto, Luca Marafioti, Joseph Margulies,

Enrico Marzaduri, Luca Masera, Jean Pierre Matus Acuña, Anna Maria Maugeri,

Oliviero Mazza, Iván Meini, Alessandro Melchionda, Chantal Meloni, Melissa Miedico,

Vincenzo Militello, Fernando Miró Linares, Vincenzo Mongillo,

Renzo Orlandi, Francesco Palazzo, Carlenrico Paliero, Michele Papa, Raphaële Parizot,

Claudia Pecorella, Marco Pelissero, Lorenzo Picotti, Paolo Pisa, Oreste Pollicino,

Domenico Pulitanò, Tommaso Rafaraci, Paolo Renon, Mario Romano,

Maria Ángeles Rueda Martín, Carlo Ruga Riva, Stefano Ruggieri, Francesca Ruggieri,

Marco Scoletta, Sergio Seminara, Paola Severino, Nicola Selvaggi, Rosaria Sicurella,

Jesús María Silva Sánchez, Carlo Sotis, Giulio Ubertis, Inma Valeije Álvarez, Antonio

Vallini, Vito Velluzzi, Paolo Veneziani, Costantino Visconti, Javier Willenmann von Bernath,

Francesco Zacchè

Editore Associazione "Progetto giustizia penale", c/o Università degli Studi di Milano,  
Dipartimento di Scienze Giuridiche "C. Beccaria" - Via Festa del Perdono, 7 - 20122 MILANO - c.f. 97792250157  
ANNO 2020 - CODICE ISSN 2240-7618 - Registrazione presso il Tribunale di Milano, al n. 554 del 18 novembre 2011.  
Impaginazione a cura di Chiara Pavesi

**Diritto penale contemporaneo – Rivista trimestrale** è un periodico on line ad accesso libero e non ha fine di profitto. Tutte le collaborazioni organizzative ed editoriali sono a titolo gratuito e agli autori non sono imposti costi di elaborazione e pubblicazione. La rivista, registrata presso il Tribunale di Milano, al n. 554 del 18 novembre 2011, è edita attualmente dall'associazione "Progetto giustizia penale", con sede a Milano, ed è pubblicata con la collaborazione scientifica e il supporto dell'Università Commerciale Luigi Bocconi di Milano, dell'Università degli Studi di Milano, dell'Università di Roma Tre, dell'Università LUISS Guido Carli, dell'Universitat de Barcelona e dell'Università Diego Portales di Santiago del Cile.

La rivista pubblica contributi inediti relativi a temi di interesse per le scienze penalistiche a livello internazionale, in lingua italiana, spagnolo, inglese, francese, tedesca e portoghese. Ogni contributo è corredato da un breve abstract in italiano, spagnolo e inglese.

La rivista è classificata dall'ANVUR come rivista scientifica per l'area 12 (scienze giuridiche), di classe A per i settori scientifici G1 (diritto penale) e G2 (diritto processuale penale). È indicizzata in DoGI e DOAJ.

Il lettore può leggere, condividere, riprodurre, distribuire, stampare, comunicare al pubblico, esporre in pubblico, cercare e segnalare tramite collegamento ipertestuale ogni lavoro pubblicato su "Diritto penale contemporaneo – Rivista trimestrale", con qualsiasi mezzo e formato, per qualsiasi scopo lecito e non commerciale, nei limiti consentiti dalla licenza Creative Commons - Attribuzione - Non commerciale 3.0 Italia (CC BY-NC 3.0 IT), in particolare conservando l'indicazione della fonte, del logo e del formato grafico originale, nonché dell'autore del contributo.

La rivista può essere citata in forma abbreviata con l'acronimo: *DPC-RT*, corredato dall'indicazione dell'anno di edizione e del fascicolo.

La rivista fa proprio il [Code of Conduct and Best Practice Guidelines for Journal Editors](#) elaborato dal COPE (Committee on Publication Ethics).

La rivista si conforma alle norme del Regolamento UE 2016/679 in materia di tutela dei dati personali e di uso dei cookies ([clicca qui](#) per dettagli).

Ogni contributo proposto per la pubblicazione è preliminarmente esaminato dalla direzione, che verifica l'attinenza con i temi trattati dalla rivista e il rispetto dei requisiti minimi della pubblicazione.

In caso di esito positivo di questa prima valutazione, la direzione invia il contributo in forma anonima a due revisori, individuati secondo criteri di rotazione tra i membri dell'Editorial Advisory Board in relazione alla rispettiva competenza per materia e alle conoscenze linguistiche. I revisori ricevono una scheda di valutazione, da consegnare compilata alla direzione entro il termine da essa indicato. Nel caso di tardiva o mancata consegna della scheda, la direzione si riserva la facoltà di scegliere un nuovo revisore.

La direzione comunica all'autore l'esito della valutazione, garantendo l'anonimato dei revisori. Se entrambe le valutazioni sono positive, il contributo è pubblicato. Se una o entrambe le valutazioni raccomandano modifiche, il contributo è pubblicato previa revisione dell'autore, in base ai commenti ricevuti, e verifica del loro accoglimento da parte della direzione. Il contributo non è pubblicato se uno o entrambi i revisori esprimono parere negativo alla pubblicazione.

La direzione si riserva la facoltà di pubblicare, in casi eccezionali, contributi non previamente sottoposti alla procedura di peer review. Di ciò è data notizia nella prima pagina del contributo, con indicazione delle ragioni relative.

I contributi da sottoporre alla Rivista possono essere inviati al seguente indirizzo mail: [editor.criminaljusticenetwork@gmail.com](mailto:editor.criminaljusticenetwork@gmail.com). I contributi che saranno ritenuti dalla direzione di potenziale interesse per la rivista saranno sottoposti alla procedura di peer review sopra descritta. I contributi proposti alla rivista per la pubblicazione dovranno rispettare i criteri redazionali [scaricabili qui](#).

**Diritto penale contemporaneo – Rivista trimestrale** es una publicación periódica *on line*, de libre acceso y sin ánimo de lucro. Todas las colaboraciones de carácter organizativo y editorial se realizan gratuitamente y no se imponen a los autores costes de maquetación y publicación. La Revista, registrada en el Tribunal de Milan, en el n. 554 del 18 de noviembre de 2011, se edita actualmente por la asociación “Progetto giustizia penale”, con sede en Milán, y se publica con la colaboración científica y el soporte de la *Università Commerciale Luigi Bocconi* di Milano, la *Università degli Studi di Milano*, la *Università di Roma Tre*, la *Università LUISS Guido Carli*, la *Universitat de Barcelona* y la *Universidad Diego Portales de Santiago de Chile*.

La Revista publica contribuciones inéditas, sobre temas de interés para la ciencia penal a nivel internacional, escritas en lengua italiana, española, inglesa, francesa, alemana o portuguesa. Todas las contribuciones van acompañadas de un breve abstract en italiano, español e inglés.

El lector puede leer, compartir, reproducir, distribuir, imprimir, comunicar a terceros, exponer en público, buscar y señalar mediante enlaces de hipervínculo todos los trabajos publicados en “Diritto penale contemporaneo – Rivista trimestrale”, con cualquier medio y formato, para cualquier fin lícito y no comercial, dentro de los límites que permite la licencia *Creative Commons - Attribuzione - Non commerciale 3.0 Italia* (CC BY-NC 3.0 IT) y, en particular, debiendo mantenerse la indicación de la fuente, el logo, el formato gráfico original, así como el autor de la contribución.

La Revista se puede citar de forma abreviada con el acrónimo *DPC-RT*, indicando el año de edición y el fascículo.

La Revista asume el [Code of Conduct and Best Practice Guidelines for Journal Editors](#) elaborado por el COPE (*Comitte on Publication Ethics*).

La Revista cumple lo dispuesto en el Reglamento UE 2016/679 en materia de protección de datos personales ([clica aquí](#) para los detalles sobre protección de la privacy y uso de cookies).

Todas las contribuciones cuya publicación se propone serán examinadas previamente por la Dirección, que verificará la correspondencia con los temas tratados en la Revista y el respeto de los requisitos mínimos para su publicación.

En el caso de que se supere con éxito aquella primera valoración, la Dirección enviará la contribución de forma anónima a dos evaluadores, escogidos entre los miembros del *Editorial Advisory Board*, siguiendo criterios de rotación, de competencia por razón de la materia y atendiendo también al idioma del texto. Los evaluadores recibirán un formulario, que deberán devolver a la Dirección en el plazo indicado. En el caso de que la devolución del formulario se retrasara o no llegara a producirse, la Dirección se reserva la facultad de escoger un nuevo evaluador.

La Dirección comunicará el resultado de la evaluación al autor, garantizando el anonimato de los evaluadores. Si ambas evaluaciones son positivas, la contribución se publicará. Si alguna de las evaluaciones recomienda modificaciones, la contribución se publicará después de que su autor la haya revisado sobre la base de los comentarios recibidos y de que la Dirección haya verificado que tales comentarios han sido atendidos. La contribución no se publicará cuando uno o ambos evaluadores se pronuncien negativamente sobre su publicación.

La Dirección se reserva la facultad de publicar, en casos excepcionales, contribuciones que no hayan sido previamente sometidas a *peer review*. Se informará de ello en la primera página de la contribución, indicando las razones.

Si deseas proponer una publicación en nuestra revista, envía un mail a la dirección [editor.criminaljusticenetwork@gmail.com](mailto:editor.criminaljusticenetwork@gmail.com). Las contribuciones que la Dirección considere de potencial interés para la Revista se someterán al proceso de *peer review* descrito arriba. Las contribuciones que se propongan a la Revista para su publicación deberán respetar los criterios de redacción (se pueden [descargar aquí](#)).



**Diritto penale contemporaneo – Rivista trimestrale** is an on-line, open-access, non-profit legal journal. All of the organisational and publishing partnerships are provided free of charge with no author processing fees. The journal, registered with the Court of Milan (n° 554 - 18/11/2011), is currently produced by the association “Progetto giustizia penale”, based in Milan and is published with the support of Bocconi University of Milan, the University of Milan, Roma Tre University, the University LUISS Guido Carli, the University of Barcelona and Diego Portales University of Santiago, Chile.

The journal welcomes unpublished papers on topics of interest to the international community of criminal scholars and practitioners in the following languages; Italian, Spanish, English, French, German and Portuguese. Each paper is accompanied by a short abstract in Italian, Spanish and English.

Visitors to the site may share, reproduce, distribute, print, communicate to the public, search and cite using a hyperlink every article published in the journal, in any medium and format, for any legal non-commercial purposes, under the terms of the Creative Commons License - Attribution – Non-commercial 3.0 Italy (CC BY-NC 3.0 IT). The source, logo, original graphic format and authorship must be preserved.

For citation purposes the journal’s abbreviated reference format may be used: *DPC-RT*, indicating year of publication and issue.

The journal strictly adheres to the [Code of Conduct and Best Practice Guidelines for Journal Editors](#) drawn up by COPE (Committee on Publication Ethics).

The journal complies with the General Data Protection Regulation (EU) 2016/679 (GDPR) ([click here](#) for details on protection of privacy and use of cookies).

All articles submitted for publication are first assessed by the Editorial Board to verify pertinence to topics addressed by the journal and to ensure that the publication’s minimum standards and format requirements are met.

Should the paper in question be deemed suitable, the Editorial Board, maintaining the anonymity of the author, will send the submission to two reviewers selected in rotation from the Editorial Advisory Board, based on their areas of expertise and linguistic competence. The reviewers are provided with a feedback form to compile and submit back to the editorial board within an established timeframe. If the timeline is not heeded to or if no feedback is submitted, the editorial board reserves the right to choose a new reviewer.

The Editorial Board, whilst guaranteeing the anonymity of the reviewers, will inform the author of the decision on publication. If both evaluations are positive, the paper is published. If one or both of the evaluations recommends changes the paper will be published subsequent to revision by the author based on the comments received and verification by the editorial board. The paper will not be published should one or both of the reviewers provide negative feedback.

In exceptional cases the Editorial Board reserves the right to publish papers that have not undergone the peer review process. This will be noted on the first page of the paper and an explanation provided.

If you wish to submit a paper to our publication please email us at [editor.criminaljusticenetwork@gmail.com](mailto:editor.criminaljusticenetwork@gmail.com). All papers considered of interest by the editorial board will be subject to peer review process detailed above. All papers submitted for publication must abide by the editorial guidelines ([download here](#)).

POLITICA CRIMINALE, PRINCIPI E DIRITTI	<b>Il penale tra teoria e politica</b>	1
<i>POLÍTICA CRIMINAL, PRINCIPIOS Y DERECHOS</i>	<i>El derecho penal entre teoría y política</i> <i>Criminal Law Between Theory and Politics</i> Domenico Pulitanò	
<i>PRINCIPLES, RIGHTS AND CRIMINAL POLICY</i>	<b>Interpretazione convenzionalmente conforme e bilanciamento. Un'appendice</b>	20
	<i>Interpretación convencionalmente conforme y ponderación. Un apéndice</i> <i>ECHR Driven Interpretation and Balance. An Appendix</i> Alessandro Tesauro	
	<b>Prospettive di criminalizzazione delle terapie di conversione sessuale</b>	33
	<i>Perspectivas de criminalización de las terapias de conversión sexual</i> <i>Criminalisation Perspectives About Sex Conversion Treatments</i> Elisa Scaroina	
	<b>Diffamazione a mezzo stampa e libertà di espressione nell'orizzonte della tutela integrata dei diritti fondamentali</b>	56
	<i>Difamación por medio de la prensa y libertad de expresión en el contexto de la tutela integrada de los derechos fundamentales</i> <i>Defamation Through the Press and Freedom of Expression in a Framework of Integrated Protection of Fundamental Rights</i> Laura Tomasi	
GIUSTIZIA PENALE E NUOVE TECNOLOGIE	<b>Intelligenza artificiale, giustizia penale, controllo umano significativo</b>	75
<i>JUSTICIA PENAL Y NUEVAS TECNOLOGÍAS</i>	<i>Inteligencia artificial, justicia penal, control humano significativo</i> <i>Artificial Intelligence, Criminal Justice, Meaningful Human Control</i> Giulio Ubertis	
<i>CRIMINAL JUSTICE AND NEW TECHNOLOGIES</i>		

<p>REATI DEI COLLETTI BIANCHI E DIRITTO PENALE D'IMPRESA</p> <p><i>DELITOS DE CUELLO Y CORBATA Y DERECHO PENAL DE LAS EMPRESAS</i></p> <p><i>WHITE-COLLAR CRIME AND CORPORATE CRIMINAL LAW</i></p>	<p><b>La misura giudiziaria della corruzione: il terzo livello dell'effettività penale</b></p> <p><i>La medición judicial de la corrupción: el tercer nivel de eficacia penal</i></p> <p><i>Judicial Measurement of Corruption: the Criminal Law Effectiveness Third Level</i></p> <p>Elena Ammannato</p>	<p>90</p>
<p><i>WHITE-COLLAR CRIME AND CORPORATE CRIMINAL LAW</i></p>	<p><b>L'ente nel doppio binario punitivo. Note sulla configurazione meta-individuale dei doppi binari sanzionatori</b></p> <p><i>La persona jurídica en el sistema sancionatorio de doble vía. Notas sobre la configuración metaindividual de los sistemas sancionatorios de doble vía</i></p> <p><i>Corporations and 'Double-Track Punishment Systems'. Notes on Meta-Individual Structure of Double-Track Sanctioning</i></p> <p>Andrea Francesco Tripodi</p>	<p>118</p>
<p>RIFORME IN DISCUSSIONE</p> <p><i>REFORMAS EN DISCUSIÓN</i></p> <p><i>REFORMS UNDER DISCUSSION</i></p>	<p><b>Gli obblighi antiriciclaggio degli operatori in moneta virtuale: verso l'autocertificazione per gli utenti della blockchain?</b></p> <p><i>Las obligaciones de los operadores de criptomonedas en contra del lavado de activos: ¿hacia la autocertificación para los usuarios de blockchain?</i></p> <p><i>The Anti-Money Laundering Obligations of Virtual Currency Operators: Towards Self-Certification for Blockchain Users?</i></p> <p>Gaspare Jucan Sicignano</p>	<p>146</p>
<p>RIFORME IN DISCUSSIONE</p> <p><i>REFORMAS EN DISCUSIÓN</i></p> <p><i>REFORMS UNDER DISCUSSION</i></p>	<p><b>La riforma dei reati a tutela della salute pubblica e della sicurezza alimentare. Appunti sul d.d.l. 2427</b></p> <p><i>La reforma de los delitos contra la salud pública y la seguridad alimentaria. Observaciones respecto del D.D.L. 2327</i></p> <p><i>The Reform of Public Health and Food Safety Offences. Notes on d.d.l. 2427</i></p> <p>Donato Castronuovo</p>	<p>165</p>

NOTE A SENTENZA	<b>«Tempi moderni» e Manovre speculative su merci: quale spazio applicativo per l'art. 501 bis c.p.?</b>	185
COMENTARIO DE SENTENCIA	«Tiempos modernos» y Maniobras especulativas sobre bienes: ¿Cuál es el espacio de aplicación del art. 501 bis c.p.?	
CASES AND COMMENTS	«Modern Times» and Speculative Manoeuvres on Goods: Which is the Area of Application of Art. 501 bis c.p.?	
	Francesca Brembati	
	<b>L'errore sulla legittima difesa e l'eccesso colposo: osservazioni a margine di un 'caso da manuale'</b>	208
	<i>El error en la legítima defensa y el exceso culposo: observaciones sobre un "caso de manual"</i>	
	<i>Excessive and Mistaken Self-Defense: Observations on a Real-Life 'Textbook Example'</i>	
	Marco Mossa Verre	



REATI DEI COLLETTI BIANCHI E DIRITTO PENALE D'IMPRESA  
*DELITOS DE CUELLO Y CORBATA Y DERECHO PENAL DE LAS EMPRESAS*  
*WHITE-COLLAR CRIME AND CORPORATE CRIMINAL LAW*

- 90 **La misura giudiziaria della corruzione: il terzo livello dell'effettività penale**  
*La medición judicial de la corrupción: el tercer nivel de eficacia penal*  
*Judicial Measurement of Corruption: the Criminal Law Effectiveness Third Level*  
Elena Ammannato
- 118 **L'ente nel doppio binario punitivo. Note sulla configurazione meta-individuale dei doppi binari sanzionatori**  
*La persona jurídica en el sistema sancionatorio de doble vía. Notas sobre la configuración metaindividual de los sistemas sancionatorios de doble vía*  
*Corporations and 'Double-Track Punishment Systems'. Notes on Meta-Individual Structure of Double-Track Sanctioning*  
Andrea Francesco Tripodi
- 146 **Gli obblighi antiriciclaggio degli operatori in moneta virtuale: verso l'autocertificazione per gli utenti della blockchain?**  
*Las obligaciones de los operadores de criptomonedas en contra del lavado de activos: ¿hacia la autocertificación para los usuarios de blockchain?*  
*The Anti-Money Laundering Obligations of Virtual Currency Operators: Towards Self-Certification for Blockchain Users?*  
Gaspare Jucan Sicignano

## Gli obblighi antiriciclaggio degli operatori in moneta virtuale: verso l'autocertificazione per gli utenti della blockchain?

*Las obligaciones contra el lavado de dinero de los operadores en  
moneda virtual: ¿hacia la autocertificación para los usuarios de  
blockchain?*

*The anti-money laundering obligations of virtual currency operators:  
towards self-certification for blockchain users?*

GASPARE JUCAN SICIGNANO

*Ricercatore in diritto penale presso l'Università degli Studi di Napoli, Suor Orsola Benincasa  
gaspere.sicignano@unisob.na.it*

RICICLAGGIO

LAVADO DE ACTIVOS

MONEY LAUNDERING

---

### ABSTRACTS

La repentina diffusione delle monete virtuali solleva da tempo molte preoccupazioni circa un eventuale utilizzo delle stesse a fini di riciclaggio. Proprio per far fronte a questi rischi, il legislatore ha da tempo elaborato una serie di obblighi per gli operatori in cryptocurrency. Il lavoro affronta questo aspetto, soprattutto al fine di comprendere se l'attuale normativa antiriciclaggio sia sufficiente oppure se necessiti di correttivi.

La repentina expansión de las monedas virtuales ha generado durante algún tiempo muchas preocupaciones sobre su posible uso para fines de reciclaje. Para hacer frente a estos riesgos, el legislador ha elaborado durante mucho tiempo una serie de obligaciones para los operadores de criptomonedas. El trabajo aborda este aspecto, especialmente para entender si la legislación actual contra el lavado de dinero es suficiente o si necesita correcciones.

The rapid spread of virtual coins has long raised many concerns about their possible use for recycling. Precisely to address these risks, the legislator has long drawn up a series of anti-money laundering obligations for cryptocurrency operators. The work addresses this aspect, especially in order to understand whether the current anti-money laundering legislation is sufficient or whether it needs to be remedied.

## SOMMARIO

1. Introduzione. – 2. Gli operatori in moneta virtuale. – 2.1. *Segue*. Il prestatore di servizi relativi all'utilizzo di valuta virtuale. – 2.2. *Segue*. Il prestatore di servizi di portafoglio digitale. – 3. Gli obblighi anticiclaggio degli operatori in moneta virtuale. – 4. La violazione degli obblighi anticiclaggio: le responsabilità penali. – 4.1. *Segue*. Le responsabilità da illecito amministrativo. – 5. Osservazioni conclusive: verso l'autocertificazione per gli utenti della *blockchain*?

## 1.

## Introduzione.

Il Procuratore nazionale antimafia e antiterrorismo, nel corso di una recente audizione innanzi alla Commissione giustizia, ebbe a sostenere: «*le nuove tecnologie, la globalizzazione delle transazioni finanziarie e la nascita di sistemi di pagamento alternativi, il cui anonimato ne consente il potenziale uso improprio per scopi criminali, rappresentano alcune delle tendenze per arginare le quali si rende necessaria l'adozione di nuove misure volte a garantire la maggiore trasparenza del contesto economico e finanziario nazionale e europeo*»<sup>1</sup>. Queste parole esprimono tutte le preoccupazioni delle varie istituzioni, nazionali e internazionali, circa un eventuale utilizzo delle monete virtuali a fini di riciclaggio.

In realtà, a spaventare le varie autorità anticiclaggio è il fatto che le monete virtuali assicurano l'anonimato ai vari utilizzatori<sup>2</sup>. Come evidenziato nella V° direttiva anticiclaggio (Direttiva n. 843/2018/UE) «*l'anonimato delle valute virtuali ne consente il potenziale uso improprio per scopi criminali*»<sup>3</sup>. Infatti, mentre le varie transazioni in moneta virtuale sono generalmente pubbliche, in quanto registrate su un database, l'indirizzo a cui è collegato un determinato utente virtuale è sempre anonimo. Spesso è un mero elenco di cifre e non fornisce alcuna indicazione espressa sull'identificazione del suo proprietario. Di conseguenza, se in un determinato portafoglio c'è un quantitativo sospetto di moneta virtuale, non è possibile *prima facie* identificare il proprietario. Si sostiene infatti che «*il pericolo che la criptovaluta divenga lo strumento principale per attività di riciclaggio sarebbe insito nelle sue caratteristiche, essendo la stessa idonea per natura a dissimulare il valore oggetto del suo trasferimento nella vastità della realtà virtuale*»<sup>4</sup>.

Per contrastare i rischi legati all'anonimato delle monete virtuali, il legislatore è intervenuto recentemente con due provvedimenti normativi istituendo dei veri e propri obblighi

<sup>1</sup> Audizione del Procuratore nazionale antimafia e antiterrorismo Federico Cafiero de Raho, 17 settembre 2019, p. 8, visibile su: <http://www.senato.it>. In questo senso si è espresso anche il Gruppo d'azione finanziaria internazionale (Gafi) nella *Guidance for a Risk-Based Approach to Virtual Asset Service Providers* del 2019, ad avviso del quale le nuove tecnologie consentono a criminali e terroristi di riciclare velocemente i loro proventi illeciti. Si veda Gafi, *Guidance for a Risk-Based Approach to Virtual Asset Service Providers*, giugno 2019. Conforme CASTRONUOVO (2019), secondo cui: «*nella relazione DLA 2018 è emerso che, in Germania, la 'ndrangheta intendesse pagare i carichi di droga ai loro referenti locali sudamericani attraverso l'uso di una valuta virtuale! In definitiva, per arginare la "narcorivoluzione multiculturale" in atto occorre un'altrettanta estensione della rete di prevenzione prevista con la V Direttiva Antiriciclaggio più efficace e borderless: l'anticiclaggio 5G*». Dello stesso avviso LUDOVICO (2019). Secondo l'A.: «*scrive Francesco Polino, sostituto procuratore: "Il rischio sistemico principale è quello di assistere, de facto, alla creazione nel web di un paradiso finanziario virtuale". Con tre fattori in gioco. "Il sistema delle criptovalute ha natura decentralizzata, ogni computer ha eguale accesso alle risorse comuni". Inoltre "le transazioni possono avvenire non soltanto tra soggetti residenti in Stati diversi, ma anche essere riconducibili a più account in realtà riferibili sempre alla medesima persona". Ed "esistono sempre più espedienti capaci di assicurare un maggior grado di anonimato"*». Anche secondo PICOTTI (2018) le criptovalute sono sfruttate prevalentemente a fini illeciti di riciclaggio o svolgimento di attività criminose. Per un approfondimento, in chiave critica, sia consentito rimandare a SICIGNANO (2019).

<sup>2</sup> Si veda ARCELLA e MANENTE (2020), p. 23 e ss., secondo cui, sul tema delle valute virtuali, «*da un lato, infatti, si sottolineano problemi di privacy, stante l'eccessiva trasparenza della tecnologia blockchain e soprattutto la permanenza indelebile nel tempo delle informazioni che contiene, dall'altro però si evidenziano possibili rischi di riciclaggio del denaro, stante l'opacità della predetta tecnologia. Ma com'è possibile che un'iniziativa relativa alla nascita di una criptovaluta possa sollevare contemporaneamente dubbi tra loro diametralmente opposti? Com'è possibile in altre parole affermare che le criptovalute pongano contemporaneamente problemi per la privacy dei cittadini, ma al contempo assicurino anche eccessiva "segretezza" per potenziali delinquenti?*».

<sup>3</sup> Direttiva (UE) 2018/843 del Parlamento Europeo e del Consiglio, del 30 maggio 2018, in <https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32018L0843&from=IT>.

<sup>4</sup> INGRAO (2019), p. 149. Si veda DI VIZIO (2019), p. 1. Secondo l'A. il fatto che le criptovalute consentano lo spostamento di valori patrimoniali senza l'intermediazione di soggetti istituzionali è la ragione che ostacola le attività di controllo degli organi pubblici. Spiega infatti: «*il pericolo di opacità nell'individuazione del soggetto che controlla effettivamente la risorsa decartolarizzata – si possa parlare di anonimato o anche solo di pseudoanonimato – rappresenta la premessa che amplifica le problematiche interferenze, già presenti, con l'area delle ricchezze tradizionali. Tale relazione con l'economia "reale" è favorita, anzitutto, dalla convertibilità – diretta o indiretta, immediata o mediata – delle valute virtuali rispetto alle monete tradizionali. Ulteriore elemento di complicazione dei controlli, poi, è rappresentato dalla rapidità del trasferimento delle risorse virtuali tra gli utenti; profilo che rivela come l'ipotetica ricostruibilità a posteriori di un'operazione che le interessi non preclude la configurabilità di dissimulazioni antagonistiche*».

antiriciclaggio per alcuni operatori in moneta virtuale. Ci si riferisce al decreto legislativo 25 maggio 2017, n. 90, adottato in attuazione della IV<sup>o</sup> direttiva antiriciclaggio (Direttiva n. 849/2015/UE), e al decreto legislativo 4 ottobre 2019 n. 125, adottato in attuazione della V direttiva antiriciclaggio, i quali hanno modificato, in tempi diversi, la normativa antiriciclaggio di cui al decreto legislativo 21 novembre 2007, n. 231<sup>5</sup>.

Nelle pagine seguenti si analizzeranno le varie innovazioni introdotte da questi due decreti legislativi, sviluppando alcune considerazioni in ordine alla possibilità, prospettata dalla V direttiva antiriciclaggio, di istituire una autocertificazione per gli utenti della *blockchain*.

## 2. Gli operatori in moneta valuta virtuale.

Molti sono i soggetti che operano in moneta virtuale<sup>6</sup>. L'attuale legge antiriciclaggio ne prende in considerazione due: il prestatore di servizi relativi all'utilizzo di valuta virtuale e il prestatore di servizi di portafoglio digitale.

### 2.1. Segue. Il prestatore di servizi relativi all'utilizzo di valuta virtuale

La figura del prestatore di servizi relativi all'utilizzo di valuta virtuale è stata introdotta dal d.lgs. 25 maggio 2017, n. 90<sup>7</sup>, che con essa fa riferimento a «ogni persona fisica o giuridica che

<sup>5</sup> Se la IV direttiva antiriciclaggio nulla aveva previsto in merito alle monete virtuali e il legislatore italiano con il decreto del 2017 è andato al di là degli impegni europei. Secondo INGRAO (2019), p. 151, «tale mancata previsione si è rivelata fallace. Gli attacchi terroristici che hanno interessato il nord Europa negli ultimi anni, infatti, hanno evidenziato l'emergere di nuove tendenze per quanto attiene alle modalità con cui i gruppi terroristici finanziari e svolgono le proprie operazioni. Alcuni servizi basati sulle moderne tecnologie, come le monete virtuali, in particolare, sono divenuti sempre più popolari come sistemi finanziari alternativi, posto che a lungo sono rimasti al di fuori dell'ambito di applicazione del diritto europeo o hanno beneficiato di deroghe all'applicazione di obblighi giuridici che con il tempo non hanno più trovato giustificazione. Il web, infatti, se, da un lato, ha offerto e offre soluzioni nuove per le operazioni finanziarie, dall'altro, ha fornito la possibilità alla criminalità di giovare di innovativi metodi di riciclaggio o di finanziamento al terrorismo». Con la V direttiva antiriciclaggio, invece, l'Unione europea si è occupata espressamente delle monete virtuali. Il decreto attuativo del 2019, infatti, è consistito in una fedele riproduzione delle richieste europee. La quinta direttiva antiriciclaggio presenta caratteristiche particolari rispetto a quelle che l'hanno preceduta. Anzitutto è stata emanata a soli tre anni di distanza dalla precedente, la n. 2015/849 o quarta direttiva antiriciclaggio. Entrata in vigore il 9 luglio 2019, venti giorni dopo la sua pubblicazione sulla Gazzetta ufficiale dell'Unione europea, aveva richiesto un termine di recepimento di diciotto mesi, ossia entro il 10 gennaio 2020. Si veda VALLEFUOCO (2019), p. 6, secondo cui: «nell'Unione europea e di conseguenza in Italia è divenuta sempre più attuale e meritevole di regolamentazione la tematica delle valute virtuali in materia di antiriciclaggio. Con l'emanazione della direttiva Ue 2018/843 (la quinta direttiva antiriciclaggio) il Consiglio e il Parlamento europeo hanno previsto una serie di disposizioni con la specifica finalità di andare a rafforzare e implementare le disposizioni della quarta direttiva. L'introduzione di nuove tecnologie finanziarie, come nuove forme di pagamento che non erano oggetto di regolamentazione o addirittura soggette a deroghe vistose, andavano a minare la trasparenza delle operazioni finanziarie delle società e degli altri soggetti giuridici, così da consentire la proliferazione di zone grigie in cui soggetti criminali hanno spazio di manovra per poter perpetrare azioni terroristiche. Particolare rilievo normativo quindi rivestono le disposizioni che aggiungono due importanti previsioni indicando come soggetti obbligati i prestatori di servizi la cui attività consiste nella fornitura di servizi di cambio tra valute virtuali e valute aventi corso forzoso».

<sup>6</sup> Una delle caratteristiche più importanti e delle monete virtuali è rappresentata dal fatto che le stesse utilizzano un protocollo decentralizzato che si basa sulla tecnologia *peer-to-peer*. Questo comporta che non esiste una entità centralizzata che convalidi le varie transazioni, formando gli utenti della piattaforma un grande e collegato *network* che autorizza tutti i trasferimenti di denaro e controlla sulla validità di ogni pagamento. Può ben dirsi quindi che i protagonisti delle attività connesse alle monete virtuali sono i più vari. Innanzitutto, vi sono i cambiavalute, che si occupano della conversione della moneta virtuale in moneta legale e viceversa, e i gestori di portafogli virtuali, che si dedicano alla conservazione delle *password* di accesso ad ogni singolo *account*. Ma possono essere considerati come operatori in moneta virtuale anche gli utenti della piattaforma, che partecipano alla estrazione della moneta (il c.d. *mining*) e alla convalida delle relative transazioni, anche riunendosi talvolta in gruppi (le c.d. "*mining pool*"). Allo stesso tempo rientrano in questa figura anche coloro che ricevono i pagamenti in moneta virtuale, ad esempio gli eventuali commercianti che accettano la moneta virtuale in della cessione di un bene o di un servizio.

<sup>7</sup> Tra le varie innovazioni, il decreto del 2017 ha definito anche la nozione di «valuta virtuale», disponendo che essa debba intendersi come una «rappresentazione digitale di valore, non emessa da una banca centrale o da un'autorità pubblica, non necessariamente collegata a una valuta avente corso legale, utilizzata come mezzo di scambio per l'acquisto di beni e servizi e trasferita, archiviata e negoziata elettronicamente». Sul punto, si veda DE LUCA E PASSARETTA (2020), p. 571 e ss., secondo cui la definizione si connota di un elemento in positivo, di uno in negativo e di una destinazione funzionale: l'elemento in positivo è rappresentato dal fatto che la moneta virtuale deve consistere in una rappresentazione digitale di valore trasferita, archiviata e negoziata elettronicamente; quello in negativo dalla necessità che la moneta non sia emessa da una banca centrale o da un'autorità pubblica; la destinazione funzionale dall'utilizzo della moneta virtuale come mezzo di scambio per l'acquisto di beni e servizi. Anche questa nozione di valuta virtuale è stata modificata con il d.lgs. 4 ottobre 2019, n. 125. All'articolo 1, comma 2, lettera qq), dopo le parole «non emessa» sono stati inseriti i vocaboli «né garantita» e dopo le parole «di beni e servizi» è stato inserito l'inciso «o per finalità di investimento». Alla luce del d.lgs. 4 ottobre 2019, n. 125, quindi, si intende per valuta virtuale «la rappresentazione digitale di valore, non emessa né garantita da una banca centrale o da un'autorità pubblica, non necessariamente collegata a una valuta avente corso legale, utilizzata come mezzo di scambio per l'acquisto di beni e servizi o per finalità di investimento e trasferita, archiviata e negoziata elettronicamente». Dal confronto della nuova nozione con quella previgente emerge un ampliamento della definizione. Se la moneta virtuale, infatti, continua a essere una rappresentazione digitale di valore trasferita, archiviata e negoziata elettronicamente, nel decreto del 2019 è specificato che essa non solo non deve essere emessa da una banca centrale o da un'autorità pubblica, ma non deve essere nemmeno da esse garantita. Inoltre, è moneta virtuale sia quella utilizzata

fornisce a terzi, a titolo professionale, servizi funzionali all'utilizzo, allo scambio, alla conservazione di valuta virtuale e alla loro conversione da ovvero in valute aventi corso legale». Si tratterebbe del «cambialvalute virtuale» o dell'«exchange platform»<sup>8</sup>. Con il decreto del 2017, il cambialvalute virtuale è stato ricompreso nell'ambito della categoria degli «altri operatori non finanziari», di cui al comma 5 dell'art. 3, pur «limitatamente allo svolgimento dell'attività di conversione di valute virtuali da, ovvero in, valute aventi corso forzoso»<sup>9</sup>.

La nozione è stata tuttavia ampliata con il d.lgs. 4 ottobre 2019, n. 125<sup>10</sup>, identificandosi ora in questa figura «ogni persona fisica o giuridica che fornisce a terzi, a titolo professionale, anche online, servizi funzionali all'utilizzo, allo scambio, alla conservazione di valuta virtuale e alla loro conversione da ovvero in valute aventi corso legale o in rappresentazioni digitali di valore, ivi comprese quelle convertibili in altre valute virtuali nonché i servizi di emissione, offerta, trasferimento e compensazione e ogni altro servizio funzionale all'acquisizione, alla negoziazione o all'intermediazione nello scambio delle medesime valute».

Sono state introdotte, in particolare, tre modifiche rispetto alla formulazione previgente: a) è stato specificato che rientrano in questa figura anche coloro svolgono la propria attività online; b) sono state ricomprese nella fattispecie anche le attività di conversione di moneta virtuale in altra moneta virtuale, a chiarimento della precedente formulazione che sembrava riferirsi esclusivamente alla conversione di moneta virtuale «da ovvero in valute aventi corso legale»; c) è stata estesa la figura dei «prestatori di servizi relativi all'utilizzo di valuta virtuale» anche a coloro che forniscono a titolo professionale i servizi di emissione, offerta, trasferimento e compensazione e ogni altro servizio funzionale all'acquisizione, alla negoziazione o all'intermediazione nello scambio delle medesime valute. In questo senso si era espresso il GAFI, che, nelle linee guida del giugno 2019<sup>11</sup>, aveva inteso come «prestatore di servizi in materia di virtual asset» qualsiasi persona fisica o giuridica che, su base professionale, conduce una o più delle attività o operazioni prima menzionate, in nome o per conto di un'altra persona fisica o giuridica.

Il decreto del 2019 ha eliminato l'inciso «limitatamente allo svolgimento dell'attività di conversione di valute virtuali da ovvero in valute aventi corso forzoso» presente all'art. 3, comma 5, lett. i) d.lgs. 21 novembre 2007, n. 231. Come appena visto, con il decreto del 2017 la figura dei prestatori di servizi relativi all'utilizzo di valuta virtuale era stata inclusa tra gli altri operatori non finanziari, ma con una limitazione costituita dallo svolgimento dell'attività di conversione di valute virtuali da ovvero in valute aventi corso forzoso. All'esito dell'adozione della V diret-

---

come mezzo di scambio per l'acquisto di beni e servizi, sia quella impiegata per finalità di investimento. L'intento della riforma è duplice: da una parte, introdurre la possibilità per le banche e le autorità pubbliche di garantire monete virtuali, senza applicare in questi casi la normativa antiriciclaggio; dall'altra, colpire anche quelle ipotesi di utilizzo di monete virtuali per finalità speculativa. Attualmente, l'utilizzo delle monete virtuali per finalità speculative è molto diffuso, forse anche di più rispetto allo scambio di beni e servizi. Si veda PERNICE (2019), p. 535, che ha rilevato criticamente «il silenzio, nella descrizione, di due elementi fondamentali che stanno alla base della efficacia tecnica delle criptovalute come mezzo di scambio: la circostanza che è basata sulla crittografia (caratteristica che ne rende univoco ed irripetibile l'utilizzo) e che è registrata nella blockchain (tecnologia che ne archivia e certifica l'uso in termini planetari)». Più di recente, sulla qualificazione giuridica delle monete virtuali, Cass. pen. Sez. II, 17/09/2020, n. 26807 (rv. 279590-01), in *Guida al diritto* 2020, 49, 105, secondo cui «le criptovalute (valute virtuali o bitcoin) sono prodotti finanziari laddove la vendita delle stesse sia reclamizzata come una proposta di investimento e, in tal caso, trattandosi di attività soggetta agli adempimenti di cui al Testo unico delle disposizioni in materia di intermediazione finanziaria (Tuf), l'omissione integra il reato di abusivismo finanziario di cui all'articolo 166, comma 1, lettera c), del Tuf (decreto legislativo 24 febbraio 1998 n. 58)». Per un approfondimento del d.lgs. 25 maggio 2017, n. 90, CAPOLUPO (2017), p. 3146; VALLEFUOCO (2017), p. 3252; GAMBONI (2017), p. 523 ss.; VADALÀ (2017), p. 234 ss. Si veda altresì per un raffronto con la disciplina previgente BELLAVIA (2008); BURATTI (2008); CAPOLUPO, CARBONE e STURZO (2011); CENCI (2010); COCUZZA (2008); CORRADINO (2002); DE NIGRIS (2017), p. 407 ss.; FISICARO (2008); FUGGETTI (2011); KROGH (2009); LEMBO e SCIALOJA (2014); LICINI (2008); RAZZANTE (2011).

<sup>8</sup> GARAVAGLIA (2017). Si veda altresì DE RITIS (2018). Secondo alcuni la norma del 2017 si riferiva anche ai *wallet provider*, ovvero coloro che offrono servizi di custodia dei portafogli virtuali. In questo senso BIXIO (2017), p. 2676. Conforme PASSARETTA (2019), p. 472.

<sup>9</sup> Si veda in argomento LUCEV e BONCOMPAGNI (2018).

<sup>10</sup> Come si legge nella relazione illustrativa allo schema di decreto, il provvedimento normativo contiene sia disposizioni necessarie ad assicurare il recepimento della direttiva (UE) 843/2018 (cd. V direttiva antiriciclaggio), sia alcuni «aggiustamenti, di carattere prevalentemente editoriale», introdotti in accoglimento delle osservazioni formulate dalla Commissione europea, a causa del non completo recepimento della IV direttiva antiriciclaggio. Si veda schema di decreto legislativo concernente disposizioni integrative e correttive al decreto legislativo 25 maggio 2017, n. 90 e al decreto legislativo 25 maggio 2017, n. 92 recanti attuazione della direttiva 2015/849/UE, nonché attuazione della direttiva 2018/843/UE che modifica la direttiva 2015/849/UE relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo e che modifica le direttive 2009/138/CE e 2013/36/UE, trasmesso alla presidenza del senato il 4 luglio 2019, p. 1, visibile su <http://www.senato.it/service/PDF/PDFServer/BGT/1117874.pdf>, nonché Gazzetta Ufficiale, serie generale, 26 ottobre 2019, anno 160, nr. 252, p. 27. Per un primo commento: BELLUZZO (2020), p. 7 - 15; BERGAMINI (2020), p. 21-35; BRONZO (2019), p. 3840; CARBONE (2019), p. 295; CAPOLUPO (2019), p. 4053; CASTRONUOVO (2019); DI VIZIO (2020), p. 177 e ss.; FERRAJOLI (2019), p. 58-63; GAVIOLI (2019), p. 33 e ss.; Razzante (2019); SABATINI, SCALZO e TOMASSI (2019), p. 17 - 24; VADALÀ (2020); VALLEFUOCO (2019); Vitolo (2019), p. 295 e ss.

<sup>11</sup> Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, visibile su <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets.html>

tiva antiriciclaggio, il legislatore nazionale ha eliminato l'inciso per ottemperare alla direttiva europea che aveva imposto di ricomprendere questa figura tra i soggetti obbligati senza alcuna limitazione.

I cambiavalute virtuali, inoltre, sono sottoposti alla vigilanza delle autorità di settore e sono obbligati a iscriversi in una sezione speciale del registro dei cambiavalute, tenuto dall'OAM, ovvero l'organismo degli agenti e dei mediatori<sup>12</sup>. In caso di esercizio dell'attività senza iscrizione nell'apposito registro, è prevista una sanzione amministrativa da 2.065 euro a 10.329 euro da parte del Ministero dell'economia e delle finanze<sup>13</sup>.

Per taluni questo impianto normativo garantirebbe un migliore monitoraggio da parte dell'UIF, con possibilità di istituire una banca dati centrale, in cui registrare le identità degli utenti e gli indirizzi dei portafogli<sup>14</sup>. Si sostiene infatti che «il legislatore ha individuato nelle operazioni di conversione delle valute virtuali verso e dal mondo delle risorse tradizionali (i cd "cambiavalute virtuali") il primo pericolo di riciclaggio. Si tratta, all'evidenza, di un'impostazione che non esclude la problematicità delle diverse operazioni che possono interessare le valute virtuali: siano esse la custodia, il trasferimento, l'emissione o l'impiego per il pagamento. Così la normativa di settore procede per implementazioni progressive, muovendo da definizioni che aggiorna, adatta, precisa, estende al mutare delle caratteristiche prevalenti di alcune valute virtuali o all'emergere dei loro impieghi illeciti nell'esperienza investigativa»<sup>15</sup>. A parere di altri, invece, la norma si rivelerebbe insufficiente, «essendo il ruolo svolto dagli scambiatori nel vasto palcoscenico del sistema Bitcoin, in realtà meramente eventuale»<sup>16</sup>. Si ritiene infatti che l'ampliamento degli obblighi antiriciclaggio degli operatori in moneta virtuale «non consentirà comunque di assicurare il completo monitoraggio delle transazioni in valuta virtuale, atteso che continueranno a permanere non presidiati, anche in prospettiva, gli scambi diretti tra utenti»<sup>17</sup>. E' stato inoltre criticato il fatto che le transazioni tra privati in monete virtuali sono totalmente libere a prescindere dall'importo trasferito, mentre sussiste un obbligo di ricorrere agli intermediari di cui all'art. 49, comma 1, d.lgs. 231 del 2007, per i trasferimenti superiori ai tremila euro, valido solo per i cambiavalute<sup>18</sup>.

## 2.2.

### *Segue. Il prestatore di servizi di portafoglio digitale.*

La figura del prestatore di servizi di portafoglio digitale è stata introdotta con il d.lgs. 4 ottobre 2019, n. 125. Essa ricomprende «ogni persona fisica o giuridica che fornisce, a terzi, a titolo professionale, anche online, servizi di salvaguardia di chiavi crittografiche private per conto dei propri clienti, al fine di detenere, memorizzare e trasferire valute virtuali».

In quanto tali, i prestatori di servizi di portafoglio digitale rientrano nell'ambito degli altri

<sup>12</sup> L'art. 8, d.lgs. n. 90/2017, al comma 1 prevede: «al Decreto legislativo 13 agosto 2010, n. 141, come modificato dal Decreto legislativo 14 dicembre 2010, n. 218 e dal Decreto legislativo 19 settembre 2012, n. 169, all'art. 17-bis, dopo il comma 8, sono aggiunti: 8-bis. Le previsioni di cui al presente articolo si applicano, altresì, ai prestatori di servizi relativi all'utilizzo di valuta virtuale, come definiti nell'art. 1, comma 2, lettera ff), del Decreto legislativo 21 novembre 2007, n. 231, e successive modificazioni tenuti, in forza della presente disposizione, all'iscrizione in una sezione speciale del registro di cui al comma 1. 8-ter. Ai fini dell'efficiente popolamento della sezione speciale di cui al comma 8-bis, con Decreto del Ministro dell'Economia e delle Finanze sono stabilite le modalità e la tempistica con cui i prestatori di servizi relativi all'utilizzo di valuta virtuale sono tenuti a comunicare al Ministero dell'Economia e delle Finanze la propria operatività sul territorio nazionale. La comunicazione costituisce condizione essenziale per l'esercizio legale dell'attività da parte dei suddetti prestatori. Con il Decreto di cui al presente comma sono stabilite forme di cooperazione tra il Ministero dell'Economia e delle Finanze e le forze di polizia, idonee ad interdire l'erogazione dei servizi relativi all'utilizzo di valuta virtuale da parte dei prestatori che non ottemperino all'obbligo di comunicazione». È previsto tuttavia che il Ministro dell'Economia e delle Finanze stabilisca con decreto le modalità e la tempistica degli obblighi di iscrizione dei cambiavalute. Nello schema di decreto che il Ministro dell'Economia e delle Finanze ha esposto a consultazione pubblica si estende l'obbligo di iscrizione a tutti gli «operatori commerciali che accettano valuta virtuale quale corrispettivo di qualsivoglia prestazione avente ad oggetto beni, servizi o altre utilità».

<sup>13</sup> DI VIZIO (2019), p. 15, secondo cui: «in tal modo sono state create le premesse di un censimento delle piattaforme di scambio e dei gestori di portafogli elettronici oltre che di una riserva di attività sulla quale edificare doveri di collaborazione passiva ed attiva dell'antiriciclaggio. Ciò in funzione dell'istituzione di una banca dati centrale affidata al monitoraggio dell'UIF nella quale devono essere registrati l'identità degli utenti e gli indirizzi dei portafogli».

<sup>14</sup> Si veda ancora PASSARETTA (2018), p. 1171. Si veda altresì ACCINNI (2018), p. 20.

<sup>15</sup> DI VIZIO (2019), p. 3.

<sup>16</sup> STURZO L. (2018), p. 29. Conforme PERNICE (2019), p. 530 nonché NADDEO (2019), p. 103.

<sup>17</sup> Relazione Annuale 2018 della Direzione nazionale Antimafia ed Antiterrorismo, pp. 442-443.

<sup>18</sup> DI VIZIO (2019), p. 14. Contra ARCELLA e MANENTE (2020), p. 33, secondo cui le transazioni in criptovalute rientrano nell'ambito della normativa limitativa dell'uso del contante. Questo perché l'art. 49, D.Lgs. n. 231/2007, «nel vietare testualmente "il trasferimento di denaro contante e di titoli al portatore (...)" ricomprende per l'appunto anche i titoli al portatore nell'alveo delle limitazioni applicabili al denaro contante, con la particolarità che, mentre per il denaro, il richiamo alla definizione normativa conduce al requisito del "corso legale", analogo requisito non appare richiesto per i titoli al portatore».

operatori non finanziari e sono quindi obbligati ai relativi adempimenti antiriciclaggio. Come evidenziato in dottrina: «fanno dunque carico agli stessi anche gli obblighi di adeguata verifica del cliente e del titolare effettivo (art. 17, d.lgs. 231/2007), nonché l'obbligo di inoltrare segnalazioni per operazioni sospette (artt. 35-41, d.lgs. 231/2007)»<sup>19</sup>.

Anche per questi soggetti il decreto del 2019 ha previsto l'iscrizione in una sezione speciale del registro dei cambiavalute gestito dall'Organismo degli agenti in attività finanziaria e dei mediatori creditizi (OAM). Nella relazione illustrativa allo schema del d.lgs. 4 ottobre 2019, n. 125 si evidenzia che «la puntualizzazione della definizione di prestatori relativi all'utilizzo di valuta virtuale, nonché la previsione dell'iscrizione nel registro OAM per i prestatori di servizi di portafoglio digitale tiene conto di tutti i possibili utilizzi della valuta virtuale e, quindi, prende in considerazione tutte le attività connesse, anche tenuto conto delle modifiche apportate, dal FATF/GAFI, allo standard n. 15 e al relativo glossario, con riferimento agli standard internazionali in materie di valute virtuali»<sup>20</sup>.

Se una parte della dottrina ha accolto con favore l'intervento legislativo del 2019, evidenziando che «con queste modifiche il legislatore nazionale colma le lacune di tutela presenti nella precedente disciplina, che di fatto consentiva una verifica ai fini antiriciclaggio solo in fase di conversione delle valute virtuali in moneta fisica, lasciando esenti dalla collaborazione i soggetti che ne consentivano la detenzione e la movimentazione come tali»<sup>21</sup>, altro orientamento si è mostrato di parere contrario. Si è sostenuto infatti che «la scelta di sottoporre alla disciplina antiriciclaggio soggetti solo eventualmente ricompresi nella transazione non è utile ad affievolire l'elevata minaccia di riciclaggio intrinsecamente presente nelle caratteristiche delle monete virtuali»<sup>22</sup>.

### 3.

## Gli obblighi antiriciclaggio degli operatori in moneta virtuale.

Come prima visto, il prestatore di servizi relativi all'utilizzo di valuta virtuale e il prestatore di servizi di portafoglio digitale rientrano nella categoria degli operatori non finanziari. Sono quindi obbligati ai relativi adempimenti antiriciclaggio<sup>23</sup>.

Innanzitutto, sono tenuti ad una adeguata verifica della clientela (Titolo II, Capo I – art. 17 ss.)<sup>24</sup>. Questo sia in occasione dell'instaurazione di un rapporto continuato, sia in caso di contatto meramente occasionale. In quest'ultima ipotesi, deve emergere una movimentazione di mezzi di pagamento di importo pari o superiore a 15.000 euro<sup>25</sup>. In presenza di un basso rischio di riciclaggio o di finanziamento del terrorismo, possono applicarsi misure di adegua-

<sup>19</sup> DE STASIO (2020), p. 241. Secondo l'A. la disciplina antiriciclaggio «non esaurisce gli obblighi che la legge pone a carico degli operatori in valute virtuali. Se si accede a una considerazione funzionale della disciplina di tutela dei clienti di tali operatori, si potrà ammettere che, a seconda della fattispecie concreta, si applicherà la disciplina dei servizi di pagamento o quella dei servizi di investimento». In questo senso anche PERNICE (2018), p. 271 e ss.

<sup>20</sup> Schema di decreto legislativo concernente disposizioni integrative e correttive al decreto legislativo 25 maggio 2017, n. 90 e al decreto legislativo 25 maggio 2017, n. 92 recanti attuazione della direttiva 2015/849/UE, nonché attuazione della direttiva 2018/843/UE che modifica la direttiva 2015/849/UE relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo e che modifica le direttive 2009/138/CE e 2013/36/UE, cit., p. 3.

<sup>21</sup> VADALÀ (2020). Questo pur sottolineando che – ancorché lo schema del decreto ministeriale, avente ad oggetto le modalità e la tempistica con cui i prestatori di servizi relativi all'utilizzo di valuta virtuale saranno tenuti a comunicare al Ministero dell'economia e delle finanze la loro operatività sul territorio nazionale, include nell'ambito di sua applicazione anche gli operatori commerciali che accettano valuta virtuale quale corrispettivo di qualsivoglia prestazione avente ad oggetto beni, servizi o altre utilità – ad oggi non è ancora stata emanata alcuna provvedimento in tal senso.

<sup>22</sup> INGRAO (2019), p. 154.

<sup>23</sup> Come noto, la legge antiriciclaggio contiene una serie di obblighi, finalizzati a prevenire e contrastare l'uso del sistema economico e finanziario a scopo di riciclaggio, rivolti a cinque categorie di soggetti: gli intermediari finanziari, gli altri operatori finanziari, i professionisti, gli altri operatori non finanziari e i prestatori di servizi di gioco. Per una completa disamina del d.lgs. n. 231/2007, si veda, tra tanti, GENTILE (2015), p. 31 e ss.; nonché CUCUZZA e GIOFFRÉ (2006); FAIELLA (2001), p. 236; FLICK (1994), p. 1217; FRIGO (1995), p. 3134; GROSSO (1993), p. 1027. Si veda altresì RAZZANTE (2003), p. 646, e RAZZANTE (2003), p. 580. Si veda ancora CRAVETTO (2018), p. 277. Secondo l'A. «la definizione di riciclaggio ricavabile dai commi 4 e 5 dell'art. 2 e dal comma 2, lett. b) dell'art. 1, del d.lgs. n. 231 del 2007, ha limitato la nozione amministrativa di riciclaggio alle sole condotte poste in essere «essendo a conoscenza che [i beni] provengono da un'attività criminosa o da una partecipazione a tale attività», dove l'attività criminosa viene per la prima volta definita come «la realizzazione o il coinvolgimento nella realizzazione di un delitto non colposo». Sono così per la prima volta espunte dalla definizione di riciclaggio amministrativo le condotte che vedono i beni oggetto di riciclaggio provenire da una fattispecie contravvenzionale o da un delitto colposo, con allineamento, se pur nella più ampia nozione di cui al d.lgs. n. 231 del 2007, tra l'individuazione dei reati presupposto delle fattispecie di riciclaggio e autoriciclaggio nell'ordinamento penale e amministrativo».

<sup>24</sup> La verifica della clientela si attua mediante: a) identificazione del cliente con un documento di identità o altro documento di riconoscimento; b) identificazione del titolare effettivo del rapporto e verifica della sua identità; c) acquisizione e valutazione di informazioni sullo scopo e la natura del rapporto o della prestazione professionale; d) controllo del rapporto con il cliente per tutta la sua durata, attraverso l'esame della complessiva operatività del cliente.

<sup>25</sup> Analogo obbligo si applica in caso di un trasferimento fondi occasionale superiore a 1.000 euro.

ta verifica della clientela semplificate sotto il profilo dell'estensione e della frequenza degli adempimenti prescritti. L'identificazione e la verifica del cliente devono avvenire mediante l'acquisizione dei dati identificativi forniti dall'interessato e mediante la verifica dei medesimi, attraverso il confronto con una fonte affidabile e indipendente<sup>26</sup>. In data 30 luglio 2019, la Banca d'Italia ha specificato il contenuto di quest'obbligo, prevedendo disposizioni specifiche in materia di operatività a distanza (Parte II Sezione VIII) e in tema di procedura di video identificazione<sup>27</sup>.

Il d.lgs. 4 ottobre 2019, n. 125 ha operato alcune modifiche alla procedura connessa agli obblighi di adeguata verifica della clientela<sup>28</sup>. Con una prima modifica, riguardante l'art. 17,

<sup>26</sup> ACCINNI (2018), p. 20.

<sup>27</sup> Disposizioni in materia di adeguata verifica della clientela per il contrasto del riciclaggio e del finanziamento del terrorismo, visibile su: <https://www.bancaditalia.it/compiti/vigilanza/normativa/archivio-norme/disposizioni/20190730-dispo/index.html>.

<sup>28</sup> Quanto ai criteri per la determinazione della titolarità effettiva di clienti diversi dalle persone fisiche, sono stati invertiti i commi 4 e 5 dell'originario art. 20, decreto legislativo 21 novembre 2007, n. 231. Nel nuovo comma 4 viene previsto quanto disciplinato dal precedente comma 5, ovvero che «nel caso in cui il cliente sia una persona giuridica privata, di cui al decreto del Presidente della Repubblica 10 febbraio 2000, n. 361, si considerano titolari effettivi: a) i fondatori, ove in vita; b) i beneficiari, quando individuati o facilmente individuabili; c) i titolari di poteri di rappresentanza legale, direzione e amministrazione»; nel nuovo comma 5, quanto disposto nel precedente comma 4, ovvero che «qualora l'applicazione dei criteri di cui ai precedenti commi non consenta di individuare univocamente uno o più titolari effettivi, il titolare effettivo coincide con la persona fisica o le persone fisiche titolari, conformemente ai rispettivi assetti organizzativi o statutari, di poteri di rappresentanza legale, amministrazione o direzione della società o del cliente comunque diverso dalla persona fisica». Secondo la relazione illustrativa allo schema di decreto, l'inversione è funzionale a rendere più intellegibile la norma, evidenziando, rispetto ai criteri elencati nei commi precedenti, il carattere residuale del criterio che consente di individuare il titolare effettivo nei soggetti titolari di funzioni di direzione o amministrazione delle persone giuridiche. Questo soprattutto al fine di evitare una prassi comune degli ultimi anni, ovvero che i soggetti obbligati identifichino automaticamente negli amministratori il titolare effettivo dei loro clienti. E' stata ampliata poi la possibilità del pubblico di accedere alle informazioni sulla titolarità effettiva di persone giuridiche e trust. Innanzitutto, è stato previsto che l'accesso alla sezione del Registro delle imprese contenente le informazioni relative alla titolarità effettiva non è più "riservato". Nel nuovo art. 21, comma 2, la lettera f) decreto legislativo 21 novembre 2007, n. 231 è consentito al pubblico, dietro pagamento dei diritti di segreteria, l'accesso alle informazioni sulla titolarità effettiva di persone giuridiche. In questo caso, l'accesso ha ad oggetto il nome, il cognome, il mese e l'anno di nascita, il paese di residenza e la cittadinanza del titolare effettivo e le condizioni, di cui all'articolo 20, in forza delle quali il titolare effettivo è tale. Si dispone tuttavia che, in circostanze eccezionali, l'accesso alle informazioni sulla titolarità effettiva può essere escluso, in tutto o in parte, qualora l'accesso esponga il titolare effettivo a un rischio sproporzionato di frode, rapimento, ricatto, estorsione, molestia, violenza o intimidazione ovvero qualora il titolare effettivo sia una persona incapace o minore d'età, secondo un approccio caso per caso e previa dettagliata valutazione della natura eccezionale delle circostanze. Analogo potere di accesso è consentito in merito alle informazioni di cui all'articolo 22, comma 5, relative alla titolarità effettiva dei trust. In questo caso, tuttavia, possono accedere solo i soggetti privati, compresi quelli portatori di interessi diffusi, titolari di un interesse giuridico rilevante e differenziato, nei casi in cui la conoscenza della titolarità effettiva sia necessaria per curare o difendere un interesse corrispondente ad una situazione giuridicamente tutelata, qualora abbiano evidenze concrete e documentate della non corrispondenza tra titolarità effettiva e titolarità legale. Si specifica che «l'interesse deve essere diretto, concreto ed attuale e, nel caso di enti rappresentativi di interessi diffusi, non deve coincidere con l'interesse di singoli appartenenti alla categoria rappresentata». Gli obblighi di adeguata verifica della clientela, inoltre, già previsti per trust e persone giuridiche, sono stati estesi anche agli «istituti giuridici affini», soprattutto al fine di rafforzare la trasparenza di queste strutture e garantire l'integrità del sistema finanziario. La definizione di questa figura è resa dall'art. 22, comma 5 bis, secondo cui «per le finalità di cui al presente decreto, si considerano istituti giuridici affini al trust gli enti e gli istituti che, per assetto e funzioni, determinano effetti giuridici equivalenti a quelli dei trust espressi, anche avuto riguardo alla destinazione dei beni ad uno scopo ed al controllo da parte di un soggetto diverso dal proprietario, nell'interesse di uno o più beneficiari o per il perseguimento di uno specifico fine». Ne consegue, quindi che, secondo l'art. 21, comma 3, decreto legislativo 21 novembre 2007, n. 231, l'obbligo di comunicare le informazioni sul titolare effettivo dei trust è stato esteso anche «agli istituti giuridici affini, stabiliti o residenti sul territorio della Repubblica italiana». Allo stesso tempo, a norma dell'art. 21, comma 5, lettera a), decreto legislativo 21 novembre 2007, n. 231, con decreto del Ministro dell'economia e delle finanze, di concerto con il Ministro dello sviluppo economico, sono stabiliti: «a) i dati e le informazioni sulla titolarità effettiva delle imprese dotate di personalità giuridica, delle persone giuridiche private e dei trust e degli istituti giuridici affini, stabiliti o residenti sul territorio della Repubblica italiana da comunicare al Registro delle imprese nonché le modalità e i termini entro cui effettuare la comunicazione»; «b) le modalità attraverso cui le informazioni sulla titolarità effettiva delle imprese dotate di personalità giuridica, delle persone giuridiche private e dei trust e degli istituti giuridici affini, stabiliti o residenti sul territorio della Repubblica italiana sono rese tempestivamente accessibili alle autorità di cui al comma 2, lettera a)». Si aggiunge inoltre che, con riferimento ai titolari effettivi individuati ai poteri di rappresentanza o direzione, oltre alla conservazione delle tracce delle verifiche effettuate, andrà anche motivata la scelta dell'opzione considerata. Il decreto del 2019 è intervenuto anche sul problema delle misure semplificate di adeguata verifica della clientela e di quelle rafforzate. Nella specie, sono state modificate le soglie per l'identificazione dei titolari di carte prepagate e di quelli che effettuano operazioni di pagamento a distanza. E' stato poi introdotto un nuovo fattore di rischio, individuato nelle operazioni relative a petrolio, armi, metalli preziosi, prodotti del tabacco, artefatti culturali e altri beni mobili di importanza archeologica, storica, culturale e religiosa o di raro valore scientifico, nonché avorio e specie protette. E' stato disposto inoltre che i soggetti obbligati, nell'adottare misure rafforzate di adeguata verifica della clientela, devono tenere conto dello specifico fattore di rischio rappresentato da rapporti continuativi, prestazioni professionali od operazioni occasionali a distanza, non assistiti da procedure di riconoscimento elettroniche sicure, regolamentate, riconosciute dalle autorità nazionali. Devono essere adottate misure rafforzate di adeguata verifica anche nel caso in cui il rapporto continuativo, la prestazione professionale o l'operazione siano resi o eseguiti con clienti e relativi titolari effettivi che sono persone politicamente esposte. Il nuovo art. 24, comma 6 bis, decreto legislativo 21 novembre 2007, n. 231, inoltre, ha previsto che i soggetti obbligati devono valutare, in base al rischio, se applicare misure rafforzate di adeguata verifica nei confronti di succursali o filiazioni, aventi sede in paesi terzi ad alto rischio, controllate da soggetti obbligati aventi sede nel territorio della Repubblica o di altro Stato membro dell'Unione, qualora tali succursali o filiazioni si conformino alle politiche e alle procedure di gruppo, a norma dell'articolo 45 della direttiva. Al successivo art. 25, si specifica che, nei casi di rapporti continuativi, prestazioni professionali e operazioni che coinvolgono paesi terzi ad alto rischio, i soggetti obbligati: «a) acquisiscono informazioni aggiuntive in merito allo scopo e alla natura del rapporto continuativo o della prestazione professionale; b) acquisiscono informazioni sull'origine dei fondi e sulla situazione economico-patrimoniale del cliente e del titolare effettivo; c) acquisiscono informazioni sulle motivazioni delle operazioni previste o eseguite; d) acquisiscono l'autorizzazione dei soggetti titolari di poteri di



comma 4, decreto legislativo 21 novembre 2007, n. 231, si è stabilito che «in caso di clienti già acquisiti, i soggetti obbligati adempiono alle predette disposizioni in occasione dell'assolvimento degli obblighi prescritti dalla direttiva 2011/16/UE del Consiglio, del 15 febbraio 2011, relativa alla cooperazione amministrativa nel settore fiscale e che abroga la direttiva 77/799/CEE e dalla pertinente normativa nazionale di recepimento in materia di cooperazione amministrativa nel settore fiscale». Il testo definitivo non contiene più la disposizione presente nello schema di decreto, che obbligava la reiterazione dell'adempimento anche sulla base di disposizioni di legge sopravvenute oltre che del mutato livello di rischio di riciclaggio o di finanziamento del terrorismo associato al cliente<sup>29</sup>.

Il decreto ha modificato anche l'art. 19, comma, lettera a), n. 2, decreto legislativo 21 novembre 2007, n. 231, prevedendo la possibilità di ricorrere a procedure di identificazione elettronica sicure e regolamentate ovvero autorizzate o riconosciute dall'Agenzia per l'Italia digitale<sup>30</sup>. In realtà, prima di questa riforma, l'art. 19 già consentiva l'equiparazione all'identità digitale attribuita nell'ambito del sistema "SPID" delle identità digitali o dei certificati per la generazione di firma digitale, «rilasciati nell'ambito di un regime di identificazione elettronica compreso nell'elenco pubblicato dalla Commissione europea a norma dell'articolo 9 del regolamento EU n. 910/2014». La disposizione, tuttavia, escludeva dal proprio ambito le identità conformi alle regole e-IDAS, rilasciate in altro Paese Ue e quelle non rientranti nel circuito e-IDAS. Con il decreto del 2019 si è posto rimedio a questa lacuna, riconoscendo validità alle identità conformi alle regole e-IDAS, se caratterizzate da un livello massimo di sicurezza, e a quelle non rientranti nel circuito e-IDAS, «purché sicure e regolamentate dalle autorità ovvero autorizzate o riconosciute dall'autorità nazionale preposta alla diffusione dell'utilizzo delle tecnologie dell'informazione e della comunicazione e all'attuazione dell'agenda digitale nazionale»<sup>31</sup>.

Il prestatore di servizi relativi all'utilizzo di valuta virtuale e il prestatore di servizi di portafoglio digitale sono tenuti poi agli obblighi di conservazione dei documenti, dei dati e delle informazioni utili a prevenire, individuare o accertare eventuali attività di riciclaggio o di finanziamento del terrorismo (Titolo II, Capo II – art. 31 ss.). Rispetto alla previgente formulazione, con il decreto del 2017 sono stati eliminati tutti i riferimenti agli obblighi di

---

amministrazione o direzione ovvero di loro delegati o, comunque, di soggetti che svolgono una funzione equivalente, prima di avviare o perseguire o intrattenere un rapporto continuativo, una prestazione professionale o effettuare un'operazione che coinvolga paesi terzi ad alto rischio; e) assicurano un controllo costante e rafforzato del rapporto continuativo o della prestazione professionale, aumentando la frequenza e l'intensità dei controlli effettuati e individuando schemi operativi da sottoporre ad approfondimento». Si aggiunge che, in questi casi, le autorità di vigilanza di settore e gli organismi di autoregolamentazione possono prevedere ulteriori misure di adeguata verifica rafforzata della clientela. Le autorità di vigilanza di settore possono inoltre prevedere obblighi di informativa periodica delle operazioni che coinvolgono paesi terzi ad alto rischio nonché limitazioni all'apertura o alla prosecuzione di rapporti continuativi o il divieto di effettuare operazioni con soggetti residenti aventi sede nei medesimi paesi. Secondo il comma 4 ter, poi, le autorità di vigilanza di settore possono: «a) negare l'autorizzazione all'esercizio dell'attività bancaria o finanziaria sul territorio della Repubblica a società controllate da intermediari con sede nei paesi terzi ad alto rischio ovvero negare agli stessi intermediari l'autorizzazione allo stabilimento di succursali nel territorio della Repubblica; b) negare agli intermediari bancari e finanziari con sede nel territorio della Repubblica l'autorizzazione a istituire succursali sul territorio dei predetti paesi terzi ad alto rischio; c) richiedere agli intermediari bancari e finanziari con sede nel territorio della Repubblica di rafforzare i controlli sui conti correnti di corrispondenza e sui rapporti ad essi assimilabili, intrattenuti con intermediari corrispondenti con sede nei predetti paesi terzi e, se necessario, chiuderli; d) richiedere agli intermediari bancari e finanziari con sede nel territorio della Repubblica di intensificare le verifiche, anche ispettive, sulle società controllate o sulle succursali insediate in paesi terzi ad alto rischio». Una ulteriore modifica ha riguardato la sezione III, del capo I, titolo II, relativa all'esecuzione degli obblighi di adeguata verifica da parte di terzi. Secondo l'art 26 del decreto legislativo 21 novembre 2007, n. 231, i soggetti obbligati possono ricorrere a terzi per l'assolvimento degli obblighi di adeguata verifica. Con il decreto del 2019 è stata eliminata la disposizione che consentiva di avvalersi di agenti in attività finanziaria italiani per svolgere tutte le attività di adeguata verifica nel caso di operazioni occasionali di pagamento inferiori a 15 mila euro. L'intervento è stato necessario in quanto la norma previgente, che consentiva questa attività, creava una disparità di trattamento con gli agenti che, invece, prestavano servizi di pagamento per conto di intermediari dell'unione europea, i quali possono eseguire esclusivamente la fase dell'identificazione, restando in capo all'intermediario mandante la conclusione dell'adeguata verifica. Al nuovo articolo 30, comma 1 bis, decreto legislativo 21 novembre 2007, n. 231, è stata operata una cauta apertura all'esternalizzazione di specifici adempimenti di adeguata verifica. Si prevede infatti che le autorità di vigilanza di settore possono individuare specifici presidi organizzativi in presenza dei quali l'assolvimento di alcuni obblighi di adeguata verifica può essere esternalizzato a terzi diversi da quelli di cui all'articolo 26, comma 2. La disposizione consente l'adeguamento della disciplina italiana a quella di molti Paesi europei, in cui è consentita la piena esternalizzazione degli obblighi di adeguata verifica a imprese specializzate.

<sup>29</sup> VALLEFUOCO (2019).

<sup>30</sup> Una importante modifica è stata prevista per le attività di assicurazione. All'articolo 19, comma 3, sono state soppresse le parole «Per le attività di assicurazione vita o altre forme di assicurazione legate ad investimenti» e le parole «i soggetti obbligati» sono sostituite dalle seguenti: «I soggetti obbligati» e le parole «del contratto di assicurazione vita o di altra assicurazione legata ad investimenti» sono sostituite dalle seguenti: «della prestazione assicurativa». In sostanza la norma non ha fatto altro che estendere gli obblighi di adeguata verifica della clientela a tutte le prestazioni assicurative.

<sup>31</sup> Schema di decreto legislativo concernente disposizioni integrative e correttive al decreto legislativo 25 maggio 2017, n. 90 e al decreto legislativo 25 maggio 2017, n. 92 recanti attuazione della direttiva 2015/849/UE, nonché attuazione della direttiva 2018/843/UE che modifica la direttiva 2015/849/UE relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo e che modifica le direttive 2009/138/CE e 2013/36/UE, cit., p. 9.

registrazione con specifiche modalità tecniche, prevenendo un sistema di «norme più snelle», finalizzate a rendere immediatamente disponibili i dati e le informazioni necessarie per la prevenzione del riciclaggio e di finanziamento del terrorismo<sup>32</sup>. Con il decreto del 2019 l'adempimento è stato esteso anche ai dati identificativi, acquisiti tramite identità digitali o altri strumenti di identificazione previsti dal regolamento EI – DaS.

Gli operatori in moneta virtuale di cui in precedenza inoltre sono obbligati alla segnalazione delle operazioni sospette quando sanno, sospettano o hanno motivi ragionevoli per sospettare che siano in corso o che siano state compiute o tentate operazioni di riciclaggio o di finanziamento del terrorismo o che comunque i fondi, indipendentemente dalla loro entità, provengano da attività criminosa (Titolo II, Capo III, art. 35). Il sospetto va desunto dalle caratteristiche, dall'entità, dalla natura delle operazioni, dal loro collegamento o frazionamento, in relazione anche alla coerenza economica del soggetto che la pone in essere o ad altre anomalie rilevabili dal profilo soggettivo<sup>33</sup>. È previsto inoltre il divieto di comunicare l'avvenuta segnalazione al cliente interessato o a terzi, nonché il divieto di rendere conoscibile il c.d. «flusso di ritorno delle informazioni»<sup>34</sup>.

Con il decreto del 2019 si è specificato che i dati e le informazioni individuate in base a criteri oggettivi, concernenti operazioni a rischio riciclaggio e finanziamento del terrorismo, possono essere utilizzati per l'analisi finanziaria e l'approfondimento investigativo di operazioni sospette e «per effettuare analisi di fenomeni o tipologie di riciclaggio o di finanziamento del terrorismo, mediante modalità di cooperazione e scambio stabilite con protocolli d'intesa tra la UIF, la Direzione nazionale antimafia e antiterrorismo, il Nucleo speciale di polizia valutaria della Guardia di finanza e la Direzione investigativa antimafia, idonei a garantire l'adozione di adeguati presidi di riservatezza dei dati», al fine di garantire che queste informazioni siano utilizzate efficacemente anche per un eventuale approfondimento investigativo delle relative operazioni.

Non si applicano agli operatori in moneta virtuale citati dalla legge antiriciclaggio gli obblighi di invio dei dati aggregati alla Unità d'informazione finanziaria (UIF) di cui all'art. 33, esonerando la norma espressamente da questo adempimento i soggetti appena citati.

## 4. La violazione degli obblighi antiriciclaggio: le responsabilità penali.

La violazione degli obblighi antiriciclaggio da parte degli operatori in moneta virtuale può determinare responsabilità penali e amministrative.

Quanto alle prime, occorre richiamare quanto sostenuto in dottrina, ovvero che «agli exchangers che non dovessero segnalare operazioni sospette si potrebbe astrattamente contestare un concorso nell'altrui reato di riciclaggio, di cui all'art. 648 bis c.p., dovendo in ogni caso essere provata la sussistenza dell'elemento psicologico del reato, ossia il dolo generico, consistente nella rappresentazione della provenienza delittuosa dei beni e nella volontà di compiere le attività relative ad impedire l'identificazione della provenienza delittuosa stessa, ciò in conformità con quanto stabilito dalla Corte di Cassazione nell'ipotesi di un direttore di banca che aveva autorizzato operazioni sospette»<sup>35</sup>. Il punto assume rilievo anche nel caso in cui gli operatori in moneta virtuale forniscano un contributo causale per la commissione di una condotta autoriciclatoria ad opera dell'autore del c.d. predicate crime. In questo caso, si ritiene ricorrere il delitto di autoriciclaggio in capo all'autore del reato presupposto e quello di riciclaggio in capo al terzo<sup>36</sup>.

In caso di violazione degli obblighi antiriciclaggio, inoltre, i prestatori di servizi relativo all'utilizzo di valuta virtuale e di portafoglio digitale potrebbero rispondere anche degli illeciti previsti dal Capo I del Titolo V del d.lgs. n. 231/2007, così come modificato dal d.lgs. 25 maggio 2017, n. 90<sup>37</sup>. In realtà, secondo parte della dottrina, queste disposizioni sono destinate

<sup>32</sup> Rossi (2018), p. 34.

<sup>33</sup> BIXIO (2017), p. 2676.

<sup>34</sup> Rossi (2018), p. 34.

<sup>35</sup> INGRAO (2019), p.154.

<sup>36</sup> Contra STURZO (2018), p. 28, secondo cui il terzo exchanger potrebbe essere ritenuto concorrente *extraneus* nel reato di autoriciclaggio, «in quanto l'autore del reato presupposto non avrebbe potuto procedere al trasferimento del bene (bitcoin) proveniente dal delitto non colposo (ad es. traffico di stupefacenti) in un'attività economica finanziaria (attività di cambio valute) ostacolandone concreta-mente l'identificazione della loro provenienza in mancanza del contributo da questi realizzato».

<sup>37</sup> I reati sono previsti all'art. 55: mentre ai commi 1, 2 e 3 sono state introdotte nuove fattispecie, ai commi 4 e 5 sono state riprodotte alcune

nella pratica ad essere inapplicabili in quanto assorbite dal delitto di cui all'art. 648-bis c.p.<sup>38</sup>.

Ebbene, in caso di falsificazione dei dati e delle informazioni relative al cliente, al titolare effettivo, all'esecutore, allo scopo e alla natura del rapporto continuativo o della prestazione professionale e all'operazione, gli operatori in moneta virtuale potrebbero rispondere del reato di cui al comma 1 dell'art. 55. Discorso analogo vale nelle ipotesi di utilizzazione di dati e informazioni false in occasione dell'adempimento degli obblighi di adeguata verifica. Si tratta di un reato proprio a soggettività ristretta<sup>39</sup>, essendo la soggettività limitata a coloro che sono sottoposti agli obblighi di verifica della clientela. La condotta di falsificazione ricomprende le ipotesi sia di falso ideologico sia di falso materiale<sup>40</sup>. In relazione alla condotta di utilizzo, sarà necessario che l'agente abbia conoscenza della falsità delle informazioni utilizzate<sup>41</sup>. Si discute in quest'ultimo caso se il soggetto attivo debba essere persona diversa dal falsificatore, considerato che – pur in assenza di una clausola di riserva espressa – se un medesimo soggetto falsifica i dati e poi li utilizza, sarà integrato un solo reato, rappresentando l'utilizzo un post fatto non punibile<sup>42</sup>.

Altra ipotesi di reato è prevista nel caso di chi, pur essendo tenuto agli obblighi di conservazione (Titolo II, Capo II), acquisisce o conserva dati falsi o informazioni non veritiere sul cliente, sul titolare effettivo, sull'esecutore, sullo scopo e sulla natura del rapporto continuativo o della prestazione professionale e sull'operazione; nonché laddove chi si avvale di mezzi fraudolenti al fine di pregiudicare la corretta conservazione dei dati e delle informazioni. Nella specie risulta integrato il reato di cui al comma 2 dell'art. 55. Anche questa fattispecie costituisce un reato proprio. I mezzi fraudolenti consistono in ogni attività ingannevole idonea a pregiudicare la corretta conservazione dei dati e delle informazioni. Mentre la prima delle condotte descritte richiede la mera conoscenza della natura falsa o non veritiera dei dati, la seconda presuppone il dolo specifico del fine di pregiudicare la corretta conservazione dei dati<sup>43</sup>.

I prestatori di servizi relativi all'utilizzo di valuta virtuale e di portafoglio digitale potrebbero rispondere poi del reato di cui al comma 4 dell'art. 55. La disposizione incrimina il fatto di chi, essendovi tenuto, viola il divieto di comunicazione di cui agli artt. 39, comma 1, e 41, com-

---

delle ipotesi di reato già previste nel testo precedente. E' il caso dell'originario art. 55 comma 8, confluito nel nuovo art. 55, comma 4, e dell'art. 55, comma 9, confluito nel nuovo art. 55, comma 5. Si veda SENATORE (2019), p. 137, secondo cui il legislatore ha limitato le ipotesi di reato a condotte commissive, connotate dal carattere della fraudolenza, trasferendo nell'area degli illeciti amministrativi tutte le fattispecie di tipo omissivo. Secondo ROMANO (2018), p. 597 ss. nonché ROSSI (2018), p. 38, è stata abbandonata (quasi) la tecnica del rinvio che caratterizzava il sistema previgente ed è stata limitata l'area di rilevanza penale a quelle condotte caratterizzate da un maggiore disvalore. Per comodità di consultazione si riporta l'art. 55, d.lgs. n. 231/2007, così come modificato dal d.lgs. 25 maggio 2017, n. 90: «*capo I (Sanzioni penali) – Art. 55 (Fattispecie incriminatrici).* – 1. *Chiunque, essendo tenuto all'osservanza degli obblighi di adeguata verifica ai sensi del presente decreto, falsifica i dati e le informazioni relative al cliente, al titolare effettivo, all'esecutore, allo scopo e alla natura del rapporto continuativo o della prestazione professionale e all'operazione è punito con la reclusione da sei mesi a tre anni e con la multa da 10.000 euro a 30.000 euro. Alla medesima pena soggiace chiunque essendo tenuto all'osservanza degli obblighi di adeguata verifica ai sensi del presente decreto, in occasione dell'adempimento dei predetti obblighi, utilizza dati e informazioni falsi relativi al cliente, al titolare effettivo, all'esecutore, allo scopo e alla natura del rapporto continuativo o della prestazione professionale e all'operazione.* 2. *Chiunque, essendo tenuto all'osservanza degli obblighi di conservazione ai sensi del presente decreto, acquisisce o conserva dati falsi o informazioni non veritiere sul cliente, sul titolare effettivo, sull'esecutore, sullo scopo e sulla natura del rapporto continuativo o della prestazione professionale e sull'operazione ovvero si avvale di mezzi fraudolenti al fine di pregiudicare la corretta conservazione dei predetti dati e informazioni è punito con la reclusione da sei mesi a tre anni e con la multa da 10.000 euro a 30.000 euro.* 3. *Salvo che il fatto costituisca più grave reato, chiunque essendo obbligato, ai sensi del presente decreto, a fornire i dati e le informazioni necessarie ai fini dell'adeguata verifica della clientela, fornisce dati falsi o informazioni non veritiere, è punito con la reclusione da sei mesi a tre anni e con la multa da 10.000 euro a 30.000 euro.* 4. *Salvo che il fatto costituisca più grave reato, chiunque, essendovi tenuto, viola il divieto di comunicazione di cui agli articoli 39, comma 1, e 41, comma 3, è punito con l'arresto da sei mesi a un anno e con l'ammenda da 5.000 euro a 30.000 euro.* 5. *Chiunque al fine di trarne profitto per sé o per altri indebitamente utilizza, non essendone titolare, carte di credito o di pagamento, ovvero qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi, è punito con la reclusione da uno a cinque anni e con la multa da 310 euro a 1.550 euro. Alla stessa pena soggiace chi, al fine di trarne profitto per sé o per altri, falsifica o altera carte di credito o di pagamento o qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi, ovvero possiede, cede o acquisisce tali carte o documenti di provenienza illecita o comunque falsificati o alterati, nonché ordini di pagamento prodotti con essi.* 6. *Per le violazioni delle disposizioni di cui all'articolo 131-ter del decreto legislativo 1° settembre 1993, n. 385, è ordinata, nei confronti degli agenti in attività finanziaria che prestano servizi di pagamento attraverso il servizio di rimessa di denaro di cui all'articolo 1, comma 1, lettera n), del decreto legislativo 27 gennaio 2010, n. 11, la confisca degli strumenti che sono serviti a commettere il reato. In caso di condanna o di applicazione della pena su richiesta delle parti a norma dell'articolo 444 del codice di procedura penale per il delitto di cui al comma 5 è ordinata la confisca delle cose che servirono o furono destinate a commettere il reato, nonché del profitto o del prodotto, salvo che appartengano a persona estranea al reato, ovvero quando essa non è possibile, la confisca di beni, somme di denaro e altre utilità di cui il reo ha la disponibilità per un valore corrispondente a tale profitto o prodotto.* 7. *Gli strumenti sequestrati ai fini della confisca di cui al comma 6 nel corso delle operazioni di polizia giudiziaria, sono affidati dall'Autorità giudiziaria agli organi di polizia che ne facciano richiesta».*

<sup>38</sup> SENATORE (2019), p. 137.

<sup>39</sup> ROSSI (2018), p. 39.

<sup>40</sup> GAMBONI (2008), p. 527.

<sup>41</sup> ACCINNI (2018), p. 25.

<sup>42</sup> In questo senso ROSSI (2018), p. 40.

<sup>43</sup> ACCINNI (2018), p. 25.

ma 3. Soggetti attivi del reato sono coloro che, avendo ottemperato all'obbligo di segnalazione, comunicano l'avvenuta segnalazione a terzi. Si tratta di una fattispecie contravvenzionale di tipo commissivo, che può essere realizzata sia con dolo sia con colpa<sup>44</sup>. In dottrina ha destato perplessità la scelta del legislatore di attribuire a tale fattispecie carattere contravvenzionale, nonostante essa sia stata posta a presidio di beni giuridici di rilievo<sup>45</sup>. Il bene tutelato è infatti rappresentato dalla riservatezza dell'attività di segnalazione<sup>46</sup>.

Anche la fattispecie di cui al comma 5 potrebbe essere contestata agli operatori in moneta virtuale indicati dalla legge antiriciclaggio. La fattispecie è realizzabile dai soggetti dediti all'attività di cambiavalute virtuale e di portafoglio digitale, in concorso con il soggetto che riceve la carta di credito, omettendo i dovuti controlli in cambio di un eventuale profitto. Tale norma oggi è collocata nell'art. 493-ter c.p., ("Indebito utilizzo e falsificazione di carte di credito e di pagamento") nell'ambito dei delitti "contro la fede pubblica"<sup>47</sup>, in forza del d.lgs. 1° marzo 2018, n. 21, attuativo della c.d. riserva di codice<sup>48</sup>. È punito chiunque, al fine di trarne profitto per sé o per altri, indebitamente utilizza, non essendone titolare, carte di credito o di pagamento, ovvero qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi. Si tratta di un reato comune, posto a tutela della fede pubblica e dell'interesse generale a che il sistema elettronico di pagamento sia utilizzato in modo corretto<sup>49</sup>. Il reato è a dolo specifico, richiedendosi il fine di trarne profitto<sup>50</sup>.

Non sembra tuttavia applicabile al prestatore di servizi relativi all'utilizzo di valuta virtuale e al prestatore di servizi di portafoglio digitale il comma 3 dell'art. 55. A essere sanzionati sono i soggetti che devono comunicare le informazioni necessarie all'assolvimento dell'adeguata verifica e, in tale sede, forniscono dati o informazioni non veritiere. La disposizione si applica ai "clienti", i quali – ai sensi dell'art. 22, d.lgs. n. 90/2017 –devono fornire per iscritto tutte le informazioni necessarie e aggiornate per consentire ai soggetti obbligati di adempiere ai doveri di adeguata verifica. Si tratta di una norma sussidiaria, essendo presente la clausola "salvo che il fatto costituisce più grave reato", mentre l'elemento psicologico è integrato dal dolo generico<sup>51</sup>. In dottrina, è stata molto criticata la scelta del legislatore di disporre per la fattispecie di cui al comma 3 la stessa sanzione prevista per le ipotesi di cui ai commi 1 e 2. Si è sostenuto infatti che «la scelta desta perplessità, quantomeno con riferimento alla equiparazione, sul piano sanzionatorio, tra chi si rende direttamente autore della falsificazione dei dati e delle informazioni e chi ne fa semplicemente uso»<sup>52</sup>. La norma non sembra applicabile agli operatori in moneta virtuale individuati dalla legge antiriciclaggio, essendo destinatari del precetto i soli "clienti". Possono quindi essere sanzionati eventuali acquirenti di *cryptocurrency*. Stesso discorso vale se un *exchanger* dovesse utilizzare le informazioni falsificate fornite dal cliente, essendo a conoscenza della loro non corrispondenza alla realtà. In questo caso, risponderà del delitto di cui alla seconda parte del comma 1 e non della fattispecie di cui al comma 3<sup>53</sup>.

<sup>44</sup> *Ibidem*.

<sup>45</sup> *Ibidem*, p. 126.

<sup>46</sup> Si veda TROYER e ZANCAN (2018), p. 521 ss., secondo cui a seguito del d.lgs. n. 90/2017 «l'assetto sanzionatorio è sensibilmente mutato perché oltre ad essere stata innalzata la misura dell'ammenda, ora la pena detentiva non è più alternativa, bensì cumulativa, il che comporta che non è più possibile estinguere il reato mediante oblazione ai sensi dell'art. 162-bis c.p. Inoltre com'è stato giustamente notato da attenta dottrina, vi è stato un ampliamento della condotta vietata, derivante dall'estensione del divieto di comunicazione anche circa l'esistenza ovvero la probabilità di indagini o approfondimenti in materia di riciclaggio o di finanziamento del terrorismo».

<sup>47</sup> In merito al d.lgs. 1° marzo 2018, n. 21, si veda tra tanti RICCARDI (2018).

<sup>48</sup> Si veda TROYER e ZANCAN (2018), p. 521 ss., secondo cui «non si tratta di una abolitio criminis: la condotta continua ad assumere rilevanza penale, ma è collocata in altro testo normativo».

<sup>49</sup> *Ibidem*, p. 576.

<sup>50</sup> *Ibidem*, p. 577.

<sup>51</sup> GAMBOGI (2008), p. 575.

<sup>52</sup> SENATORE (2019), p. 143.

<sup>53</sup> Al comma 6 dell'art 55 è ribadita l'ipotesi speciale di confisca degli strumenti che sono serviti a commettere il reato, applicabile anche agli agenti in attività finanziaria che prestano servizi di pagamento attraverso la rimessa di denaro. In caso di condanna o di applicazione della pena ai sensi dell'art. 444 c.p.p., è stata introdotta la confisca delle cose che servirono o furono destinate a commettere il reato di cui al comma 5, nonché del profitto o del prodotto, anche nella forma per equivalente. La possibilità di applicare tale disposizione alle monete virtuali non è scontata. Molte monete virtuali, infatti, basandosi su un sistema decentrato, incompatibile con l'intervento di qualsiasi autorità centrale, non possono essere confiscate. Se gli organi inquirenti non sono in possesso delle singole *password* (o meglio, delle chiavi di crittografia) di un determinato *wallet*, non possono sequestrare alcunché.

## 4.1. *Segue. Le responsabilità da illecito amministrativo*

La violazione degli obblighi antiriciclaggio determina anche una eventuale responsabilità degli operatori in moneta virtuale per gli illeciti amministrativi previsti nel Capo II del Titolo V del d.lgs. n. 231/2007. Il sistema si muove in un'ottica di *favor rei*, prevedendosi all'art. 69, comma 1, che «nessuno può essere sanzionato per un fatto che alla data di entrata in vigore delle disposizioni di cui al presente Titolo non costituisce più illecito» e, all'art. 69, comma 2, che «per le violazioni commesse anteriormente all'entrata in vigore del presente decreto, sanzionate in via amministrativa, si applica la legge vigente all'epoca della commessa violazione, se più favorevole, ivi compresa l'applicabilità del pagamento in misura ridotta». Il disposto capovolge un principio cardine della disciplina delle sanzioni amministrative di cui alla legge n. 689/1981, alla luce del quale non si applica in maniera retroattiva la disciplina successiva più favorevole.

È sicuramente applicabile agli operatori in moneta virtuale indicati dalla normativa antiriciclaggio l'illecito amministrativo di cui all'art. 56. La disposizione, all'esito della riforma operata con il d.lgs. 25 maggio 2017, n. 90, ricomprende le fattispecie in precedenza previste ai commi 1, 2 e 3 dell'originario art. 55, depenalizzandole. In realtà il comma 1 del vecchio art. 55 era già stato depenalizzato, prima dell'intervento della nuova legge antiriciclaggio, dal d.lgs. 15 gennaio 2016, n. 8 339.

La norma sanziona il fatto di quei soggetti obbligati che, in violazione delle disposizioni in materia di adeguata verifica della clientela, omettano di acquisire e verificare i dati identificativi e le informazioni sul cliente, sul titolare effettivo, sull'esecutore, sullo scopo e sulla natura del rapporto continuativo o della prestazione professionale. Al comma 2 è previsto che, nelle ipotesi di violazioni gravi, ripetute o sistematiche ovvero plurime, la sanzione pecuniaria venga aumentata. Si tratta sostanzialmente di una ipotesi omissiva propria, applicabile a tutti soggetti obbligati all'adeguata verifica della clientela.

Anche l'illecito di cui all'art. 57 è applicabile ai soggetti dediti all'attività di cambiavalute virtuale e di portafoglio digitale<sup>54</sup>. La norma riprende nella sostanza il comma 4 dell'originario art. 55. Anche in questo caso, la norma era già stata depenalizzata dal d.lgs. n. 8/2016. La disposizione sanziona il fatto dei soggetti obbligati che non effettuino, in tutto o in parte, la conservazione dei dati, dei documenti e delle informazioni più volte richiamati o la effettuino tardivamente. Anche in questo caso, al comma 2, sono previsti incrementi sanzionatori per le ipotesi di violazioni gravi, ripetute o sistematiche ovvero plurime.

L'illecito di cui all'art. 58 consiste nell'omissione della segnalazione di operazioni sospette da parte dei soggetti obbligati. La norma è di natura sussidiaria, essendo prevista la clausola «salvo che il fatto costituisca reato». Per le violazioni gravi, ripetute o sistematiche ovvero plurime è prevista una maggiorazione delle sanzioni pecuniarie. Anche questa fattispecie è applicabile agli operatori in moneta virtuali individuati dalla legge antiriciclaggio<sup>55</sup>. Essi, come

<sup>54</sup> Per comodità di consultazione si riporta l'art. 57, d.lgs. n. 231/2007, così come modificato dal d.lgs. 25 maggio 2017, n. 90: «Art. 57 (Inosservanza degli obblighi di conservazione). 1. Ai soggetti obbligati che, in violazione di quanto disposto dagli articoli 31 e 32, non effettuano, in tutto o in parte, la conservazione dei dati, dei documenti e delle informazioni ivi previsti o la effettuano tardivamente si applica la sanzione amministrativa pecuniaria pari a 2.000 euro. 2. Fuori dei casi di cui al comma 1 e salvo quanto previsto dall'articolo 62, commi 1 e 5, nelle ipotesi di violazioni gravi, ripetute o sistematiche ovvero plurime, si applica la sanzione amministrativa pecuniaria da 2.500 euro a 50.000 euro. La gravità della violazione è determinata anche tenuto conto: a) dell'intensità e del grado dell'elemento soggettivo, anche avuto riguardo all'ascrivibilità, in tutto o in parte, della violazione alla carenza, all'incompletezza o alla non adeguata diffusione di prassi operative e procedure di controllo interno; b) del grado di collaborazione con le autorità di cui all'articolo 21, comma 2, lettera a); c) della rilevanza ed evidenza dei motivi del sospetto, anche avuto riguardo al valore dell'operazione e alla loro incoerenza rispetto alle caratteristiche del cliente e del relativo rapporto; d) della reiterazione e diffusione dei comportamenti, anche in relazione alle dimensioni, alla complessità organizzativa e all'operatività del soggetto obbligato».

<sup>55</sup> Per comodità di consultazione si riporta l'art. 58, d.lgs. n. 231/2007, così come modificato dal d.lgs. 25 maggio 2017, n. 90: «Art. 58 (Inosservanza delle disposizioni relative all'obbligo di segnalazione delle operazioni sospette). – 1. Salvo che il fatto costituisca reato, ai soggetti obbligati che omettono di effettuare la segnalazione di operazioni sospette, si applica una sanzione amministrativa pecuniaria pari a 3.000 euro. 2. Salvo che il fatto costituisca reato e salvo quanto previsto dall'articolo 62, commi 1 e 5, nelle ipotesi di violazioni gravi, ripetute o sistematiche ovvero plurime, si applica la sanzione amministrativa pecuniaria da 30.000 euro a 300.000 euro. La gravità della violazione è determinata anche tenuto conto: a) dell'intensità e del grado dell'elemento soggettivo, anche avuto riguardo all'ascrivibilità, in tutto o in parte, della violazione alla carenza, all'incompletezza o alla non adeguata diffusione di prassi operative e procedure di controllo interno; b) del grado di collaborazione con le autorità di cui all'articolo 21, comma 2, lettera a); c) della rilevanza ed evidenza dei motivi del sospetto, anche avuto riguardo al valore dell'operazione e al grado della sua incoerenza rispetto alle caratteristiche del cliente e del relativo rapporto; d) della reiterazione e diffusione dei comportamenti, anche in relazione alle dimensioni, alla complessità organizzativa e all'operatività del soggetto obbligato. 3. La medesima sanzione di cui ai commi 1 e 2 si applica al personale dei soggetti obbligati di cui all'articolo 3, comma 2 e all'articolo 3, comma 3, lettera a), tenuto alla comunicazione o alla segnalazione, ai sensi dell'articolo 36, commi 2 e 6 e responsabile, in via esclusiva o concorrente con l'ente presso cui operano, dell'omessa segnalazione di operazione sospetta. 4. Nel caso in cui le violazioni gravi, ripetute o sistematiche ovvero plurime producono un vantaggio economico, l'importo massimo della sanzione di cui al comma 2: a) è elevato fino al doppio dell'ammontare del vantaggio medesimo, qualora detto vantaggio sia determinato o determinabile e, comunque, non

ricordato, sono tenuti alla segnalazione di operazioni sospette.

Non sembrano in teoria applicabili ai soggetti dediti all'attività di cambiavalute virtuale e di portafoglio digitale gli ulteriori illeciti amministrativi previsti all'art. 59 (inosservanza degli obblighi di comunicazione da parte dei componenti degli organi di controllo dei soggetti obbligati, che riprende il vecchio art. 55, comma 5); all'art. 60 (inosservanza degli obblighi formativi nei riguardi dell'UIF e degli ispettori del Ministero dell'economia e delle finanze); all'art. 61 (inosservanza delle disposizioni specifiche in materia di soggetti convenzionati e agenti di prestatori di servizi di pagamento e istituti emittenti moneta elettronica); all'art. 62 (in cui sono previste disposizioni sanzionatorie specifiche per soggetti obbligati vigilati); all'art. 63 (inosservanza delle disposizioni di cui al Titolo III) e all'art. 64 (inosservanza delle disposizioni di cui al Titolo IV commesse da distributori ed esercenti nel comparto del gioco).

L'art. 59, in particolare, prevede una sanzione per i componenti degli organi di controllo dei soggetti obbligati che omettono un obbligo di comunicazione. La disposizione potrebbe applicarsi ai soggetti dediti all'attività di cambiavalute virtuale e di portafoglio digitale, solo laddove gli stessi, per la loro organizzazione societaria, posseggano un organo di controllo. È questa tuttavia una eventualità molto residuale e poco comune nella pratica. L'art. 60, invece, sanziona i destinatari degli obblighi di trasmissione e informazione nei confronti dell'UIF. Tali obblighi non riguardano gli operatori in moneta virtuale indicati dalla legge antiriciclaggio, prevedendo l'art. 33 un esonero per queste figure. Anche l'art. 61 non sembra applicabile, essendo destinato ai soggetti convenzionati, agli agenti di prestatori di servizi di pagamento e agli istituti emittenti moneta elettronica. Stesso discorso vale per l'art. 62, che si applica agli intermediari bancari e finanziari<sup>56</sup>. Il disposto trova fondamento nella necessità di sanzionare comportamenti e attività di soggetti che possano minare la stabilità dei mercati finanziari e, quindi, l'intero sistema economico<sup>57</sup>. Anche l'art. 63 non è applicabile ai soggetti dediti all'attività di cambiavalute virtuale e di portafoglio digitale, riguardando le violazioni delle disposizioni di cui al Titolo III, che concernono sostanzialmente alcune limitazioni per l'uso del contante e dei titoli al portatore, tra cui, come è noto, non rientrano le monete virtuali. Le stesse conclusioni valgono per la sfera di operatività dell'art. 64, che riguarda esclusivamente i distributori e gli esercenti operanti nel comparto del gioco.

## 5. Osservazioni conclusive: verso l'autocertificazione per gli utenti della blockchain?

Sia il d.lgs. 25 maggio 2017, n. 90, sia il d.lgs. 4 ottobre 2019, n. 125, non hanno previsto obblighi per gli utenti privati, che svolgono le loro operazioni in moneta virtuale senza ricorrere a un cambiavalute o a un *wallet provider*. Eppure per il considerando 9 della V direttiva antiriciclaggio «*le unità nazionali di informazione finanziaria (UIF) dovrebbero poter ottenere informazioni che consentano loro di associare gli indirizzi della valuta virtuale all'identità del proprietario di tale valuta. Occorre inoltre esaminare ulteriormente la possibilità di consentire agli utenti di presentare, su base volontaria, un'autodichiarazione alle autorità designate*».

La scelta operata dal legislatore nazionale sembra corretta.

Com'è noto, l'intera normativa antiriciclaggio è modellata sulla base del principio dell'approccio basato sul rischio (*risk based approach*). Secondo il considerando 22 della IV direttiva antiriciclaggio «*il rischio di riciclaggio e di finanziamento del terrorismo non è sempre lo stesso in ogni caso. Di conseguenza, dovrebbe essere adottato un approccio olistico basato sul rischio. Tale approccio basato sul rischio non costituisce un'opzione indebitamente permissiva per gli Stati membri e per i soggetti obbligati: implica processi decisionali basati sull'evidenza fattuale, al fine di individuare in maniera più efficace i rischi di riciclaggio e di finanziamento del terrorismo che gravano sull'Unione e su coloro che vi operano*». In questa prospettiva, l'art. 7 prevede che «*ciascuno Stato membro*

*sia inferiore a 450.000 euro; b) è elevato fino ad un milione di euro, qualora il predetto vantaggio non sia determinato o determinabile. 5. Ai soggetti obbligati che, con una o più azioni od omissioni, commettono, anche in tempi diversi, una o più violazioni della stessa o di diverse norme previste dal presente decreto in materia di adeguata verifica della clientela e di conservazione da cui derivi, come conseguenza immediata e diretta, l'inosservanza dell'obbligo di segnalazione di operazione sospetta, si applicano unicamente le sanzioni previste dal presente articolo. 6. Ai soggetti obbligati che omettono di dare esecuzione al provvedimento di sospensione dell'operazione sospetta, disposto dalla UIF ai sensi dell'articolo 6, comma 4, lettera c), si applica la sanzione amministrativa pecuniaria da 5.000 euro a 50.000 euro».*

<sup>56</sup> Si veda TROYER e ZANCAN (2018), p. 521 ss.

<sup>57</sup> Relazione illustrativa al d.lgs. 25 maggio 2017, n. 90, cit., p. 18.

adotta opportune misure per individuare, valutare, comprendere e mitigare i rischi di riciclaggio e di finanziamento del terrorismo che lo riguardano, nonché le eventuali problematiche connesse in materia di protezione dei dati. Esso tiene aggiornata tale valutazione del rischio». Anche il GAFI nelle raccomandazioni del 2012 ha sottolineato l'importanza del *risk based approach* e la conseguente necessità per gli Stati di identificare, valutare e comprendere i rischi cui sono esposti<sup>58</sup>.

In Italia il compito di identificare, analizzare e valutare il relativo rischio di riciclaggio di denaro e di finanziamento del terrorismo spetta – con cadenza triennale, salva la facoltà di procedere al relativo aggiornamento quando insorgano nuovi rischi e ogni qualvolta lo si ritenga opportuno – al Comitato di sicurezza finanziaria (CSF). E' prevista inoltre la possibilità per i rappresentanti della Presidenza del Consiglio dei ministri e di altre Amministrazioni con competenze specifiche su temi di interesse di partecipare all'analisi del *risk assessment nazionale*. E' suggerita altresì la collaborazione di studiosi e rappresentanti del mondo accademico e delle associazioni private rappresentative delle categorie interessate.

In relazione alle monete virtuali, va ora valutato se il rischio di riciclaggio in esse presente sia tale da giustificare una misura così invasiva come quella ipotizzata, volta a identificare ogni utente privato che svolga le sue operazioni in moneta virtuale, senza ricorrere a un cambiavalute o a un *wallet provider*.

A tal proposito appare significativo quanto affermato nella relazione di aggiornamento dell'analisi nazionale sui rischi di riciclaggio e finanziamento del terrorismo, resa dal Comitato di sicurezza finanziaria (CSF) nello scorso giugno 2019<sup>59</sup>: «sebbene le valute virtuali possano potenzialmente prestarsi all'utilizzo per finalità di riciclaggio e finanziamento del terrorismo, allo stato attuale, le evidenze risultanti sia dall'analisi delle operazioni sospette sia dalle attività investigative, insieme alle novità normative introdotte nell'ordinamento giuridico italiano, sono tali da far ritenere che, seppur in presenza di un rischio potenziale elevato, il rischio inerente di utilizzo delle valute virtuali per il riciclaggio e finanziamento del terrorismo si attesta ad un livello poco significativo»<sup>60</sup>.

A mio avviso, in un contesto in cui il rischio di riciclaggio mediante monete virtuali si attesta «ad un livello poco significativo» e in cui non si segnalano nemmeno particolari indagini della magistratura che abbiano accertato un rilevante utilizzo di moneta virtuale a fini di riciclaggio, ipotizzare una schedatura di massa di tutti gli utenti della *blockchain*, anche se mediante una mera autocertificazione, appare sproporzionato. Sembra quasi di trovarsi in una pagina del celebre romanzo “1984” di George Orwell, tra psicoreati, teleschermi, neolingua e Grande Fratello. Se «il desiderio è psicoreato», adottando la terminologia orwelliana potremmo dire che una normativa che finisce per reprimere non il riciclaggio in sé, ma – forse – il mero desiderio di esso potrebbe aver dato vita a un reato del tutto nuovo: lo psicoriciclaggio.

---

## Bibliografia.

ACCINNI, Giovanni Paolo (2018): “Profili di rilevanza penale delle “criptovalute” (nella riforma della disciplina antiriciclaggio del 2017)”, Archivio penale, p. 20.

ARCELLA, Gea, MANENTE, Michele (2020): “Le criptovalute e le loro contraddizioni: tra rischi di opacità e di eccessiva trasparenza”, Notariato, 1, p. 23 e ss.

<sup>58</sup> Si veda CARBONE (2019), p. 491 – 492.

<sup>59</sup> Aggiornamento dell'analisi nazionale sui rischi di riciclaggio e finanziamento del terrorismo (National Risk Assessment - NRA) resa dal Comitato di sicurezza finanziaria (CSF), giugno 2019, visibile su: [http://www.dt.mef.gov.it/export/sites/sitodt/modules/documenti\\_it/prevenzione\\_reati\\_finanziari/prevenzione\\_reati\\_finanziari/Analisi\\_dei\\_rischi\\_di\\_riciclaggio\\_e\\_di\\_finanziamento\\_del\\_terrorismo\\_2018\\_-\\_Sintesi.pdf](http://www.dt.mef.gov.it/export/sites/sitodt/modules/documenti_it/prevenzione_reati_finanziari/prevenzione_reati_finanziari/Analisi_dei_rischi_di_riciclaggio_e_di_finanziamento_del_terrorismo_2018_-_Sintesi.pdf)

<sup>60</sup> Ibidem, p. 40. Si veda altresì ARCELLA e MANENTE (2020), p. 30, secondo cui «non è un caso, pertanto, che sia stata proprio la legislazione antiriciclaggio, sin dal 2017, ad essere la prima ad aver proposto una definizione normativa delle valute virtuali e dei prestatori di servizi ad esse collegate e dal 10 novembre 2019 sono entrate in vigore le nuove norme (v. nuovo testo D.Lgs. n. 231/2007) in tema di criptovalute, operatori in valute virtuali (c.d. exchange) e prestatori di servizi di portafoglio digitale (c.d. wallet provider), segno di come questo mondo sia oggetto di un tentativo di regolamentazione per contrastarne i possibili usi a fini di riciclaggio che possono riguardarlo». Viene da replicare che oramai, non è più l'eventuale utilizzo delle monete virtuali a fini di riciclaggio a giustificare una severa regolamentazione, ma quest'ultima a dimostrare l'eventuale utilizzo delle monete virtuali a fini di riciclaggio.

BELLAVIA, Gian Gaetano (2008): "Gli ordini professionali nella legge antiriciclaggio", in DANОВI, Remo (a cura di), "La nuova normativa antiriciclaggio e le professioni" (Milano, Giuffrè)

BIXIO, Ivan (2017): "Valute virtuali e adempimenti antiriciclaggio: riflessi sui soggetti obbligati, nuovi e non", *Corriere tributario*, n. 34, p. 2676

BRONZO, Pasquale (2019): "Attuazione della quinta direttiva antiriciclaggio", *Cassazione penale*, 2019, 11, p. 3840;

BURATTI, Bruno (2008): "Segnalazioni sospette e investigazioni", in DANОВI, Remo (a cura di), "La nuova normativa antiriciclaggio e le professioni" (Milano, Giuffrè)

CAPOLUPO, Saverio (2017): "L'approfondimento delle segnalazioni sospette", *Il fisco*, n. 32-33, p. 3146

CAPOLUPO, Saverio (2019): "Attuata la V direttiva antiriciclaggio", *Il fisco*, 42, p. 4053

CAPOLUPO, Saverio, CARBONE, Michele, STURZO, Gaspare (2011): "Antiriciclaggio – obblighi per i professionisti, intermediari e altri soggetti", (Milano, Ipsoa)

CARBONE, Michele, BIANCHI, Pasquale, VALLEFUOCO Valerio (2019): "Le nuove regole antiriciclaggio", (Milano, Ipsoa)

CASTRONUOVO, Alessio (2019): "Antiriciclaggio 5G, quali novità?", *Diritto24*

CENCI, Pietro (2010): "La nuova normativa antiriciclaggio – Direttive comunitarie e normativa nazionale", (Padova, Cedam)

COCUZZA, Claudio (2008): "Antiriciclaggio e segreto professionale: un passaggio difficile per la professione forense e le professioni libere", in DANОВI, Remo (a cura di), "La nuova normativa antiriciclaggio e le professioni" (Milano, Giuffrè)

COCUZZA, Claudio, GIOFFRÉ, Michele (2006): "Antiriciclaggio e professione forense: i nuovi compiti e le responsabilità dell'avvocato", (Milano, Ipsoa)

CORRADINO, Michele (2002): "Strategie normative di contrasto al riciclaggio di denaro di provenienza illecita", in DI BRINA, Leonardo e PICCHIO FORLATI, Laura (a cura di), "Normativa antiriciclaggio e contrasto alla criminalità economica" (Padova, Cedam)

CRAVETTO, Camilla (2018): "Le nuove norme sulla prevenzione del riciclaggio in attuazione della IV Direttiva europea", *Studium iuris*, n. 3, p. 277

D'AVIRRO, Antonio, DI VIZIO, Fabio, MANZIONE, Domenico (2020), "Profili penali dell'attività bancaria", (Milano, Giuffrè)

DE FLAMINNEIS, Siro (2017): "Gli strumenti di prevenzione del riciclaggio", *Diritto penale contemporaneo*, rivista trimestrale, 5, p. 259 ss.

DE LUCA, Nicola, PASSARETTA, Mario (2020): "Le valute virtuali: tra nuovi strumenti di pagamento e forme alternative d'investimento", *Società*, 5, p. 571 e ss.

DE NIGRIS, Marilisa (2017): "Nuove disposizioni antiriciclaggio e antiterrorismo D.Lgs. 25 maggio 2017, n. 90, Obblighi degli operatori in materia di antiriciclaggio", *Il diritto penale della globalizzazione*, p. 407 ss.;

DE STASIO, Vincenzo (2020): "Le monete virtuali: natura giuridica e disciplina dei prestatori di servizi connessi", in CIAN, Marco, SANDEI, Claudia (a cura di), *Diritto del Fintech*, (Padova, Cedam), p. 218.

DI VIZIO, Fabio (2019): "Gli obblighi antiriciclaggio per operatori in valute virtuali", *Discrimen.it*

DI VIZIO, Fabio (2020): "Il decreto legislativo 125/19 e l'attuazione della quinta direttiva europea antiriciclaggio", *Foro italiano*, parte V, col. 66



- FAIELLA, Simone (2001): "L'integrazione europea nella disciplina antiriciclaggio", *Giustizia penale*, II, p. 236
- FERRAJOLI, Luigi (2019): "Il contrasto punta a una cooperazione più forte e allargata", *Guida al diritto*, n. 48, p. 58-63;
- FISICARO, Emanuele (2008): "Antiriciclaggio e terza direttiva UE – Obblighi a carico dei professionisti intermediari finanziari e operatori non finanziari alla luce del D.Lgs. 231/2007", (Milano, Giuffrè)
- FLICK, Giovanni Maria (1994): "Accessi al settore finanziario e segnalazioni degli intermediari: controlli, obblighi, responsabilità", *Rivista italiana di diritto e procedura penale*, p. 1217
- FRIGO, Giuseppe (1995): "Norme procedurali antiriciclaggio, usura e indagine penale", *Cassazione penale*, p. 3134
- FUGGETTI, Cinzia (2011): "Dagli impulsi dell'Unione Europea alla normativa antiriciclaggio", in BERNASCONI Costanza, GIUNTA, Fausto (a cura di), *Riciclaggio e obblighi dei professionisti* (Milano, Giuffrè)
- GALMARINI, Sabrina, SABA, Claudio (2018): "IV Direttiva Antiriciclaggio e approccio basato sul rischio", *Diritto Bancario.it*
- GAMBOGI, Gianluca (2008): "Le violazioni di rilevanza penale dei nuovi obblighi antiriciclaggio", *Corriere tributario*, p. 940
- GAMBOGI, Gianluca (2017): "La disciplina sanzionatoria della nuova normativa antiriciclaggio di cui al d.lgs. 25 maggio 2017 n. 90", in MAIELLO, Vincenzo, DELLA RAGIONE, LUCA (a cura di), "Riciclaggio e reati nella gestione dei flussi di denaro sporco. Aggiornato al D.Lgs. n. 90/2017" (Milano, Giuffrè), p. 523 ss.
- GARAVAGLIA, Roberto (2017): "Valute virtuali e moneta elettronica: cosa cambia con il recepimento in Italia della quarta direttiva antiriciclaggio", *Pagamentidigitali.it*
- GENTILE, Gianluca (2015): "La disciplina sanzionatoria della normativa antiriciclaggio", in MAIELLO, Vincenzo (a cura di), *La legislazione penale in materia di criminalità organizzata, misure di prevenzione e armi*, (Torino, Giappichelli), p. 31 e ss.
- GIACOMETTI Tatiana, FORMENTI, Oliviero (2017): "La nuova disciplina in materia di prevenzione del riciclaggio e di finanziamento del terrorismo (d.lgs. 25 maggio 2017, n. 90)", *Diritto penale contemporaneo*
- GROSSO, Carlo Federico (1993): "Commento all'art. 5 L. 197/1991", in *Le nuove leggi civili commentate*, p. 1027
- GUERINI, Tommaso, INSOLERA, Gaetano (2019): "Diritto penale e criminalità organizzata", (Torino, Giappichelli)
- INGRAO, Cristina (2019): "Gli strumenti di prevenzione nazionali ed europei in materia di valute virtuali e riciclaggio", *Diritto penale contemporaneo, rivista trimestrale*, 2, p. 149
- INSOLERA, Gaetano (1996): "Diritto penale e criminalità organizzata", (Bologna, Il Mulino)
- KROGH, Marco (2009): "I principali obblighi antiriciclaggio ed antifinanziamento del terrorismo a carico dei professionisti", in KROGH, Marco, LICINI, Cesare (a cura di), "La normativa antiriciclaggio e antiterrorismo per i professionisti" (Milano, Ipsoa)
- LEMBO, Massimo, SCIALOJA, Antonio (2014): "Antiriciclaggio. Guida normativa e adempimenti obbligatori", (Rimini, Maggioli)
- LICINI, Cesare (2008): "Antiriciclaggio e antiterrorismo: gli obblighi di adeguata verifica della clientela a carico dei professionisti nel D.lgs. 231 del 2007", in DANOVÌ, Remo (a cura di), "La nuova normativa antiriciclaggio e le professioni" (Milano, Giuffrè)

- LUCEV, Riccardo, BONCOMPAGNI, Federico (2018): “Criptovalute e profili di rischio penale nella attività degli exchanger”, *Giurisprudenza penale web*, n. 3.
- LUDOVICO, Marco (2019): “Criptovalute, allarme Antimafia: “Paradiso finanziario virtuale”, *Il Sole 24 Ore*
- NADDEO, Marco (2019): “Nuove frontiere del risparmio, Bit Coin Exchange e rischio penale”, *Diritto penale e processo*, 1, p. 103
- PASSARETTA, Mario (2018): “Il primo intervento del legislatore italiano in materia di “valute virtuali”, *Le nuove leggi civili commentate*, 5, p. 1171.
- PASSARETTA, Mario (2019): “La nuova disciplina antiriciclaggio: tra sistemi di pagamento innovativi e nuove forme di finanziamento alle imprese”, in FIMMANÒ, Francesco, FALCONE, Giovanni (a cura di), *FinTech*, (Napoli, Edizioni scientifiche italiane), p. 472
- PERNICE, Carla (2018): “Digital currency e obbligazioni pecuniarie”, (Napoli, Edizioni scientifiche italiane)
- PERNICE, Carla (2019): “Criptovalute e bitcoin: stato dell’arte e questioni ancora aperte”, in FIMMANÒ, Francesco, FALCONE, Giovanni (a cura di), *FinTech*, (Napoli, Edizioni scientifiche italiane), p. 530
- PICOTTI, Lorenzo (2018): “Profili penali del cyberlaundering: le nuove tecniche di riciclaggio”, in *Rivista trimestrale di diritto penale dell’economia*, 2018, 3-4, 599.
- RAZZANTE, Ranieri (2003): “Osservazioni in tema di normativa antiriciclaggio e dovere di fedeltà dei dipendenti bancari”, *Giurisprudenza italiana*, p. 646
- RAZZANTE, Ranieri (2003b): “L’insostenibile soggettività della valutazione di operazioni sospette di riciclaggio”, *Diritto banca e mercato finanziario*, p. 580
- RAZZANTE, Ranieri (2007): “La regolamentazione antiriciclaggio in Italia”, (Torino, Giappichelli)
- RAZZANTE, Ranieri (2011): “La normativa antiriciclaggio in Italia” (Torino, Giappichelli)
- RAZZANTE, Ranieri (2011b): “La regolamentazione antiriciclaggio in Italia. Aggiornato alla delibera della Banca di Italia 10 marzo 2011” (Torino, Giappichelli)
- RAZZANTE, Ranieri (2013): “Antiriciclaggio e professionisti”, (Rimini, Maggioli)
- RAZZANTE, Ranieri (2019): “L’individuazione va documentata e motivata”, *Norme e Tributi Plus Fisco*
- RICCARDI, Giuseppe (2018): “voce Riserva di codice”, *Diritto penale contemporaneo*
- ROSSI, Alessandra (2018): “Prevenzione del riciclaggio e finanziamento del terrorismo: finalità e normative introduttive”, *Diritto penale contemporaneo, rivista trimestrale*, n. 1, p. 25.
- ROSSI, Alessandra (2018b): “Prevenzione del riciclaggio e finanziamento del terrorismo: finalità e novità normative ([Prevention of money laundering and terrorist financing: goals and regulatory changes]) Commento a d.lg. 25 maggio 2017, n. 90”, *Diritto penale e processo*, n. 1, p. 34
- RUBINO DE RITIS, Massimo (2018): “Bitcoin: una moneta senza frontiere e senza padrone? Il recente intervento del legislatore italiano”, in *Giustizia civile.com*, n. 3
- SAVONA, ERNESTO (1994): “La grande corsa: mafia e legislazione antiriciclaggio”, *Politica del diritto*, p. 55
- SCIANCELEPORE, Giovanni (a cura di) (2019): “Le operazioni sospette di riciclaggio”, (Torino, Giappichelli)

- SICIGNANO, Gaspere Jucan (2019): “*Bitcoin* e riciclaggio” (Torino, Giappichelli)
- SICIGNANO, Gaspere Jucan (2020): “L’acquisto di *bitcoin* con denaro di provenienza illecita”, Archivio penale, 2
- STURZO, Ludovica (2018): “*Bitcoin* e riciclaggio 2.0”, Diritto penale contemporaneo, n. 5, p. 29
- TROYER, Luca, ZANCAN, Monica (2018): “Giurisprudenza e attualità Giurisprudenza e attualità in materia di diritto penale d’impresa”, Rivista dottori commercialisti, n. 3, p. 521
- VADALÀ, Rosa Maria (2017): “La provenienza illecita nel delitto di riciclaggio: possibili novità dalla quarta direttiva antiriciclaggio?”, Rivista trimestrale di diritto penale dell’economia, n. 1-2, p. 234 ss.
- VADALÀ, Rosa Maria (2020): “Criptovalute e cyberlaundering: novità antiriciclaggio nell’attesa del recepimento della Direttiva (UE) 2018/1673 sulla lotta al riciclaggio mediante il diritto penale”, Sistema Penale
- VADALÀ, Rosa Maria (2020b): “La disciplina sugli usi e abusi delle valute virtuali”, in Diritto di Internet, n. 3, p. 397.
- VALLEFUOCO, Valerio (2019): “I gestori di criptovalute non sfuggono più ai vincoli”, Norme e Tributi, p. 6
- VALLEFUOCO, Valerio (2019b): “Antiriciclaggio, decreto in «Gazzetta»: adeguate verifiche da aggiornare entro il 30 giugno”, Norme e Tributi Plus Fisco
- VALLEFUOCO, Valerio (2017): “Antiriciclaggio: sanzioni proporzionate alla gravità delle violazioni”, Il fisco, n. 34, p. 3252
- VITOLO, Francesco (2019): “Il fenomeno del riciclaggio e del finanziamento al terrorismo mediante criptovalute: studio, applicazioni e metodologie di contrasto di una nuova «zona grigia»”, Rivista di diritto tributario, 2, p. 295 e ss.



Diritto Penale Contemporaneo

R I V I S T A   T R I M E S T R A L E

---

REVISTA TRIMESTRAL DE DERECHO PENAL  
A QUARTERLY REVIEW FOR CRIMINAL JUSTICE

<http://dpc-rivista-trimestrale.criminaljusticenetwork.eu>