UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO

I BATTELLI DEL RENO

Rivista on-line di diritto ed economia dell'impresa

(www.ibattellidelreno.uniba.it – www.ibattellidelreno.it)

Direzione

Gianvito Giannelli, Ugo Patroni Griffi, Antonio Felice Uricchio

Comitato scientifico

Sabino Fortunato **(coordinatore)** - Lorenzo De Angelis - Pietro Masi - Cinzia Motti - Antonio Nuzzo - Luigi Filippo Paolucci - Salvatore Patti - Michele Sandulli - Gustavo Visentini

Redazione di Bari

Emma Sabatelli, Giuseppina Pellegrino, Eustachio Cardinale, Francesco Belviso, Rosella Calderazzi, Barbara Francone, Anna De Simone, Valentino Lenoci, Enrico Scoditti, Emma Chicco, Claudio D'Alonzo, Giuditta Lagonigro, Manuela Magistro, Francesco Salerno, Concetta Simone, Rocco Lombardi

Redazione di Foggia

Michele Bertani, Andrea Tucci, Giuseppe Di Sabato, Corrado Aquilino, Pierluigi Pellegrino, Grazia Pennella, Annalisa Postiglione

Redazione di Lecce

Maria Cecilia Cardarelli, Alessandro Silvestrini, Giuseppe Positano, Andrea Sticchi Damiani

Redazione di Napoli

Andrea Patroni Griffi, Alfonso M. Cecere, Nicola De Luca, Carlo Iannello, Sergio Marotta, Francesco Sbordone, Pasquale Serrao d'Aquino

Redazione di Roma

Giustino Enzo Di Cecco, Paolo Valensise, Vincenzo Vitalone, Valeria Panzironi, Ermanno La Marca, Valentina Depau, Davide De Filippis

Redazione di Taranto

Daniela Caterino, Giuseppe Labanca, Cira Grippa, Gabriele Dell'Atti, Giuseppe Sanseverino, Pietro Genoviva, Francesco Sporta Caputi, Barbara Mele

Direzione
Piazza Luigi di Savoia n. 41/a
70100 – BARI - (Italy)
tel. (+39) 080 5246122 • fax (+39) 080 5247329
direzione.ibattellidelreno@uniba.it

Coordinatore della pubblicazione on-line: Giuseppe Sanseverino
Redazione: presso il Dipartimento Jonico in Sistemi Giuridici ed Economici del Mediterraneo: Società, Ambiente, Culture - Sezione di Economia -
Via Lago Maggiore angolo Via Ancona
74121 - TARANTO - (Italy)
tel (+39) 099 7720616 • fax (+39) 099 7723011
redazione.ibattellidelreno@uniba.it
giuseppe.sanseverino@uniba.it

ISSN 2282-2461 I Battelli del Reno [on line]

I Battelli del Reno, rivista on line di diritto ed economia dell'impresa, è registrata presso il Tribunale di Bari (decreto n. 16/2012)

La rivista è licenziata con Creative Commons Attribuzione – Non commerciale - Non opere derivate 3.0 Italia (CC BY-NC-ND 3.0 IT)

Alma Agnese Rinaldi – Antonio Uricchio

La prevenzione del riciclaggio nell'era delle cripto-attività: verso un modello europeo di vigilanza multilivello.

Sommario**:** 1. Tecniche di riciclaggio mediante cripto-asset e necessità di un rinnovato sistema di prevenzione. - 2. La tracciabilità dei flussi finanziari come principio strutturale della legalità economica nell'era digitale. - 3. Verso una regolazione integrata delle cripto-attività: dal Decreto Antiriciclaggio alla vigilanza europea centralizzata - 4. La genesi dell'AMLA come "tournant" nel nuovo quadro regolatorio europeo - 5. L'architettura istituzionale dell'AMLA e il modello multilivello di vigilanza europea -

Abstract

Il saggio analizza l'evoluzione del quadro normativo europeo e nazionale in materia di prevenzione del riciclaggio e del finanziamento del terrorismo con particolare riguardo alle cripto-attività. A partire dalla V Direttiva Antiriciclaggio, che per la prima volta introduce una definizione normativa di valuta virtuale e ne estende la disciplina ai prestatori di servizi di cambio e di portafoglio digitale, lo studio ricostruisce il percorso di progressiva integrazione tra la regolazione unionale e la disciplina italiana, culminato con l'attuazione del D.lgs. n. 231/2007 e con l'istituzione del registro OAM per gli operatori in valute virtuali.

L'indagine si sofferma, altresì, sul successivo sviluppo del sistema europeo di vigilanza, segnato dall'adozione del Regolamento (UE) 2023/1113 e del Regolamento (UE) 2023/1114 (MiCAR), nonché dalla nascita dell'*Anti-Money Laundering Authority* (AMLA). Quest'ultima viene esaminata quale architrave della nuova governance multilivello della compliance finanziaria, dotata di poteri ispettivi, conformativi e sanzionatori volti a garantire un'applicazione uniforme delle norme AML/CFT in tutti gli Stati membri.

Il contributo propone una lettura sistematica del processo di europeizzazione della vigilanza, evidenziando come l'AMLA si configuri non solo quale autorità tecnica, ma come autentico strumento di armonizzazione giuridica, capace di bilanciare l'esigenza di

effettività dei controlli con il rispetto dei principi di proporzionalità, sussidiarietà e tutela dei diritti degli operatori economici.

In tale prospettiva, la disciplina delle cripto-attività diviene il banco di prova di un diritto dell'economia europeo orientato alla trasparenza digitale, alla legalità finanziaria e alla cooperazione istituzionale.

The paper examines the evolution of the European and national regulatory framework on anti-money laundering (AML) and counter-terrorist financing (CTF), with particular reference to crypto-assets. Starting from the Fifth Anti-Money Laundering Directive, which for the first time provided a legal definition of virtual currencies and extended AML obligations to exchange and wallet service providers, the study traces the progressive alignment between EU regulation and the Italian legal framework, implemented through Legislative Decree No. 231/2007 and the establishment of the OAM register for virtual-asset operators.
The analysis then focuses on the subsequent development of the European supervisory system, marked by the adoption of Regulation (EU) 2023/1113 and Regulation (EU) 2023/1114 (*Markets in Crypto-Assets Regulation* – MiCAR), as well as by the creation of the *Anti-Money Laundering Authority* (AMLA). The paper explores the AMLA's role as the cornerstone of a new multilayered governance structure, endowed with investigative, supervisory and sanctioning powers aimed at ensuring uniform enforcement of AML/CFT rules throughout the Union.

From a systemic perspective, the article argues that the AMLA represents not merely a technical authority but a genuine instrument of legal harmonisation, designed to reconcile the effectiveness of enforcement with the principles of proportionality, subsidiarity and procedural fairness.

Within this framework, the regulation of crypto-assets emerges as a testing ground for a European economic law grounded in digital transparency, financial integrity and institutional cooperation.

1. Tecniche di riciclaggio mediante cripto-asset e necessità di un rinnovato sistema di prevenzione.

Lo sviluppo delle cripto-attività e, più in generale, il più ampio processo di digitalizzazione dell'economia e della finanza hanno sollevato questioni di particolare complessità circa la tenuta dei regimi giuridici esistenti e l'idoneità degli strumenti normativi tradizionali a fronteggiare le nuove forme di circolazione della ricchezza abilitate dalla tecnologia.

Le tecnologie a registro distribuito (*Distributed Ledger Technologies – DLT*) e, più in particolare, la *blockchain,* hanno infatti introdotto modalità di rappresentazione e di trasferimento del valore che si collocano ai margini – e talvolta al di fuori – delle categorie giuridiche consolidate, costringendo dottrina e autorità di vigilanza a interrogarsi sulla qualificazione delle cripto-attività e sul loro corretto inquadramento regolamentare.

Le criptovalute hanno rappresentato una delle più significative espressioni dell'innovazione tecnologico-finanziaria degli ultimi anni, pur continuando a sollevare interrogativi di fondo circa la loro effettiva utilità per il mercato e, soprattutto, circa la natura degli interessi che ne orientano l'utilizzo.

Ci si interroga, infatti, se esse costituiscano un progresso funzionale allo sviluppo economico o, piuttosto, uno strumento suscettibile di impiego selettivo, da parte di determinati soggetti, per finalità talvolta non lecite.

Sotto tale profilo, è opportuno precisare che la pericolosità connessa alle criptovalute non risiede tanto nello strumento in sé, quanto nell'uso che ne viene fatto: esse rappresentano un mezzo potenzialmente neutro, che può essere impiegato sia per scopi leciti sia per attività criminose. Il rischio emerge, dunque, non come carattere intrinseco della tecnologia, ma come conseguenza delle condotte illecite di chi ne sfrutta le peculiarità per fini di riciclaggio o di finanziamento del terrorismo.

Da ciò discende la necessità, oggi unanimemente riconosciuta, di rafforzare i presidi di vigilanza e i controlli di conformità, ponendo la prevenzione di tali fenomeni al centro delle priorità regolatorie e operative.

In tale contesto, gli operatori vigilati sono chiamati a implementare sistemi di controllo interni solidi e aggiornati, in grado di assicurare l'efficacia delle misure antiriciclaggio e antiterrorismo[1].

[1] Tra i molti, su questi temi, si vedano i contributi di E. GIRINO, *Criptovalute: un problema di legalità funzionale*, in *Riv. dir. banc.*, 2019, p. 733 ss.; G. RINALDI, *Approcci normativi e qualificazione giuridica delle criptomonete, in Contr. e impresa*, 2019, pp. 257 ss.; U. MALVAGNA – F. SARTORI, *Cryptocurrencies as Fungible Digital Assets Within the Italian Legal System: Regulatory and Private Law Issues*, in *The Italian Law Journal,* 2022, p. 481 ss.; R. BATTAGLINI – M.T. GIORDANO, *Blockchain e smart contract,* Giuffrè, Milano, 2019; A. DAVOLA, *Algoritmi decisionali e trasparenza bancaria,* Giappichelli, Torino, 2020; ID., *Quali controlli per le valute virtuali?* in *Riv. trim. dir. econ.,* Suppl. 3, 2022, pp. 52 ss.; A.A.V.V., *Tech Law. Il diritto di fronte alle nuove tecnologie*, Napoli, 2021; G. FINOCCHIARO, *Riflessioni sugli smart contract e sull'intelligenza artificiale*, in *Giustiziacivile.com*, 2020, pp. 1 ss.; G. FINOCCHIARO - C. BOMPREZZI, *A legal analysis of the use of blockchain technology for the formation of smart legal contracts*, in *Medialaws*, 2020, p. 111 ss.; M. PELLEGRINI, *L'intelligenza artificiale nell'organizzazione bancaria: quali sfide per il regolatore?* in *Riv. trim. dir. econ.*, 2021, pp. 422 ss.; V. LEMMA, *The public intervention on cryptocurrencies between innovation and regulation,* in *Open Review of Management Banking and Finance*, 2022; F. CAPRIGLIONE *Le cripto attività tra innovazione tecnologica ed esigenze regolamentari*, in *Riv. trim. dir. econ.,* 2022, pp. 225 ss.; M. IRRERA

È tuttavia indispensabile distinguere tra gli intermediari finanziari sottoposti a vigilanza prudenziale e la moltitudine di soggetti eterogenei che operano nell'ambito delle cripto-attività.

Sotto questo aspetto, permane una notevole asimmetria tra le strutture di compliance AML/CFT degli operatori tradizionali – che agiscono prevalentemente nel sistema "fiat-based" – e le c.d. "cripto-imprese", le quali hanno iniziato a confrontarsi con la normativa di settore, anche in materia di prevenzione del riciclaggio, soltanto in tempi recenti.

L'adozione di un approccio basato sul rischio specifico del singolo cripto-asset rappresenta, pertanto, un elemento cruciale; e tale approccio deve fondarsi su un processo di valutazione e aggiornamento costante, volto ad analizzare le tecniche e le caratteristiche operative proprie di ciascuna tipologia di cripto-attività, poiché ogni asset digitale presenta specificità tecniche e funzionali che possono essere sfruttate in modo diverso dagli autori di condotte illecite.

È ormai acquisito che i cripto-asset non costituiscano una categoria omogenea e che i soggetti criminali abbiano dimostrato una capacità di adattamento e di sfruttamento delle loro peculiarità assai più rapida rispetto a quella dei regolatori e, talvolta, degli stessi intermediari vigilati.

Ciò impone di abbandonare un approccio meramente teorico o "filosofico" al fenomeno, per privilegiare un'impostazione eminentemente tecnica e operativa, incentrata sulla comprensione profonda delle dinamiche informatiche e delle modalità di funzionamento delle blockchain e dei protocolli decentralizzati.

Molte delle tipologie di rischio di riciclaggio e di finanziamento del terrorismo che le imprese di cripto valute incontrano sono le stesse che si trovano ad affrontare tutte le istituzioni finanziarie.

L'analisi delle condotte criminali evidenzia, in effetti, un certo grado di uniformità nelle tecniche utilizzate – quali il *layering*, il *dusting*, il *money muling*, le transazioni *off-chain* o *cross-chain* – che costituiscono veri e propri schemi ricorrenti di dissimulazione e movimentazione dei proventi illeciti all'interno dell'ecosistema digitale.

Il fenomeno del *cyberlaundering* assume oggi una rilevanza di assoluta attualità, in quanto si colloca all'intersezione di due direttrici di innovazione giuridica ed economica. Da un

- M.S. CATALANO, *Criptovalute e NFT: il quadro normativo di riferimento,* in *Diritto ed economia dell'impresa*, 2022, pp. 614 ss.

lato, esso si connette alla progressiva emersione di nuovi *reati economici presupposto*, la cui configurazione risulta contraddistinta da un'elevata capacità espansiva e da una costante evoluzione nelle modalità di attuazione, resa possibile dall'impiego delle tecnologie digitali. Dall'altro, si inserisce nel più ampio alveo del *cybercrime*, categoria ormai consolidata nell'elaborazione dottrinale e giurisprudenziale, che comprende l'insieme delle condotte criminose realizzate attraverso, o ai danni, delle infrastrutture informatiche e telematiche.

Tale fenomenologia, da tempo oggetto di attenzione da parte delle autorità di *law enforcement,* delle magistrature nazionali, nonché degli organismi internazionali e sovranazionali – tra cui il *Financial Action Task Force (FATF-GAFI)* – è stata più volte segnalata come area ad alto rischio sistemico per l'integrità dei mercati e la sicurezza globale.

Le stesse Autorità sovranazionali e gli organismi di vigilanza intergovernativi hanno ripetutamente richiamato l'attenzione dei legislatori nazionali e dell'opinione pubblica sulla necessità di presidiare con strumenti normativi adeguati le molteplici e mutevoli forme di illecito che si sviluppano nel cosiddetto *cyberspace*, ambiente nel quale la dematerializzazione dei valori e la velocità dei flussi informativi rendono particolarmente complessa l'attività di prevenzione, identificazione e repressione delle operazioni di riciclaggio[2].

Il *Cyberlaudering*, inteso in senso a-tecnico, può essere descritto come l'insieme delle attività illecite finalizzate alla "ripulitura" non soltanto del denaro in senso stretto – definito nel linguaggio del web 3.0 come *valuta fiat* – ma altresì di ogni altra forma di bene, valore o utilità, incluse le cripto-attività, mediante l'impiego di strumenti o infrastrutture informatiche.

Tale fenomeno comprende, pertanto, sia l'utilizzo distorto di sistemi formalmente leciti e trasparenti – come i servizi di pagamento digitale, la moneta elettronica, le piattaforme di *crowdfunding* e, più in generale, la tecnologia *blockchain* – sia il ricorso a protocolli di comunicazione volti a garantire un elevato livello di anonimato, quali il *dark web* e il *deep web*, spesso impiegati per finalità elusive o chiaramente illecite.

Sotto il profilo strutturale, il reato di cyberlaundering non si discosta in modo sostanziale dal paradigma classico del riciclaggio delineato dalla prassi e dalla dottrina penalistica. Con le dovute cautele e adattamenti, può infatti affermarsi che la tradizionale articolazione "tripartita" del riciclaggio – placement, layering e integration – sia suscettibile di applicazione anche al contesto digitale.
Tali fasi corrispondono, rispettivamente, alle operazioni di sostituzione, trasferimento o

[2] Sul punto si richiama il lavoro di L. PICOTTI, *Profili penali del Cyberlaundering: le nuove tecniche di riciclaggio,* in *Riv. Trim. Dir. Pen. Dell'Econ.*, Cedam, 3-4, 2018.

compimento di altre condotte idonee a ostacolare l'identificazione dell'origine delittuosa dei capitali, tanto in forma di "valuta fiat" quanto di cripto-asset.

In linea teorica, le suddette attività possono essere ricondotte alle ipotesi tipiche di cui agli artt. 648-bis, 648-ter e 648-ter.1 c.p., rispettivamente in materia di riciclaggio, reimpiego e autoriciclaggio, nonché ad altre figure di reato strumentali o accessorie, accomunate dalla funzione di dissimulare o reimpiegare beni, capitali o utilità di provenienza illecita. In particolare, le operazioni di compravendita di cripto-asset, la loro conversione in valuta *fiat* o in altri token digitali, e più in generale l'utilizzo di infrastrutture decentralizzate per occultare la tracciabilità dei flussi, costituiscono modalità operative che consentono di realizzare in chiave digitale le medesime fasi del processo di "ripulitura" del denaro già note nella prassi tradizionale.

Dal punto di vista della rilevanza penale, appare sempre più evidente il ricorso a circuiti extra-bancari, deregolamentati o decentralizzati, che sfuggono ai tradizionali presidi di vigilanza, rendendo complesso – se non impossibile – il tracciamento dell'origine delle transazioni e l'identificazione dei soggetti effettivamente coinvolti.

La natura crittografica delle cripto-valute, fondata sulla pseudonimità e sulla distribuzione del registro, costituisce un ulteriore fattore di opacità che indebolisce l'efficacia degli strumenti investigativi tradizionali.

A ciò si aggiunge la profonda disomogeneità delle discipline nazionali che regolano la raccolta, l'investimento e lo scambio di somme, crediti e valori nel cyberspazio. Tale frammentazione normativa – sintomatica della mancanza di un quadro armonizzato a livello internazionale – genera vaste aree di incertezza giuridica, le cosiddette zone grigie, che vengono sistematicamente sfruttate dagli operatori criminali per eludere i controlli e sottrarsi alle responsabilità derivanti dalle normative antiriciclaggio[3].

La conoscenza e il monitoraggio di tali schemi si rivelano dunque imprescindibili per la predisposizione di efficaci sistemi di prevenzione, fondati sulla cooperazione tra autorità di vigilanza, intermediari vigilati e operatori tecnologici del settore delle cripto-attività[4].

---

[3] Ampiamente sul tema del Cyberlaundering e sulle nuove tecniche di riciclaggio e finanziamento mediante crypto -asset, si veda, G. MAGGIO, *Tecniche di riciclaggio e di finanziamento del terrorismo mediante crypto-asset,* in (a cura di) F. Annunzziata – D. Varani, *Cripto attività. Antiriciclaggio e gestione dei rischi aziendali,* Pacini Giuridica, 2024, p. 81 ss.

[4] Cfr., J.G. MICKINLAY, *Enforcing the Rights of Cyptocreditors,* in *Barkeley Business Law Journal,* (20) (1), 2023, p. 83 ss.

ISSN 2282-2461 I BATTELLI DEL RENO [ON LINE]

Nondimeno, persistono significative sfumature interpretative e aree di divergenza che impediscono di ricondurre le diverse manifestazioni del rischio antiriciclaggio a un unico insieme di indicatori di anomalia.

Ogni tipologia di operatività in cripto-asset, infatti, presenta proprie peculiarità tecniche e dinamiche transazionali che rendono necessaria una costante revisione dei parametri di valutazione e degli strumenti di monitoraggio.

L'evoluzione del quadro normativo, tanto a livello europeo quanto nazionale, può comportare modifiche sostanziali ai framework di compliance esistenti o richiedere la predisposizione di regolamenti interni specificamente dedicati alla gestione delle attività in cripto-asset, siano esse già operative o ancora in fase di sviluppo.

Le innovazioni, spesso spinte dall'evoluzione tecnologica e dalla creatività degli operatori del settore, impongono alle istituzioni finanziarie e ai soggetti vigilati di aggiornare in modo continuo i propri presidi di prevenzione, tenendo conto delle nuove fattispecie di rischio e delle modalità operative emergenti.

Nel contesto crittografico, la complessità con cui gli eventi si manifestano risulta sensibilmente superiore rispetto al sistema finanziario tradizionale, già di per sé articolato. Le combinazioni che possono originarsi dall'interazione tra i meccanismi delle blockchain e gli spazi del dark web generano scenari di difficile monitoraggio, assai più problematici rispetto alla tracciabilità delle operazioni monetarie convenzionali, sulle quali il sistema di vigilanza ha maturato decenni di esperienza e di prassi consolidate.

In tale quadro, le conseguenze della mancata conformità alla normativa antiriciclaggio e di contrasto al finanziamento del terrorismo per gli intermediari vigilati assumono una rilevanza sempre più incisiva.

Gli operatori che dimostrino una supervisione inefficiente – non solo rispetto ai prodotti e servizi offerti, ma soprattutto riguardo al comportamento della propria clientela che opera in autonomia su piattaforme di scambio, anche estere – espongono sé stessi a gravi rischi sanzionatori, a rilevanti danni reputazionali e alla possibile erosione del fatturato derivante da attività non conformi.

Le ripercussioni di tali inefficienze si riverberano, inoltre, sull'intero sistema bancario e finanziario, minandone la stabilità complessiva e, soprattutto, la fiducia dei mercati.

Parallelamente, mentre i governi e le autorità di vigilanza a livello globale sono impegnati a delineare i rispettivi quadri regolatori in materia di cripto-attività e a predisporre meccanismi di controllo e di supervisione più sofisticati, le strategie della

criminalità finanziaria si evolvono con rapidità, adattandosi alle nuove tecnologie e sfruttando le aree grigie della regolamentazione.

Le imprese e gli intermediari si trovano, così, ad affrontare un contesto in costante mutamento, caratterizzato dall'emersione di modelli operativi sconosciuti persino ai regolatori.

Questa continua trasformazione del rischio presenta, al tempo stesso, ampi margini di opportunità economica per gli operatori che sappiano coniugare innovazione e compliance: la solidità del business dipende, infatti, dal grado di effettiva attuazione dei presidi normativi e dalla capacità di integrare la conformità AML/CFT nei processi aziendali, evitando che essa resti una mera dichiarazione di principio o, peggio, un adempimento formale eluso.

La principale sfida per gli intermediari che intendano operare nel settore delle criptovalute resta, dunque, la frammentazione regolamentare tra i diversi ordinamenti. L'assenza di standard comuni internazionali rende complessa l'applicazione coerente delle norme antiriciclaggio, ostacolando la creazione di un ecosistema realmente sicuro, competitivo e armonizzato. Da ciò deriva la necessità, sempre più avvertita, di un coordinamento sovranazionale che garantisca un equilibrio tra innovazione, competitività e integrità dei mercati finanziari digitali[5].

In questa prospettiva, i principali organismi internazionali – dal Comitato di Basilea per la vigilanza bancaria al Financial Stability Board (FSB), passando per il FATF-GAFI– hanno richiamato la necessità di una risposta coordinata ai rischi derivanti dalla crescente interconnessione tra mercati finanziari tradizionali e mercati delle cripto-attività.

Come osservato in più occasioni dal FSB, l'espansione delle forme di "*tokenization*" e la diffusione di strumenti digitali di investimento e pagamento, stanno progressivamente erodendo i confini tra finanza regolamentata e finanza decentralizzata, ponendo in discussione la tradizionale segmentazione tra intermediari vigilati e operatori non regolamentati[6].

---

[5] Cfr. P. GIUDICI – G. FERRARINI, *Digital Offerings and Mnadatory Disclosure: A Market Based Critique of MiCA*, in (cura di) E. Avgouleas – M.H. Arjosola, *Digital Finance in Europe: Law, Regulation and Governance*, De Gruyter, 2022, p. 87 ss.

[6] Cfr., su questi aspetti, M. LORENZONI - G. FREGA, *Il "Fintech" e la "Dark finance": quali rischi per i risparmiatori,* in (a cura di) L. Ammanniti, A. Canepa, G.L. Greco, U. Minneci, *Mercati finanziari e transizione digitale. Una tassonomia*, Giappichelli, 2025, p. 71 ss. Cfr., anche, L. GANDOLFI, *Cripto-asset e intermediari vigilati: una guida per progettare e presentare un piano AML volto a mitigare efficacemente i rischi,* in (a cura di) F. Annunziata – D. Varani, *Cripto attività. Antiriciclaggio e gestione dei rischi aziendali*, Pacini Giuridica, 2024, p. 51 ss.

Le nuove modalità di circolazione della ricchezza hanno reso sempre più arduo per i regolatori individuare, caso per caso, la disciplina giuridica applicabile a tali strumenti, dovendo ricondurre le diverse tipologie di cripto-attività – in ragione dei diritti o dei valori che esse incorporano – alle appropriate categorie giuridiche (finanziarie, valutarie, patrimoniali o ibride).

A ciò si è accompagnata una crescente frammentazione normativa e interpretativa, tanto a livello sovranazionale quanto interno, che ha prodotto un quadro regolatorio disomogeneo, fonte di incertezza per gli operatori e potenzialmente suscettibile di agevolare fenomeni di "*regulatory arbitrage"* e di *"moral hazard"*.

Per superare tali criticità e promuovere uno sviluppo ordinato, sicuro e trasparente dei mercati digitali, l'Unione europea ha adottato il Digital Finance Package, presentato nel 2020 e destinato a costituire la nuova architettura regolatoria della finanza digitale.

Elemento cardine del pacchetto è il Regolamento (UE) 2023/1114 del 31 maggio 2023 *(Markets in Crypto-Assets Regulation – MiCAR)*, il quale introduce una disciplina organica delle cripto-attività non ancora ricomprese nel perimetro delle regolazioni finanziarie previgenti (quali la MiFID II o la PSD2), regolando tanto l'emissione e l'offerta dei *token*, quanto la prestazione dei servizi connessi alla loro negoziazione, custodia e scambio[7].

[7] Il MiCAR adotta un regime ad hoc per tutte le cripto-attività che non si qualificano come strumenti finanziari, distinguendoli in tre classi: e prime due classi, token collegati ad attività e token di moneta elettronica, includono cripto-attività che legano il loro valore a un asset specifico o a un insieme di asset e sono note sul mercato come "stablecoin". Il MiCAR dedica loro un'attenzione particolare soprattutto perché laddove fossero ampiamente utilizzate come mezzo di pagamento potrebbero sollevare questioni di stabilità finanziaria e sovranità monetaria. La terza classe comprende invece i c.d. utility token, definiti come un tipo di cripto-attività destinata a fornire l'accesso a un bene o servizio digitale prestato dall'emittente. Non è chiaro se nella categoria residuale rientrino token diversi dagli utility token. Comunque, la categoria è stata creata per imporre obblighi informativi in relazione a progetti non ancora operativi per cui c'è il rischio che il bene o il servizio proposto non venga mai fornito. Il MiCAR regolamenta anche i prestatori di servizi per la cripto attività, assoggettandoli ad una disciplina del tutto simile alla disciplina dei prestatori di servizi finanziari, imponendo quindi i requisiti patrimoniali, di governance e obblighi di custodia. I servizi offerti comprendono sia i servizi tipicamente prestati dagli intermediari tradizionali che svolgono attività di trading e post-trading, sia i servizi tipicamente prestati dalle imprese di investimento. È lo stesso MiCAR che identifica il servizio finanziario corrispondente nella regolamentazione finanziaria. Il MiCAR non ha però regolamentato due servizi che stanno acquisendo sempre più importanza, ovvero i prestiti di cripto-attività e il servizio di staking. Si tratta di un servizio offerto in relazione a quelle block chain che usano la cosiddetta Proof of Stake al fine di validare le nuove transazioni. I validatori, che nella prassi di mercato sono i cripto-mercati, raccolgono dagli utenti le cripto-attività e le utilizzano nell'ambito dell'attività di validazione. Le cripto-attività generate come forma di remunerazione per l'attività di validazione sono distribuite dai cripto-mercati agli utenti pro-quota, dedotte le commissioni per il servizio. I prestiti in cripto-attività sono organizzati dei cripto-mercati mettendo a disposizione degli utenti una piattaforma che consente di mettere in contatto quelli che intendono fornire i prestiti e coloro che desiderano riceverli. É anche possibile che siano gli stessi cripto-mercati ad effettuare i prestiti in cripto-attività ai propri clienti. Infine la MiCAR non

Il *Digital Finance Package* include, inoltre, il Regolamento (UE) 2022/858 relativo ai sistemi basati su DLT e il Regolamento (UE) 2022/2554 (*Digital Operational Resilience Act – DORA)*, volto a rafforzare la resilienza operativa digitale del settore finanziario.

Insieme, questi strumenti costituiscono il primo tentativo di costruire un corpus normativo coerente che affronti in modo unitario le sfide della digitalizzazione dei mercati finanziari, coniugando innovazione e tutela della stabilità[8].

La diffusione delle cripto-attività ha inevitabilmente posto in evidenza anche le implicazioni sotto il profilo della prevenzione del riciclaggio e del finanziamento del terrorismo, incidendo sulla tenuta e sull'efficacia dei presidi di controllo tradizionalmente previsti dal sistema AML/CFT.

Un cambio di paradigma potrà compiutamente realizzarsi con l'entrata in vigore del citato *AML Package,* nel quadro organico delle sue molteplici componenti normative. In un approccio improntato alla necessaria integrazione e convergenza tra le diverse fonti, il coordinamento del regolamento concernente i dati informativi che accompagnano i trasferimenti di cripto-attività con il Regolamento *Markets in Crypto-Assets (MiCA)* appare idoneo ad assicurare un livello di tracciabilità esteso e capillare, non solo in relazione al luogo, all'importo, all'oggetto, alla data della singola transazione e ai soggetti coinvolti, ma anche rispetto alla sequenza temporale delle operazioni che, progressivamente, abbiano interessato i medesimi fondi o asset digitali.

Tale ricostruzione dinamica consente di individuare eventuali profili di rischio o di anomalia, agevolando l'emersione di condotte potenzialmente criminose e l'individuazione dei nessi causali e temporali tra operazioni apparentemente frazionate o dissimulate.

Grazie all'equiparazione, ai fini giuridici e di vigilanza, tra i trasferimenti di cripto-attività e i trasferimenti bancari di fondi — attualmente riferiti alla moneta reale, scritturale o elettronica — il Regolamento (UE) 2023/1113 estende alle operazioni in cripto-attività

si occupa dell'attività di compensazione svolta dei cripto-mercati, ovvero l'attività di gestione delle garanzie raccolte dai clienti a copertura delle reciproche esposizioni debitorie nei casi, per esempio, di prestiti di cripto-attività. Cfr., in argomento, D. SARTI, La funzione non finanziaria dei token MiCAR, Riv. Orizzonti dir. comm., n. 3, 2024.

[8] Cfr., R. LENER, *I mercati finanziari e il sistema di vigilanza*, in A.A.V.V., *Diritto del mercato finanziario*. Saggi, Torino, 2011; S. AMOROSINO, *Mercati finanziari (vigilanza sui)* in (diretto da) S. Cassese, *Dizionario del diritto pubblico,* Milano, 2006; R. COSTI, *L'ordinamento bancario*, Bologna, 2012; C. BRESCIA MORRA, Il diritto delle banche, Bologna, 2016, p. 774 ss.

il regime di tracciabilità già vigente per la finanza tradizionale, con particolare riferimento alla "*travel rule*"[9].

Quest'ultima impone che le informazioni relative all'origine e alla destinazione finale dei cripto-asset accompagnino la transazione lungo l'intero percorso operativo e siano conservate da entrambi i soggetti partecipanti — ordinante e beneficiario — garantendo, così, una catena informativa continua e verificabile.

Un assetto normativo efficace, coerente con i principi di proporzionalità e di neutralità tecnologica, deve pertanto assicurare che le cripto-attività che presentano rischi analoghi a quelli propri delle attività finanziarie tradizionali siano sottoposte a obblighi regolatori e a presidi di controllo equivalenti, evitando zone d'ombra o asimmetrie di vigilanza che potrebbero compromettere la solidità e l'integrità complessiva del sistema finanziario dell'Unione.

Già il FATF-GAFI**,** sin dal 2019, aveva raccomandato l'estensione degli obblighi di "*customer due diligence*", conservazione dei dati e segnalazione delle operazioni sospette ai *Virtual Asset Service Providers (VASP),* riconoscendo l'esigenza di un approccio globale fondato sul principio di "*same activity, same risk, same rules*"[10].

Anche le Autorità europee di vigilanza – EBA (*European Bancking Authority*)**,** ESMA **(***European Securities and Markets Authority)* ed EIOPA (*European Insurance and Occupational Pensions Authority)* – hanno successivamente evidenziato la necessità di un coordinamento più stretto tra la disciplina prudenziale e quella antiriciclaggio, in modo da garantire la tracciabilità dei flussi in cripto-attività e la protezione dell'integrità del mercato unico[11].

---

[9] Adottato ufficialmente dalla FATF-GAFI, a partire dal 2019, la "travel rule" rappresenta una delle pietre angolari sulle quali costruire un efficace, specifico, presidio antiriciclaggio a livello globale: dal momento che, sul piano tecnico, non esiste una soluzione univoca per tutti i Virtual asset service providers essa costituisce al tempo stesso una delle più importanti sfide di conformità: cfr. L. GANDOLFI, *Cripto-asset e intermediari vigilati: una guida per progettare e presentare un piano AML volto a mitigare efficacemente i rischi,* in (a cura di) F. Annunziata – D. Varani, *Criptoattività. Antiriciclaggio e gestione dei rischi aziendali,* cit., p. 51 ss.

[10] Approccio rinvenibile anche nello Statement pubblicato dal Financial Stability Board del luglio 2022, centrato sull'idea di una regolamentazione di una supervisione delle criptovalute dei relativi mercati efficaci e commisurati ai rischi che comportano, sia a livello nazionale che internazionale.

[11] Le tre autorità di vigilanza europee (EBA, EIOPA ed ESMA – le ESAs) hanno pubblicato in data 12 luglio 2024 in consultazione le linee guida ai sensi del Regolamento delle cripto-attività MiCAR, che stabilisce modelli per le spiegazioni e i pareri legali relativi alla classificazione dei crypto-asset e un test standardizzato per promuovere un approccio comune alla classificazione (si veda, CONSULTATION PAPER, *Draft Guidelines on templates for explanations and opinions, and the standardised test for the classification of crypto-assets, under Article 97(1) of Regulation (EU) 2023/1114,* in dirittobancario.it). Le linee guida devono inoltre includere un modello per la spiegazione e il parere e un test standardizzato per la classificazione dei cripto-asset. Per

In questo contesto, il 20 luglio 2021 la Commissione europea ha presentato un pacchetto di riforme volto a istituire un nuovo quadro unitario europeo per la prevenzione del riciclaggio e del finanziamento del terrorismo.

La riforma, tuttora in corso di attuazione, si articola in quattro pilastri fondamentali:

(i) il Regolamento istitutivo dell'Anti-Money Laundering Authority (AMLA), chiamata a esercitare funzioni di vigilanza diretta sui soggetti a rischio transfrontaliero[12];
(ii) il Regolamento AML/CFT contenente norme direttamente applicabili in materia di adeguata verifica della clientela, titolarità effettiva e obblighi di segnalazione;
(iii) la nuova Direttiva AMLD6, destinata a sostituire la Direttiva (UE) 2015/849 e a regolare gli aspetti di cooperazione giudiziaria e penale;
(iv) la revisione del Regolamento (UE) n. 2015/847 sui trasferimenti di fondi, volta a garantire la piena tracciabilità dei trasferimenti di cripto-attività (*Transfer of Funds Regulation – TFR*)[13].

L'insieme di questi interventi riflette una strategia normativa ambiziosa, finalizzata a costruire un ecosistema giuridico integrato della finanza digitale, in cui l'innovazione tecnologica e la prevenzione dei rischi di riciclaggio non si pongano in antitesi, ma come componenti complementari di un medesimo obiettivo di legalità economica, trasparenza e stabilità sistemica.

---

supportare i partecipanti al mercato e le autorità di vigilanza nell'adozione di un approccio convergente alla classificazione dei cripto-asset, le Linee guida pubblicate in consultazione propongono quindi un test standardizzato, nonché dei modelli di spiegazioni e pareri legali, che forniscono descrizioni della classificazione regolamentare dei cripto-asset nei seguenti casi:

- token con riferimento all'attività (ART): il libro bianco per l'emissione degli ART, che contiene informazioni complete sulla criptovaluta, deve essere accompagnato da un parere legale che spieghi la classificazione della criptovaluta, e, in particolare, il fatto che non si tratta di un EMT né di una criptovaluta che potrebbe essere considerata esclusa dall'ambito di applicazione del MiCAR.
- cripto-asset che non sono ART o EMT ai sensi del MiCAR: il libro bianco per il cripto-asset deve essere accompagnato da una spiegazione della classificazione del cripto-asset, e, in particolare, il fatto che non sia un EMT, un ART o un cripto-asset escluso dall'ambito di applicazione del MiCAR.

[12] Regolamento (UE) 2024/1620 del Parlamento europeo e del Consiglio, del 31 maggio 2024, che istituisce l'Autorità per la lotta al riciclaggio di denaro e al finanziamento del terrorismo e che modifica i regolamenti (UE) n. 1093/2010, (UE) n. 1094/2010 e (UE) n. 1095/2010 (Testo rilevante ai fini del SEE) PE/35/2024/INIT, consultabile al sito *eur-lex.europa.eu*

[13] I tre atti normativi, che rappresentano l'*AML package,* sono stati oggetto della delega, finalizzata al loro recepimento e adeguamento della normativa nazionale, attribuita al Governo con l'articolo 14 della legge 13 giugno 2025, n.91 (legge di delegazione europea).

Alla luce di tale evoluzione, si rende necessario esaminare criticamente non solo i profili più significativi dell'attuale e futuro assetto regolatorio europeo, ma anche le ricadute operative per gli intermediari e le autorità nazionali, chiamati ad adeguare i propri modelli di vigilanza ai nuovi paradigmi di movimentazione digitale della ricchezza e ai rischi emergenti di *money laundering* tecnologico (*tech-enabled laundering*)[14].

2. La tracciabilità dei flussi finanziari come principio strutturale della legalità economica nell'era digitale.

Nel diritto dell'economia contemporaneo, la tracciabilità dei flussi finanziari non rappresenta soltanto uno strumento tecnico di controllo, ma un vero e proprio principio ordinante dell'ordinamento finanziario. Essa esprime la tensione costante fra libertà di circolazione del capitale e tutela dell'integrità del sistema, divenendo il criterio attraverso cui si misura la capacità dello Stato e, oggi, dell'Unione Europea di esercitare una sovranità effettiva su fenomeni economici globalizzati e digitalizzati.

Laddove la tracciabilità venga meno, si apre inevitabilmente lo spazio per forme di criminalità economica ad alta sofisticazione, le quali sfruttano la smaterializzazione del valore e la transnazionalità dei mercati per sottrarsi ai tradizionali presìdi di legalità. L'impossibilità o la rilevante difficoltà di ricostruire retrospettivamente i movimenti di ricchezza fino a individuare gli autori o i beneficiari finali delle operazioni genera un deficit di conoscenza che è, prima ancora che tecnico, giuridico: un vuoto informativo che impedisce l'imputazione della responsabilità e compromette la stessa effettività della norma penale e amministrativa.

In questo vuoto si radicano le manifestazioni più gravi di criminalità economica — evasione fiscale, corruzione, traffici illeciti, riciclaggio e finanziamento del terrorismo — che, sfruttando le opacità dei nuovi strumenti finanziari digitali, minano la fiducia sistemica su cui si fonda il mercato e disarticolano il nesso di reciprocità fra libertà economica e responsabilità giuridica.

La stessa stabilità del sistema finanziario, nella sua dimensione macroeconomica e sistemica, risulta in tal caso inevitabilmente minacciata, con effetti potenzialmente destabilizzanti tanto per i mercati quanto per gli operatori che agiscono nel rispetto della legalità economica.

[14] Cfr., E. AVGOULEAS – E. SERETAKIS, *How Should Crypto Lending Be Regulated under EU Law? in European Business Organization Law Review,* 24, 2023, p. 429 ss. Si veda anche *Cryptovantage, Top Crypto Margin Trading Exchanges*, in *,cryptovantage.com*

Non sorprende, pertanto, che le istituzioni europee e internazionali abbiano da tempo maturato piena consapevolezza della natura pervasiva di tali rischi, sottolineando l'urgenza di una regolamentazione idonea a contemperare libertà di iniziativa economica, integrità del sistema e tracciabilità dei flussi.

Consapevoli di tale interrelazione, le istituzioni internazionali ed europee hanno progressivamente teorizzato un diritto alla tracciabilità come corollario della accountability finanziaria. In questa direzione si collocano i lavori del Financial Action Task Force (FATF-GAFI), i rapporti della Banca Centrale Europea (Report on Virtual Currency Schemes, 2012; A Further Analysis, 2015) e l'Opinion on Virtual Currencies dell'EBA (2014).

Tali contributi, lungi dal limitarsi a un'analisi tecnica, hanno messo in luce la valenza sistemica delle valute virtuali e delle cripto-attività, segnalando il passaggio da un'economia basata su entità patrimoniali identificabili a un'economia di valori algoritmici, in cui l'identità giuridica del titolare tende a dissolversi dietro la pseudonimia informatica.

In questo contesto, l'EBA ha distinto cinque categorie di rischio — per gli utenti, indipendenti dai partecipanti, per l'integrità del sistema, di cambio e per le autorità di vigilanza — individuando proprio nei rischi per l'integrità del sistema la minaccia più elevata. Si tratta dei rischi che nascono quando la funzione di anonimato tecnologico viene piegata a finalità di riciclaggio, occultamento patrimoniale o finanziamento illecito. L'anonimato, da garanzia di privacy, diviene così uno strumento di opacità, capace di neutralizzare i tradizionali meccanismi di imputazione soggettiva e di tracciamento oggettivo delle operazioni.

La progressiva presa d'atto di tali rischi ha spinto il legislatore europeo a rafforzare, in chiave evolutiva, la disciplina della trasparenza digitale, estendendone la portata oltre il perimetro dei mercati tradizionali. Tuttavia, il diritto positivo continua a confrontarsi con una difficoltà definitoria di fondo: la mancanza di una nozione giuridica univoca di criptovaluta o valuta virtuale. Tale incertezza non è meramente semantica, ma riflette la natura ibrida e metamorfica delle cripto-attività, che si collocano in uno spazio intermedio fra strumento di pagamento, bene di investimento e veicolo di valore.

La definizione introdotta dalla Direttiva (UE) 2018/843 (V Direttiva AML) — poi recepita nell'ordinamento italiano con il D.lgs. n. 125/2019 — rappresenta un tentativo di giuridificazione del fenomeno, nel solco della nozione proposta dall'EBA nel 2014. L'art. 1, comma 2, lett. qq), del D.lgs. 231/2007, come modificato, definisce la valuta virtuale come:

«una rappresentazione digitale di valore che non è emessa né garantita da una banca centrale o da un'autorità pubblica, non è necessariamente collegata a una valuta avente corso legale, non possiede lo status giuridico di valuta o moneta, ma è accettata da persone fisiche o giuridiche e utilizzata come mezzo di scambio per l'acquisto di beni e servizi, per finalità di investimento, e può essere trasferita, archiviata e negoziata elettronicamente».

La menzione esplicita della finalità di investimento segna il riconoscimento legislativo della trasformazione delle valute virtuali in asset finanziari a pieno titolo[15], idonei a incidere sulla stabilità dei mercati e sul sistema dei controlli antiriciclaggio.

La cripto-attività non è più un mero strumento di scambio, ma un oggetto giuridico complesso, in cui convergono funzioni economiche, tecnologiche e speculative.

In tal senso, la distinzione operata dalla BCE fra Closed, Unidirectional e Bidirectional Virtual Currency Schemes acquista rilievo sistematico: solo quest'ultima categoria, caratterizzata dalla piena convertibilità con le valute *fiat*, realizza quella permeabilità tra sfera digitale e reale che costituisce la premessa logica e giuridica del rischio di riciclaggio.

La disciplina europea più recente, culminata nel Regolamento (UE) 2023/1114 (Markets in Crypto-Assets Regulation – MiCAR), sostituisce la terminologia tradizionale con la più ampia nozione di cripto-attività, definita come:

«una rappresentazione digitale di un valore o di un diritto che può essere trasferita e memorizzata elettronicamente, utilizzando la tecnologia di registro distribuito o una tecnologia analoga» (art. 3).

La portata volutamente generale di tale definizione risponde all'esigenza di predisporre un quadro regolatorio adattivo, capace di accogliere le continue metamorfosi della tecnologia DLT.

Non meno significativo è il coordinamento con il Regolamento (UE) 2023/1113 sui trasferimenti di fondi, che rinvia espressamente alle definizioni del MiCAR, sancendo la nascita di un ecosistema normativo integrato tra disciplina dei mercati digitali e normativa AML/CFT.

Un rilievo paradigmatico deve essere, in questa sede, riconosciuto alla prima e tuttora più diffusa delle criptovalute: il Bitcoin che costituisce il prototipo attraverso cui indagare

[15] "Assets that are contained on a blockchain network, where they appear as digital units of account, are referred to as "crypto-assets"; così, M. LEHMANN – S. OMLOR – M. LINK, *Kryptowährungen und Token*, 2, ed. 2023, cap. 5, par. 28, p. 41.

le principali implicazioni, anche penalistiche, della (non) tracciabilità delle transazioni in cripto-attività[16].

Nei sistemi occidentali, la circolazione del denaro è da sempre soggetta a una doppia verifica — formale, mediante l'identificazione del soggetto, e sostanziale, mediante la riconducibilità dei flussi al titolare effettivo — che assicura la compatibilità tra mercato e legalità.

L'innovazione FinTech ha invece incrinato tale paradigma, creando una dimensione finanziaria de-territorializzata, nella quale la tecnologia sostituisce il diritto come infrastruttura della fiducia[17].

Si delinea così una "zona franca digitale", nella quale la decentralizzazione e l'anonimato, nati per emancipare l'economia dalla mediazione istituzionale, possono trasformarsi in spazi di invisibilità giuridica.

In tali spazi, la sovranità normativa rischia di dissolversi, e con essa la capacità dell'ordinamento di garantire la riconducibilità dei flussi e la legittimità delle transazioni.

[16] Lo considerano una cattiva moneta, M. AMATO - L. FANTACCI, *Per un pugno di bitcoin. Rischi e opportunità delle monete virtuali*, Milano, 2018, p. 189, secondo cui «l'attenzione mediatica che ha suscitato Bitcoin è del tutto smisurata rispetto alla sua importanza e al suo significato economico, attuale e potenziale». Per una critica circa l'uso del termine "valuta" che finirebbe per creare confusione sulla reale natura di bitcoin, v. N. VARDI, "*Criptovalute" e dintorni: alcune considerazioni sulla natura giuridica dei bitcoin,* in *Dir. inf. e inform.*, 2015, p. 445 ss., che richiamando la distinzione tra moneta e, per l'appunto valuta, evidenzia come la seconda si riferisca, di norma, alla moneta avente corso legale, ex lege, ossia quanto di più lontano ci possa essere dalle *cryptocurrencies*, tipo bitcoin. Per una ricostruzione del contesto in cui è nato bitcoin, v. G. LEMME - S. PELUSO, *Criptomoneta e distacco dalla moneta legale: il caso bitcoin*, in *Riv. dir. banc.*, 2016, p. 389, che richiama il sistema ecash, brevettato da David Chaum (1995-1998) e il Linden Dollar di Second Life. Più approfonditamente su questo tema v. G. MACARIO, *Il passato, presente e futuro del mondo virtuale Second Life,* Roma, 2014; M.A. KAPLAN - M. HANLEIN, *Consumer use and business potential of virtual worlds: the case of Second Life,* in *International Journal of Media Management,* 2009, p. 93 ss.

[17] Cfr. R. RAZZANTE, *Bitcoin e criptovalute. Profili fiscali, giuridici e finanziari*, Milano, 2018; nonché sempre di R. RAZZANTE, *Criptovalute e conferimenti aziendali,* in *Giur. it.*, 2019; R. RAZZANTE, *Criptovalute e rischi per la sicurezza*, in *Rass. Arma Car.*, 2018, 3, pp. 61-68. Si vedano anche, D. DELFRATE – G. COSSENTINO, *Criptovalute: risvolti fiscali per le persone fisiche*, in *Riv. Gdf.* 2024, 6, p. 1737 ss.; M. MISITI, *Monete virtuali e valute virtuali,* in *penaledp.it,* 29 novembre 2024. Piu recentemente, un documento della BANCA PER I REGOLAMENTI INTERNAZIONALI, *Criptovalute e finanza decentralizzata*, n. 156, in *www.bis.org*, aprile 2025.

Appare evidente il rischio che l'impiego di strumenti digitali di pagamento riduca sensibilmente la possibilità di ricostruire il nesso tra il soggetto riciclatore e l'attività illecita da cui traggono origine i capitali movimentati[18].

In tale prospettiva, è necessario chiarire la distinzione concettuale tra il termine "identificazione", proprio della disciplina antiriciclaggio, e la nozione di "tracciabilità", più strettamente connessa alle operazioni di pagamento effettuate, ad esempio, mediante Bitcoin o altre criptovalute.

Il primo concetto si riferisce, in estrema sintesi, all'individuazione dell'identità anagrafica del soggetto che pone in essere la transazione; il secondo, invece, attiene alla mera registrazione informatica delle operazioni compiute da un detentore di chiave privata verso un altro soggetto titolare, a sua volta, di una diversa chiave privata, attraverso un sistema crittografico a chiave pubblica.

Da ciò discende che il tracciamento digitale della transazione non necessariamente consente di risalire all'identità reale dei soggetti coinvolti, limitandosi a documentare il movimento delle unità di valore tra indirizzi pseudonimizzati.

Tali strumenti, pur presentando caratteristiche di liquidità assimilabili a quelle della moneta avente corso legale, sono stati progettati per conservarne i tratti funzionali essenziali – quali la convertibilità, la trasferibilità e, in parte, l'anonimato – ma con un livello di rischio più contenuto, maggiore flessibilità operativa e costi di transazione significativamente ridotti.

Proprio da tali vantaggi, derivanti dalla velocità e dall'efficienza delle comunicazioni in rete, si spiega la crescente predilezione della criminalità organizzata per l'utilizzo di Internet quale infrastruttura privilegiata per il compimento di operazioni di riciclaggio.

[18] Gli scambi finanziari che utilizzano la rete come strumento di contatto offrono alle organizzazioni criminali numerosi canali di riciclaggio estremamente innovativi rispetto a quelli tradizionali.si è soliti parlare a tal riguardo di Cyberlaundering (o riciclaggio digitale) per indicare le condotte di occultamento dell'origine illecita dei fondi attraverso l'utilizzo delle reti informatiche, soprattutto dei nuovi sistemi di pagamento. Sul punto, rimane importanza assume il RAPPORTO EUROPOL COMMON CHALLENGE IN CYBERCRIME 2024, in *Review by Eurojust and Europol,* 31 gennaio 2025, il quale analizza le principali difficoltà nelle indagini sui crimini informatici e l'impatto delle nuove misure legislative dell'UE. Tra le sfide principali evidenziate spiccano il crescente volume di dati digitali, il rischio di perdita di informazioni cruciali e le barriere legali e tecniche all'accesso ai dati. L'uso diffuso di strumenti di anemizzazione rende ancora più difficile tracciare le attività criminali online. Per affrontare questi problemi, la relazione esamina le potenzialità di strumenti normativi come l'E-Evidence Package, il Digital Services Act e l'EU AI Act, «volti a migliorare la cooperazione transfrontaliera e facilitare l'accesso ai dati digitali per le indagini».

La rete, infatti, offre un'ampia gamma di beni e servizi, ma soprattutto si caratterizza per l'assenza di un sistema giuridico internazionale solido e coerente, in grado di disciplinare efficacemente le condotte illecite informatiche[19].

L'attuale assetto normativo sovranazionale, ancora frammentato e lacunoso, si rivela pertanto inadatto a fronteggiare i rischi connessi alla globalizzazione delle attività economiche, garantendo a chiunque – spesso in forma anonima e a costi irrisori – l'accesso a servizi che possono agevolare l'occultamento o la movimentazione di proventi di origine delittuosa.

L'attività di controllo da parte delle autorità risulta, inoltre, particolarmente complessa, poiché l'accesso ai siti che offrono tali servizi è difficilmente monitorabile e gli intermediari che li gestiscono operano frequentemente in una zona di confine tra legalità e illegalità, invocando esigenze di tutela della riservatezza degli utenti.

Molte di queste piattaforme, inoltre, stabiliscono la propria sede legale in Paesi che adottano normative particolarmente permissive o comunque non armonizzate rispetto agli standard europei e internazionali in materia di antiriciclaggio.

Tale scenario ha imposto, quale reazione necessaria, un progressivo rafforzamento delle legislazioni nazionali in tema di trasparenza dei flussi finanziari e di controllo dei movimenti di capitale**,** accompagnato da un'intensificazione della cooperazione internazionale sia sul piano normativo che operativo.

Le Autorità di vigilanza e le Unità di Intelligence Finanziaria (UIF) dei principali ordinamenti hanno, in questa prospettiva, sviluppato forme di coordinamento sempre più strette, volte a condividere informazioni, prassi di analisi e strumenti tecnologici idonei a individuare tempestivamente le transazioni sospette e a ricostruire le catene di trasferimento dei capitali illeciti[20].

Il diritto europeo, attraverso la costruzione di presidi regolatori come il MiCAR e la neoistituita AMLA, tenta di ricondurre questa nuova dimensione finanziaria entro un orizzonte di legalità tecnologicamente mediata, restituendo al principio di tracciabilità la

[19] Più diffusamente sui reati informatici, cfr. R. RAZZANTE, *Attribuzione dei cyber attacchi,* in *European Journal of Privacy Law &Technologies,* n. 2, 2022, p. 215 ss., S. UNGARO, *Autenticità dei dati: l'altro pilastro fondamentale della cybersecurity, in Riv. El. Diritto, economia e management,* 2025, n. 1, p. 122 ss.

[20] L'autorità maggiormente caratterizzante l'architettura istituzionale dell'antiriciclaggio è l'unità di informazione finanziaria (UIF). Identifica quella Financial Intelligence Unit (FIU), di cui le raccomandazioni del GAFI e il diritto euro-unitario hanno sempre auspicato l'istituzione ai fini di una efficace tempestiva azione di prevenzione del riciclaggio: ovvero un'organizzazione pubblica «che funga da centro nazionale per la ricezione e l'analisi delle segnalazioni di operazioni sospette per la diffusione degli esiti di tale analisi».

sua centralità come fondamento della "financial integrity" e come misura della civiltà giuridica del mercato digitale.

Ancora una volta, il punto discriminante risiede nelle caratteristiche tecniche di funzionamento della *blockchain*: l'irrevocabilità e l'immutabilità delle operazioni una volta registrate, la certezza della marcatura temporale e la stabilità delle registrazioni, se da un lato costituiscono garanzie di integrità e affidabilità del sistema, dall'altro ne accentuano l'ambiguità funzionale**,** poiché consentono un anonimato che può sfuggire al controllo degli ordinamenti giuridici.

Per converso, se le tecnologie basate su "*distributed ledger*" garantiscono, sul piano oggettivo, la trasparenza delle registrazioni e l'immutabilità delle operazioni compiute, esse realizzano, sul versante soggettivo, forme più o meno stabili e irreversibili di opacità e occultamento dell'identità personale degli operatori coinvolti. La dimensione transnazionale, l'istantaneità delle transazioni e la vocazione originaria all'anonimato costituiscono, in tale prospettiva, le condizioni ideali per la commissione di reati finanziari e informatici di difficile perseguibilità[21].

L'assenza di un collegamento diretto e immediato tra l'autore materiale dell'operazione e la manifestazione esterna del negozio digitale determina, infatti, un vuoto di riferibilità giuridica, che rischia di tradursi in una sostanziale impunità per condotte illecite quali il riciclaggio, la corruzione, l'evasione fiscale o il finanziamento del terrorismo.

Il paradigma identificativo che connota la circolazione dei Bitcoin non realizza, tuttavia, una condizione di anonimato assoluto, bensì una forma di pseudonimato funzionale, nel senso che l'identità reale degli utenti risulta celata dietro un codice alfanumerico – la cosiddetta "chiave pubblica" – che rappresenta l'indirizzo attraverso il quale vengono effettuate le transazioni. Tale pseudonimato, per quanto idoneo a dissimulare l'identità personale dell'operatore, non è di per sé invalicabile: le autorità competenti, avvalendosi di strumenti tecnologici avanzati di *blockchain analysis*, possono infrangere il velo dell'anonimato, correlando gli indirizzi informatici ai titolari effettivi dei conti digitali e consentendo così di perseguire le violazioni penalmente rilevanti secondo le norme interne e internazionali in materia di *Anti-Money Laundering* (AML)[22].

---

[21] Cfr. D. MAJORANA, *Disciplina giuridiche fiscali delle criptovalute: sfida al legislatore dal web*, in *Corriere trib.,* 2018, p. 630; M. BELLINO, *I rischi legati all'ecosistema Bitcoin: i nuovi intermediari,* in *Riv. dir. banc.*, 2018.; I. BIXIO, *Valute virtuali adempimenti antiriciclaggio: riflessi su soggetti obbligati, nuovi e non,* in *Corriere trib*., 2017, p. 2676.

[22] Cfr. L. MURTAS, *Antiriclaggio e criptoattività*, in (a cura di) F. Annunziata – D. Varani, *Criptoattività,. Antiriciclaggio e gestione dei rischi aziendali*, Pacini giuridica, 2024, p. 38 ss., ad avviso del quale il legislatore europeo intende così «affrontare il problema degli ampi spazi di anonimato consentiti ai soggetti coinvolti

La trasparenza integrale del registro blockchain, infatti, consente di associare univocamente ogni operazione a una determinata chiave pubblica, rendendo in ogni caso identificabili l'account di partenza, quello di destinazione e l'importo trasferito. L'utilizzo di software specializzati consente, in alcuni casi, di risalire alla chiave privata corrispondente, e dunque all'identità dell'utente, consentendo la tracciabilità *ex post* dei flussi finanziari digitali e il disvelamento di operazioni riconducibili a persone fisiche o giuridiche.

Tuttavia, tale tracciabilità selettiva e secondaria, limitata ai casi in cui sia possibile un intervento tecnico di decrittazione, si trasforma nuovamente in anonimato integrale allorché vengano impiegati ulteriori strumenti di cifratura e offuscamento dei dati, capaci di occultare o disperdere irreversibilmente i riferimenti identificativi all'interno della rete blockchain.

La tecnologia DLT[23] e la blockchain si fondano, com'è noto, su un sistema di crittografia asimmetrica, in cui ciascun utente dispone di una coppia di chiavi – una privata, conservata segretamente, e una pubblica, derivata dalla prima – che consente l'interazione e lo scambio di dati con altri soggetti.

Nel sistema Bitcoin, chiunque può generare tali chiavi senza necessità di preventiva identificazione personale, e il numero di coppie di chiavi potenzialmente generabili è teoricamente infinito. Ne deriva che una singola identità – già di per sé pseudonimato – può essere associata a una molteplicità di chiavi pubbliche e private, ciascuna riferibile a una specifica transazione[24].

Questo fenomeno rende frammentario e disaggregato il collegamento tra utente-disponente, utente-destinatario e singole operazioni, ostacolando gravemente la possibilità di ricondurre i flussi a un unico soggetto[25].

---

nelle transazioni» che radicano l'attitudine ad agevolare il riciclaggio del denaro sporco e il finanziamento delle attività terroristiche internazionali.

[23] "The term DLT does in the present scenarios describe technologies that enable the creation of a decentralized public register, containing all the transactions carried out by the members of the respective system and updatable by each independently of the other."; così, A. PERRONE, *Il diritto del mercato dei capitali,* Milano, 2024, p. 36 ff.

[24] Cfr., ex multis, M. LEHMANN, *Crypto-èconomic et droit international,* in *Recuell des cours,* 438, Leiden/Boston, 2024, 36 ff.

[25] Cfr., E. PEDERZINI, *La tracciabilità dei movimenti finanziari tra anonimato e pseudonimato: FinTech, incorporazione del diritto nella tecnica e paradigma by design,* in *Riv. dir. banc.*, n. 1, 2022, p. 79 ss.

A tale opacità contribuiscono ulteriormente i sistemi di "mixing" o "tumbling", sempre più diffusi nel mercato delle cripto-attività, che operano mediante la commistione artificiale degli indirizzi di origine e di destinazione delle transazioni. Attraverso questi meccanismi, i movimenti di cripto-attività vengono frazionati e rimescolati in modo casuale, così da impedire la ricostruzione puntuale della sequenza temporale e logica delle operazioni.

Chi offre un servizio di *mixer* realizza, di fatto, un oscuramento totale delle origini, della destinazione e delle parti coinvolte, generando un effetto di dissimulazione che, pur non essendo di per sé illecito, può facilmente prestarsi a finalità di riciclaggio o di finanziamento illecito.

Tali sistemi, concepiti originariamente per garantire un più elevato livello di privacy degli utenti e tutelarne la riservatezza nei rapporti digitali, si collocano in una zona giuridicamente ambigua: da strumenti di protezione dei dati, possono divenire mezzi di elusione sistematica della normativa antiriciclaggio. Proprio per tale ragione, il divieto di impiego di tecniche di *mixing* o *tumbling* è stato individuato come uno degli snodi cruciali della nuova strategia regolatoria. In ambito europeo, tale orientamento è confluito nel pacchetto normativo "Anti-Money Laundering VI" (AML Package 2021), che prevede il rafforzamento dei presidi di tracciabilità delle operazioni in cripto-attività. Analogamente, negli Stati Uniti, il "Blockchain Integrity Act", attualmente all'esame del Congresso, propone una moratoria biennale sull'utilizzo di mixer e altri strumenti di offuscamento, al fine di consentire alle autorità di valutare i rischi sistemici derivanti dalla non tracciabilità delle transazioni.

L'ambivalenza di tali strumenti, a metà strada tra garanzia di libertà individuale e potenziale veicolo di illeciti finanziari, evidenzia la necessità di un approccio regolatorio bilanciato, capace di preservare la tutela della privacy senza compromettere la capacità di vigilanza e di enforcement degli ordinamenti giuridici.

In ciò si misura, oggi, una delle sfide più complesse e paradigmatiche della disciplina europea delle cripto-attività: coniugare innovazione tecnologica, trasparenza dei mercati e responsabilità giuridica in un contesto che tende strutturalmente a sfuggire ai confini tradizionali del diritto.

Accanto alla possibilità – sempre più concreta – che le ricchezze accumulate attraverso attività illecite non vengano reimmesse nei circuiti della moneta legale, ma continuino a circolare in forma di cripto-attività accettate come mezzo di pagamento o utilizzate a fini di investimento e di riserva di valore, si colloca la problematica della conversione e reimmissione dei fondi al di fuori di qualunque canale di intermediazione regolamentata.

La costante evoluzione tecnologica e l'effetto di progressiva disintermediazione che ne deriva su tutti i livelli del sistema finanziario amplificano tale rischio, poiché consentono lo svolgimento di operazioni di scambio, conversione o trasferimento di ricchezza digitale senza l'ausilio di piattaforme centralizzate o di prestatori di servizi di cambio autorizzati.

In questo contesto, permane l'interrogativo circa gli strumenti tecnici di cui le Unità di Informazione Finanziaria (FIU) dovrebbero disporre per associare, in modo certo, un indirizzo di valuta virtuale all'identità del suo reale titolare effettivo – come auspicato dalla normativa europea –. Ad oggi, tuttavia, non sembrano esistere tecnologie universalmente adottate o sistemi informativi realmente efficaci che consentano di stabilire un collegamento univoco tra la persona fisica e l'account digitale attraverso il quale vengono effettuate operazioni espresse in Bitcoin o in altre Altcoins.

Nella maggior parte dei casi, è possibile risalire unicamente all'indirizzo IP del terminale utilizzato per la trasmissione o la ricezione dei fondi, elemento che, da solo, non garantisce la certezza dell'identificazione soggettiva.

In questo scenario, il legislatore italiano ha mostrato una notevole lungimiranza e sensibilità rispetto ai profili di rischio connessi alla crescente smaterializzazione dei mezzi di pagamento e alla prospettica centralità dei mercati fondati su valori digitali.

Consapevole della continua e imprevedibile evoluzione tecnologica, egli ha progressivamente ampliato il perimetro soggettivo della disciplina, estendendone l'applicazione non solo ai prestatori di servizi di cambio tra valute aventi corso legale e valute virtuali, ma anche alle attività di conversione tra differenti rappresentazioni digitali di valore (c.d. crypto-to-crypto exchange), accanto alle più tradizionali operazioni di cambio da e verso la moneta avente corso forzoso.

L'inasprimento della normativa, pertanto, risponde all'esigenza di presidiare anche i segmenti più innovativi e sfuggenti del mercato delle cripto-attività, ove la possibilità di anonimato e la mancanza di controllo intermedio rendono più insidiosa la prevenzione del riciclaggio.

Parallelamente, si assiste a un significativo rafforzamento degli strumenti di *compliance* digitale, con il crescente impiego, da parte degli intermediari finanziari, di tecnologie di identificazione a distanza, sistemi di *machine learning* e reti neurali per la profilazione automatica del rischio, la selezione e classificazione delle operazioni anomale e il monitoraggio dei flussi sospetti.

L'utilizzo di tecniche di artificial intelligence nel settore AML/CFT mira a coniugare efficienza procedurale e affidabilità analitica, consentendo una più accurata individuazione

dei comportamenti di rischio e un miglioramento della capacità predittiva delle strutture di vigilanza interna.

Un quadro normativo efficace deve, dunque, operare secondo un principio di equivalenza funzionale: le cripto-attività che presentano rischi analoghi a quelli delle attività finanziarie tradizionali devono essere assoggettate agli stessi obblighi regolamentari e ai medesimi meccanismi di controllo.

Solo in tal modo è possibile garantire la neutralità tecnologica della disciplina e prevenire arbitraggi regolamentari che minerebbero la coerenza dell'intero sistema di prevenzione.

In dottrina si è tuttavia osservato come, argomentando a partire dalla natura intrinsecamente tracciabile e immutabile delle registrazioni blockchain, la tecnologia stessa possa prestarsi – in una prospettiva rovesciata – a un uso virtuoso a fini di legalità economica[26].

La tracciabilità oggettiva, l'accessibilità (totale o parziale) del registro e la sua inalterabilità temporale costituiscono, infatti, caratteristiche che, se opportunamente valorizzate, potrebbero trasformare il Bitcoin da veicolo di illeciti a strumento di contrasto ai reati commessi attraverso l'uso del denaro contante.

Alcuni studi recenti hanno teorizzato che un sistema basato su monete digitali concorrenziali, se pienamente tracciabile e interoperabile, potrebbe ridurre drasticamente i fenomeni di evasione, corruzione e criminalità finanziaria, fino a rendere superflua la circolazione del contante e a garantire una più elevata stabilità macroeconomica.

Tali teorie, pur suggestive, assumono talora tratti utopici, prospettando l'abolizione della moneta legale e la scomparsa delle crisi finanziarie e dell'inflazione grazie all'avvento di un'economia fondata esclusivamente su monete digitali.

In realtà, l'apporto della tecnologia DLT al sistema finanziario può tradursi in un effettivo rafforzamento dell'affidabilità e della sicurezza solo nella misura in cui sia accompagnato da un solido apparato normativo e istituzionale.

La tracciabilità oggettiva delle operazioni – cioè l'accessibilità pubblica, o parzialmente pubblica, del database che raccoglie in modo permanente e immodificabile tutte le

[26] Si veda, in tema, V. BARBARESI – P. GIUDICI, *Quattro a ragioni per cui la Blockchain non ha (ancora?) Rivoluzionato i mercati finanziari*, in (a cura di) C. Pagliarin – C. Perathoner – S. Laimer – W. Crepaz, *Criptovalute e monete digitali. Riflessioni giuridiche,* Collana Economia e Diritto Italiano, Europeo e Internazionale, Giuffrè lefebvre, 2025, p. 17 ss.

transazioni effettuate tra gli utenti – costituisce una condizione necessaria, ma non sufficiente, per garantire la legalità del sistema. Senza una parallela tracciabilità soggettiva, assicurata da norme capaci di ricondurre con certezza le operazioni ai titolari effettivi, il rischio è che i benefici tecnologici vengano vanificati, dando luogo al paradosso di un ambiente ideale per la commissione dei reati che la disciplina intende prevenire[27].

3. Verso una regolazione integrata delle cripto-attività: dal Decreto Antiriciclaggio alla vigilanza europea centralizzata.

Nel panorama dei sistemi giuridici avanzati, la prevenzione del riciclaggio dei proventi di attività criminose e del finanziamento del terrorismo ha assunto una funzione strutturale nell'ambito della legislazione economico-finanziaria, divenendo presidio essenziale della legalità dei mercati e componente stabile della governance della stabilità finanziaria.

Essa costituisce, infatti, uno dei cardini del diritto dell'economia contemporaneo, in quanto strumento volto non solo alla repressione delle condotte illecite, ma alla protezione sistemica dell'integrità e della trasparenza del mercato.

Il modello italiano di prevenzione si è progressivamente evoluto in stretta connessione con l'elaborazione dei principi internazionali promossi dal Financial Action Task Force (FATF)[28] – Groupe d'Action Financière Internationale (GAFI)[29] e recepiti, a livello europeo, attraverso le cinque direttive antiriciclaggio (Direttive 91/308/CEE, 2001/97/CE, 2005/60/CE, 2015/849/UE e 2018/843/UE).

[27] Cfr. E. PEDERZINI, *Antiriciclaggio e tracciabilità dei movimenti finanziari,* in (a cura di) M. Cian – C. Sandei, *Diritto del Fintech*, Cedam, 2024, pp. 79-80.

[28] Cfr., FATF, *Annual Report 2023/2024*, in *fatf-gafi.org,* 30 giugno 2024.

[29] Si veda, GAFI, *Annual Report, 2023/2024*, in *antiriciclaggiocompliance.it*, 2 febbraio 2025. «Nell'anno di riferimento il GAFI ha compiuto notevoli progressi nella lotta alla criminalità finanziaria, concentrandosi su diversi aspetti chiave quali: rafforzamento della conformità globale agli standard del Gruppo; la trasparenza sulla titolarità effettiva; le modifiche degli standard GAFI sulle organizzazioni non profit (ONP); il rafforzamento della rete globale; la promozione dell'inclusività di genere all'interno del Gruppo e della sua rete globale; il monitoraggio dei rischi emergenti, con approfondimento su frodi informatiche, uso illecito del crowdfunding per il finanziamento del terrorismo e abusi dei programmi di cittadinanza e residenza per investimenti, oltre a indagini sul ransomware e sulla corruzione; l'aggiornamento degli standard internazionali su questo tema è la collaborazione rafforzata con INTERPOL per migliorare l'applicazione operativa di tali misure; e, infine, la predisposizione di un elenco delle giurisdizioni coinvolte nella fornitura di servizi di attività virtuali (VASP). Questi progressi evidenziano un impegno continuo per contrastare la criminalità finanziaria, rafforzare la cooperazione internazionale e a dettasi alle nuove sfide del panorama globale».

L'ordinamento nazionale ha avviato un organico processo di adeguamento già con la L. 5 luglio 1991, n. 197, poi sistematizzato nel D. Lgs. 21 novembre 2007, n. 231 (il c.d. *Decreto Antiriciclaggio)*, che rappresenta tuttora l'asse portante della disciplina italiana in materia di *Anti-Money Laundering* (AML) e *Counter-Terrorist Financing* (CTF).

La riforma del 2007 ha segnato, come a breve si dirà meglio, una cesura concettuale nel sistema di prevenzione, introducendo un approccio di tipo collaborativo e proattivo fondato sull'interazione tra autorità pubbliche, intermediari bancari, operatori finanziari e professionisti.

Elemento qualificante dell'assetto istituzionale è l'istituzione, presso la Banca d'Italia, dell'Unità di Informazione Finanziaria per l'Italia (UIF), organo indipendente deputato a ricevere, analizzare e diffondere le segnalazioni di operazioni sospette trasmesse dai soggetti obbligati[2].

La creazione della UIF ha conferito al sistema una dimensione tecnica e analitica di livello superiore, idonea a rafforzare la capacità di prevenzione rispetto ai rischi di riciclaggio

La sua istituzione ha impresso al sistema antiriciclaggio una decisa svolta sul piano tecnico e analitico, conferendogli una capacità di elaborazione e di valutazione del rischio di livello superiore, idonea a rafforzarne l'efficacia preventiva[30].

L'evoluzione del modello italiano — oggi riconosciuto quale *best practice* a livello internazionale — ha contribuito a consolidare la fiducia reciproca tra operatori, autorità di vigilanza e sistema giudiziario, ponendo le basi per una sinergia istituzionale stabile e funzionale. Tale cooperazione ha progressivamente assunto un valore sistemico, trasformandosi in uno dei pilastri della cultura giuridico-finanziaria nazionale e in un paradigma di riferimento per la costruzione di un ordinamento europeo di prevenzione e contrasto del riciclaggio fondato sulla trasparenza, sulla tracciabilità e sulla responsabilità condivisa[31].

---

[30] Cfr. Raccomandazioni GAFI, n. 29, ai sensi del quale «i Paesi devono istituire un'Unità d'Informazione Finanziaria (UIF) che funga da centro nazionale per la ricezione e l'analisi di: a) segnalazioni di operazioni sospette; b) altre informazioni rilevanti relative al riciclaggio di denaro, ai reati-presupposto associati e al finanziamento del terrorismo, e per la diffusione degli esiti di tali analisi. L' Unità di Informazione Finanziaria deve essere in grado di ottenere ulteriori informazioni dei soggetti segnalanti, e deve avere tempestivamente accesso alle informazioni finanziarie, amministrative e delle forze dell'ordine necessarie per esercitare correttamente le proprie funzioni.

[31] Sul tema della regolazione e dell"architettura europea della supervisione, si vedano, D..SICLARI, *La regolazione bancaria e dei mercati finanziari: dalla 'neutralizzazione' dell'indirizzo politico sul mercato all'unificazione europea,* in *Riv. it. dir. pubbl. com.*, 2016, pp. 189 ss.; F. CAPRIGLIONE - A. SACCO GINEVRI, *Metamorfosi della*

La struttura delineata dal legislatore si fonda su una chiara ripartizione di competenze: all'UIF spetta l'attività di analisi finanziaria e intelligence preventiva, mentre le funzioni di indagine penale e di contrasto repressivo sono affidate a organismi specializzati, in primis al Nucleo Speciale di Polizia Valutaria della Guardia di Finanza e alla Direzione Investigativa Antimafia (DIA)[5].

L'integrazione tra tali soggetti ha favorito la costruzione di un sistema multilivello di cooperazione che, seppure migliorabile sotto il profilo della piena interoperabilità delle basi dati, rappresenta un modello efficiente di sinergia istituzionale e di interconnessione informativa.

La collaborazione tra UIF e Autorità giudiziaria, in particolare, ha assunto un rilievo strategico nella ricostruzione dei flussi finanziari e nella valorizzazione investigativa delle segnalazioni.

Un ulteriore rafforzamento del coordinamento interistituzionale è derivato dal recepimento della IV Direttiva (UE) 2015/849, che ha formalmente incluso la Direzione Nazionale Antimafia e Antiterrorismo (DNA) nel circuito di prevenzione[6], consentendo incroci sistematici tra le banche dati UIF e DNA e potenziando la capacità di individuare operazioni riconducibili alla criminalità organizzata.

Il sistema italiano di *financial intelligence* ha inoltre esteso progressivamente il proprio perimetro applicativo, includendo – oltre alla prevenzione del riciclaggio e del finanziamento del terrorismo – anche la proliferazione delle armi di distruzione di massa, le attività connesse a materiali bellici e mine antiuomo, nonché la prevenzione della corruzione e dell'evasione fiscale, nella prospettiva più ampia di una "financial integrity governance"[32].

In questa visione, la UIF non è soltanto un organo tecnico di raccolta dati, ma un fulcro strategico della legalità economica, destinato a integrare le logiche di prevenzione

governance bancaria, Utet Giuridica, Milano, 2019; G. SCIASCIA, *La regolazione giuridica del rischio sistemico. Stabilità finanziaria e politiche macroprudenziali,* Giuffrè, Milano, 2021; R. LO CONTE, *L'ordinamento pubblico europeo del credito: profili evolutivi,* in *dir.publ.eu.*- Rassegna Online, 2023, p. 401 ss.

[32] Cfr. V. MITSILEGAS, *New Forms of Trasnational Policing: The Emergence of Financial Intelligence Units in the European Union and the Challenge of Human Rights*, in *Journal of Money Laundering Control*, 2000, p. 250 ss.; R.J. LOWE, *Anti-Money Laundering, The need for intelligence, in Journal of Financial Crime,* 2017, p. 472 ss.; O. REZNIK – M. UTKINA – O. BONDARENKO, *Financial Intelligence (monitoring) as an effective way in the field of combating money laundering,* in *Journal of Money Laundering Control,* 2023, p. 94 ss.

finanziaria con le politiche pubbliche di contrasto alla criminalità economica e alla destabilizzazione dei mercati[33].

[33] Le origini dell'attuale organismo competente, tra le altre funzioni, alla ricezione e all'analisi delle segnalazioni di operazioni sospette (*suspicious transaction reports* – STR), non sono recenti. Come già osservato, l'assetto originario del sistema antiriciclaggio italiano si caratterizzava per una struttura poco specializzata e fortemente frammentata, nella quale le procedure di trasmissione e valutazione delle segnalazioni risultavano particolarmente complesse e inefficaci. In base al meccanismo allora vigente, i soggetti obbligati dovevano inoltrare le segnalazioni di operazioni sospette alle Questure, che a loro volta le trasmettevano al Nucleo Speciale di Polizia Valutaria della Guardia di Finanza. Mancava, pertanto, una struttura istituzionalmente dedicata alla ricezione centralizzata e all'analisi tecnico-finanziaria delle segnalazioni, con la conseguenza che l'intero procedimento si caratterizzava per una duplice criticità: da un lato, l'eccessiva stratificazione procedimentale, causa di ritardi nella valutazione delle operazioni sospette; dall'altro, l'assenza di un'adeguata competenza finanziaria e di strumenti analitici evoluti, poiché gli organi coinvolti operavano prevalentemente su un piano investigativo e repressivo, piuttosto che preventivo e di intelligence economica.

Il primo significativo rimedio a tali inefficienze fu introdotto dal D. lgs. 26 maggio 1997, n. 153, che attribuì **all'**Ufficio Italiano dei Cambi (UIC) la funzione di ricezione e analisi finanziaria delle SOS. L'UIC esercitò tale ruolo per circa un decennio, fino alla sua soppressione, avvenuta in attuazione del processo di riorganizzazione della Banca d'Italia. In via transitoria, le funzioni di Financial Intelligence Unit (FIU) furono affidate alla Divisione Servizio Antiriciclaggio della stessa Banca d'Italia, sino alla formale istituzione, nel gennaio 2008, dell'attuale Unità di Informazione Finanziaria per l'Italia (UIF), che subentrò nel ruolo di organo centrale di ricezione, analisi e trasmissione delle informazioni in materia di prevenzione del riciclaggio e del finanziamento del terrorismo. La UIF è strutturata secondo un modello amministrativo indipendente, privo di personalità giuridica propria, ma istituito presso la Banca d'Italia, che ne disciplina l'organizzazione e il funzionamento (cfr., I BORRELLO, *Financial Intelligence Unit (FIU)*, in (a cura di) D. Siclari, *Italian Banking and Financial Law. Supervisory Authorities and Supervision*, Londra, 2015, p. 261 ss.; I BORRELLO, *I presidi antiriciclaggio e il contrasto alla corruzione.l'esperienza dell'Unità di Informazione Finanziaria per l'Italia,* in *Riv. econ. Cult. Ric. Soc.*, 2017, p. 25). Tale configurazione determina l'impossibilità di qualificare la UIF come vero e proprio ente pubblico, dovendo piuttosto considerarla una struttura autonoma di primo livello, incardinata nell'organizzazione della Banca d'Italia ma dotata di autonomia operativa e decisionale. La collocazione presso la Banca d'Italia non implica, tuttavia, l'esistenza di un rapporto gerarchico o di direzione. La UIF non è soggetta a poteri di comando o di controllo da parte della Banca, e la giurisprudenza si è limitata a descrivere tale relazione come un "forte rapporto di compenetrazione" (si veda, Cons. St., Ad. Gen., 3 agosto 2018, n. 2018, in *giustizia-amministrativa.it*) senza peraltro pervenire a una qualificazione giuridica univoca.

In termini funzionali, il legame tra le due strutture può essere definito come una relazione di strumentalità reciproca e di coordinamento paritetico, improntata a criteri di equiordinazione (con riguardo al coordinamento nelle relazioni equiordinate, Cfr. G. CLEMENTE DI SAN LUCA, *Organizzazione amministrativa. Rapporti organizzativi*, in *Treccani.it*, 2015). Da tale configurazione derivano due conseguenze fondamentali.

In primo luogo, la bidirezionalità dei flussi informativi: l'attività di controllo antiriciclaggio svolta dalla UIF costituisce un complemento funzionale della vigilanza bancaria esercitata dalla Banca d'Italia, e, simmetricamente, i dati e le informazioni raccolti dalla Banca mediante i propri poteri di supervisione risultano strumentali all'attività di analisi e monitoraggio dell'Unità. In secondo luogo, la Banca d'Italia dispone di un potere di coordinamento, inteso come quell'insieme di strumenti che, pur nel rispetto dell'autonomia dell'organismo coordinato, mirano ad assicurare l'armonizzazione delle rispettive funzioni, anche mediante l'intervento su profili organizzativi e procedurali. In altri termini, la Banca d'Italia non esercita sulla UIF un potere di direzione, ma piuttosto un potere di coordinamento funzionale, volto a garantire coerenza sistemica e continuità operativa tra le due sfere di attività, in un quadro di equilibrio istituzionale. Il vero nodo problematico – spesso trascurato dalla dottrina – riguarda tuttavia l'opportunità

ISSN 2282-2461 I BATTELLI DEL RENO [ON LINE]

L'esperienza maturata consente di considerare il modello italiano di prevenzione e intelligence finanziaria uno dei più avanzati in Europa, per ampiezza dei flussi informativi, efficacia dell'analisi e capacità di cooperazione multilivello - operata con l'istituzione dell'Anti-Money Laundering Authority (AMLA) a livello europeo - impone oggi una riflessione critica sulla necessità di una integrazione armonica tra disciplina nazionale e quadro sovranazionale, nella direzione di un sistema unitario di vigilanza AML/CFT che preservi la qualità e l'autonomia del modello italiano, inserendolo nel più ampio disegno di convergenza europea.

La cosiddetta *V Direttiva Antiriciclaggio* segna un punto di svolta nel panorama normativo dell'Unione europea, rappresentando il primo intervento legislativo in cui il fenomeno delle *valute virtuali* – sino ad allora sviluppatosi in un contesto privo di una disciplina giuridica specifica – riceve una regolamentazione positiva e, contestualmente, una definizione normativa.

I Considerando nn. 8, 9 e 10 della direttiva delineano in modo chiaro il quadro di riferimento che ha orientato il legislatore europeo.

Da essi emergono alcuni profili di rilievo: anzitutto, si evidenzia come i prestatori di servizi la cui attività consista nello scambio tra valute virtuali e valute aventi corso legale, nonché i prestatori di servizi di portafoglio digital[34] e, non fossero inizialmente soggetti all'obbligo – previsto dalla disciplina unionale – di identificare le operazioni sospette.

---

di mantenere la UIF come struttura priva di personalità giuridica, e quindi formalmente inserita nell'organizzazione della Banca d'Italia. L'opzione di collocarla presso quest'ultima rispondeva, in origine, all'intento di valorizzare le sinergie tra la vigilanza prudenziale e l'analisi delle operazioni sospette, nella consapevolezza della reciproca interdipendenza tra la stabilità del sistema bancario e l'efficacia della disciplina antiriciclaggio. Tale giustificazione, tuttavia, appare oggi parzialmente superata dall'evoluzione della normativa e dalla progressiva espansione del perimetro soggettivo dei destinatari degli obblighi AML/CFT, che non si limita più agli intermediari bancari e finanziari, ma comprende un'ampia platea di operatori economici e professionali. Ne consegue che l'attività della UIF non può più essere considerata meramente strumentale alla sola vigilanza bancaria, ma si pone in una logica interistituzionale, funzionale alle prerogative di diverse autorità – nazionali e internazionali – impegnate nella tutela della legalità economica e finanziaria. La prospettiva che si apre con la futura istituzione dell'Autorità Europea Antiriciclaggio (AMLA) impone, in tale ottica, una riflessione rinnovata sulla natura giuridica e sull'assetto istituzionale della UIF, affinché la sua integrazione nel sistema europeo avvenga in condizioni di piena autonomia e cooperazione paritaria con le altre *Financial Intelligence Units* dell'Unione.

[34] Cfr. I rilievi di G.P. ACCINNI, *Regole antiriciclaggio e risvolti penalisti dell'operatività in valute virtuali,* in *Riv. soc.,* 2018, 1516 ss., e di G. GAMBOGI, *La disciplina sanzionatorie della nuova normativa antiriciclaggio di cui al d. lgs. 25 maggio 2017, n. 90,* in (a cura di) V. Maiello – L. Della Ragione, *Riciclaggio i reati nella gestione dei flussi di denaro sporco,* Milano, 2018.

Tale lacuna regolatoria, unitamente al carattere tendenzialmente anonimo delle transazioni effettuate tramite piattaforme di scambio, ha reso possibile che organizzazioni criminali e gruppi terroristici potessero trasferire fondi verso il sistema finanziario dell'Unione o all'interno delle reti di valute virtuali, dissimulando la provenienza dei capitali o beneficiando di un livello di opacità difficilmente penetrabile.

Il legislatore europeo ha pertanto riconosciuto che l'anonimato connaturato alle valute virtuali ne consente un potenziale impiego distorto per finalità illecite. Pur includendo nell'ambito soggettivo di applicazione della direttiva i prestatori di servizi di cambio tra valute virtuali e valute aventi corso legale, nonché i fornitori di portafogli digitali, il legislatore ammette che tale estensione non sia idonea a risolvere integralmente la problematica dell'anonimato. Invero, gli utenti possono porre in essere operazioni anche al di fuori dell'intermediazione di tali soggetti, sicché una parte consistente dell'ecosistema delle valute virtuali continuerà a caratterizzarsi per l'impossibilità di ricondurre con certezza le transazioni ai rispettivi titolari effettivi.

La direttiva, inoltre, chiarisce che le valute virtuali non devono essere confuse né con la moneta elettronica, come definita dall'art. 2, par. 2, della direttiva 2009/110/CE, né con il concetto più ampio di "fondi" di cui all'art. 4, punto 25, della direttiva (UE) 2015/2366 (*Payment Services Directive 2*). Esse non coincidono, altresì, con il valore monetario utilizzato per l'esecuzione di operazioni di pagamento, né con le valute di gioco destinate esclusivamente a circolare in un ambiente virtuale delimitato.

L'obiettivo perseguito dalla *V Direttiva Antiriciclaggio* è, pertanto, quello di estendere il perimetro della normativa a tutte le possibili modalità di utilizzo delle valute virtuali, assicurando una copertura quanto più ampia possibile dei rischi connessi al loro impiego.

Da ciò traspare con evidenza l'urgenza di fornire una regolamentazione positiva a un fenomeno ormai radicato nella prassi economico-finanziaria e potenzialmente funzionale a condotte illecite. Tuttavia, permane la consapevolezza che l'intervento normativo, pur rappresentando un passo significativo verso una maggiore trasparenza del sistema, non sia sufficiente a neutralizzare in modo definitivo gli usi distorti delle valute virtuali, anche in considerazione delle intrinseche difficoltà di pervenire a una definizione giuridica univoca e condivisa dello strumento.

Non a caso, già da alcuni anni, le principali autorità e organismi internazionali si erano attivati nel tentativo di elaborare una tassonomia comune e coerente del fenomeno, idonea

a favorire una più efficace cooperazione sovranazionale nella prevenzione e repressione dei rischi connessi all'impiego delle criptovalute nei circuiti finanziari globali[35].

La Banca Centrale Europea (BCE), in una propria pubblicazione del 2012, fornì una delle prime definizioni istituzionali di valuta virtuale, qualificandola come *«a type of unregulated digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community»*. Tale definizione, come precisato nel medesimo rapporto, era suscettibile di futuri adattamenti, in considerazione dell'evoluzione delle caratteristiche strutturali e funzionali degli strumenti in questione.

In quella sede, l'analisi della BCE si concentrava in particolare su due schemi di riferimento che, all'epoca, godevano di un'elevata diffusione: il *Bitcoin Scheme* e il *Second Life Scheme*. Lo studio mirava, da un lato, a fornire una classificazione economico-giuridica delle valute virtuali e delle loro interazioni con le monete aventi corso legale e con le economie reali; dall'altro, ad evidenziare i rischi connessi al possibile impiego distorto di tali strumenti, con specifico riguardo ai profili di riciclaggio e di finanziamento del terrorismo.

In tale prospettiva, veniva segnalato come l'assenza di una regolamentazione organica e l'elevato grado di anonimato dei soggetti coinvolti nelle transazioni costituissero fattori idonei ad agevolare fenomeni di riciclaggio, rendendo più complessa l'attività di tracciamento e di vigilanza da parte delle autorità competenti.

Nel 2014, il *Financial Action Task Force – Groupe d'Action Financière Internationale* (FATF-GAFI) dedicò al tema delle valute virtuali un rapporto specifico, interamente focalizzato sui rischi di utilizzo illecito dello strumento.

In tale documento, il FATF-GAFI definì la valuta virtuale come *«a digital representation of value that can be digitally traded and functions as (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value, but does not have legal tender status (…) in any jurisdiction. It is not issued nor guaranteed by any jurisdiction, and fulfils currency functions»*[36].

Pur muovendo da prospettive metodologiche differenti, le posizioni espresse dal Financial Action Task Force (FATF-GAFI) e dalla Banca Centrale Europea convergono

[35] In argomento, cfr. J. AVGOULEAS, *Digital Finance, Crypto-Assets and Systemic Risk: A New Legal Paradigm*, Cambridge University Press, 2024 e I. ZETZSCHE, *Regulating Crypto-Assets within the EU's New Financial Architecture*, in *Journal of Banking Regulation*, 2023, p. 211 ss.

[36] Cfr. FATF, *Virtual Currencies: Key Definitions and Potential AML/CFT Risks*, June 2014.

nel riconoscere la natura strutturalmente rischiosa delle valute virtuali, quale riflesso dell'anonimato tecnologico e dell'assenza, nel momento originario della loro diffusione, di un quadro regolatorio uniforme.

Entrambe le istituzioni giungono, seppur attraverso itinerari analitici diversi, a una conclusione comune: il deficit di trasparenza e di accountability che connota la circolazione delle cripto-attività costituisce un fattore idoneo a compromettere l'effettività delle strategie di prevenzione del riciclaggio e del finanziamento del terrorismo, rendendo sostanzialmente illusorio il presidio di legalità economica.

In particolare, il documento del FATF-GAFI, pur discostandosi in parte dalle classificazioni operate dalla BCE, ne condivideva la preoccupazione di fondo, individuando i principali profili di rischio in tre elementi cardine:

– l'anonimato dei soggetti coinvolti nelle operazioni, che ostacola l'identificazione dei titolari effettivi e sottrae le transazioni al circuito della tracciabilità giuridica;

– l'assenza di un corpus normativo vincolante che definisca gli obblighi di condotta, i limiti operativi e le responsabilità degli intermediari;

– e la facilità tecnologica di elusione dei controlli, che consente la disaggregazione dei servizi e la creazione di architetture transfrontaliere opache, refrattarie all'azione coercitiva delle autorità nazionali.

La possibilità di realizzare operazioni al di fuori della giurisdizione territoriale delle autorità competenti ha determinato una vera e propria evanescenza della responsabilità di vigilanza e di compliance, con il conseguente svuotamento dell'efficacia delle norme antiriciclaggio.

Si delinea, così, una frattura tra la dimensione tecnologica globale e la capacità regolatoria degli Stati, che rappresenta uno dei punti di crisi più significativi della sovranità finanziaria nel contesto digitale.

Il diritto tradizionale, costruito su presupposti di territorialità, si è trovato improvvisamente dinanzi a un fenomeno che trascende i confini giuridici, rendendo necessaria una reazione normativa di livello sovranazionale.

Sebbene le posizioni di BCE e FATF-GAFI non esauriscano la complessità della questione definitoria e classificatoria delle valute virtuali – sulla quale si è sviluppata, negli anni successivi, una copiosa riflessione dottrinale e istituzionale – esse costituiscono il punto di svolta concettuale che ha orientato il legislatore europeo verso la costruzione di

un nuovo paradigma regolatorio. Le analisi di tali organismi hanno, infatti, svolto una funzione di anticipazione e di legittimazione epistemica del futuro intervento legislativo unionale, segnando il passaggio da una percezione episodica del rischio a una concezione sistemica della minaccia derivante dall'uso distorto delle tecnologie decentralizzate.

È in questo contesto che la questione del riciclaggio e del finanziamento del terrorismo connessa all'impiego delle valute virtuali ha assunto un rilievo crescente, fino a divenire uno dei pilastri della V Direttiva Antiriciclaggio (Direttiva UE 2018/843).

Il legislatore europeo, facendo proprie le valutazioni di BCE e FATF-GAFI, ha inteso trasfondere nell'ordinamento dell'Unione una concezione ampliata della prevenzione, non più limitata ai canali bancari tradizionali ma estesa a tutti i soggetti e strumenti che, anche solo potenzialmente, possono fungere da veicolo di trasferimento di valore.

Da tale impostazione discende il principio, oggi cardine dell'assetto AML/CFT europeo, secondo cui ogni innovazione finanziaria che consenta la movimentazione di valore deve essere accompagnata da un corrispettivo presidio di tracciabilità e responsabilità.

Il passaggio dalla segnalazione del rischio alla normazione positiva evidenzia, dunque, la funzione propulsiva del diritto sovranazionale come risposta alla crisi di efficacia delle normative interne, incapaci di fronteggiare fenomeni globali e tecnologicamente sofisticati.

In questo senso, la V Direttiva non nasce soltanto come atto di armonizzazione, ma come strumento di ricomposizione del rapporto tra libertà economica e sicurezza giuridica, restituendo alla tracciabilità la sua valenza di principio strutturale dell'ordine finanziario europeo[37].

Ciò emerge sin dalle premesse dei *Considerando*, nei quali il legislatore europeo manifesta la volontà di estendere il perimetro della disciplina alle nuove tecnologie finanziarie, riconoscendo l'esigenza di garantire un equilibrio tra innovazione digitale e integrità del mercato finanziario dell'Unione[38].

---

[37] Il recepimento della V Direttiva è avvenuto attraverso il D. Lgs. 4 ottobre 2019, n. 125, a distanza relativamente breve dall'entrata in vigore del recepimento della IV Direttiva, avvenuto con il D. Lgs 25 maggio 2017, n. 90, entrato in vigore il 4 luglio 2017. Si veda, S. DELLA CASA, *Il recepimento italiano della V Direttiva AML e la disciplina dei prestatori di servizi in valute virtuali*, in *Dir. del comm. Intern.,* 2022, p. 389 ss.

[38] Il Considerando n. 2 della V Direttiva Antiriciclaggio evidenzia l'emersione di nuove tendenze in materia di finanziamento del terrorismo, richiamando l'attenzione sulle modalità attraverso le quali i gruppi terroristici reperiscono e movimentano risorse economiche, anche mediante l'utilizzo di strumenti innovativi. In particolare, viene sottolineato come le moderne tecnologie – progressivamente affermatesi

In un'ottica di prevenzione del riciclaggio e di contrasto al finanziamento del terrorismo (AML/CFT), il legislatore europeo ha progressivamente riconosciuto l'esigenza di assicurare alle autorità competenti strumenti idonei a monitorare, attraverso l'azione mediata dei soggetti obbligati, l'impiego delle valute virtuali nei circuiti economico-finanziari.

L'intervento normativo, ispirato al principio di proporzionalità e alla logica della prevenzione collaborativa, mira a costruire un sistema di controllo capace di contemperare due istanze solo apparentemente antitetiche: da un lato, la tutela dell'integrità del mercato e la tracciabilità dei flussi di valore; dall'altro, la salvaguardia dell'innovazione tecnologica, della sperimentazione finanziaria e delle nuove forme di imprenditorialità sociale fondate su paradigmi di finanza etica e trasparente.

Il Considerando n. 9 della V Direttiva antiriciclaggio rappresenta un punto di svolta in tale prospettiva, poiché individua nell'anonimato intrinseco delle valute virtuali la principale vulnerabilità sistemica dell'intero ecosistema digitale.

L'anonimato, infatti, costituisce il presupposto tecnico che consente il potenziale utilizzo distorto degli strumenti digitali per finalità criminose, eludendo la rete di tracciabilità e di responsabilità che sorregge la disciplina AML/CFT.

Pur estendendo gli obblighi di compliance ai prestatori di servizi di cambio tra valute virtuali e valute aventi corso legale, nonché ai fornitori di servizi di portafoglio digitale, il legislatore europeo ha riconosciuto che tale estensione non è sufficiente, di per sé, a neutralizzare il rischio derivante dalla possibilità per gli utenti di compiere transazioni in valuta virtuale al di fuori di qualunque intermediazione regolamentata.

---

quali sistemi finanziari alternativi rispetto a quelli tradizionali – stiano acquisendo un ruolo crescente nel supportare tali attività, offrendo canali operativi più difficilmente tracciabili dalle autorità di vigilanza.

Il Considerando n. 8, in stretta correlazione con quanto precede, ribadisce che i prestatori di servizi la cui attività consista nella fornitura di servizi di cambio tra valute virtuali e valute aventi corso legale – vale a dire le monete e le banconote dotate di corso legale, nonché la moneta elettronica emessa in un determinato Stato e accettata come mezzo di pagamento nel relativo ordinamento – e i prestatori di servizi di portafoglio digitale non siano, allo stato, soggetti agli obblighi previsti dal diritto dell'Unione in materia di identificazione delle operazioni sospette. Tale lacuna regolatoria, come rilevato dal legislatore europeo, può essere sfruttata da organizzazioni terroristiche per trasferire fondi verso il sistema finanziario dell'Unione o, in alternativa, per movimentarli all'interno delle reti di valute virtuali, dissimulando la provenienza delle risorse o avvalendosi dei margini di anonimato garantiti dalle piattaforme tecnologiche che consentono tali operazioni. Ne deriva, dunque, l'esigenza di estendere il perimetro soggettivo degli obblighi di *anti-money laundering* e *counter-terrorist financing* anche ai prestatori di servizi attivi nel comparto delle valute virtuali, così da colmare il vuoto normativo e rafforzare l'efficacia del sistema europeo di prevenzione.

La conseguenza è che una parte significativa delle operazioni rimane collocata in uno spazio giuridico "grigio", connotato da un alto grado di opacità circa l'identità dei soggetti coinvolti e l'origine dei flussi finanziari.

Per attenuare tale rischio, la normativa unionale sollecita un rafforzamento delle prerogative delle Financial Intelligence Units (FIU) nazionali, le quali dovrebbero poter disporre di strumenti informativi e tecnologici idonei a collegare gli indirizzi delle valute virtuali all'identità effettiva dei titolari.

L'obiettivo è quello di ricondurre la tracciabilità digitale entro coordinate giuridiche certe, superando – o quantomeno riducendo – l'anonimato strutturale che caratterizza le transazioni in cripto-attività.

Tale approccio rivela la consapevolezza del legislatore europeo circa il limite intrinseco della regolamentazione, che, per quanto puntuale e sistematica, non può eliminare integralmente le vulnerabilità connesse alla natura decentralizzata e pseudonima delle tecnologie a registro distribuito.

La normativa, pertanto, non si limita a delineare un apparato prescrittivo, ma mira a costruire un sistema dinamico di vigilanza multilivello, fondato sulla collaborazione attiva tra autorità pubbliche e operatori privati, chiamati a concorrere alla tutela dell'integrità del mercato finanziario.

In questa prospettiva, la regolazione deve anzitutto individuare con precisione il perimetro soggettivo degli operatori economici tenuti agli obblighi di adeguata verifica della clientela, di conservazione dei dati e di segnalazione delle operazioni sospette; in secondo luogo, deve promuovere – anche attraverso l'attività di vigilanza – il rafforzamento dei presidi organizzativi e delle difese strutturali dei sistemi economici e sociali contro l'immissione di capitali illeciti o il finanziamento occulto di attività terroristiche.

Rimane, tuttavia, la consapevolezza che una quota non trascurabile delle operazioni in valuta virtuale continuerà a svolgersi in circuiti non regolamentati, perpetuando così le stesse criticità che la direttiva intende contenere: l'anonimato dei soggetti, la difficoltà di tracciamento delle transazioni e la conseguente elusione dei meccanismi di controllo.

Nonostante tali limiti, la delimitazione di un perimetro definito di soggetti obbligati e di misure preventive rappresenta un progresso significativo nel processo di consolidamento della strategia europea di contrasto al riciclaggio e al finanziamento del terrorismo, delineando un modello di governance finanziaria che si fonda non solo

sull'enforcement normativo, ma sulla costruzione di una cultura condivisa della trasparenza economica.

Il Considerando n. 10 della V Direttiva Antiriciclaggio assume una valenza cruciale nella ricostruzione dogmatica della nozione di "valuta virtuale", in quanto si premura di delinearne con precisione i confini concettuali e sistematici, evitando indebite sovrapposizioni con altre categorie di strumenti di pagamento già disciplinate dal diritto dell'Unione.

Il legislatore europeo, consapevole della crescente convergenza tecnologica tra strumenti di pagamento elettronici e cripto-attività, ha inteso definire un perimetro normativo chiaro e coerente, idoneo a preservare l'armonia interna del sistema e a scongiurare incertezze interpretative.

In tale prospettiva, viene espressamente chiarito che le valute virtuali non possono essere assimilate né alla moneta elettronica, di cui all'art. 2, paragrafo 2, della direttiva 2009/110/CE, né al concetto più ampio di "fondi" contemplato dall'art. 4, punto 25, della direttiva (UE) 2015/2366 (Payment Services Directive 2).

Esse non coincidono, altresì, con il valore monetario impiegato per l'esecuzione di operazioni di pagamento, né con le cosiddette "valute di gioco", ossia i valori digitali destinati a circolare unicamente all'interno di un ambiente virtuale chiuso e non convertibili all'esterno.

Questa precisazione, lungi dal costituire una mera puntualizzazione definitoria, assolve a una funzione sistematica essenziale: essa consente di individuare con esattezza l'ambito di applicazione della disciplina antiriciclaggio e di evitare la sovrapposizione tra il regime delle cripto-attività e quello, già consolidato, degli strumenti di pagamento elettronici.

La distinzione operata dal legislatore unionale si fonda su un criterio eminentemente sostanziale, imperniato sulla diversa natura giuridico-funzionale dei due istituti: mentre la moneta elettronica e gli altri mezzi di pagamento digitali rappresentano forme di valore emesse da un soggetto autorizzato e garantite da un ordinamento giuridico, le valute virtuali si caratterizzano per l'assenza di un emittente riconosciuto e per la decentralizzazione del processo di validazione e trasferimento, fondato sulla distributed ledger technology (DLT).

L'intento che permea tale distinzione è duplice; da un lato, il legislatore europeo mira a costruire un quadro di vigilanza coerente con la finalità preventiva e di trasparenza che ispira la disciplina AML/CFT; dall'altro, intende garantire che l'applicazione delle regole

antiriciclaggio si estenda a tutte le forme di utilizzazione delle valute virtuali, indipendentemente dalla loro diffusione o dalla specifica tecnologia sottostante.

In tal modo, la direttiva persegue l'obiettivo di assicurare una copertura normativa quanto più ampia possibile, capace di intercettare anche i fenomeni emergenti di innovazione finanziaria e di ridurre il rischio che nuove soluzioni tecnologiche possano sfuggire ai presidi di controllo.

L'ampiezza dell'approccio europeo non si traduce, tuttavia, in una posizione di chiusura rispetto al progresso tecnologico. Al contrario, la direttiva si colloca in una prospettiva di equilibrio dinamico, nella quale l'esigenza di prevenire l'uso illecito delle cripto-attività convive con il riconoscimento del loro potenziale innovativo e del contributo che esse possono offrire allo sviluppo di mercati digitali più inclusivi, trasparenti e competitivi.

In tal senso, la V Direttiva Antiriciclaggio rappresenta una tappa di mediazione tra la rigidità dei meccanismi di controllo finanziario tradizionali e la flessibilità richiesta dalle nuove architetture economiche digitali, configurandosi come il primo tentativo organico di integrare la logica della tracciabilità con quella dell'innovazione sostenibile[39].

L'attenzione del legislatore europeo al bilanciamento tra le esigenze di prevenzione dei fenomeni di riciclaggio e finanziamento del terrorismo e la promozione dell'innovazione tecnologica evidenzia, in ultima analisi, la volontà dell'Unione di adottare un approccio regolatorio flessibile e proporzionato.

Si tratta di un modello di governance normativa che mira a coniugare la tutela dell'integrità del sistema finanziario con il riconoscimento del potenziale trasformativo delle tecnologie fintech e dei nuovi strumenti di pagamento digitali, nella consapevolezza che la rigidità dei meccanismi di controllo tradizionali non è più compatibile con la dinamicità dell'economia digitale globale[40].

---

[39] Cfr. G. GUIZZI, *La vigilanza europea antiriciclaggio: verso un modello accentrato di supervisione*, in *Banca, Borsa e Titoli di Credito*, 2023, p. 319 ss.

[40] Si veda, F. CAPRIGLIONE, *Finanza digitale e legalità economica nel diritto dell'Unione europea*, in *Riv. trim. di dir. dell'econ.*, 2022, p. 75 ss. Il termine FinTech è in particolare qui impiegato quale variegato ecosistema composto da eterogenee situazioni, tutte connotate dal fatto di essere considerate «as financial activities which provide an added value by means of digital technology»; Così G. SERAFIN, *FinTech: tra piattaforme di crowdfunding, valute virtuali e contrasto del riciclaggio,* in *Ricerche giuridiche*, 8, 1/2019, p. 121 e nota 5. «Dalla creazione di nuovi sistemi di pagamento, ai canali di finanziamento alternativi; dalla creazione di nuove valute virtuali sino ai nuovi processi attraverso i quali vengono offerti servizi finanziari già conosciuti» ibidem. Possono essere considerati servizi innovativi quelli del marketplace lending e della supply chain finance, rispettivamente di finanziamento a mediolungo periodo e breve periodo, tra cui collocare l'equity crowdfunding e il lending crowdfunding, differenziati in base all'assunzione o meno da parte della piattaforma di posizioni creditorie. Per un'analisi tecnica di questi istituti si rinvia a V. BOSCIA – V.

Il legislatore italiano, in tale contesto, ha proceduto a recepire la V Direttiva Antiriciclaggio con tempestività, anche in ragione del fatto che, già in sede di attuazione della IV Direttiva (Direttiva (UE) 2015/849), l'Italia aveva parzialmente anticipato il quadro normativo unionale, introducendo nel D.Lgs. 21 novembre 2007, n. 231 – il cosiddetto "Decreto Antiriciclaggio" – definizioni autonome di "valuta virtuale" e di "prestatore di servizi relativi all'utilizzo di valuta virtuale".

Tali formulazioni, tuttavia, si caratterizzavano per un'impostazione ancora embrionale e per la presenza di profili definitori suscettibili di ambiguità o incompletezza, che rischiavano di essere rapidamente superati dall'evoluzione tecnologica e dall'emersione di nuove categorie di operatori digitali.

Con il recepimento della V Direttiva, il legislatore nazionale ha colto l'occasione per armonizzare la disciplina interna agli standard elaborati in sede europea, aggiornando la definizione di valuta virtuale e includendo tra le finalità espresse anche quella dell'investimento, fino ad allora esclusa.

L'intervento ha permesso di allineare il lessico normativo italiano alle formulazioni comunitarie, non solo per garantire una maggiore coerenza terminologica, ma anche per assicurare una piena interoperabilità tra i diversi livelli di regolazione – nazionale, unionale e internazionale.

L'integrazione di tale finalità riflette un mutamento di prospettiva di non trascurabile rilievo sistematico: il legislatore riconosce esplicitamente che le valute virtuali, lungi dall'essere meri strumenti di scambio o mezzi di pagamento alternativi, si configurano sempre più come veicoli di investimento, suscettibili di impiego nei mercati finanziari e nei circuiti di finanza decentralizzata.

In tal senso, la disciplina antiriciclaggio si apre a una dimensione più ampia, che travalica la mera prevenzione dei flussi illeciti per estendersi alla regolazione di nuovi fenomeni economici connessi alla digitalizzazione della finanza.

Ne deriva che l'ordinamento nazionale, pur mantenendo un solido ancoraggio ai principi fondanti della trasparenza e della tracciabilità, si inserisce in un percorso di

---

STEFANELLI – L. SAPRIO, *L'impatto delle digital technologies nei processi di finanziamento: le risposte delle banche incumbents e delle FinTech*, in (a cura di) V. Boscia, C. Schena, V. Stefanelli, *Digital Banking e Fin tech. L'intermediazione finanziaria tra cambiamenti tecnologici e sfide di mercato,* ABIServizi, 2020, pp. 212-222. Nella medesima opera per l'esame di servizi già noti di e-payments, quali carte di credito o di debito utilizzabili via internet, o di mobile payments fino alle forme più evolute di voice ed instant payments, nonché delle valute virtuali, si rinvia a V. BOSCIA – V. STEFANELLI – R. VERGALLO – A. CAIONE, *Le innovazioni tecnologiche digitali nei servizi di pagamento: tra instant payments e voice banking*, pp. 184-197.

progressiva convergenza con il diritto dell'Unione, fondato su un equilibrio dinamico tra esigenze di sicurezza giuridico-finanziaria e libertà dell'iniziativa economica.

In questa prospettiva, la V Direttiva Antiriciclaggio non rappresenta soltanto un'evoluzione del quadro normativo esistente, ma un vero e proprio snodo di transizione verso un modello integrato di regolazione dei mercati digitali, nel quale la funzione preventiva del diritto si coniuga con quella propulsiva dell'innovazione tecnologica[41].

Nella sua formulazione attuale, l'art. 1, comma 2, lett. *qq)*, del D.Lgs. n. 231/2007 definisce la valuta virtuale come «la 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 o a fini di investimento e trasferibile, memorizzabile e negoziabile elettronicamente». La disposizione, che recepisce la definizione contenuta nella V Direttiva Antiriciclaggio, cristallizza un concetto volutamente ampio e tecnologicamente neutro, idoneo a ricomprendere la molteplicità delle manifestazioni concrete assunte dal fenomeno delle cripto-attività. Essa valorizza, inoltre, la finalità d'investimento accanto a quella di scambio, riconoscendo così la funzione ibrida e poliedrica delle valute virtuali, suscettibili di operare simultaneamente come mezzo di pagamento, riserva di valore e strumento speculativo.

La successiva lett. *ff)* del medesimo comma individua, poi, i "prestatori di servizi relativi all'utilizzo di valuta virtuale" in «ogni persona fisica o giuridica che, a titolo professionale, anche tramite mezzi elettronici, fornisce a terzi servizi funzionali all'utilizzo, allo scambio o alla conservazione di valute virtuali, nonché alla loro conversione da ovvero in valute aventi corso legale o in altre rappresentazioni digitali di valore, comprese quelle convertibili in ulteriori valute virtuali».

La norma, di ampia portata, include un insieme eterogeneo di attività riconducibili alla sfera della prestazione professionale, comprendendo non solo i servizi di emissione, offerta, trasferimento o compensazione, ma anche ogni ulteriore attività idonea a consentire l'acquisizione, la negoziazione o l'intermediazione nello scambio di tali strumenti.

In tal modo, il legislatore nazionale ha inteso costruire un perimetro definitorio estensivo, capace di intercettare anche gli operatori che, pur non assumendo formalmente

[41] Cfr. A. SCIARRONE ALIBRANDI, *La V Direttiva antiriciclaggio e le sfide della digitalizzazione finanziaria*, in *Riv. di dir. banc. e fin.* 2023, p. 201 ss.

la veste di intermediari finanziari, svolgono un ruolo funzionale alla circolazione o alla custodia delle cripto-attività.

Nello stesso contesto, il recepimento della V Direttiva ha comportato l'introduzione, mediante l'aggiunta della lett. *ff-bis)* al citato art. 1, comma 2, di una ulteriore figura soggettiva: quella dei "prestatori di servizi di portafoglio digitale".

Tali soggetti vengono qualificati come «ogni persona fisica o giuridica che, a titolo professionale, anche online, presta servizi di salvaguardia di chiavi crittografiche private per conto dei propri clienti, al fine di detenere, memorizzare e trasferire valute virtuali».

La previsione assume un rilievo sistemico di particolare importanza, in quanto consente di attrarre nell'ambito applicativo della disciplina antiriciclaggio una categoria di operatori che, pur non gestendo direttamente i flussi finanziari, svolgono una funzione determinante nel garantire la sicurezza informatica e la custodia delle chiavi di accesso agli asset digitali.

Si tratta, pertanto, di soggetti che, per la natura fiduciaria e sensibile delle attività esercitate, devono essere sottoposti a obblighi di identificazione, adeguata verifica e segnalazione delle operazioni sospette, al pari degli altri operatori tradizionalmente inclusi nel perimetro antiriciclaggio.

Nonostante tali interventi, il quadro definitorio e regolatorio non può ancora considerarsi stabilizzato. La disciplina delineata dal D.Lgs. n. 231/2007 – pur profondamente innovata dal recepimento della V Direttiva – è stata infatti oggetto di ulteriori e significative trasformazioni a seguito dell'adozione del Regolamento (UE) 2023/1114 (MiCAR)[42].

Quest'ultimo ha introdotto un corpus normativo unitario e direttamente applicabile, destinato a incidere in modo strutturale sulla qualificazione giuridica delle cripto-attività e sulla definizione delle categorie di operatori sottoposti a vigilanza, proiettando la disciplina antiriciclaggio in una dimensione di compiuta integrazione europea[43].

---

[42] Si vedano, in argomento, gli interessanti contribute di C. BRUMMER**,** *Cryptoassets, Regulation, and Global Financial Stability*, Oxford University Press, 2023; R. HOUBEN – A. SNYERS, *Crypto-Assets and the Fight against Money Laundering and Terrorist Financing*, European Parliament Study, 2022.

[43] L'emanazione del *Regolamento (UE) 2023/1113,* concernente i dati informativi che accompagnano i trasferimenti di fondi e di determinate cripto-attività, rappresenta uno snodo decisivo nel processo di evoluzione del diritto dell'Unione in materia di prevenzione del riciclaggio e del finanziamento del terrorismo. Esso si inserisce nel più ampio *pacchetto antiriciclaggio* varato dalla Commissione nel 2021, e si coordina in modo sistemico con il *Regolamento (UE) 2023/1114* – meglio noto come *MiCAR (Markets in Crypto-Assets Regulation)* – e con la proposta di istituzione dell'Autorità europea antiriciclaggio (*AMLA*). Con tali interventi, il legislatore europeo abbandona definitivamente la prospettiva frammentaria delle precedenti

Tale regolamento, volto ad assicurare la tracciabilità delle operazioni effettuate mediante

direttive, per adottare un modello pienamente *regolamentare* e direttamente applicabile negli ordinamenti nazionali. Si realizza così un passaggio paradigmatico: dal mero coordinamento tra normative interne alla creazione di un *level playing field* unitario, nel quale la disciplina AML/CFT si integra con la regolazione prudenziale e di condotta dei mercati digitali. Il Regolamento (UE) 2023/1113, in particolare, impone ai fornitori di servizi di cripto-attività l'obbligo di trasmettere informazioni standardizzate relative all'identità dell'ordinante e del beneficiario per ciascun trasferimento, riproducendo, in sostanza, la logica della *travel rule* già prevista per gli operatori tradizionali di pagamento. Tale obbligo mira a garantire la tracciabilità end-to-end dei flussi digitali, consentendo alle *Financial Intelligence Units* e alle autorità competenti di ricostruire la catena delle transazioni e di prevenire l'uso dei nuovi strumenti tecnologici per finalità di occultamento o riciclaggio. La portata innovativa di questa disciplina emerge dal superamento dell'asimmetria informativa che, fino ad oggi, aveva caratterizzato le operazioni in cripto-attività: il principio di *pseudonimato* su cui si fondano i registri distribuiti viene bilanciato da un regime di trasparenza obbligatoria che non incide sulla struttura tecnologica della blockchain, ma ne neutralizza gli effetti elusivi. Si realizza così una forma di *accountability tecnologica* che estende le responsabilità di *compliance* lungo l'intera catena del valore digitale, imponendo a ciascun operatore – dall'exchanger al custodian wallet provider – di adottare presidi di *know-your-customer* (KYC) e di *record keeping* conformi ai principi del diritto antiriciclaggio.

Parallelamente, il *Regolamento MiCAR* delinea un quadro omnicomprensivo per l'emissione, l'offerta al pubblico e l'ammissione alla negoziazione delle cripto-attività, distinguendo tra *asset-referenced tokens*, *e-money tokens* e altri tipi di *crypto-assets*. La logica sottesa è quella di costruire un regime autorizzativo e di vigilanza armonizzato, in grado di assicurare parità di condizioni concorrenziali e tutela dell'integrità del mercato interno.

L'interazione tra MiCAR e il Regolamento (UE) 2023/1113 produce un effetto sistemico: da un lato, l'introduzione di obblighi informativi rafforza il presidio AML/CFT; dall'altro, la regolazione di prodotto e di condotta stabilisce le condizioni per una maggiore certezza giuridica delle operazioni digitali, contribuendo alla *main streaming* delle cripto-attività nel mercato finanziario europeo. Nel contesto italiano, tali innovazioni comportano una profonda ridefinizione del *Decreto Antiriciclaggio* e delle competenze dell'Unità di Informazione Finanziaria (UIF) e dell'Organismo degli Agenti e dei Mediatori (OAM), cui spetta la tenuta del registro dei prestatori di servizi relativi all'utilizzo di valute virtuali. Le autorità nazionali dovranno procedere a un'armonizzazione interpretativa che eviti sovrapposizioni tra il perimetro soggettivo dei *virtual asset service providers* e quello dei *crypto-asset service providers* disciplinati dal MiCAR, garantendo coerenza tra gli obblighi di vigilanza prudenziale e quelli antiriciclaggio. Da un punto di vista sistematico, la combinazione dei due regolamenti realizza una progressiva "*europeizzazione*" del diritto antiriciclaggio applicato alle cripto-attività, segnando il passaggio da una regolazione eminentemente nazionale a una *supervisione integrata* di matrice unionale.

Tale evoluzione, tuttavia, solleva questioni interpretative e applicative di non poco momento: la delimitazione delle competenze tra AMLA e autorità nazionali, la disciplina del trattamento dei dati personali nel contesto delle *travel rules* e l'interazione tra obblighi di trasparenza e tutela della privacy rappresentano, infatti, i nodi più delicati della nuova architettura normativa. In prospettiva, l'attuazione coordinata del MiCAR e del Regolamento (UE) 2023/1113 sembra prefigurare l'avvio di *una finanza digitale regolata,* nella quale l'innovazione tecnologica non costituisce più un fattore di deregolazione, bensì un terreno di applicazione dei principi di proporzionalità, trasparenza e responsabilità che informano l'intero diritto dell'economia dell'Unione. Si tratta, dunque, di un passaggio evolutivo che conduce verso una concezione del diritto antiriciclaggio non più confinata alla dimensione repressiva, ma proiettata alla costruzione di un ecosistema digitale sicuro, interoperabile e conforme ai valori fondamentali dell'ordinamento europeo.

cripto-attività[44], introduce ulteriori obblighi di trasparenza e di comunicazione, incidendo profondamente sull'assetto del diritto antiriciclaggio europeo e nazionale, e segnando un ulteriore passo verso l'integrazione del regime AML/CFT con la nuova architettura regolatoria dei mercati digitali dell'Unione[45].

In tale prospettiva, la scelta del legislatore italiano si è rivelata coerente con le finalità perseguite dal legislatore europeo: individuare con chiarezza le categorie di soggetti tenuti all'osservanza degli obblighi antiriciclaggio e, attraverso questi, rendere effettiva la strategia di contrasto ai fenomeni di criminalità finanziaria.

Il quadro normativo definito a livello legislativo dal *Decreto Antiriciclaggio* ha infatti consentito di avviare le prime forme di vigilanza pubblica sugli operatori specializzati in servizi connessi alle valute virtuali, segnando il passaggio da una fase di mera osservazione del fenomeno a una di regolazione progressiva e istituzionalmente accentrata.

Con il *Decreto del Ministero dell'Economia e delle Finanze del 13 febbraio 2022,* è stata istituita, all'interno del registro dei cambiavalute previsto dall'art. 17-bis, comma 1, del D.lgs. 13 agosto 2010, n. 141, una *sezione speciale* dedicata ai soggetti autorizzati, nel territorio della Repubblica, a esercitare i servizi relativi all'utilizzo di valute virtuali e i servizi di portafoglio digitale.
La tenuta di tale sezione è stata affidata all'*Organismo per la gestione degli elenchi degli agenti in attività finanziaria e dei mediatori creditizi* (OAM), il quale, in attesa di una più compiuta definizione delle proprie funzioni di vigilanza e controllo, rappresenta oggi il primo presidio istituzionale deputato al monitoraggio di questo comparto.

La disciplina nazionale vigente, codificata nel D.Lgs. 21 novembre 2007, n. 231 (c.d. *Decreto Antiriciclaggio)*, pur richiedendo oggi interventi di riordino e di maggiore coordinamento sistematico con la normativa europea di ultima generazione, ha nondimeno posto le basi per l'edificazione di un quadro regolatorio e di vigilanza sul comparto delle valute virtuali.

Essa ha rappresentato, in particolare, il primo tentativo organico di ricondurre le cripto-attività entro una dimensione giuridicamente strutturata, superando la fase iniziale di

[44] Si veda, V. SANTORO, *La tracciabilità delle cripto-attività e la prevenzione del riciclaggio: dal D.lgs. 231/2007 al Regolamento (UE) 2023/1113*, in *Rivista di diritto dell'economia*, 2024, p. 103 ss.

[45] Cfr. M. MAUGERI, *La regolazione europea delle cripto-attività tra innovazione e tutela del mercato*, in *Banca, Borsa e Titoli di Credito*, 2024, p. 145 ss.

sostanziale deregolamentazione che aveva favorito una rapida, ma disordinata, espansione del fenomeno.

In assenza di tale intervento normativo, il settore delle valute virtuali sarebbe rimasto esposto a un regime di libertà assoluta, con il rischio di perpetuare quelle medesime caratteristiche di opacità e di autoregolazione che, se da un lato avevano costituito il motore della crescita esponenziale del mercato, dall'altro ne avevano evidenziato la fragilità strutturale.

Queste criticità non si esauriscono nella mera volatilità dei valori di riferimento o nella difficoltà di assicurare una protezione effettiva agli investitori, ma si estendono, sotto un profilo più propriamente sistemico, all'impossibilità di ricondurre l'utilizzo delle valute virtuali entro un contesto regolamentato e concorrenziale, fondato su principi di trasparenza, parità informativa e correttezza operativa.

In tale prospettiva, la scelta del legislatore italiano si è mostrata pienamente coerente con le finalità perseguite a livello europeo, ispirandosi all'esigenza di identificare con precisione le categorie di soggetti tenuti all'osservanza degli obblighi antiriciclaggio e, attraverso di essi, di rafforzare l'efficacia della strategia complessiva di contrasto alla criminalità finanziaria.

L'intervento nazionale si colloca così nel solco del processo di armonizzazione multilivello avviato dal legislatore unionale, fungendo da strumento di implementazione anticipata dei principi di *compliance* e *transparency* propri della disciplina AML/CFT.

Il quadro normativo delineato dal *Decreto Antiriciclaggio* ha, infatti, consentito di avviare le prime forme di vigilanza pubblica sugli operatori specializzati nei servizi connessi alle valute virtuali, segnando il passaggio da una fase di mera osservazione del fenomeno a una fase di regolazione progressiva e istituzionalmente accentrata.

Un passaggio che ha comportato, in termini funzionali, il riconoscimento dell'esigenza di sottoporre tali operatori a un controllo pubblico strutturato, quale condizione imprescindibile per la stabilità e l'affidabilità del sistema economico-finanziario[46].

[46] In tema, si vedano, F. CAPRIGLIONE, *Intervento pubblico e ordinamento del credito*, Milano, 1978.; S. AMOROSINO, *Tipologie e funzioni delle vigilanze pubbliche sulle attività economiche*, in E. Bani - M. Giusti (a cura di), *Vigilanze economiche. Le regole e gli effetti*, CEDAM 2004, p. 743, il quale parla di vigilanza regolamentare precetti, vigilanza autorizzativa, vigilanza informativa ispettiva, vigilanza conformativa/ correttiva e vigilanza sanzionatorie. Piu di recente, sempre S. AMOROSINO, *Le regolazioni pubbliche delle attività economiche*, Giappichelli, 2021.

A tale scopo, il Decreto del Ministero dell'Economia e delle Finanze del 13 febbraio 2022 ha istituito, all'interno del registro dei cambiavalute previsto dall'art. 17-bis, comma 1, del D.Lgs. 13 agosto 2010, n. 141, una *sezione speciale* dedicata ai soggetti autorizzati, nel territorio della Repubblica, all'esercizio dei servizi relativi all'utilizzo di valute virtuali e dei servizi di portafoglio digitale. La tenuta di tale sezione è stata affidata all'Organismo per la gestione degli elenchi degli agenti in attività finanziaria e dei mediatori creditizi (OAM), che, in attesa di una più compiuta definizione delle proprie funzioni di vigilanza e controllo, rappresenta oggi il primo presidio istituzionale di monitoraggio sul comparto.

L'istituzione del registro OAM non ha una mera funzione ricognitiva, ma assume una valenza giuridica sostanziale: l'iscrizione costituisce condizione necessaria per l'esercizio legittimo dell'attività, mentre l'eventuale esercizio abusivo comporta l'applicazione delle sanzioni amministrative e penali previste dall'ordinamento.

Tale meccanismo, oltre a perseguire obiettivi di correttezza e trasparenza, mira a tutelare la concorrenza e a garantire la stabilità del sistema finanziario, prevenendo l'ingresso di operatori non qualificati o potenzialmente opachi in un settore particolarmente esposto a rischi di abuso, frode e infiltrazione criminale.

In questa prospettiva, il registro degli operatori in valute virtuali costituisce il primo passo verso la costruzione di un sistema di vigilanza strutturato, in grado di coniugare la funzione di tracciabilità economico-finanziaria con quella di garanzia della leale concorrenza e dell'affidabilità degli intermediari digitali[47].

Dal punto di vista sostanziale, l'iscrizione nel registro istituito presso l'OAM comporta la piena applicabilità, nei confronti dei prestatori di servizi relativi all'utilizzo di valute virtuali e di portafogli digitali, dell'intero apparato di obblighi previsto dal *Decreto Antiriciclaggio*.
Essi sono pertanto tenuti a rispettare i doveri di adeguata verifica della clientela (*customer due diligence*), di conservazione dei dati e delle informazioni e di tempestiva segnalazione delle operazioni sospette alle autorità competenti, secondo le modalità e i criteri delineati dalle disposizioni attuative della Banca d'Italia[48].

---

[47] Sull'evoluzione normativa delle criptovalute in Italia e sul ruolo dell'OAM, si veda, F. LUCHETTI - F. RUGGIERO, *Criptovalute. Quadro regolamentare nazionale e prospettive future: il ruolo dell'Organismo degli agenti in attività finanziaria e dei mediatori creditizi (OAM)*, in *Mercati finanziari e transizione digitale. Una tassonomia,* cit., p. 116 ss.

[48] Senza alcuna pretesa di esaustività, tra i molti, si vedano, G. DELL'AMORE, *Il processo di costituzione della Banca centrale in Italia*, Milano, 1967; G. PUCCINI, *L'autonomia dalla Banca d'Italia*, Milano, 1978; F. MERUSI, *Per uno studio sui poteri della Banca centrale nel governo della moneta,* in *Riv. Trim. dir. pubbl.*, 1972, p. 1425 ss; ID., *La posizione costituzionale della Banca centrale in Italia,* in *Riv. Trim. dir. pubbl.,* 1982, p. 1081 ss.; F. CAPRIGLIONE, *Intervento pubblico e ordinamento del credito*, Milano, 1978; S. ORTINO, *Banca d'Italia e Costituzione*, Pisa, 1979; P. DE VECCHIS, *Banca d'Italia*, in *Dig. disc. pubbl.*, 1987, p. 151 ss.; C. GIANNINI, *L'età delle banche centrali*, Bologna

L'estensione di tali obblighi agli operatori del comparto delle cripto-attività segna un passaggio paradigmatico: la disciplina antiriciclaggio, da mera cornice di prevenzione generale, diviene strumento effettivo di regolazione e di presidio di legalità all'interno dell'economia digitale.

Pur se l'attuale assetto regolamentare risulta, ad oggi, meno articolato rispetto a quello previsto per gli intermediari bancari e finanziari tradizionali, esso rappresenta nondimeno il primo nucleo di un sistema di vigilanza specificamente dedicato al mercato delle cripto-attività.

L'introduzione di presidi di compliance, di obblighi di monitoraggio e di canali di segnalazione istituzionali configura, infatti, il fondamento di una strategia di supervisione effettiva e progressivamente integrata, coerente con la visione del Regolatore europeo, che mira a garantire un controllo strutturato e omogeneo dei mercati digitali a fini di prevenzione del riciclaggio e del finanziamento del terrorismo.

L'inclusione dei prestatori di servizi in valute virtuali in un perimetro giuridico formalmente definito risponde alla logica di costruire un universo regolamentato di soggetti obbligati, il cui accesso all'attività economica sia subordinato a un processo autorizzativo e alla vigilanza di un'autorità competente.

In questa prospettiva, la disciplina antiriciclaggio opera come meccanismo selettivo e di legittimazione dell'attività economica nel settore digitale, trasformando la trasparenza e la tracciabilità da meri principi programmatici in veri e propri strumenti di tutela dell'integrità dei mercati, della stabilità finanziaria e della concorrenza leale.

La progressiva assimilazione dei prestatori di servizi in cripto-attività agli intermediari finanziari regolamentati tradizionali rappresenta, dunque, non solo un rafforzamento della funzione di prevenzione, ma anche un tassello essenziale nel processo di istituzionalizzazione del mercato delle valute virtuali.

Attraverso tale inquadramento, il diritto dell'economia compie un passo decisivo verso la costruzione di un ecosistema finanziario digitale fondato su regole comuni, sulla responsabilità degli operatori e sulla tracciabilità delle operazioni, in linea con i più avanzati standard internazionali di "*financial integrity*".

2004; L. TORCHIA, *Verso una Banca d'Italia repubblicana ed europea?* in *Giorn. Dir. amm.*, 2006, p. 273 ss.; G. MINERVINI, *La Banca d'Italia*, in *Banca, Borsa e tit. cred.,* 2006, p. 619 ss.; P. FERRO-LUZZI, *Cosa è la Banca d'Italia*, in *Banca, Borsa e tit. cred.*, 2007, p. 364 ss.; A. URBANI, *La riforma della governance e delle competenze della Banca d'Italia,* in *Dir. banc. Merc.*, 2008, p. 273 ss.

È verosimile che, con l'evolversi della disciplina europea e con l'entrata in piena operatività del Regolamento MiCAR[49] e del Regolamento (UE) 2023/1113, gli adempimenti antiriciclaggio richiesti a questa categoria di soggetti si intensificheranno anche sotto il profilo dei requisiti organizzativi, di *governance* e di controllo interno.

Tuttavia, l'impianto attuale rappresenta già una tappa fondamentale di questo percorso evolutivo, in quanto contribuisce a superare una delle principali criticità che gli organismi nazionali e internazionali hanno costantemente evidenziato sin dalle prime manifestazioni del fenomeno delle valute virtuali: la loro naturale attitudine a favorire operazioni di riciclaggio e di finanziamento del terrorismo, in ragione dell'ampia area di anonimato che caratterizza i soggetti coinvolti nelle transazioni aventi ad oggetto tali strumenti[50].

L'evoluzione normativa sin qui delineata dimostra come l'ordinamento italiano, pur attraverso un processo di progressiva maturazione e non esente da incertezze applicative, sia riuscito ad allinearsi alla traiettoria evolutiva tracciata dal legislatore dell'Unione, ponendosi in posizione di convergenza sostanziale rispetto ai più recenti sviluppi del quadro regolatorio europeo in materia di AML/CFT.

L'adozione di strumenti di vigilanza specifici – quali la sezione speciale del registro OAM – e l'estensione degli obblighi antiriciclaggio ai prestatori di servizi in valute virtuali rappresentano, in tale prospettiva, una tappa di rilievo nel percorso verso la costruzione di una cornice normativa armonizzata, fondata su principi comuni di trasparenza, responsabilità e cooperazione interistituzionale.

L'integrazione fra disciplina interna e sistema europeo si configura, dunque, non come un mero esercizio di adeguamento formale, bensì come un'evoluzione strutturale del modello di vigilanza, orientata al superamento delle tradizionali frammentazioni nazionali e alla realizzazione di un effettivo coordinamento multilivello tra autorità competenti.

Tuttavia, la sola armonizzazione legislativa – pur costituendo un progresso significativo – non appare sufficiente, di per sé, a garantire l'effettività sostanziale del sistema di prevenzione.
Le esperienze maturate nei diversi ordinamenti nazionali hanno messo in luce come l'eterogeneità delle prassi di vigilanza, la disomogeneità delle capacità tecniche delle autorità competenti e la persistente frammentazione dei flussi informativi abbiano finito

[49] Si veda, G. DE LUCA, *Il Regolamento MiCAR e la disciplina dei mercati delle cripto-attività*, in *Orizzonti del dir. comm.*, 2024, p. 221 ss.

[50] Cfr., A. FICI, *Le valute virtuali tra libertà d'impresa e controllo pubblico: la prospettiva del diritto dell'economia*, in *Il Diritto dell'Economia*, 2023, p. 57 ss.

per attenuare la portata integrativa del quadro europeo, ostacolando l'instaurazione di un contrasto realmente unitario ai fenomeni di riciclaggio e di finanziamento del terrorismo.

Tale organismo, concepito quale vertice del sistema europeo di prevenzione e contrasto dei flussi finanziari illeciti, nasce con la finalità di rafforzare l'integrazione funzionale dei meccanismi di vigilanza, garantendo, da un lato, la supervisione diretta sui soggetti a più elevato rischio transfrontaliero e, dall'altro, il coordinamento centralizzato delle autorità nazionali competenti[51].

La creazione dell'AMLA si colloca, dunque, nel solco di un disegno di governance finanziaria europea ispirato ai principi di uniformità regolatoria e di coerenza applicativa, volto a superare le asimmetrie operative che ancora caratterizzano l'attività di prevenzione del riciclaggio nei diversi Stati membri e a promuovere una *financial integrity union* effettiva e credibile[52].

La sua istituzione, destinata a divenire pienamente operativa nei prossimi anni, rappresenta la risposta più ambiziosa e strutturata dell'Unione europea alla necessità di superare il tradizionale paradigma del mutuo riconoscimento, che per lungo tempo ha caratterizzato la cooperazione interstatale in materia di prevenzione del riciclaggio e del finanziamento del terrorismo.

Il nuovo assetto si fonda, invece, su un modello di vigilanza accentrata, basato su procedure uniformi di controllo, criteri armonizzati di *compliance* e un apparato sanzionatorio coerente e direttamente applicabile, in linea con la logica di piena integrazione del mercato finanziario europeo.

Alla nuova Autorità è affidato il compito di garantire l'applicazione uniforme delle norme AML/CFT in tutti gli Stati membri, promuovendo la convergenza sostanziale delle prassi di vigilanza e il coordinamento operativo tra le autorità nazionali competenti.

L'Autorità eserciterà poteri di supervisione diretta sui soggetti obbligati a elevato rischio transfrontaliero, di monitoraggio sull'effettività dei presidi di controllo interni e di indirizzo tecnico-metodologico nei confronti delle *Financial Intelligence Units* (FIU) nazionali, delle quali coordinerà l'attività di scambio informativo e di analisi strategica.

---

[51] Cfr. R. D'AMBROSIO – M. LAMANDINI, *La «prima volta» del Tribunale dell'Unione europea in materia di Meccanismo di Vigilanza Unico,* in *Giur. comm.*, 2017, p. 594 ss.; F. ANNUNZIATA, *Chi ha paura della Banca Centrale Europea? Riflessioni a margine del caso Landeskreditbank c. BCE,* in *Giur. comm.,* 2017, pp. 111 e 8 ss.

[52] Cfr. A. ZORZI, *L'integrazione multilivello nella governance AML/CFT europea*, in *Riv. di dir. pubbl. dell'economia*, 2024, p. 77 ss.

Sotto il profilo sistematico, la creazione dell'AMLA si colloca come l'esito naturale – e, per certi versi, necessario – di un processo di progressiva europeizzazione della disciplina antiriciclaggio, inaugurato dalle prime direttive e consolidatosi attraverso un percorso di graduale rafforzamento dei poteri sovranazionali in materia di vigilanza finanziaria.

Il nuovo quadro regolatorio, oggi rappresentato da un corpus unitario che comprende il Regolamento (UE) 2023/1114 sui mercati delle cripto-attività (*MiCAR*), il Regolamento (UE) 2023/1113 sui trasferimenti di fondi e il Regolamento istitutivo dell'AMLA, segna la transizione da una logica di armonizzazione minima a una di vera e propria unificazione funzionale del sistema AML/CFT europeo.

In questa prospettiva, la dimensione tecnologica delle cripto-attività assume un rilievo paradigmatico: essa diviene non più soltanto una fonte di rischio sistemico da arginare, ma anche e soprattutto un banco di prova per l'elaborazione di un nuovo paradigma di vigilanza integrata, in cui l'innovazione digitale e la "*distributed ledger technology" (DLT)* si pongono al servizio della tracciabilità, della trasparenza e della proporzionalità dell'azione regolatoria.

Il passaggio da un sistema di vigilanza nazionale e reattiva a uno di supervisione europea, preventiva e proattiva, esprime così la volontà dell'Unione di trasformare la digitalizzazione dei mercati finanziari da fattore di vulnerabilità a strumento di garanzia dell'integrità, della legalità e della stabilità complessiva del mercato unico[53].

Per l'Italia, l'avvio del nuovo sistema europeo di vigilanza in materia di *Aantiriciclaggio* comporta una duplice sfida di natura tanto strutturale quanto funzionale.

Da un lato, si impone un profondo processo di adeguamento delle autorità nazionali competenti – in particolare dell'Organismo per la gestione degli elenchi degli Agenti in attività finanziaria e dei Mediatori creditizi (OAM) e dell'Unità di Informazione Finanziaria per l'Italia (UIF) – agli standard operativi, informativi e tecnologici delineati dall'architettura europea.

Dall'altro, è necessaria una piena integrazione del sistema domestico di vigilanza in un modello multilivello, nel quale la supervisione diretta esercitata dall'AMLA coesista e si coordini con le prerogative attribuite agli organismi nazionali, secondo un equilibrio

[53] Cfr. A. PISANESCHI, *La nuova Anti-Money Laundering Authority (AMLA): profili di indipendenza e coordinamento*, in *Il Diritto dell'Economia*, 2024, p. 5 ss.

dinamico fondato sulla complementarità funzionale e sulla condivisione delle informazioni.

Questa transizione, che segna il passaggio da un approccio nazionale ad un modello di *governance* europea integrata, non rappresenta soltanto un'evoluzione di natura istituzionale, ma riflette l'affermarsi di una nuova *ratio legis*, coerente con la fisionomia contemporanea del diritto dell'economia. Un diritto che si fonda sulla responsabilità condivisa tra livelli ordinamentali, sulla cooperazione informativa tra autorità di vigilanza e sull'impiego di strumenti di *regulatory technology (RegTech)* e *supervisory technology (SupTech),* idonei a coniugare innovazione digitale e legalità sostanziale, efficienza dei controlli e tutela dei diritti fondamentali.

In questa prospettiva, la disciplina italiana in materia di valute virtuali e prestatori di servizi in cripto-attività, pur trovandosi ancora in una fase di consolidamento, assume un rilievo paradigmatico. Essa può essere considerata, a tutti gli effetti, un laboratorio di sperimentazione giuridica e istituzionale nel quale si testano gli strumenti e i modelli di coordinamento destinati a confluire nel più ampio disegno europeo di un diritto della finanza digitale fondato sui principi di trasparenza, tracciabilità e sicurezza.

L'armonizzazione tra dimensione tecnologica e presidio giuridico, tra innovazione e controllo, segna così la via verso un ordinamento economico-finanziario capace di coniugare competitività, integrità e sostenibilità regolatoria[54].

4. La genesi dell'AMLA come "tournant" del nuovo quadro regolatorio europeo.

Nel suo complesso, il percorso evolutivo della disciplina europea e nazionale in materia di antiriciclaggio testimonia, come si è avuto modo di descrivere, il progressivo superamento di un modello di regolazione frammentato e settoriale, in favore di un sistema integrato di vigilanza, ispirato a criteri di uniformità, interoperabilità e coordinamento multilivello.

Elemento cardine del nuovo disegno istituzionale è l'istituzione dell'Autorità europea antiriciclaggio (Anti-Money Laundering Authority – AMLA), organismo dotato di personalità giuridica autonoma e di autonomia amministrativa e finanziaria, formalmente istituito con Regolamento (UE) 2024/1620 del Parlamento europeo e del Consiglio del 31 maggio 2024 ma reso operativo dal 1° luglio 2025.

[54] Cfr., R. LENER, *Dalla moneta virtuale all'asset digitale: la nuova fisionomia della disciplina europea dei mercati*, in *Banca Impresa Società*, 2023, p. 401 ss.

Al nuovo ente il legislatore unionale ha attribuito una vasta gamma di poteri e competenze funzionali all'attuazione del mandato di prevenzione e contrasto dei fenomeni di riciclaggio e finanziamento illecito[55].

La sua introduzione, l'estensione del perimetro soggettivo degli obblighi di prevenzione e la progressiva inclusione delle cripto-attività nel novero dei fenomeni giuridicamente regolati costituiscono tasselli di un unico disegno volto a costruire una "Financial Integrity Union" capace di prevenire e contrastare efficacemente i flussi finanziari illeciti in un'economia sempre più digitalizzata e interconnessa e di porre le basi per un sistema europeo fondato sulla integrazione regolamentare, l'uniformità dei controlli e la cooperazione operativa.

La prospettiva che ne deriva è quella di un diritto della finanza pubblica e privata che non si limita più a disciplinare il mercato, ma ne diviene parte integrante, accompagnandone l'innovazione tecnologica con strumenti di controllo proporzionati, dinamici e intelligenti.

In tale orizzonte, l'ordinamento italiano si trova oggi a ricoprire un ruolo cruciale: quello di cerniera tra il livello europeo di regolazione e le prassi operative degli operatori domestici, chiamati a tradurre in comportamenti concreti gli obiettivi di trasparenza e responsabilità perseguiti dal legislatore unionale.

La costruzione di un diritto europeo della finanza digitale – fondato su legalità, accountability e innovazione sostenibile – rappresenta dunque la nuova frontiera di una politica legislativa che, pur muovendo da esigenze di prevenzione, ambisce a ridefinire i rapporti tra autorità, mercato e tecnologia, in una prospettiva di integrazione sistemica e di effettiva tutela dell'integrità economica dell'Unione.

L'uniformità dei presidi AML/CFT e dei livelli di compliance rappresenta, infatti, condizione imprescindibile per evitare fenomeni di arbitraggio regolamentare, nonché per impedire che capitali di provenienza illecita si infiltrino nei sistemi finanziari attraverso giurisdizioni caratterizzate da standard di controllo meno rigorosi.

[55] Per guidare il proprio percorso di lungo termine AMLA è già a lavoro per redigere i due primi documenti di programmazione (*Single Programming Documents*, SPDs) per i periodi 2026-2028 e 2027-2029: mediante tali documenti *"sovrapposti"*, che espliciteranno gli obiettivi annuali, l'Autorità renderà nota la propria visione strategica, individuerà priorità operative e indicatori di performance e, conseguentemente, pianificherà le proprie risorse; La versione definitiva di questi documenti programmatici sarà sottoposta ad un'ampia consultazione con il coinvolgimento degli Stati membri e delle istituzioni dell'UE. L'adozione del primo degli SPDs da parte del Comitato esecutivo AMLA è prevista entro il 30 novembre 2025.

Sotto il profilo sistematico, la configurazione giuridica dell'AMLA si discosta dal modello classico delle agenzie europee decentrate, tradizionalmente concepite come strutture di supporto tecnico alla Commissione, caratterizzate da un elevato grado di strumentalità e da una collocazione ausiliaria[56]. Pur condividendone la dimensione organizzativa autonoma, l'AMLA si avvicina maggiormente al modello delle autorità indipendenti europee, in ragione della sua competenza di supervisione sovranazionale e della funzione di coordinamento delle FIU nazionali[57].

Essa rappresenta, in tal senso, un organismo indipendente di nuova generazione, in cui la dimensione tecnica della vigilanza si coniuga con l'esigenza di un presidio unitario di legalità finanziaria a livello europeo.

L'AMLA si articola intorno a una duplice missione istituzionale: da un lato, esercitare la vigilanza diretta sui soggetti finanziari ad alto rischio di riciclaggio e di finanziamento del terrorismo; dall'altro, fungere da meccanismo di coordinamento e scambio informativo tra le Unità di Informazione Finanziaria degli Stati membri.

L'Autorità si configura quale modello del tutto inedito nel panorama delle agenzie europee. Pur essendo dotata di personalità giuridica autonoma, essa conserva un rapporto funzionale di stretta connessione con il Meccanismo di Vigilanza Unico (MVU) e con gli organismi europei deputati al contrasto penale – tra i quali Europol[58], Eurojust[59] e la

[56] In argomento, cfr., V. CERULLI IRELLI, *Dalle agenzie europee alle Autorità europee di vigilanza*, in (a cura di) M.P. Chiti- A. Natalini, *Lo spazio amministrativo europeo. Le pubbliche amministrazioni dopo il Trattato di Lisbona,* Il Mulino, Bologna, 2012, p. 155 ss.; R. D'AMBROSIO, *Le Autorità di vigilanza finanziaria dell'Unione,* in (a cura di) V. Santoro - E. Tonelli, *La crisi dei mercati finanziari: analisi e prospettive*, Giuffrè, Milano, 2013, 23 ss.; ID., *Gli effetti dell'istituzione dell'European Banking Authority e dell'European Systemic Risk Board sull'ordinamento nazionale del credito*, in (a cura di) P. Bilancia, *La regolazione dei mercati di settore tra autorità indipendenti nazionali e organismi europei*, Giuffrè, Milano, 2012, p. 71 ss.

[57] Per un inquadramento generale sul modello delle Autorità indipendenti, cfr. M. PASSARO, *Le amministrazioni indipendenti,* Torino, 1996; A.A.V.V., *Regolazione e garanzia del pluralismo. Le Autorità amministrative indipendenti*, Milano, 1997; G. AMATO, *Le autorità indipendenti,* in (a cura di) L. Violante, *Storia d'Italia*, Torino, 1998; F. MERUSI, *Democrazia e autorità indipendenti. Un romanzo quasi giallo,* bologna, 2000; R. TITOMANLIO, *Autonomia e indipendenza delle Authorities: profili organizzativi,* Milano, 2000; P. LAZZARA, *Autorità indipendenti e discrezionalità*, Padova, 2021; F. MERUSI – M. PASSARO, *Le autorità indipendenti. Un potere senza partito*, Bologna, 2003; M. CLARICH, *Autorità indipendenti: bilancio prospettive di un modello*, Bologna, 2005; M. SANINO, *L'approdo dell'esperienza delle autorità indipendenti a oltre vent'anni dalla loro istituzione*, Padova, 2015.

[58] Europol, denominata ufficialmente "Agenzia dell'Unione europea per la cooperazione nell'attività di contrasto" è un'agenzia dell'UE con sede all'Aia, la cui missione è sostenere gli Stati membri nella prevenzione e nella lotta contro tutte le forme gravi di criminalità organizzata e internazionale, criminalità informatica e terrorismo.

[59] L'Agenzia dell'Unione europea per la cooperazione giudiziaria penale, Eurojust, con sede all'Aia, aiuta le amministrazioni nazionali a collaborare per combattere il terrorismo e gravi forme di criminalità organizzata che interessano più di un paese dell'UE.

Procura europea (EPPO)[60] – delineando una struttura di cooperazione sistematica tra la dimensione finanziaria e quella investigativa dell'Unione[61].

Se, da un lato, l'AMLA riproduce alcuni tratti tipici delle agenzie europee decentrate – in particolare la connotazione tecnica delle funzioni esercitate e la finalità di rafforzare il coordinamento tra il livello sovranazionale e quello interno – dall'altro lato se ne discosta sensibilmente per la maggiore sofisticazione della propria architettura di governance, per l'elevato grado di indipendenza dai poteri politici e per la capacità di incidere in senso conformativo sul piano regolatorio, attraverso l'adozione di Regulatory Technical Standards (RTS) **e** Implementing Technical Standards (ITS)**.**

Tali competenze, qualificabili come "quasi-regolatorie", accentuano la natura ibrida dell'Autorità, la quale si colloca in una posizione intermedia tra l'organo tecnico e il regolatore sovranazionale, rappresentando un punto di raccordo tra l'amministrazione europea di vigilanza e le istanze di regolazione integrata del mercato finanziario dell'Unione[62].

---

[60] EPPO, acronimo di *European Public Prosecutor's Office*, è un'istituzione indipendente dell'Unione Europea che indaga e persegue reati che ledono gli interessi finanziari dell'UE. È operativa dal 1° giugno 2021 e ha sede a Lussemburgo.

[61] Si vedano, in tema, M. CLARICH, *Le sanzioni amministrative bancarie nel meccanismo di vigilanza unico*, in *Banca, Impr. Soc.*, 2014, p. 337; si vedano, piu di recente, anche le osservazioni di A. BARONE – G. DRAGO – C. NICOLOSI,„*L'erompere della vigilanza bancaria europea,* in *Persona e Amministrazione*, (8), 1, 2021, p. 665 ss., che rilevano come nel MVU possono individuarsi fino a cinque moduli di integrazione:

a) il modello della cd. «separazione dei poteri di vigilanza»;

b) il modello della c.d. «supremazia»;

c) il modello della c.d. «collaborazione»;

d) il modello della c.d. «cooperazione»;

e) il modello della c.d. «separazione dei poteri sanzionatori».

Cfr., poi L. DE LUCIA, *Amministrazione transnazionale e ordinamento europeo. Saggio sul pluralismo amministrativo,* Giappichelli,Torino, 2009, p. 60, il quale ricorda che «le unioni di settore sono collocate in una dimensione diversa da quella nazionale e da quella comunitaria: si trovano cioè nella dimensione transnazionale comune a tutti i soggetti che vi prendono parte».

[62] Si vedano, su questi temi, si vedano, G. ROTONDO, *Il modello di controllo su banche e intermediari dopo l'integrazione con il sistema europeo di vigilanza finanziaria*, in (a cura di) M. Rispoli Farina -G. Rotondo, *Banche e imprese nella crisi: nuova regolamentazione dei soggetti e dei mercati, Atti del Seminario di studi, Università di Napoli "Federico II", 16 giugno 2014*, in *Innovazione e diritto*, 2014, p. 35 ss.; ID., *Note sulla neutralità funzionale del modello italiano di controllo sui mercati finanziari dopo l'integrazione con il Sistema Europeo di Vigilanza Finanziari*a, in *ibidem*, 2014, p. 97 ss.; ID., *Il recepimento del Sistema Europeo di Vigilanza Finanziaria nell'ordinamento italiano: l'impatto sull'architettura di vigilanza bancaria,* in *Diritto della banca e del mercato finanziario,* 2015, p. 41 ss.

ISSN 2282-2461 I BATTELLI DEL RENO [ON LINE]

Il vero elemento qualificante del nuovo organismo è, tuttavia, la garanzia di indipendenza – tanto dalle istituzioni politiche quanto dai gruppi di pressione privati – ripetutamente affermata nella Relazione illustrativa e nei Considerando del Regolamento istitutivo.

L'indipendenza è infatti esplicitamente richiesta con riferimento a tutti i principali organi interni: il Gruppo investigativo, responsabile degli approfondimenti preliminari ai procedimenti sanzionatori; i membri del Consiglio generale e del Comitato esecutivo; il Direttore esecutivo e la Commissione amministrativa di riesame.

L'assetto delineato mira ad assicurare la neutralità e l'imparzialità dell'azione di vigilanza, sottraendola a possibili condizionamenti politici o pressioni esterne e ancorandola a parametri esclusivamente tecnici, fondati sui principi di proporzionalità e adeguatezza.

Le finalità istituzionali riconosciute all'AMLA si articolano nella tutela dell'interesse pubblico, nella salvaguardia della stabilità del sistema finanziario e nel corretto funzionamento del mercato interno. Se le ultime due appaiono ormai consolidate nel diritto dell'Unione — essendo da tempo acquisita la consapevolezza che il fenomeno del riciclaggio rappresenta una minaccia per la concorrenza, la trasparenza e l'integrità complessiva dell'ordine economico-finanziario — merita invece particolare attenzione la menzione dell'"interesse pubblico", introdotta dal legislatore privo di una definizione testuale puntuale.

A tale riguardo, possono individuarsi due possibili chiavi interpretative. Una prima, di carattere restrittivo, tende a ricondurre l'interesse pubblico alla mera salvaguardia della stabilità e dell'efficienza del mercato interno. Una seconda, di più ampio respiro e maggiormente persuasiva, riconosce all'espressione un valore autonomo, idoneo a ricomprendere istanze di rango meta-economico e principi fondanti dell'ordinamento unionale.

L'impiego, nel testo normativo, della congiunzione "e" in luogo della preposizione articolata "alla" depone in favore di questa seconda impostazione, lasciando intendere che l'interesse pubblico costituisca un obiettivo distinto e più esteso, che trascende la dimensione economica per includere finalità di ordine democratico, di tutela dello Stato di diritto, di imparzialità dell'azione amministrativa e di rafforzamento della fiducia dei cittadini nelle istituzioni europee.

Nel perseguimento di tali obiettivi, l'AMLA sarà chiamata ad operare in una pluralità di settori interconnessi: dalla prevenzione dell'utilizzo del sistema finanziario a fini di riciclaggio o di finanziamento del terrorismo, alla valutazione dei rischi e alla vigilanza sull'efficacia dei presidi interni; dalla promozione della convergenza delle prassi di supervisione, al coordinamento e allo scambio informativo tra le Financial Intelligence Units (FIUs) e le autorità competenti; fino all'armonizzazione dei criteri e delle metodologie di analisi dei flussi illeciti[63].

L'Autorità si configura, pertanto, quale nodo strategico di raccordo funzionale tra la dimensione di controllo degli obblighi di compliance e quella di analisi finanziaria delle segnalazioni sospette, realizzando un continuum operativo tra la fase preventiva e quella repressiva dell'azione di contrasto.

L'effettiva operatività dell'AMLA richiederà, tuttavia, un processo di progressiva implementazione, nel quale risulterà decisiva la cooperazione delle autorità nazionali e delle FIU, chiamate a elaborare procedure, standard e metodologie di vigilanza coerenti con il nuovo assetto regolamentare europeo. In tale prospettiva, il sistema italiano sarà tenuto ad adottare un approccio proattivo e sostanziale, evitando soluzioni meramente adattive e

[63] È ormai pacificamente riconosciuto che le *Financial Intelligence Units* (FIUs) rappresentino gli organismi maggiormente qualificanti nell'architettura del sistema antiriciclaggio europeo. Ne discende che il potenziamento della loro capacità di cooperazione costituisca una priorità imprescindibile, che non avrebbe potuto mancare all'interno di un "pacchetto" normativo destinato a ridisegnare in modo organico l'intera struttura istituzionale dell'Unione in materia di prevenzione e contrasto del riciclaggio e del finanziamento del terrorismo. In tale prospettiva, il legislatore europeo ha inteso dar vita a un sistema multilivello nel quale l'AMLA occupa una posizione centrale, mentre le FIUs degli Stati membri si collocano su un piano funzionalmente decentrato, ma strettamente interconnesso. L'obiettivo è quello di assicurare un più efficiente flusso informativo e una maggiore uniformità delle prassi operative, così da garantire un livello di cooperazione effettiva e stabile tra i diversi centri di vigilanza e di analisi finanziaria. All'interno di tale assetto, l'Autorità europea sarà investita, tra gli altri, dei compiti di sostenere e coordinare l'attività delle FIUs, di contribuire all'individuazione dei casi meritevoli di analisi congiunte, di mettere a disposizione delle stesse, strumenti informatici e applicazioni basate su tecnologie di intelligenza artificiale, nonché di fornire loro assistenza tecnica e informativa specializzata. Il ruolo dell'AMLA potrà dunque sintetizzarsi in quello di autentico *coordinator* del sistema, attorno al quale si articolerà il funzionamento del meccanismo di cooperazione su un duplice binario: da un lato, quello del coordinamento, volto ad armonizzare l'azione delle diverse FIUs; dall'altro, quello del sostegno, destinato a rafforzarne la capacità operativa e l'efficacia nell'attività di prevenzione e contrasto dei fenomeni illeciti. Cfr. Art. 33, Proposta di Regolamento del Parlamento europeo e del Consiglio che istituisce l'Autorità per la lotta al riciclaggio e al finanziamento del terrorismo e che modifica i regolamenti (UE) n. 1093/20110, (UE) n. 1094/2010, (UE) n. 1095/2010, COM (2021)421 final, del 20 luglio 2021.

valorizzando il patrimonio esperienziale maturato nella prevenzione domestica dei fenomeni di riciclaggio e finanziamento del terrorismo[64].

La scelta di mantenere in capo alle autorità nazionali competenti l'esercizio dei compiti e delle funzioni finalizzate alla prevenzione dell'utilizzo del sistema finanziario per scopi di riciclaggio appare coerente con l'impianto tradizionale del cosiddetto "sistema di governo dell'antiriciclaggio"[65].

Nonostante la recente tendenza verso una progressiva centralizzazione a livello sovranazionale, culminata nella costituzione dell'Autorità europea per la lotta al riciclaggio e al finanziamento del terrorismo la struttura istituzionale del sistema antiriciclaggio è stata sin dalle origini improntata a un modello composito e multilivello, in cui la dimensione regolatoria è rimasta prevalentemente affidata ad organismi internazionali ed europei, mentre quella amministrativa e di vigilanza è rimasta radicata negli ordinamenti nazionali.

A livello globale, il ruolo di indirizzo e di standardizzazione è stato tradizionalmente svolto dal FATF-GAFI, cui si devono i principali set di raccomandazioni in materia di contrasto al riciclaggio e al finanziamento del terrorismo. Sul versante europeo, funzioni analoghe sono state progressivamente assunte dalla Commissione, dal Consiglio e dal

[64] L'AMLAR prevede, infatti, all'articolo 5, paragrafo 5, lett. h), che – al fine di consentire ad AMLA di fornire un'assistenza ottimale alle FIU e aumentare l'efficacia del meccanismo di sostegno e coordinamento delle stesse – vengano individuate e promosse *best practices* attraverso verifiche *inter pares* (ex articolo 48 AMLAR, da non confondere con le verifiche *inter pares* ex articolo 35 AMLAR riservato ai supervisori del settore non finanziario) che in tale contesto, sono state considerate lo strumento migliore per permettere una valutazione oggettiva di tali pratiche. Pertanto, AMLA è stata incaricata di organizzare tali verifiche sulla base di metodi e norme procedurali che essa stessa dovrà elaborare (AMLAR, articolo 48, paragrafo 1). Queste verifiche riguarderanno tutti gli aspetti pertinenti dei compiti delle FIU stabiliti al capo III AMLD e, quindi, l'adeguatezza delle risorse delle FIU, le misure attuate per garantire l'indipendenza e l'autonomia delle FIU sul piano operativo, le misure predisposte per tutelare la sicurezza e la riservatezza delle informazioni trattate dalle FIU, le funzioni relative al ricevimento delle segnalazioni di operazioni sospette, le funzioni relative alle analisi operative e strategiche delle FIU e alla loro diffusione, nonché gli accordi e le pratiche di cooperazione nazionale e transfrontaliera delle FIU. A seguito delle verifiche *inter pares*, AMLA potrebbe emanare orientamenti e raccomandazioni volti a promuovere *best practices* individuate e ad affrontare eventuali carenze.

[65] Per una ricognizione dell'evoluzione (globale, europea e nazionale) del sistema di governo dell'antiriciclaggio e la ricostruzione delle peculiari caratteristiche di tale sistema, si veda, D. ANDRACCHIO, *Profili evolutivi della disciplina antiriciclaggio. Integrazione europea della supervisione e sussidiarietà orizzontale del mercato,* Giuffrè, Milano, 2024. Tra gli altri, quanto alla dimensione nazionale, si vedano, E. CASSESE, *Il controllo pubblico del riciclaggio finanziario,* Giuffrè, Milano,1999; A. URBANI, *Disciplina antiriciclaggio e ordinamento del credito,* Cedam, Padova, 2005; ID., *Gli strumenti di contrasto dell'economia illegale,* in (a cura di) F. Capriglione, *Manuale di diritto bancario e finanziario*, Cedam, Padova, 2019, p. 545 ss.; P. FRATANGELO, *Prevention and Countering of Money Laundering and Terrorism Financing*, in (a cura di) D. Siclari, *Italian Banking and Financial Law. Supervisory Authoritie and Supervision*, Palgrave Macmillan, Londra, 2015, p. 105 ss.

Parlamento dell'Unione, nonché, in tempi più recenti, dall'Autorità Bancaria Europea (EBA) [66].

Le attività di vigilanza operativa, di controllo e di enforcement sull'osservanza degli obblighi antiriciclaggio sono invece rimaste attribuite alle autorità nazionali competenti, secondo un modello di distribuzione delle competenze fondato sul principio di prossimità e sul riconoscimento del ruolo centrale delle amministrazioni domestiche nella gestione del rischio.

L'intero sistema di prevenzione poggia, com'è noto, su una stretta cooperazione tra il settore pubblico e i cosiddetti "soggetti obbligati", categoria progressivamente ampliata dal legislatore al fine di ricomprendere un numero crescente di operatori economici potenzialmente esposti al rischio di essere, anche inconsapevolmente, utilizzati per finalità di riciclaggio o di reimpiego di proventi illeciti.

La disciplina nazionale di riferimento, contenuta nel D.lgs. 21 novembre 2007, n. 231, individua tale cooperazione pubblico-privato come il perno dell'intero apparato preventivo, articolandola in due principali categorie di obblighi: la collaborazione passiva e la collaborazione attiva.

La collaborazione passiva si concretizza, in primo luogo, negli obblighi di adeguata verifica della clientela, i quali impongono di accertare l'identità del cliente o del titolare effettivo, nonché lo scopo e la natura del rapporto instaurato, mediante l'acquisizione di documenti, dati e informazioni provenienti da fonti affidabili e indipendenti[67].

A tale attività di identificazione si affianca, in via complementare, l'obbligo di conservazione dei dati e delle informazioni raccolte, volto a garantire la tracciabilità delle operazioni e a consentire eventuali controlli successivi, anche a distanza di tempo, sulle movimentazioni sospette.

Nella medesima categoria rientrano, altresì, gli obblighi di predisposizione di presidi organizzativi e procedimentali adeguati, destinati a calibrare, secondo un approccio basato sul rischio (*risk-based approach*), l'intensità e la qualità delle misure di prevenzione in funzione delle caratteristiche dimensionali e operative del soggetto obbligato, assicurando

[66] Per un inquadramento dei poteri dell'EBA, cfr. D. VESE, *A Game of Thrones: ruolo e poteri dell'autorità bancaria europea alla luce degli orientamenti della Corte di Giustizia*, in *Riv. dir. banc.,* 2023, 1, p. 69.

[67] L'art. 28, par. 1, dell'AMLR prevede che l'AMLA armonizzi gli obblighi di adeguata verifica della clientela, specificando quali informazioni i soggetti obbligati devono raccogliere per svolgere l'adeguata verifica della clientela.

una più efficace individuazione di operazioni potenzialmente finalizzate all'immissione di capitali illeciti nel circuito economico legale.

La collaborazione attiva, invece, si esplica principalmente attraverso gli obblighi di segnalazione di operazioni sospette (*Suspicious Transaction Reports – STR)*, che impongono agli operatori di trasmettere all'Unità di Informazione Finanziaria (UIF) apposite comunicazioni redatte secondo modelli standardizzati, ogniqualvolta sussistano elementi oggettivi o ragionevoli motivi per ritenere che siano in corso, o siano state compiute o tentate, operazioni di riciclaggio o di finanziamento del terrorismo. Tale obbligo rappresenta il fulcro del meccanismo di collaborazione attiva, costituendo il principale strumento di alimentazione del circuito informativo tra operatori privati e autorità pubbliche e, dunque, una componente essenziale del sistema di prevenzione in senso sostanziale.

In conformità ai principi di effettività e proporzionalità che governano l'azione dell'Unione europea, l'auspicio è che la nuova disciplina, fondata sull'adozione dello strumento del regolamento – e, dunque, direttamente applicabile negli ordinamenti nazionali – possa assicurare un livello elevato di presidio e di omogeneità nell'attuazione dei controlli, evitando il rischio di compromessi di natura politica o meramente burocratica che ne indebolirebbero la portata sistemica.

Solo un impianto regolatorio realmente ispirato alle finalità sostanziali della vigilanza, capace di coniugare la semplificazione procedurale con il rigore operativo e la responsabilità istituzionale, potrà rafforzare la credibilità dell'Unione quale spazio integrato di legalità e trasparenza finanziaria.

Un simile approccio consentirebbe di consolidare il ruolo dell'ordinamento europeo non soltanto nel contrasto al riciclaggio, ma anche nella prevenzione dell'intera gamma dei fenomeni illeciti connessi all'economia globale, in coerenza con l'obiettivo – di matrice ormai sistemica – di garantire un mercato unico fondato sulla fiducia, sulla tracciabilità dei flussi e sull'integrità dei capitali[68].

[68] Cfr. M. MAUGERI, *La regolazione europea delle cripto-attività tra innovazione e tutela del mercato*, in *Banca, Borsa e Titoli di Credito*, 2024, p. 145 ss.

5. L'architettura istituzionale dell'AMLA e il nuovo modello multilivello di vigilanza europea

L'assetto del sistema europeo di supervisione in materia di prevenzione del riciclaggio e del finanziamento del terrorismo si fonda su una struttura tripartita**,** all'interno della quale l'AMLA esercita poteri e funzioni differenziati in base al grado di esposizione al rischio e alla natura transfrontaliera dei soggetti vigilati[69].

Tale modello, ispirato a una logica di integrazione multilivello, segna una svolta nel processo di europeizzazione delle politiche di *financial integrity,* delineando un equilibrio innovativo tra competenze nazionali e autorità sovranazionale.

Il primo pilastro del sistema è rappresentato dalla supervisione diretta dei soggetti obbligati selezionati**,** ossia degli operatori individuati sulla base di criteri oggettivi di rilevanza sistemica e di rischio intrinseco.

In questo ambito, l'AMLA è chiamata a effettuare una valutazione periodica e comparativa su due macro-categorie di operatori: da un lato, gli enti creditizi operanti in almeno sette Stati membri; dall'altro, gli intermediari finanziari non bancari – quali i prestatori di servizi di cambio, gli organismi di investimento collettivo, gli istituti di moneta elettronica e le imprese di assicurazione – che esercitino attività in almeno dieci Stati membri.

L'analisi di tali operatori si basa su una metodologia uniforme, definita mediante Regulatory Technical Standards (RTS) elaborati dall'AMLA e successivamente adottati dalla Commissione europea. Essa mira a individuare, in chiave comparata, il rischio intrinseco di riciclaggio e finanziamento del terrorismo al quale ciascun soggetto risulta esposto, tenendo conto di variabili oggettive quali la composizione della clientela, la

[69] Cfr., P. COSTANZO, *La disciplina antiriciclaggio,* in (a cura di) S. Amorosino – C. Rabitti Bedogni, *Manuale di diritto dei mercati finanziari*, Giuffrè, Milano, 2004, ,p. 478 ss.; M. PELLEGRINI, *Anti-Money Laundering Legislation in thelight of the Proposal of the Third EC Directive,* in *European Business Law Review*, 2005, p.1181 ss.; A. URBANI – A. MINTO, *Recent trends in designing the EU anti-money laundering regulatory landscape: the fourth AML directive between lights, shadows and future perspectives, in Review of Law & Economics*, 2016, pp. 151 ss.; ID., *La Quarta Direttiva europea in materia di antiriciclaggio, tra luci, ombre e prospettive,* in *Dir. banc. fin.,* 2017, p.119 ss.; ID., The New Anti-Money Laundering Law. First Perspectives on the 4th European Union Directive, in (a cura di) D. Siclari, Palgrave Macmillan, Londra, 2016; ID. *L'antiriciclaggio dopo la V Direttiva UE,* in *Dirigenza bancaria,* 2019, pp. 13 ss.

tipologia dei servizi e dei prodotti offerti, i canali distributivi utilizzati e le aree geografiche di operatività.

Ne discende una duplice logica di selezione: da un lato, quella della transfrontalierità**,** che riflette la proiezione sovranazionale dell'attività; dall'altro, quella del rischio sostanziale**,** inteso come grado di vulnerabilità rispetto a fenomeni di riciclaggio e finanziamento illecito.

All'esito della valutazione, gli operatori vengono classificati secondo una scala di quattro livelli di rischio – basso, medio, sostanziale o elevato – e quelli appartenenti alle categorie a maggiore esposizione vengono iscritti in un registro europeo dei soggetti sottoposti a vigilanza diretta[70]**.**

L'assoggettamento alla supervisione diretta dell'AMLA comporta l'instaurazione di un rapporto giuridico immediato tra l'Autorità europea e il soggetto vigilato, con parziale sottrazione di quest'ultimo alla competenza esclusiva delle autorità nazionali. Si realizza così un modello di vigilanza accentrata e integrata, in cui l'AMLA esercita poteri di controllo, ispezione e sanzione direttamente nei confronti degli operatori più esposti a rischio sistemico[71].

L'architettura delineata dal legislatore europeo evidenzia dunque una progressiva transizione da un modello di mera cooperazione interstatale a un sistema pienamente integrato di vigilanza, fondato su una rete multilivello di autorità interconnesse. In tale contesto, l'AMLA non si limita ad assumere un ruolo di impulso e di raccordo tra le FIUs nazionali, ma diviene il perno istituzionale di un meccanismo di supervisione unitario, nel quale la dimensione informativa e quella ispettiva si fondono in un continuum operativo[72].

---

[70] AMLAR, *Considerando 21*: *"L'Autorità dovrebbe assicurare, se del caso, l'allineamento tra la metodologia per la valutazione del profilo di rischio ai fini del processo di selezione a norma del presente regolamento e la metodologia per armonizzare la valutazione dei profili di rischio intrinseco e residuo dei soggetti obbligati a livello nazionale da mettere a punto nelle norme tecniche di regolamentazione adottate a norma dell'articolo 40, paragrafo 2, della direttiva (UE) 2024/1640".*

[71] Sui poteri di controllo, per un inquadramento generale, ci si limita a M. S. GIANNINI, *Controllo: nozione e problemi, in Riv. trim. dir. pubbl.,* 1974, p. 1263 ss.; F. GARRI, *I controlli Nell'ordinamento italiano*, Milano, 1998; G. BERTI – N. MARZONA, *Controlli amministrativi*, in *Enc. dir.,* 1999, p. 457 ss.; E. BANI – M. GIUSTI (a cura di), *Le vigilanze economiche. Le regole e gli effetti*, Cedam, Padova, 2004, p. 733 ss.; M. DE BENEDETTO, *Controlli* (dir. amm.), in *treccani.it*, 2017.

[72] Sul tema, M. PASSALACQUA, *Vigilare ispezionando*, in E. BANI, M. GIUSTI (a cura di), Vigilanze economiche. Le regole e gli effetti, cit., p. 219, che ha avvertito che il termine vigilanza, quantomeno prima facie, consta di due significati: da un lato l'attenta sorveglianza a scopo di controllo, dall'altro la cura sollecita ovvero l'accorta attenzione.

ISSN 2282-2461 I BATTELLI DEL RENO [ON LINE]

L'attuazione concreta delle funzioni di supervisione trova espressione operativa nella costituzione dei *Joint Supervisory Teams* (JSTs), ossia gruppi di vigilanza congiunti che assumono la natura di veri e propri organi misti di cooperazione amministrativa.

Ciascun gruppo è deputato al controllo di uno specifico soggetto obbligato, selezionato secondo criteri di rischio e rilevanza sistemica, e presenta una composizione interistituzionale tale da riflettere la duplice dimensione – europea e nazionale – che caratterizza l'assetto multilivello della vigilanza.

I JSTs sono composti da funzionari dell'AMLA e da personale distaccato dalle autorità nazionali competenti, sotto il coordinamento di un responsabile designato dall'Autorità europea, al quale è affidato il compito di garantire l'unitarietà metodologica e la coerenza delle attività ispettive.

Tale struttura mista non costituisce una mera soluzione di tipo organizzativo, bensì uno strumento giuridico di integrazione funzionale tra il livello sovranazionale e quello domestico, coerente con il principio di leale cooperazione sancito dall'art. 4, par. 3, TUE. Essa incarna, infatti, un modello amministrativo capace di coniugare l'autonomia decisionale delle autorità nazionali con il potere di indirizzo e di coordinamento dell'AMLA, realizzando una forma avanzata di governance composita e cooperativa.

L'attività istruttoria svolta dai gruppi congiunti rappresenta la base cognitiva su cui si fondano le determinazioni degli organi deliberativi dell'Autorità — in particolare, il Consiglio generale e il Comitato esecutivo — chiamati ad adottare i provvedimenti conclusivi di supervisione e le eventuali misure correttive o sanzionatorie.

In tale prospettiva, il sistema europeo di vigilanza AML/CFT si configura come un modello unitario e coordinato di procedimento amministrativo multilivello, nel quale la dimensione tecnico-analitica dell'attività istruttoria si salda con quella giuridico-decisionale, dando luogo a una struttura procedimentale che coniuga efficienza operativa, certezza del diritto e uniformità applicativa.

Nell'ambito della vigilanza diretta, l'Autorità europea antiriciclaggio è investita di un ampio ventaglio di poteri informativi e ispettivi, funzionali a garantire la conformità dei soggetti vigilati alla disciplina europea e nazionale di riferimento.

Tali prerogative comprendono, tra le altre, la facoltà di richiedere la trasmissione di informazioni e documenti ritenuti rilevanti ai fini dell'attività di controllo, l'accesso alle scritture contabili e ai registri aziendali, nonché la convocazione degli operatori per audizioni, chiarimenti o presentazione di osservazioni in ordine a specifiche condotte o operazioni.

L'AMLA è, inoltre, legittimata a disporre ispezioni in loco, anche senza preavviso, qualora emergano elementi indiziari di violazione della normativa o situazioni di rischio sistemico tali da compromettere la stabilità o l'integrità del mercato[73].

Questi poteri, fondati sul diritto derivato dell'Unione, rivestono una funzione di rilievo sistemico, poiché perseguono l'obiettivo di assicurare un'applicazione uniforme del diritto antiriciclaggio, rafforzando la certezza giuridica e la coerenza del quadro regolatorio all'interno del mercato finanziario unico.

Essi concretizzano, in chiave istituzionale, il principio di armonizzazione effettiva delle prassi di vigilanza e rappresentano il perno di un sistema di controllo multilivello coerente con le esigenze di integrità, trasparenza e stabilità dei mercati finanziari.

All'esito dell'attività ispettiva o dell'analisi documentale, qualora emergano irregolarità o violazioni, l'Autorità è abilitata a esercitare i propri poteri conformativi e sanzionatori. Le misure conformative – o di supervisione – sono dirette al ripristino della conformità normativa e possono consistere nell'imposizione di ordini di rafforzamento dei presidi AML/CFT, nella richiesta di adozione di piani di risanamento, nell'introduzione di modifiche alla struttura di governance ovvero nella limitazione o sospensione dell'esercizio di determinate attività ritenute sensibili.

Nei casi di maggiore gravità, in presenza di comportamenti dolosi o gravemente colposi, l'AMLA può proporre la revoca dell'autorizzazione o attivare un autonomo procedimento sanzionatorio, volto all'irrogazione di sanzioni pecuniarie proporzionate, effettive e dissuasive, conformemente ai principi sanciti dal diritto dell'Unione[74].

---

[73] Cfr. M. PASSALACQUA, *Ispezioni economiche. Tipologie, procedimenti e approcci sistematici*, Padova, 2005

[74] Sulla potestà sanzionatoria della pubblica amministrazione, tra i tantissimi, G. PAGLIARI, *Profili teorici della sanzione amministrativa,* Cedam, Padova, 1988; A. TRAVI, *Sanzioni amministrative,* in *Enc. dir.,* 1989, pp. 345 ss.; E. BANI, *Il potere sanzionatorio delle Autorità indipendenti. Spunti per un'analisi unitaria,* Giappichelli, Torino, 2000; F. GOISIS, *Discrezionalità ed autoritatività nelle sanzioni amministrative pecuniarie, tra tradizionali preoccupazioni di sistema e nuove prospettive di diritto europeo,* in *Riv. it. dir. pubbl. com.,* 2013, p. 79 ss.; A. CAGNAZZO – S. TOSCHEI – F.F. TUCCARI (a cura di), *La sanzione amministrativa,* Giuffrè, Milano, 2016; S. CIMINI, *Il potere sanzionatorio delle amministrazioni pubbliche. Uno studio critico*, Editoriale scientifica, Napoli, 2017; S.L. VITALE, *Le sanzioni amministrative tra diritto nazionale e diritto europeo*, Giappichelli, Torino, 2018.

L'intero procedimento si svolge nel rispetto del giusto procedimento amministrativo europeo, garantendo ai soggetti vigilati il diritto di difesa, la partecipazione mediante memorie e audizioni, nonché l'accesso agli atti istruttori.

La previsione di sanzioni aggiuntive, commisurate al ritardo nell'esecuzione dei provvedimenti e calcolate per giorno di inadempimento, risponde al principio di effettività dell'enforcement, rafforzando la forza vincolante delle decisioni dell'Autorità.

Nel suo complesso, l'architettura istituzionale dell'AMLA si fonda su una logica di gradualità e di proporzionalità, all'interno della quale la funzione conformativa precede quella sanzionatoria e la dimensione preventiva assume preminenza rispetto a quella repressiva. Tale impostazione risponde all'esigenza di orientare l'attività di vigilanza verso la correzione tempestiva delle disfunzioni e la promozione della compliance, in un'ottica di prevenzione sistemica del rischio.

Il sistema così configurato persegue un equilibrio dinamico tra l'efficacia dell'azione di controllo e la salvaguardia dei diritti fondamentali dei soggetti vigilati, delineando un modello europeo di *enforcement* collaborativo, improntato alla responsabilità condivisa e alla cooperazione amministrativa tra livelli istituzionali.

Attraverso la combinazione di una supervisione diretta nei confronti degli operatori caratterizzati da elevato profilo di rischio e di una vigilanza indiretta esercitata mediante i *Joint Supervisory Teams* (JSTs), l'Autorità europea realizza un sistema ibrido e multilivello, nel quale la dimensione sovranazionale e quella domestica concorrono alla realizzazione di un obiettivo comune: la tutela dell'integrità, della stabilità e della trasparenza del mercato finanziario dell'Unione.

Il disegno complessivo si inscrive, pertanto, nella prospettiva di una integrazione amministrativa di tipo funzionale, in cui l'AMLA assurge a perno di un rinnovato equilibrio tra centralizzazione e sussidiarietà[75], assicurando uniformità interpretativa, proporzionalità dell'intervento e coerenza con i principi cardine dell'amministrazione europea — *good governance*, trasparenza e *accountability*.

Il secondo pilastro della nuova architettura europea di vigilanza è rappresentato dalla supervisione indiretta sui soggetti obbligati non selezionati operanti nel settore finanziario. Tale categoria comprende, in via residuale, tutti gli enti creditizi e gli intermediari finanziari

[75] Per alcune interessanti considerazioni, G.M. FLICK, *Sussidiarietà e principio di prossimità, quali modelli per uscire dalla crisi?*, in Conversazioni AREL, 2010, p. 3 ss.

non bancari che non rientrano tra i soggetti sottoposti al controllo diretto dell'Autorità europea, rimanendo quindi affidati alla competenza delle autorità nazionali di vigilanza.

Si parla, in questo caso, di supervisione indiretta poiché l'AMLA non eserciterebbe poteri ispettivi o sanzionatori immediati nei confronti di tali operatori, ma funzioni di indirizzo, coordinamento e armonizzazione dell'attività di vigilanza condotta dalle autorità nazionali competenti. Si configura, pertanto, una forma di "vigilanza sulla vigilanza", in cui l'Autorità europea assume un ruolo di garanzia sistemica e di impulso operativo, finalizzato ad assicurare un livello omogeneo di effettività dei controlli nel territorio dell'Unione.

Nell'ambito di tali prerogative, l'AMLA risulterebbe legittimata a richiedere alle autorità nazionali di supervisione la trasmissione di ogni documento, informazione o dato utile all'esercizio dei propri compiti, nonché ad emanare orientamenti, raccomandazioni e istruzioni vincolanti circa le misure da adottare per la corretta applicazione della normativa antiriciclaggio. Tali poteri, di natura essenzialmente strumentale e conformativa, sono funzionali a consentire alle autorità nazionali di assolvere adeguatamente le attribuzioni loro conferite all'interno del secondo pilastro, che comprendono – tra le altre – la tenuta dell'elenco dei supervisori nazionali, la valutazione periodica delle risorse e dei poteri a essi attribuiti, la verifica delle strategie e delle capacità operative, la partecipazione ai collegi di supervisione, la promozione della convergenza delle prassi di vigilanza e la facilitazione dello scambio di personale e di informazioni tra le diverse giurisdizioni.

In particolare, l'AMLA sarà tenuta a svolgere valutazioni periodiche sull'adeguatezza delle risorse, degli strumenti e dell'efficacia delle autorità nazionali di vigilanza, al fine di garantire un elevato livello di efficienza e la convergenza sostanziale delle metodologie di controllo[76]. Tali valutazioni verrebbero effettuate da un Pool misto, composto da personale dell'AMLA e – su base volontaria – da membri delle autorità nazionali diverse da quella oggetto di esame. La composizione mista del gruppo ispettivo costituisce un elemento di particolare interesse, poiché consente una circolazione virtuosa di competenze e sensibilità tecniche: da un lato, l'AMLA può avvalersi della conoscenza diretta e della prospettiva operativa degli insider nazionali; dall'altro, le autorità degli Stati membri hanno la possibilità di confrontarsi con l'approccio valutativo e metodologico dell'Autorità

[76] "*AMLA will… support NCAs through training regarding colleges of supervisors, work out plans to participate in colleges in the financial sector…*", AMLA WORK PROGRAMME 2025, *Management Summary, Activities for the second half of 2025, Activities for the second half of 2025*, p.11. Si fa riferimento, ovviamente. ai *"collegi di supervisione AML/CFT"* definiti al numero 8 dell'articolo 2 AMLD come strutture permanenti *"…per la cooperazione e lo scambio di informazioni ai fini della supervisione di un gruppo o di un soggetto che opera in uno Stato membro ospitante o paese terzo"*.

europea, rafforzando così il dialogo interistituzionale e l'allineamento culturale della vigilanza.

All'esito di ciascuna valutazione, il Pool misto redigerà una relazione illustrativa nella quale saranno indicate le criticità riscontrate e le misure correttive ritenute necessarie. Sulla base di tale relazione, il Comitato esecutivo dell'AMLA adotterà orientamenti o raccomandazioni contenenti l'indicazione puntuale delle follow-up measures che le autorità nazionali dovranno porre in essere con ogni sforzo di conformazione.

Sempre nel contesto del secondo pilastro, l'AMLA sarà investita del compito di coordinare i lavori dei collegi di supervisione antiriciclaggio, organi istituiti dalle autorità nazionali al fine di esercitare congiuntamente i poteri di vigilanza nei confronti degli enti creditizi o finanziari stabiliti in almeno due Stati membri, nonché nei confronti degli operatori di Paesi terzi aventi sedi o filiali in almeno tre Stati membri dell'Unione. Tali collegi, lungi dal costituire meri organismi organizzativi, si configurano come moduli procedimentali di cooperazione multilivello, destinati a promuovere una collaborazione mista – in parte orizzontale, tra autorità nazionali, e in parte verticale, tra queste e l'Autorità europea – in un'ottica di integrazione effettiva e di progressiva armonizzazione del sistema di supervisione AML/CFT.

Non possono, pertanto, essere considerate unità dotate di autonoma soggettività giuridico-amministrativa, poiché le misure adottate all'esito delle loro riunioni continuano a rientrare nella titolarità delle singole autorità nazionali partecipanti. La funzione essenziale dei collegi di supervisione è, dunque, quella di favorire un flusso costante di informazioni, di esperienze e di prassi operative, volto a rendere effettiva una supervisione integrata sugli intermediari che operano nel territorio di più Stati membri.

Quanto al ruolo dell'AMLA in relazione a tali collegi, essa, oltre a godere del diritto di prendervi parte, è investita di un complesso di poteri ulteriori. In particolare, l'Autorità europea può intervenire nei casi di inerzia o inattività delle autorità nazionali, istituendo autonomamente collegi di supervisione antiriciclaggio, convocandone e organizzandone le riunioni, fornendo assistenza logistica e tecnica nello svolgimento delle ispezioni congiunte, nonché curando la raccolta e la condivisione delle informazioni rilevanti ai fini dell'attività di vigilanza.

Di peculiare interesse risultano, inoltre, i poteri di cui l'AMLA disporrebbe per sollecitare l'intervento delle autorità nazionali in presenza di gravi indizi circa violazioni commesse da soggetti obbligati non selezionati. Si tratta delle cosiddette *"richieste di agire"*, che si inseriscono in un articolato procedimento scandito in tre fasi successive.

La prima fase, di competenza delle autorità nazionali, si attiva quando queste ultime sono tenute a notificare all'AMLA le situazioni nelle quali l'esposizione al rischio di riciclaggio di un soggetto obbligato non selezionato raggiunga un livello tale da poter compromettere la reputazione dello Stato membro interessato o dell'Unione nel suo complesso.

Tale notifica apre la seconda fase**,** nella quale l'Autorità europea invita formalmente l'autorità nazionale competente ad agire, specificando le modalità dell'intervento. L'AMLA può, a tal fine, richiedere che siano:

a) avviate indagini volte ad accertare la sussistenza e la gravità delle violazioni;

b) adottate sanzioni amministrative nei confronti del soggetto responsabile;

c) emanati provvedimenti di natura conformativa, imponendo all'operatore l'adozione delle misure necessarie a ripristinare la conformità alla normativa antiriciclaggio.

La terza fase del procedimento si conclude qualora l'autorità nazionale si conformi alle istruzioni ricevute dall'AMLA; in caso contrario, si apre una nuova sequenza procedimentale, finalizzata alla sostituzione dell'Autorità europea all'autorità nazionale inadempiente.

In questa ipotesi, se entro dieci giorni dalla richiesta l'autorità nazionale non abbia adottato le misure indicate, l'AMLA può presentare alla Commissione una domanda motivata di autorizzazione all'avocazione dei poteri e delle funzioni della stessa autorità.

A seguito dell'esame della richiesta, la Commissione potrà decidere di respingere l'istanza, mantenendo le competenze in capo all'autorità nazionale, ovvero di accoglierla, fissando un termine oltre il quale l'esercizio dei poteri di vigilanza viene trasferito in via diretta all'Autorità europea.

Le ipotesi di sostituzione così delineate sollevano, tuttavia, alcune considerazioni di carattere sistematico e istituzionale.

La sostituzione di un organo europeo nell'esercizio di funzioni amministrative ordinariamente attribuite agli Stati membri – ai sensi degli artt. 197 e 291 del Trattato sul funzionamento dell'Unione europea – non sembra, in linea di principio, porsi in contrasto con i limiti giuridici del sistema. Ciò in quanto lo stesso Trattato di Lisbona ammette che, per assicurare l'attuazione uniforme degli atti dell'Unione giuridicamente vincolanti, le istituzioni europee possano esercitare direttamente funzioni amministrative nei casi in cui ciò risulti necessario per garantire l'effettività del diritto europeo.

Occorre tuttavia considerare che le istituzioni europee legittimate a sostituirsi alle amministrazioni nazionali nell'esecuzione del diritto dell'Unione – ivi compreso quello di recepimento interno – sono individuate espressamente nella Commissione e nel Consiglio, in ossequio al principio di equilibrio istituzionale e al principio di attribuzione delle competenze sancito dall'art. 5 del Trattato sull'Unione europea. La Corte di giustizia, in una prima fase, aveva peraltro teso a circoscrivere in modo rigoroso la possibilità di delega di funzioni esecutive alle agenzie europee**,** evidenziando la necessità di preservare la distinzione tra competenze politiche, amministrative e tecniche.

Alla luce di tali considerazioni, può ritenersi che le funzioni amministrative esercitabili dall'Autorità europea in sostituzione delle autorità nazionali, nel rispetto del principio di sussidiarietà sancito dall'art. 5 TUE, risultino pienamente conformi alle condizioni elaborate dalla giurisprudenza dell'Unione. Ne discende che il meccanismo delineato dal legislatore non comporta alcuna alterazione dell'equilibrio istituzionale europeo, configurandosi piuttosto come uno strumento idoneo ad assicurare l'uniforme applicazione del diritto dell'Unione all'interno dei diversi ordinamenti nazionali.

Le funzioni sostitutive attribuite all'AMLA trovano, infatti, fondamento esplicito in un atto legislativo dell'Unione, sono subordinate al rispetto di condizioni oggettive e predeterminate e risultano soggette a un controllo rigoroso da parte dell'istituzione delegante, vale a dire la Commissione europea, la quale conserva la facoltà di autorizzarne o negarne l'esercizio. Inoltre, i provvedimenti adottati dall'Autorità in via sostitutiva sono suscettibili di impugnazione dinanzi alla Corte di giustizia dell'Unione europea, a garanzia dell'osservanza dei principi di legalità e di tutela giurisdizionale effettiva.

Per quanto riguarda i poteri sanzionatori e regolamentari conferiti all'Autorità europea, la loro adozione si colloca entro confini strettamente tecnici e procedimentalmente garantiti[77].

Gli atti di *rule-making* e di *adjudication* che l'Autorità può emanare sono infatti vincolati a condizioni puntuali e rigorose, non implicano scelte di natura politica o strategica, e devono mantenersi entro la sfera delle competenze tecniche e operative assegnate.

Tali atti sono inoltre assoggettati ai meccanismi di accountability previsti nei confronti della Commissione europea e sottoposti ai controlli amministrativi e giurisdizionali

[77] Sui poteri regolatori delle Autorità Amministrative Indipendenti, cfr., P. BILANCIA, *Riflessi del potere normativo delle Autorità indipendenti sul sistema delle fonti, in Diritto e società*, 1999, p. 231 ss.; R. TITOMANLIO, *Potestà normativa e funzione di regolazione. La potestà regolamentare delle autorità amministrative indipendenti*, Giappichelli, Torino, 2012.

dell'ordinamento unionale: da un lato, mediante la Commissione amministrativa di riesame, che opera in funzione di garanzia interna e di verifica di legittimità procedurale; dall'altro, attraverso la Corte di giustizia dell'Unione europea, competente a pronunciarsi in via definitiva sulla legittimità sostanziale degli atti adottati dall'Autorità.

Ne emerge un sistema equilibrato, nel quale l'attribuzione all'AMLA di poteri sostitutivi e sanzionatori non si traduce in un'indebita espansione delle prerogative amministrative a livello sovranazionale, ma piuttosto in un raffinato congegno di integrazione funzionale tra il livello europeo e quello nazionale, fondato sulla leale cooperazione, sul controllo reciproco e sulla salvaguardia dei principi di proporzionalità e di equilibrio istituzionale[78].

[78] n tal senso C. P. BUTTIGIEG, *The EU Anti-Money-Laundering Authority: A strategic roadmap,* in *Journal of Financial Compliance,* Vol. 8, n. 4, p.339, *January 2025.*