

PUBBLICAZIONE TRIMESTRALE

ISSN: 2279-9737

Rivista
di Diritto Bancario

dottrina
e giurisprudenza
commentata

GENNAIO/MARZO

2022

rivista.dirittobancario.it

DIREZIONE

DANNY BUSCH, GUIDO CALABRESI, PIERRE-HENRI CONAC,
RAFFAELE DI RAIMO, ALDO ANGELO DOLMETTA, GIUSEPPE FERRI
JR., RAFFAELE LENER, UDO REIFNER, FILIPPO SARTORI,
ANTONELLA SCIARRONE ALIBRANDI, THOMAS ULEN

COMITATO DI DIREZIONE

FILIPPO ANNUNZIATA, PAOLOEFISIO CORRIAS, MATTEO DE POLI,
ALBERTO LUPOI, ROBERTO NATOLI, MADDALENA RABITTI,
MADDALENA SEMERARO, ANDREA TUCCI

COMITATO SCIENTIFICO

STEFANO AMBROSINI, SANDRO AMOROSINO, SIDO BONFATTI,
FRANCESCO CAPRIGLIONE, FULVIO CORTESE, AURELIO GENTILI,
GIUSEPPE GUIZZI, BRUNO INZITARI, MARCO LAMANDINI, DANIELE
MAFFEIS, RAINER MASERA, UGO MATTEI, ALESSANDRO
MELCHIONDA, UGO PATRONI GRIFFI, GIUSEPPE SANTONI,
FRANCESCO TESAURO⁺

COMITATO ESECUTIVO

ROBERTO NATOLI, FILIPPO SARTORI, MADDALENA SEMERARO

COMITATO EDITORIALE

GIOVANNI BERTI DE MARINIS, ANDREA CARRISI, GABRIELLA CAZZETTA, ALBERTO GALLARATI, EDOARDO GROSSULE, LUCA SERAFINO LENTINI (SEGRETARIO DI REDAZIONE), PAOLA LUCANTONI, EUGENIA MACCHIAVELLO, UGO MALVAGNA, ALBERTO MAGER, MASSIMO MAZZOLA, EMANUELA MIGLIACCIO, FRANCESCO PETROSINO, ELISABETTA PIRAS, CHIARA PRESCIANI, FRANCESCO QUARTA, CARMELA ROBUSTELLA, GIULIA TERRANOVA

COORDINAMENTO EDITORIALE

UGO MALVAGNA

DIRETTORE RESPONSABILE

FILIPPO SARTORI

NORME PER LA VALUTAZIONE E LA PUBBLICAZIONE

LA RIVISTA DI DIRITTO BANCARIO SELEZIONA I CONTRIBUTI OGGETTO DI PUBBLICAZIONE SULLA BASE DELLE NORME SEGUENTI.

I CONTRIBUTI PROPOSTI ALLA RIVISTA PER LA PUBBLICAZIONE VENGONO ASSEGNATI DAL SISTEMA INFORMATICO A DUE VALUTATORI, SORTEGGIATI ALL'INTERNO DI UN ELENCO DI ORDINARI, ASSOCIATI E RICERCATORI IN MATERIE GIURIDICHE, ESTRATTI DA UNA LISTA PERIODICAMENTE SOGGETTA A RINNOVAMENTO.

I CONTRIBUTI SONO ANONIMIZZATI PRIMA DELL'INVIO AI VALUTATORI.

LE SCHEDE DI VALUTAZIONE SONO INVIATE AGLI AUTORI PREVIA ANONIMIZZAZIONE.

QUALORA UNO O ENTRAMBI I VALUTATORI ESPRIMANO UN PARERE FAVOREVOLE ALLA PUBBLICAZIONE SUBORDINATO ALL'INTRODUZIONE DI MODIFICHE AGGIUNTE E CORREZIONI, LA DIREZIONE ESECUTIVA VERIFICA CHE L'AUTORE ABBIA APPORTATO LE MODIFICHE RICHIESTE.

QUALORA ENTRAMBI I VALUTATORI ESPRIMANO PARERE NEGATIVO ALLA PUBBLICAZIONE, IL CONTRIBUTO VIENE RIFIUTATO. QUALORA SOLO UNO DEI VALUTATORI ESPRIMA PARERE NEGATIVO ALLA PUBBLICAZIONE, IL CONTRIBUTO È SOTTOPOSTO AL COMITATO ESECUTIVO, IL QUALE ASSUME LA DECISIONE FINALE IN ORDINE ALLA PUBBLICAZIONE PREVIO PARERE DI UN COMPONENTE DELLA DIREZIONE SCELTO RATIONE MATERIAE.

SEDE DELLA REDAZIONE

UNIVERSITÀ DEGLI STUDI DI TRENTO, FACOLTÀ DI GIURISPRUDENZA, VIA VERDI 53,
(38122) TRENTO – TEL. 0461 283836

La tracciabilità dei movimenti finanziari tra anonimato e pseudonimato: *FinTech*, incorporazione del diritto nella tecnica e paradigma *by design*

SOMMARIO: 1. Introduzione: *Fintech* e diritto. – 2. *Fintech* e tracciabilità nell'intersezione tra diritto penale e diritto privato. – 3. La difficile tracciabilità soggettiva nelle operazioni in criptovalute e il rischio penale: riciclaggio di denaro di provenienza illecita e finanziamento di attività criminose. – 4. L'indelebile tracciabilità oggettiva nelle operazioni *FinTech*: il rischio relativo al trattamento indiscriminato dei dati personali.

1. Introduzione: *Fintech* e diritto

L'incessante sviluppo della tecnologia digitale, connotata da spiccata versatilità e diffusa interoperabilità tecnica e concettuale, favorisce il dispiegarsi della c.d. Quarta Rivoluzione Industriale e dei suoi effetti dirompenti. La digitalizzazione, le tecnologie di registro distribuito, gli *smart contracts*, l'intelligenza artificiale e la robotica non lasceranno inalterato il sistema economico e sociale conosciuto sino ad ora. La propagazione così intensa e veloce delle innovazioni tecnologiche, ed in particolare della Blockchain, sta inducendo una vera e propria metamorfosi anche delle organizzazioni economiche ed imprenditoriali. Si assiste alla creazione di scenari inediti che valorizzano disintermediazione e decentralizzazione. Il progresso che discende da questa nuova Rivoluzione, a differenza delle precedenti, non è contraddistinto dall'invenzione di nuovi dispositivi, strumentazioni o macchinari, ma dal potenziamento e dall'estensione della tecnologia in sé considerata, sia pure applicata al servizio di nuovi settori strategici e produttivi.

Si assiste pertanto, accanto alla evoluzione di alcuni comparti industriali (agroalimentare, medicale, *supply chain management*, etc) ad una radicale trasformazione del sistema finanziario globale determinata dalla emersione di nuovi modelli operativi e di nuovi soggetti. Come noto, con l'espressione riassuntiva *Fintech*, crasi dei termini tecnologia e finanza, s'intende stipulativamente l'insieme molteplice ed eterogeneo delle innovazioni osservabili in campo

finanziario rese possibili dall' applicazione delle nuove tecnologie sia nell'offerta di servizi agli utenti finali, sia nei processi produttivi interni alle imprese finanziarie, sia nel disegno di imprese-mercato: un complesso e proteiforme fenomeno che investe tanto lo svolgimento di attività finanziarie tradizionali rendendole più efficienti (servizi di pagamento e di investimento, attività bancarie, creditizie, assicurative, *etc*), quanto la costruzione di nuovi servizi e attività e inediti modelli di business (consulenza automatizzata per l'investimento o *robo-advice*, piattaforme digitali per il finanziamento alle imprese, *etc*)¹.

Talvolta interpretato come aggettivo, alla stregua di termine che connota o qualifica ma al quale non viene attribuita la funzione di delimitare con precisione il proprio campo operativo, prospetticamente prefigura il sorgere di una possibile nuova branca del diritto, a fronte del sempre più consistente e diffuso riconoscimento giuridico ed in forza di una più accurata definizione. Di certo il *Fintech* condivide con la tecnologia posta alle sue fondamenta (*Blockchain* o *DLT - Distributed Ledger Technology*) l'affermazione di un inedito paradigma di decentralizzazione, che ambisce ad archiviare irrevocabilmente l'antitetico, risalente e tradizionale paradigma gerarchico. *Fintech* rimanda dunque ad un concetto intersettoriale e proteiforme che riguarda e ricomprende l'innovazione relativa tanto al contenuto delle attività finanziarie quanto agli operatori, nuovi o tradizionali, che ne risultano coinvolti, accanto alla ridefinizione del ruolo ascrivibile alle pubbliche Autorità di vigilanza.

La nuova finanza digitale pone anzitutto un problema di comprensione delle innovazioni tecnologiche, finalizzata all'individuazione delle possibili applicazioni all'interno dell'ecosistema finanziario e alla ricognizione delle istanze di regolazione in relazione agli interessi considerati meritevoli di

¹ M. CIAN, C. SANDEI (a cura di), *Diritto del Fintech*, Padova, 2020; G. FINOCCHIARO, V. FALCE (a cura di), *Fintech: diritti, concorrenza, regole*, Bologna, 2019; F. FIMMANÒ, G. FALCONE (a cura di), *Fintech*, Napoli, 2019; C. SCHENA, A. TANDA, C. ARLOTTA, G. POTENZA, *Lo sviluppo del FinTech. Opportunità e rischi per l'industria finanziaria nell'era digitale* Consob, Quaderni FinTech, 1. Marzo 2018; R. LENER (a cura di), *Fintech: diritto, tecnologia, finanza*, Quaderni di Minerva Bancaria 2018; F. MATTASSOGLIO, *Gli indissolubili intrecci tra mercato finanziario, tecnologia e sicurezza*, in F. Costa, P. Pizzolato (a cura di), *Sicurezza e tecnologia*, Milano, 2017, 203 ss.; M.T. PARACAMPO (a cura di), *Fintech. Introduzione ai profili giuridici di un mercato unico tecnologico dei servizi finanziari*, Torino, 2017.

protezione. Al giurista si richiede un approccio basato su un'analisi caratterizzata da un elevato grado di interdisciplinarietà, essenziale per fornire precise o quantomeno non fuorvianti definizioni e correttamente riquadrare l'innovazione tecnologica all'interno di una consapevole cornice giuridica. In altre parole, circondare di contenuto giuridico le innovazioni che innervano il progresso tecnologico significa non solo dare una veste giuridica alle nozioni digitali, ma soprattutto coniugare la tecnica (informatica) con le esigenze di certezza del diritto².

In materia di *Fintech* plurimi sono e sono stati i metodi e diversi gli orientamenti sperimentati da una pluralità di attori, in sede nazionale come a livello sovranazionale. IOSCO, Comitato di Basilea, BCE, OECD, EBA e le principali Istituzioni europee in tempi recenti e recentissimi hanno fornito un contributo analitico che si è concretizzato in documenti, ricerche, studi, rapporti, relazioni e linee guida, in una sorta di defatigante e inefficiente – ma soprattutto controintuitivo – «diluvio documentale».

Quanto alle legislazioni nazionali, alcuni Stati hanno optato, sia pure con esiti ed esaustività anche molto differenti, per una regolamentazione ritagliata «su misura»: così Malta, Francia e Principato del Liechtenstein³. La Svizzera è ad oggi l'unico paese, nel

² «A fronte di una nuova applicazione tecnologica nasce la tentazione di affidarsi ad una legislazione emergenziale, allontanandosi dalla visione sistematica e dal metodo interpretativo che dovrebbero caratterizzare il lavoro del giurista. Piuttosto che cercare nel sistema giuridico, considerato nella sua complessità, risposte interpretative adeguate, sovente si reclama una nuova norma davanti ad un fenomeno nuovo. Tale approccio non è condivisibile, in quanto comporta una pericolosa stratificazione di norme, piuttosto che una necessaria semplificazione del sistema normativo»: così G. FINOCCHIARO, *Riflessioni su intelligenza artificiale e protezione dei dati personali*, in U. Ruffolo (a cura di), *Intelligenza artificiale*, Milano, 2020, 237.

³ Malta è intervenuta nel 2018 con l'approvazione di tre progetti di legge – MDIA Act, VFA Act e ITAS Act – componenti una articolata legislazione che ha permesso alla «Blockchain Island» di presentarsi al mondo con una regolamentazione *crypto-friendly* e sostanzialmente esaustiva. Anche la Francia ha scelto di intervenire con una disciplina dedicata, contenuta nella *Loi Pacte*. Un intervento normativo costruito però su una definizione di cripto-attività troppo generica che, come la scelta maltese, esclude dal proprio perimetro gli strumenti finanziari. Un approccio identicamente connotato da forte cautela è rinvenibile nella legislazione adottata dal Granducato del Lussemburgo, che ha optato per una regolamentazione settoriale dalla quale è scaturita una disciplina frammentata e incompleta. Si distingue la scelta compiuta dal

continente europeo, ad avere introdotto una tipologia di cripto-attività qualificabile come strumento finanziario, in particolare come «diritto valore», candidandosi ad essere l'ordinamento dotato della disciplina più avanzata e maggiormente *crypto-friendly*.

In Italia i temi della digitalizzazione della finanza e dell'emersione delle nuove tecnologie DLTs e Blockchain sono stati prima di tutto oggetto di attenzione in sede giurisprudenziale, per essere successivamente considerati dal legislatore e dalle autorità di vigilanza. Mentre l'elaborazione giurisprudenziale ha riguardato essenzialmente le cripto-valute⁴, l'interesse del legislatore si è al contrario ampliato per coinvolgere tematiche maggiormente versatili ed omnicomprensive. Con il c.d. Decreto Semplificazioni del 2018 sono state introdotte nel nostro ordinamento le definizioni di *smart contracts* e di tecnologie basate su registri distribuiti. L'anno successivo nell'ambito del c.d. Decreto Crescita, è stata prevista una *regulatory sandbox*, vale a dire un regime sperimentale prettamente dedicato al *Fintech*. Un processo *in fieri*, dunque, forse non destinato neppure ad una rapida definizione, nonostante un crescente interesse da parte degli operatori economici non meno che della dottrina.

Con la presentazione nel settembre del 2020 del *Digital Finance Package* la Commissione Europea sembra aver definitivamente stabilito la fine di quell'approccio che riconduceva la Blockchain e le DLTs pressoché esclusivamente alle cripto-valute. L'iniziativa sottende infatti una visione di strategia politico-normativa matura e di più ampio respiro, capace di sviluppare nuove riflessioni e nuovi schemi regolamentari anche al di fuori dell'angusto (benché rilevante) perimetro delle cripto-valute, con l'obiettivo di incentivare fortemente la crescita e lo sviluppo del *Fintech* in seno all'Unione Europea, senza trascurare le istanze di certezza e stabilità che ogni regolazione deve perseguire.

Principato del Liechtenstein che, con l'approvazione del TVTG, ha deciso di dotarsi di una regolamentazione esaustivamente dedicata alla c.d. *token economy*: una normativa che esplicitamente si riferisce alle tecnologie DLTs qualificandole come «affidabili», negando quindi l'accezione più diffusa in dottrina che le vede come «disruptive».

⁴ Si v. per tutte Trib. Brescia, 18 luglio 2018, in *Giur. comm.*, 2020, II, 883 ss., con nota di C. FLAIM, *Nuove frontiere del conferimento in società a responsabilità limitata: il caso delle criptovalute*.

2. *Fintech e tracciabilità nell'intersezione tra diritto penale e diritto privato*

Il tema della tracciabilità, inteso in termini generali, evoca almeno due distinti significati o ambiti di senso. Da un punto di vista oggettivo, richiama la possibilità di reperire nel tempo, in maniera stabile e duratura nonché liberamente accessibile, i segni intellegibili che diano certezza dell'accadimento di un fatto o di una situazione o condizione preesistente. Su un piano soggettivo, invece, postula la capacità di riferire un fatto, un atto, una situazione o condizione inequivocabilmente ad una ed una sola persona, chiaramente identificata o agevolmente identificabile. Nell'uno e nell'altro caso, del tutto indipendentemente dal giudizio in punto di legittimità che del fatto, dell'atto, della situazione si possa dare, e dalla giuridica imputabilità dell'atto alla persona identificata. La tracciabilità attiene, per così dire, ad una verifica di effettività e non involge, direttamente né automaticamente, un giudizio che può essere solo successivo e che riguarda non già la traccia in sé ma l'oggetto cui la traccia rinvia e/o la relazione fra l'oggetto e il soggetto al quale esso sia riferibile.

La tracciabilità riguarda quindi insiemi di informazioni, di natura tanto oggettiva quanto soggettiva, legata al fattore spazio e al fattore tempo.

Il tema della tracciabilità delle transazioni interseca *Fintech* nelle sue molteplici manifestazioni, strettamente correlate all'applicazione della tecnologia Blockchain, ed involge tanto questioni di schietto diritto penale quanto problematiche di pretta natura privatistica. Da un canto, la possibile violazione delle norme nazionali e sovranazionali volte a impedire l'utilizzo del sistema finanziario e delle criptovalute a scopo di riciclaggio dei proventi di attività criminose e finanziamento del terrorismo e di altre attività criminali. Dall'altro, il raffronto con la tutela, il trattamento e la circolazione dei dati personali nel rispetto del Regolamento Europeo (GDPR) in vigore dal 25 maggio 2018.

In particolare, la valutazione delle caratteristiche tecnico-funzionali e delle ricadute strutturali in termini di tracciabilità risulta antitetica e per così dire ribaltata nell'uno e nell'altro campo d'indagine. L'anonimato, l'elemento che meglio concretizza il rischio connesso

all'ignoto criminale, garantisce infatti pienamente la riservatezza dei dati personali così come definita dal Regolamento; mentre il suo contrario, l'imperitura tracciabilità oggettiva e la conseguente riferibilità soggettiva delle transazioni, minaccia fortemente i diritti individuali di proteggere i propri dati personali, di controllarne la circolazione e di limitare modalità e finalità del trattamento.

Il saggio intende suggerire che il problema può essere efficacemente fronteggiato sfruttando il paradigma legale e i metodi tecnici della pseudonimizzazione, come postulata in applicazione del principio generale della protezione degli interessi rilevanti sin dalla progettazione tecnica degli strumenti (*"by design"*).

Nell'immanenza del conflitto tra regole tecniche del mercato digitale e precetti di un ordinamento giuridico nazionale, occorre scongiurare un duplice rischio. Da un canto, l'abdicazione regolativa a favore di scelte esclusivamente tecniche, con la conseguente rinuncia alla selezione politica del bilanciamento tra gli interessi giudicati meritevoli di tutela; dall'altra la rigidità di un sistema che, ancorando la regolazione a categorie consolidate, costringa il nuovo entro schemi adusati, trascurando l'inafferrabile rapidità e la capacità espansiva dell'evoluzione tecnologica.

Una soluzione plausibile ed efficiente trova fondamento nella logica di quella che è stata definita incorporazione del diritto nella tecnica, secondo un modello di normazione «proattivo e preventivo», proficuamente perseguibile soprattutto avendo riguardo alla tecnologia Blockchain. Un modello rintracciabile proprio nella disciplina europea in materia di protezione dei dati personali, che tutela la persona e la sua riservatezza sin dalla fase della progettazione, traducendo in termini giuridici il principio «*by design e by default*». In particolare, tra le opzioni idonee a «integrare le tutele nel trattamento» onde realizzarne finalità e obiettivi di protezione, il Regolamento seleziona, sia pure esemplificativamente, proprio i processi volti alla minimizzazione e alla pseudonimizzazione dei dati personali.

3. La difficile tracciabilità soggettiva nelle operazioni in criptovalute e il rischio penale: riciclaggio di denaro di provenienza illecita e finanziamento di attività criminali

La possibilità di tracciare le operazioni di carattere finanziario rivela la sua assoluta centralità quando riferita alla prevenzione e repressione di fenomeni criminosi: l'impossibilità o l'estrema difficoltà di individuare e ricostruire i movimenti finanziari e le negoziazioni di valori, ripercorrendone a ritroso i passaggi sino a ricollegarli inequivocabilmente ad una o più persone determinate, costituiscono il terreno su cui possono radicarsi crimini quali l'evasione fiscale, la corruzione, il traffico illegale di armi o di sostanze stupefacenti, ma soprattutto il riciclaggio di denaro di provenienza illecita e il finanziamento occulto alle attività terroristiche. La stessa stabilità del sistema finanziario nel suo complesso ne risulta fatalmente, se non compromessa, certo gravemente minacciata con nefaste ricadute sui settori e sugli operatori che si muovono entro i cardini della legalità⁵.

Le istituzioni, in ambito tanto europeo quanto internazionale, mostrano da tempo chiara consapevolezza del problema e sottolineano l'urgenza dell'intervento regolatorio. Ci si riferisce, anzitutto, ai documenti elaborati rispettivamente dal FATF – Financial Action Task Force (il report *Virtual Currencies: Key Definitions and Potential AML/CTF Risks* – FATF 2014 e le successive linee guida *Guidance for a Risk-Based Approach to Virtual Currencies* pubblicate per la prima volta nel 2015, quindi aggiornate nel giugno di quest'anno – FATF 2019)⁶, dalla Banca Centrale Europea (report del 2012 successivamente aggiornato *Virtual Currency Schemes: a further analysis* - ECB 2015)⁷ infine dall'Autorità Bancaria Europea (*Opinion 2015/08 on virtual currencies* - EBA 2014)⁸. Tra gli oltre settanta censiti e suddivisi in

⁵ F. MAGNOLO, *Profili di rilevanza penale in materia di valute virtuali*, in G. Finocchiaro, V. Falce, *op. cit.*, 477 ss. opportunamente contrappone la tutela penale *delle* valute virtuali, intese come valore patrimonialmente rilevante che può costituire oggetto materiale di reati onde sancirne uno statuto (utilizzo fisiologico e lecito), alla tutela penale *dalle* valute virtuali, intesa propriamente come ricerca dei presidi atti a scongiurarne l'idoneità a fungere da veicoli per le più diverse transazioni criminosi e per operazioni di riciclaggio di proventi delittuosi (utilizzo criminoso).

⁶ Entrambe leggibili in www.fatf-gafi.org.

⁷ Reperibile su www.ecb.europa.eu.

⁸ Pubblicata su www.eba.europa.eu. Tra gli oltre settanta censiti e suddivisi in categorie (Rischi per gli utenti, Rischi non dipendenti dai partecipanti alle transazioni, Rischi legati all'integrità del sistema, Rischi relativi al cambio della valuta in FC, Rischi per le Autorità di regolamentazione) i *Rischi legati all'integrità del sistema* sono tutti giudicati "alti" e riguardano, tra gli altri: il riciclaggio di proventi di reato

categorie (Rischi per gli utenti, Rischi non dipendenti dai partecipanti alle transazioni, Rischi legati all'integrità del sistema, Rischi relativi al cambio della valuta in *Fiat Coins*, Rischi per le Autorità di regolamentazione) i *Rischi legati all'integrità del sistema* sono tutti giudicati dall'EBA come "alti" e riguardano in particolare: il riciclaggio di proventi di reato grazie a deposito e trasferimento delle criptovalute in forma anonima, rapida e irrevocabile a livello globale; l'occultamento della provenienza criminale dei fondi e il conseguente ostacolo al recupero, al sequestro e alla confisca; l'impiego a fini di finanziamento del terrorismo; l'estorsione anonima; la facilitazione all'ingaggio al coinvolgimento di persone in attività criminose.

Con puntuale riguardo all'Unione Europea, una Quinta Direttiva Antiriciclaggio è stata da poco approvata a compendio e modifica dei precedenti interventi di armonizzazione, a dimostrazione palese dell'attenzione rivolta a un settore cruciale per l'attuazione del mercato unico e reputato a quei fini particolarmente vulnerabile (Direttiva UE 2018/843 relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo)⁹.

Elemento comune e costitutivo quanto meno delle principali fattispecie delittuose che sulla mancanza di trasparenza, oggettiva e soggettiva, consolidano le proprie dinamiche operative è l'utilizzo di quei peculiari strumenti digitali rappresentativi di valore e suscettibili di formare oggetto di scambio che vengono identificati come criptovalute o criptomonete, a cominciare dai celeberrimi bitcoin, via

grazie a deposito e trasferimento delle CV in forma anonima, rapida e irrevocabile a livello globale; l'occultamento della provenienza criminale dei fondi e conseguente ostacolo al recupero, al sequestro e alla confisca; impiego a fini di finanziamento del terrorismo; l'estorsione anonima; la facilitazione all'ingaggio al coinvolgimento di persone in attività criminose.

⁹ Il testo integrale della Direttiva UE 2018/843 del Parlamento Europeo e del Consiglio del 30 maggio 2018 – già pubblicata in Gazzetta Ufficiale e alla quale gli Stati membri sono tenuti a conformarsi entro il prossimo 10 gennaio 2020 – è disponibile sul sito www.eur-lex.europa.eu. Le altre quattro Direttive europee in materia di antiriciclaggio e contrasto al finanziamento del terrorismo si sono succedute dal 1991 al 2015, sempre precedute dalle *Raccomandazioni* della FATF - *Financial Action Task Force* o GAFI – Gruppo di Azione Finanziaria Internazionale, istituita nel 1989 presso l'OCSE. L'urgenza della revisione della Quarta Direttiva antiriciclaggio (Dir. UE 2015/849) è da mettere in relazione con la sequela di attentati terroristici di matrice islamista che hanno funestato l'Europa a partire dalla strage di Parigi e con la vicenda nota come *Panama Papers*.

via affiancati da ethereum, litecoin, titcoin, peercoin, monero, ripple, zcash...¹⁰.

Allo stato non esiste una definizione univoca ed universalmente accettata di criptomoneta¹¹. Possiamo tuttavia accostarci anzitutto a quella di valuta virtuale che, con buon grado di approssimazione e commendevoli finalità omnicomprensive, compare proprio nella Quinta Direttiva Antiriciclaggio, che a sua volta riprende quanto già riconosciuto dall'Autorità Bancaria Europea nel 2014, e che lo stesso legislatore italiano ha recepito in occasione delle recenti novelle alla disciplina nazionale antiriciclaggio, l'ultima delle quali attuata con d. lgs. 4 ottobre 2019, n. 125: una rappresentazione digitale di valore che non è emessa né garantita da una banca centrale o da una autorità pubblica, non è necessariamente collegata a una valuta avente corso legale, non possiede lo *status* giuridico di valuta o moneta, ma è

¹⁰ Sul fenomeno *cryptoassets* e *cryptocurrencies* la letteratura è di già amplissima. Si vedano, tra i tanti: N. MANCINI, *Valute Virtuali e Bitcoin*, in *An. Giur. Econ.*, 2015; S. CAPACCIOLI, *Criptovalute e bitcoin: un'analisi giuridica*, Milano, 2015; B. KELLY, *The Bitcoin Big bang: How Alternative Currencies Are About to Change the World*, New Jersey, 2015; M. AMATO, L. FANTACCI, *Per un pugno di Bitcoin*, Milano, 2016; N. MANCINI, *Bitcoin: rischi e difficoltà normative*, in *Banca imp. soc.*, 2016, 127 ss.; H. HALABURDA, M. SARVARY, *Beyond Bitcoin: the Economics of Digital Currencies*, New York, 2016; A.M. Antonopoulos, *Mastering bitcoin: programming the open blockchain*, O'Reilly Media, 2017; G. LEMME, S. PELUSO, *Criptomoneta e distacco dalla moneta legale: il caso Bitcoin*, in *Riv. Trim. Econ.*, 2016 - Supplemento n. 1, 148 ss.; G. L. GRECO, *Monete complementari e valute virtuali*, in M. T. Paracampo, *op. cit.*, 197 ss.; A. CAPONERA, C. GOLA, *Aspetti economici e regolamentari delle crypto-attività*, Banca d'Italia – Questioni di Economia e Finanza, Marzo 2019; P. LIBERANOME, *Criptovalute tra anarchia e difficili tentativi di regolamentazione*, in F. Fimmanò, G. Falcone, *op. cit.*, 419 ss.; C. PERNICE, *Crittovalute e bitcoin: stato dell'arte e questioni ancora aperte*, in F. Fimmanò, G. Falcone, *op. cit.*, 491 ss.; G. J. SICIGNANO, *Bitcoin e riciclaggio*, Giappichelli, Torino, 2019; M. CIAN, *La criptovaluta – Alle radici dell'idea giuridica di denaro attraverso la tecnologia*, in *Banca borsa tit. cred.*, 2019, 315 ss.; A.M. GAMBINO, C. BOMPREZZI, *Blockchain e criptovalute*, in G. Finocchiaro, V. Falce, *op. cit.*, 267 ss.; M.T. CHIMIENTI, U. KOCHANSKA, A. PINNA, *Understanding the crypto-asset phenomenon, its risks and measurement issues*, ECB Economic Bulletin, Issue 5/2019; ECB *Crypto-Assets Task Force*, *Crypto-Assets: implications for financial stability, monetary policy, and payments market infrastructures*, Occasional Paper Series no. 223 / May 2019.

¹¹ Per approfondimenti si vedano i recenti saggi di V. DE STASIO, *Le monete virtuali: natura giuridica e disciplina dei prestatori di servizi connessi*, in M. Cian, C. Sandei, *op. cit.*, 215 ss. e di A.M. PANCALLO, *Le criptovalute*, in G. Alpa (a cura di), *Diritto e intelligenza artificiale*, Pisa, 2020, 591 ss.

accettata da persone fisiche e giuridiche e utilizzata come mezzo di scambio per l'acquisto di beni e servizi o per finalità di investimento e può essere trasferita, archiviata e negoziata elettronicamente (art. 1, comma 2, lett. qq) d. lgs. 21 novembre 2007 n. 231). Si noti l'inclusione esplicita della «finalità di investimento» realizzata proprio per effetto del decreto di recepimento della Quinta Direttiva: il precedente testo della norma – come novellata dal d. lgs. 25 maggio 2017, n. 90, a sua volta attuativo della Quarta Direttiva Antiriciclaggio – richiama infatti il solo utilizzo in guisa di mezzo di scambio o di pagamento benché l'Autorità Bancaria Europea già ne avesse colto l'eterogeneità applicativa, non escludendo, accanto alla finalità di scambio, la detenzione «a scopo di investimento»¹².

Seguendo la classificazione adottata dalla Banca Centrale Europea nel ricordato *Report* del 2015, tra valute virtuali e criptovalute deve istituirsi un rapporto da genere a specie dal momento che la quasi totalità delle criptomonete rientra nel novero delle *Virtual Currency Schemes with Bidirectional Flow*, connotate da piena e perfetta convertibilità in valuta avente corso legale (a differenza delle *Closed Virtual Currency Schemes*, che circolano esclusivamente all'interno di un ambiente esso pure virtuale, e delle *Virtual Currency Schemes with Unidirectional Flow*, acquistabili con moneta legale ma in essa non convertibili)¹³.

¹² Negli stessi termini si era espressa anche la Banca d'Italia, nella sua *Comunicazione del 30 gennaio 2015 sulle valute virtuali*. Coerentemente, nel Decimo *Considerando* della Direttiva UE 2018/843 si legge «Sebbene le valute virtuali possano essere spesso utilizzate come mezzo di pagamento, potrebbero essere usate anche per altri scopi e avere impiego più ampio, ad esempio come mezzo di scambio, di investimento, come prodotti di riserva di valore o essere utilizzate in un casinò on line». Come noto, la valuta o moneta virtuale si distingue tanto dalla moneta elettronica quanto dalla moneta c.d. complementare: cfr. il Decimo e Undicesimo *Considerando* della Quinta Direttiva. La Direttiva 2009/110/CE (c.d. Direttiva IMEL2) e l'art. 1, h-ter del Testo Unico Bancario definiscono moneta elettronica «il valore monetario memorizzato elettronicamente, ivi inclusa la memorizzazione magnetica, rappresentato da un credito nei confronti dell'emittente che sia emesso per effettuare operazioni di pagamento, e che sia accettato da persone fisiche e giuridiche diverse dall'emittente». In dottrina: G. L. GRECO, *op. cit.*, 197 ss.; V. DE STASIO, *Verso un concetto europeo di moneta legale*, in *Banca borsa tit. cred.*, 2018, 747 ss.

¹³ Si vedano: R. BOCCHINI, *Lo sviluppo della moneta virtuale: primi tentativi di inquadramento e disciplina tra prospettive economiche e giuridiche*, in *Dir. informaz.*

Un rilievo del tutto peculiare e, per così dire, paradigmatico, deve essere riconosciuto alla prima e a tutt'oggi più diffusa delle criptovalute, il bitcoin, al quale è quindi opportuno riferirsi per indagare i rischi e le ricadute penalistiche della (non) tracciabilità¹⁴.

Nel quadro internazionale, gli ordinamenti dei paesi a capitalismo avanzato circondano il riciclaggio e il finanziamento al terrorismo – e più in generale la circolazione del denaro – di una regolamentazione capillare improntata alla prevenzione attraverso la massima trasparenza delle negoziazioni a carattere finanziario, in modo da verificare con certezza le parti sia in senso formale (chi disponga dei fondi: a chi i fondi siano destinati) sia in senso sostanziale (corrispondenza con i destinatari effettivi) di tutte le transazioni¹⁵.

Senza sottovalutare l'affrancamento dalle coordinate spaziali o a-territorialità del fenomeno che fa del *Fintech* una plausibile zona franca potenzialmente senza confini geografici ove inabissare ricchezze destinate alle più diverse finalità illecite o fare riemergere come immacolate somme ingentissime provenienti dalla commissione di crimini informatici o tradizionali, ancora una volta il discrimine è rappresentato dalle caratteristiche tecniche di funzionamento proprie delle criptomonete. Come dianzi indicato, l'impiego della tecnologia blockchain consente, rispetto alle operazioni compiute, irretrattabilità e invariabilità, marcatura temporale certa, stabilità e incancellabilità delle registrazioni una volta avvenute. Per converso, rispetto all'identificazione dei soggetti, realizza forme più o meno definitive ed

e informatica, 2017, 27 ss. (in part. 52 ss.); G. RINALDI, *Criptovalute e blockchain*, in *Vita not.*, 2018, 1449 ss. (in part. 65 ss.).

¹⁴ B. BANDIERA, *FinTech e antiriciclaggio*, in M. T. Paracampo, *op. cit.*, 259 ss.; G. P. ACCINNI, *Profili di rilevanza penale delle "criptovalute"*, in *Arch. pen.*, 2018, 1 ss.; ID., *Regole antiriciclaggio e risvolti penalistici dell'operatività in valute virtuali*, in *Riv. soc.*, 2018, 1516 ss.; F. DI VIZIO, *Le cinte daziarie del diritto penale alla prova delle valute virtuali degli internauti. Lo statuto delle valute virtuali. Le discipline e i controlli*, in F. Fimmanò, G. Falcone, *op. cit.*, 291 ss.; M. KROGH, *Bitcoin, Blockchain e le transazioni in valute virtuali ed i rischi di riciclaggio. Il ruolo del notaio*, *ivi*, 385 ss.; ID., *Transazioni in valute virtuali e rischi di riciclaggio. Il ruolo del notaio*, in *Notariato*, 2018, 155 ss.; R. RAZZANTE, *L'utilizzo illecito delle valute virtuali*, in R. Razzante (a cura di), *Bitcoin e criptovalute*, Rimini, 2018, 63 ss.; G. J. SICIGNANO, *op. cit.*, 108 ss.; M. NADDEO, *Nuove frontiere del risparmio, Bit Coin Exchange e rischio penale*, in *Dir. pen e processo*, 2019, 99 ss.

¹⁵ M. KROGH, *op. cit.*, 157.

irreversibili di opacità e occultamento. La dimensione sconfinata in un mondo globalizzato, l'immediatezza istantanea delle transazioni e la vocazione all'anonimato rappresentano così le condizioni ideali per la commissione di crimini che, in ragione della strutturale inafferrabilità e dell'impossibilità di imputarne univocamente la commissione ad una persona determinata, rischiano di rimanere drammaticamente impuniti.

Il paradigma della riferibilità soggettiva collegata alla circolazione dei bitcoin è qualificabile tuttavia in termini non già di vero e proprio anonimato, quanto piuttosto di *pseudonimato*¹⁶. La non immediatezza dell'identificazione, celata dietro l'usbergo di un codice informatico alfanumerico, risulta infatti superabile grazie all'impiego di particolari *software*, dotandosi dei quali le autorità dei diversi paesi potrebbero infrangere lo pseudonimo e disvelare l'identità dell'utente che se ne sia avvalso attivando un account, onde irrogare le sanzioni penali previste dall'ordinamento e scongiurare il rischio della sua sistematica elusione.

La completa trasparenza di tutte le registrazioni consente di imputare univocamente ciascuna operazione alla chiave pubblica ad essa associata: se la certezza "accessibile" riguarda sempre l'account di partenza, l'account d'arrivo e gli importi singolarmente negoziati tra l'uno e l'altro, il disvelamento tecnologico consente di risalire alla chiave privata e quindi alla reale identità dei singoli che i bitcoin abbiano utilizzato, scambiato o fatto circolare sulla Blockchain.

La possibile tracciabilità secondaria e selettiva dello pseudonimato, dovuta ad accorgimenti tecnologici, sconfina tuttavia nel più invalicabile *anonimato* per effetto dell'applicazione di altri strumenti tecnologici che l'identità reale degli utenti/contraenti dissimulano e inabissano irreversibilmente nelle dinamiche della blockchain¹⁷.

Nel sistema Bitcoin chiunque può ottenere una coppia di chiavi, pubblica e privata, per trasferire criptomoneta senza alcuna necessità di

¹⁶ M. MÖSER, R. BÖHME, D. BREUKER, *An Inquiry into Money Laundering Tools in the Bitcoin Ecosystem* in *Ecrime Researchers Summit*, 2013, 1 ss.; E. IMWINKELRIED, J. LUU, *The Challenge of Bitcoin Pseudo-Anonymity to Computer Forensics*, in *Criminal Law Bulletin*, 2016; F. DI VIZIO, *op. cit.*, 304 ss.: «Bitcoin utilizza la crittografia a chiave pubblica, cioè un algoritmo crittografico asimmetrico che si serve di due chiavi, generate matematicamente: la chiave privata, impiegata per 'crittografare' o firmare digitalmente il documento, il 'denaro digitale', e la chiave pubblica, che viene usata per 'decrittografare' il messaggio o per verificare la firma».

¹⁷ G. P. Accinni, *Profili di rilevanza penale delle "criptovalute"*, cit., 5 ss.

previa identificazione e il numero delle chiavi pubbliche generate e generabili dal sistema è potenzialmente infinito: ad una identità personale, comunque mascherata, possono perciò essere associate tante chiavi pubbliche – ed altrettante private – quante sono le transazioni compiute, agevolmente spezzando la corrispondenza tra utente – disponente o utente – destinatario e somma di registrazioni, non più ricollegabili neppure ad un unico account¹⁸. Sistemi, sempre più disponibili sul mercato, di *software* realizzano il c.d. *mixing* o *tumbler*, vale a dire il mescolamento tra gli account di origine e di destinazione, cosicché i singoli movimenti finanziari e i pagamenti effettuati vengano spargliati in maniera casuale come le carte di un mazzo su un tavolo da gioco, impedendo la ricostruzione puntuale della catena cronologica, l'aggregazione e la simmetria tra le registrazioni¹⁹.

Ai primigeni bitcoin si sono andate via via affiancando altre criptovalute, con espressione genericamente riassuntiva indicate come *Alternative Coins* o *Altcoins*, alcune delle quali in grado di garantire un livello pressoché inaccessibile di anonimato grazie a differenti algoritmi di funzionamento²⁰. Così *Monero*, immessa sul mercato nel 2014, caratterizzata dalla corrispondenza di una diversa coppia di chiavi per ogni singola operazione e automaticamente governata da un sistema di *mixing* e *ZCash*, lanciata nel 2016, che lascia gli utenti liberi di occultare le transazioni effettuate, i destinatari e i relativi importi²¹. Allo stato dell'arte, nulla sembra impedire, peraltro, che gli stessi criminali possano scegliere di generare una loro propria criptomoneta con la quale movimentare o scambiare indiscriminatamente ingenti ricchezze, e ripulire i proventi di ogni forma di attività illecita.

In questa cornice, nella quale l'ambiente tecnologico sembra rifuggire qualunque pretesa di normazione, le reazioni dei regolatori si attestano sul limitare del mondo (e dell'economia) reale, intervenendo

¹⁸ M. MARTONI, *Documento informatico e firme elettroniche*, in C. DI COCCO, G. SARTOR (a cura di), *Temi di diritto dell'informatica*, Torino, 2017, 27 ss.

¹⁹ Plurimi i sistemi di *mixing service* dai nomi evocativi quali Bitcoin Laundry, Bitcoin Fog, Bitlaunder, Cleanbit, Safewallet, Darkbit, Easycoin...

²⁰ Al momento attuale risultano censite quasi 2500 criptovalute nate successivamente e, per l'appunto, "alternative" al bitcoin, benché quest'ultimo continui a rappresentare oltre il 60% del mercato complessivo (www.coinmarket.cap).

²¹ L. D'AGOSTINO, *Operazioni di emissione, cambio e trasferimento di criptovaluta: considerazioni sui profili di esercizio (abusivo) di attività finanziaria a seguito dell'emanazione del D. Lgs. 90/2017*, in questa Rivista, 2018, 12 ss.

nel momento e all'atto della conversione della valuta virtuale in moneta avente corso legale. A mente dell'Ottavo *Considerando* della menzionata Quinta Direttiva *Anti Money Laundering*, al fine di contrastare riciclaggio e finanziamento al terrorismo internazionale, le autorità competenti dei paesi membri della UE debbono essere in grado di monitorare l'uso delle valute virtuali attraverso il costante controllo su una pluralità di soggetti sottoposti a stringenti obblighi di informazione e verifica. Si sottolinea pertanto la «fondamentale importanza» di ampliare l'ambito di applicazione della precedente Quarta Direttiva (Dir. UE 2015/849) in modo da includervi i prestatori di servizi la cui attività consista nel cambio tra valute virtuali e valute aventi corso legale – vale a dire le monete e le banconote considerate a corso legale e la moneta elettronica di un paese, accettate quale mezzo di scambio nel paese emittente – e i prestatori di servizi di portafoglio digitale²².

Nella medesima direzione, prima ancora della scadenza per l'attuazione, fissata al 10 gennaio 2020, ma già all'atto del recepimento della cennata e modificata Quarta Direttiva, si era mosso, primo fra tutti i regolatori europei, il legislatore italiano. Il d. lgs. 25 maggio 2017, n. 90 aveva infatti riformato il d. lgs. 21 novembre 2007 n. 231, recante la disciplina interna concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo, estendendo l'insieme delle misure preventive intese a scongiurare il meccanismo di occultamento della tracciabilità finanziaria, quando realizzata per mezzo di moneta digitale virtuale, ai *virtual currency exchangers*, ovverosia agli operatori professionali che, convertendo la criptovaluta in moneta avente corso legale e la valuta legale in criptomoneta, fungono da “porte” di accesso e di uscita e sono quindi in grado di identificare le persone che entrano ed escono dal sistema digitale (artt. 1, comma 2, lett. ff) e 3, comma 5, lett. i) d. lgs. 231/2007). In particolare, ai cambiavalute digitali si estendono gli obblighi di «adeguata verifica della clientela»

²² Si veda *supra* nota 6. In dottrina, si vedano i rilievi di: G. P. ACCINNI, *Regole antiriciclaggio e risvolti penalistici dell'operatività in valute virtuali*, in *Riv. soc.*, 2018, 1516 ss. e di G. GAMBOGI, *La disciplina sanzionatoria della nuova normativa antiriciclaggio di cui al d. lgs. 25 maggio 2017 n. 90*, in V. MAIELLO, L. DELLA RAGIONE (a cura di), *Riciclaggio e reati nella gestione dei flussi di denaro sporco*, Milano, 2018.

(identificazione del cliente e verifica della sua identità, identificazione del titolare effettivo dei fondi e della sua identità, acquisizione e valutazione di informazioni sullo scopo e sulla natura del rapporto continuativo o della prestazione professionale, controllo costante del rapporto con il cliente) e gli obblighi di segnalazione all'UIF-Unità di Informazione Finanziaria delle «operazioni sospette» in ragione delle loro caratteristiche, dell'entità, della natura, del collegamento o frazionamento delle stesse, tenuto conto anche della capacità economica e dell'attività svolta dal soggetto cui sono riferibili (oltre agli obblighi di conservazione dei dati e delle informazioni raccolte mediante sistemi idonei a garantire il rispetto delle norme dettate dal Codice in materia di protezione e trattamento dei dati personali)²³. L'attuazione della Quinta Direttiva ha rappresentato l'occasione per l'esplicita estensione degli obblighi di trasparenza antiriciclaggio anche agli *e-wallet providers*, gestori per conto degli utenti dei portafogli digitali, conti elettronici in cui la valuta virtuale è detenuta grazie alla salvaguardia delle chiavi crittografiche, e che della valuta virtuale permettono la movimentazione con transazioni, acquisti, rimesse, riconversioni con altri utenti, registrando tutte le operazioni e fornendo un saldo. A mente dei novellati artt. 1, comma 2, lett. ff-bis) e 3, comma 5, lett. i-bis) d. lgs. 231/2007, gli obblighi di adeguata verifica, registrazione e segnalazione incombono ora anche su «ogni persona fisica o giuridica che fornisce a terzi, a titolo professionale, anche *online*, servizi di salvaguardia di chiavi crittografiche private per conto dei propri clienti, al fine di detenere, memorizzare e trasferire valute virtuali» (prestatori di servizi di portafoglio digitale)²⁴.

²³ G. P. ACCINNI, *Profili di rilevanza penale delle "criptovalute"*, cit., 19 ss.; M. PASSARETTA, *La nuova disciplina antiriciclaggio: tra sistemi di pagamento innovativi e nuove forme di finanziamento alle imprese*, in F. Fimmano, G. Falcone, op. cit., 470 ss.; C. PERNICE, op. cit., 528 ss.; G. J. SICIGNANO, op. cit., 185 ss.

²⁴ Prima dell'entrata in vigore del d. lgs. 125/2019 era indubitabile la loro ricomprensione nel novero dei soggetti che forniscono «a terzi, a titolo professionale, servizi funzionali all'utilizzo, allo scambio, alla conservazione di valuta virtuale» ai sensi dell'art. 1 comma 2, lett. ff) d. lgs. 231/2007: fermo l'obbligo di iscrizione in una sezione speciale del registro tenuto dall'OAM, istituito ai sensi dell'art. 128-undecies del Testo Unico Bancario, si poteva ritenere che andassero soggetti agli obblighi antiriciclaggio allorché svolgessero anche «attività di conversione di valute virtuali da ovvero in valute aventi corso forzoso» ai sensi dell'art. 3, comma 5, lett. i) d. lgs. 231/2007. Cfr. I. BIXIO, *Valute virtuali e adempimenti antiriciclaggio: riflessi su*

L'insufficienza dei presidi così creati non sfugge tuttavia allo stesso regolatore europeo. Nel Nono *Considerando* della Quinta Direttiva si legge infatti: «L'anonimato delle valute virtuali ne consente il potenziale uso improprio per scopi criminali. L'inclusione dei prestatori di servizi la cui attività consiste nella fornitura di servizi di cambio tra valute virtuali e valute reali e dei prestatori di servizi di portafoglio digitale non risolve completamente il problema dell'anonimato delle operazioni in valuta virtuale: infatti, poiché gli utenti possono effettuare operazioni anche senza ricorrere a tali prestatori, gran parte dell'ambiente delle valute virtuali rimarrà caratterizzato dall'anonimato. Per contrastare i rischi legati all'anonimato, le *Financial Intelligence Unit* (FIU) dovrebbero poter ottenere informazioni che consentano loro di associare gli indirizzi della valuta virtuale all'identità del proprietario di tale valuta. Occorre inoltre esaminare ulteriormente la possibilità di consentire agli utenti di presentare, su base volontaria, un'autodichiarazione alle autorità designate». Nel momento stesso in cui intercettano e colpiscono esclusivamente l'uscita e il reingresso nel mondo reale controllando i guardiani del passaggio, le *cinte daziarie* rivelano la loro inadeguatezza a regolare il fenomeno nella sua dimensione autenticamente virtuale e inestricabilmente correlata all'evoluzione tecnologica²⁵.

Accanto all'eventualità di non fare riemergere nelle forme della moneta legale le ricchezze accumulate grazie alle attività criminose (vieppiù plausibile in concomitanza con la diffusa accettazione della criptomoneta come mezzo di pagamento e con la riscontrata attitudine a formare altresì oggetto di investimento e riserva di valore), alla possibilità di operazioni di conversione e reimmissione dei fondi senza valersi dell'ausilio di cambiavalute digitali (favorita proprio dall'incessante sviluppo della tecnologia e dal conseguente effetto di progressiva disintermediazione a tutti i livelli), non è chiaro di quali strumenti le unità nazionali di informazione finanziaria dovrebbero

soggetti obbligati, nuovi e non, in *Corr. trib.*, 2017, 2676; M. BELLINO, *I rischi legati all'ecosistema Bitcoin: i nuovi intermediari*, in questa *Rivista*, 2018, segnalava come la linea di confine tra gli uni e gli altri si facesse sempre più sfumata dal momento che il 52% degli *e-wallet providers* forniva contemporaneamente anche servizi di *exchange*.

²⁵ D. MAJORANA, *Disciplina giuridica e fiscale delle criptovalute: sfida al legislatore dal web*, in *Corr. trib.*, 2018, 630; F. DI VIZIO, *op. cit.*, 293 ss.

dotarsi per poter associare gli indirizzi della valuta virtuale all'identità del reale proprietario, così come auspicato dalla normativa europea: né attualmente sembrano disponibili tecnologie o sistemi in grado di ricollegare l'identità certa di un singolo utente ad un account digitale al quale o dal quale siano stati trasferiti importi espressi in bitcoin o altri Altcoins (potendo eventualmente risalire al solo indirizzo IP del terminale singolarmente utilizzato per l'invio o la ricezione)²⁶.

Il legislatore italiano ha peraltro dimostrato una certa lungimiranza e una sensibilità acuta rispetto alla rischiosità del fenomeno, particolarmente attenta proprio alla incessante ed imprevedibile crescita tecnologica e alla prospettiva centralità di un mercato su valori unicamente digitali e dematerializzati a scapito delle porte girevoli tra criptomoneta e denaro "reale". L'inasprimento ulteriore della disciplina è infatti avvenuto con la ricomprensione non solo delle attività rese esclusivamente *on line*, ma anche delle attività di conversione in altre rappresentazioni digitali di valore, ivi comprese quelle a loro volta convertibili in altre valute virtuali (c.d. cripto su cripto), accanto ai più tradizionali servizi di cambio da e in valuta avente corso forzoso.

«*Anty Money Laundering in Bitcoin has to deal with imperfect knowledge of identifies, but may exploit perfect knowledge of all transactions*»²⁷. L'icastico asserto sulla natura anfibologica della criptomoneta per eccellenza, tale da compendiare perfetta trasparenza e imperitura registrazione degli oggetti con forme di occultamento (dell'identità dei) soggetti, dal più vulnerabile pseudonimato sino al pieno e irreversibile anonimato, giustifica la separata considerazione dei plausibili benefici che dall'impiego dei bitcoin e, più in generale, della tecnologia Bitcoin / blockchain, possono ridondare a favore dell'intero sistema finanziario, senza eccezione per le politiche di contrasto al riciclaggio dei proventi illeciti e al finanziamento delle attività terroristiche.

Argomentando dalla natura di tecnologia interamente tracciata, dunque totalmente trasparente, impossibile da falsificare e difficile da rubare, uno studio recente ha teorizzato una rivalutazione dei bitcoin come strumento non già per assecondare ma per contrastare i numerosi

²⁶ S. CAPACCIOLI, *op. cit.*, 253 ss.; G. P. ACCINNI, *Regole antiriciclaggio e risvolti penalistici dell'operatività in valute virtuali*, cit., 1519.

²⁷ M. MÖSER, R. BÖHME, D. BREUKER, *An Inquiry into Money Laundering Tools in the Bitcoin Ecosystem*, *ibidem*.

illeciti commessi con il denaro contante²⁸. Nell’asserzione secondo cui la abolizione della moneta legale in favore di un sistema basato su monete digitali in concorrenza tra loro apporterebbe benefici enormi legati alla conseguente superfluità delle banche, alla scomparsa dell’inflazione e delle crisi finanziarie pilotate, alla sparizione di molteplici fattispecie criminose connesse con la circolazione del denaro sembra di sentir riecheggiare le utopie e gli ideali anarcoidi del movimento *Cypherpunk*, ai quali non mancava certo la consapevolezza di plumbee minacce. «Due persone potranno scambiarsi messaggi, fare affari e negoziare contratti in maniera completamente anonima, senza necessità di conoscere il Nome Vero o l’identità legale l’uno dell’altro. [...] Lo Stato cercherà ovviamente di fermare o rallentare lo sviluppo di questa tecnologia, citando problemi di sicurezza nazionale o l’utilizzo di questa tecnologia da parte di narcotraffickanti ed evasori fiscali. Molte di queste preoccupazioni saranno fondate: la criptoanarchia consentirà il libero commercio di segreti di Stato e permetterà anche il commercio di materiali illeciti o addirittura rubati. Un mercato anonimo computerizzato renderà possibile un riprovevole commercio di assassinii ed estorsioni. Criminali ed altri elementi estranei ai nostri valori diventeranno utenti attivi di *CryptoNet*. Ma questo non fermerà la criptoanarchia [...] La criptoanarchia creerà un mercato liquido per ogni tipo di merce possibile»²⁹.

L’innegabile contributo che la nuova “dirompente” tecnologia potrebbe apportare in termini di sicurezza e affidabilità al sistema finanziario rimane legata alla tracciabilità oggettiva della struttura, vale a dire all’accessibilità – completamente o parzialmente pubblica – del *database* sul quale sono state condivise e registrate in maniera

²⁸ Per una disamina dei potenziali benefici riconnessi alla sostituzione della moneta legale con una valuta virtuale si veda G. J. SICIGNANO, *op. cit.*, *passim*, ma in part. 215 ss. Sul funzionamento di tecnologie capaci di disvelare l’identità di chi si celi dietro il codice alfanumerico delle chiavi crittografiche v. P. DE FILIPPI, *The Interplay between Decentralization and Privacy: The Case of Blockchain Technologies*, in *Journal of Peer Production*, Issue n. 7: *Alternative Internets* (<https://ssrn.com/abstract=2852689>).

²⁹ E. HUGHES, *A Cypherpunk’s Manifesto*, 9 March 1993, consultabile al sito <https://activism.net/>; si veda anche S. CAPACCIOLI, *op. cit.*, 40 ss.; P. FRANCO, *Understanding Bitcoin. Cryptography, Engineering and Economics*, Padstow, 2014, 160 ss.; M. ATZORI, *Blockchain Technology and Decentrated Governance: Is the State Still Necessary?*, <https://ssrn.com>.

incancellabile, irretrattabile e immodificabile tutte le transazioni avvenute tra gli utenti – i blocchi – della catena. Solo l'introduzione di un apparato normativo in grado di scongiurare, o quantomeno di ridimensionare, i rischi riconnessi al difetto di tracciabilità soggettiva può tuttavia impedire che i potenziali benefici vengano fatalmente compromessi, annullati dalla creazione dell'ambiente esemplarmente ideale per la commissione dei crimini che si intende prevenire³⁰.

4. *L'indelebile tracciabilità oggettiva nelle operazioni FinTech: il rischio relativo al trattamento indiscriminato dei dati personali*

Il dilemma regolativo posto dal fenomeno *Fintech* non può essere risolto affidandosi interamente alle soluzioni offerte dalla tecnologia, se non al prezzo di una inaccettabile abdicazione ai principî di certezza e salvaguardia degli interessi che ciascun ordinamento reputi meritevoli di protezione: d'altronde, la scelta di imporre controlli capillari tradizionali e di dettare regole stringenti che non tengano conto della strutturale, sfuggente specificità dell'innovazione tecnologica e della sua inarrestabile evoluzione, si rivelerebbe del tutto inadeguata nella pretesa di governare un fenomeno inafferrabile secondo logiche (e categorie) tradizionali³¹. Qualunque regolazione non può dunque prescindere da alcuni caratteri indefettibili: dimensione sovranazionale e transfrontaliera, per assecondare la vocazione globale del fenomeno regolato, consapevolezza e stretta correlazione, seppur non abdicativa, con l'architettura tecnologica e il suo prevedibile progredire, creazione di spazi onde non ostacolarne od imbrigliarne il benefico sviluppo e le

³⁰ Sottolinea la natura duale o anfibologica della tecnologia Blockchain, potenzialmente in grado – allo stato di sviluppo attuale – di prevenire quanto di agevolare la commissione di reati (digitali) a livello globale R. VUOSI, *Blockchain Technology and Digital Crimes*, in A. Borroni (a cura di), *Legal perspective on Blockchain theory, outcomes and outlooks*, Napoli, 2019, 216. Sulle difficoltà teoriche e applicative quando riferite alla AI, si veda P. SEVERINO, *Intelligenza artificiale e diritto penale*, in U. Ruffolo, *op. cit.*, 531 ss.

³¹ «Sorge pur sempre la necessità di disciplinare i comportamenti e le attività al fine di non rendere tutto ciò che è tecnologicamente possibile, solo per questo giuridicamente legittimo»: M. GIULIANO, *La blockchain e gli smart contracts nell'innovazione del diritto del terzo millennio*, in *Dir. inf.*, 2018, 6, 992 ss.

positive ricadute, come riconosciuto anche dalle Istituzioni Europee in funzione della realizzazione del c.d. Mercato Unico Digitale³².

A verificare soluzioni predicabili ed efficienti, soccorre la disamina dell'altro comparto normativo con il quale la tecnologia blockchain / Bitcoin deve essere a posta a raffronto onde valutarne la conciliabilità, ovverosia la disciplina in materia di protezione e trattamento dei dati personali, come formulata dal *GDPR*, acronimo per intendere *General Data Protection Regulation*, vale a dire il Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, che in Italia ha reso necessario l'adeguamento del d. lgs. 30 giugno 2003, n. 196 recante *Codice in materia di protezione dei dati personali*, attuato mediante d. lgs. 10 agosto 2018, n. 101³³.

Sotto un primo angolo di visuale, non possono essere sottovalutate le positive ricadute dello sviluppo della tecnologia blockchain rispetto alla salvaguardia dei dati personali, potendo il suo utilizzo garantire al contempo sicurezza, in termini di integrità e inalterabilità, e corretta gestione, in termini di controllo sull'accessibilità e sulla circolazione,

³² Il 10 aprile 2018, in occasione del *Digital Day*, ventidue paesi membri della Ue hanno sottoscritto un documento d'intesa per la costituzione di un partenariato sulla *blockchain*, con l'obiettivo della creazione del Mercato Unico Digitale (*Declaration – Cooperation on a European Blockchain Partnership*). L'Italia, che non figurava tra i firmatari, ha successivamente aderito, nel corso del mese di settembre del medesimo anno.

³³ Si vedano: D'ANTONIO, G. RICCIO, S. SICA (a cura di), *La nuova disciplina europea della privacy*, Padova 2016; G. FINOCCHIARO (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, 2017; L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/279*, Napoli, 2017; F. PIZZETTI, *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, 2018; R. PANETTA (a cura di), *Circolazione e protezione dei dati personali tra libertà e regole del mercato*, Milano, 2018; N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Padova, 2019; E. TOSI (a cura di), *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Milano, 2019; G. FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d. lgs. 10 agosto 2018, n. 101*, Bologna, 2019; F. COSTA, P. PIZZOLATO (a cura di), *Sicurezza e tecnologia*, Milano, 2017; G. D'ACQUISTO, M. NALDI (a cura di), *Big data e privacy by design. Anonimizzazione, pseudonimizzazione, sicurezza*, Torino, 2017.

secondo una direttrice pienamente coerente con l'impostazione del Regolamento. Non hanno mancato di sottolinearlo con forza le stesse Istituzioni Europee, in particolare il Parlamento che, nella sua *Resolution of 3 october 2018 on distributed ledger technologies and blockchains: building trust with disintermediation* vi ha riconosciuto uno strumento capace di rafforzare l'autonomia dei cittadini dando loro l'opportunità di controllare i propri dati e decidere quali condividere nel registro, nonché la capacità di scegliere chi e come quei dati possa vedere³⁴.

Dal raffronto con la nuova normativa europea plurimi appaiono tuttavia i punti di autentica collisione tra il funzionamento della tecnologia blockchain, la circolazione e la movimentazione delle criptovalute e, più in generale, le operazioni finanziarie ascrivibili all'ambito *FinTech* e le regole intese a garantire un elevato livello di protezione dei dati personali³⁵.

In particolare, la valutazione delle caratteristiche tecnico-funzionali e le strutturali ricadute in punto di tracciabilità si presenta qui rovesciata e antitetica rispetto alla riflessione di ordine penalistico dianzi compiuta. A munire di tetragona guarentigia la *riservatezza* dei dati personali come definiti dall'art. 4 del Regolamento («qualsiasi informazione riguardante una persona fisica identificata o identificabile») è, propriamente, l'elemento che maggiormente concretizza l'incognita criminosa, mentre l'elevato livello di *trasparenza e immutabilità* che da quella allontana rischia di

³⁴ www.europarl.europa.eu (RSP 2017/2772, così il *Considerando A*). In dottrina, si leggano M. FINCK, *Blockchain regulation and Governance in Europe*, Cambridge, 2018, 113 ss.; Y. ZHAO, B. DUNCAN, *The impact of cryptocurrency risks on the use of blockchain for cloud security and privacy*, 2018; M. BERBERICH, M. STEINER, *Blockchain technology and the GDPR: how to reconcile Privacy and Distributed Ledgers?*, *Eur. Data Protection Law Review*, 2016, 425 ss.; G. ZYSKIND, O. NATHAN, A. PENTLAND, *Decentralizing privacy: using blockchain to protect personal data*, in *IEEE CS Security and Privacy Workshops*, 2015. In termini non dissimili, ne sottolineano le potenzialità anche A.M. GAMBINO, C. BOMPRESZI, *Blockchain e protezione dei dati personali*, in *Dir. informaz. e informatica*, 2019, 628 ss.

³⁵ S. CAPACCIOLI, *op. cit.*, 29 ss.; M. BERBERICH, M. STEINER, *op. cit.*, 425 ss.; H. CHANG, *Blockchain: disrupting Data Protection?*, University of Hong Kong Faculty of Law Research Paper, 2017, <https://papers.ssrn.com>; M. GIULIANO, *op. cit.*, 1011 ss.; G. LEMME, *Blockchain, smart contracts, privacy o del nuovo manifestarsi della libertà contrattuale*, in E. Tosi, *op. cit.*, 318 ss.; A.M. GAMBINO, C. BOMPRESZI, *Blockchain e protezione dei dati personali*, *cit.*, 619 ss.

contraddire in maniera irreversibile il programmatico potere di controllo dell'interessato sui suoi dati personali e sulla loro circolazione.

Da un canto, infatti, la non tracciabilità soggettiva, quindi il completo *anonimato* delle parti sottrae i dati ad esse riferibili, eventualmente registrati su piattaforme o condivisi attraverso i “blocchi della catena”, all'area stessa di applicazione del Regolamento, rendendo quindi l'operatività mediante blockchain perfettamente compatibile, in astratto, con la stringente salvaguardia in esso prefigurata (art. 1 Reg. UE 679/2016)³⁶. Di contro, l'imperitura tracciabilità oggettiva delle transazioni – in uno con la natura distribuita, la libera accessibilità e la trasparenza del sistema – minacciano fortemente il diritto dei singoli alla protezione dei dati personali, al controllo sulla loro circolazione e alla limitazione nelle modalità e finalità del trattamento (artt. 5-6-7 Reg.). Confliggono poi con i principi di limitazione della conservazione dei dati «in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati» (art. 5, par. 1, lett. e) Reg.), di rettifica dei dati personali inesatti e di integrazione dei dati incompleti (art. 16 Reg.); infine, di cancellazione senza ingiustificato ritardo dei dati personali allorché non più necessari rispetto alle finalità per le quali sono stati raccolti o trattati, ovvero in caso di revoca del consenso reso per il trattamento, oppure di successiva opposizione, o ancora in ipotesi di trattamento illecito (art. 17 Reg.)³⁷.

La prospettiva adottata dal *GDPR* asseconda il passaggio concettuale che vede la tutela della *privacy* muovere da un modello proprietario, basato sul consenso, verso un modello procedimentale, fondato sul controllo e sulla gestione, privilegiando un approccio pragmatico che mira alla predisposizione di una tutela *ex ante* rispetto

³⁶ V. DEL FEDERICO, A. POPOLI, *Disposizioni generali*, in G. Finocchiaro (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, cit., 65 ss. G. FINOCCHIARO, *Riflessioni su intelligenza artificiale e protezione dei dati personali*, cit., 243 sottolinea tuttavia la natura relativa dello stesso anonimato, così come la qualifica di dato anonimo è a sua volta dinamica e soggetta a verifica continua, condizionata da numerosi variabili e fattori dal momento che si configura in relazione a determinati soggetti, all'evoluzione delle tecnologie o a circostanze specifiche, destinate a mutare di tempo in tempo e caso per caso.

³⁷ Gli utenti possono sempre inserire sulla catena dati incompatibili con quelli precedentemente immessi che, però, rimarrebbero comunque visibili.

alla inesorabile, massiccia, sistematica circolazione anche extraterritoriale dei dati personali³⁸.

A mente dell'art. 25 del Regolamento, una delle principali misure in cui si estrinseca la prevenzione nella protezione dei dati personali è affidata alla regola di *data protection by design*, che si affianca a quella di *data protection by default*. Con la prima espressione si intende l'obbligo di predisporre sin dalla fase della *progettazione* di prodotti e servizi misure tecniche e organizzative adeguate che, tenendo conto dello stato dell'arte e dei costi di attuazione nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, attuino soluzioni in grado di tutelare *ex ante* la riservatezza dei dati e la sicurezza dei singoli. Con la seconda locuzione s'intende invece la predisposizione di misure tecniche e organizzative adeguate che, *per impostazione predefinita*, garantiscano sia la raccolta selettiva esclusivamente dei dati personali necessari in relazione ad ogni specifica finalità del trattamento, sia la prevenzione dall'accessibilità indiscriminata a un numero indefinito di persone fisiche³⁹. La stessa norma ascrive espressamente (e sia pure esemplificativamente: si veda il *Considerando* n. 28) al novero delle misure tecniche e organizzative adeguate a concretizzare la *data protection by design* la *pseudonimizzazione* dei dati: ai sensi dell'art. 4, n. 5 il trattamento

³⁸ E. ROPPO, *Informatica e tutela della privacy e diritti di libertà*, in G. Alpa (a cura di), *Computers e responsabilità civile*, Milano, 1985, 23; A. DI MAJO, *Il trattamento dei dati personali tra diritto sostanziale e modelli di tutela*, in V. Cuffaro, V. Ricciuto, V. Zeno Zencovich (a cura di), *Trattamento dei dati e tutela della persona*, Milano, 1998, 233 ss.; S. MAZZAMUTO, *Il principio del consenso e il potere della revoca*, in R. Panetta (a cura di), *Libera circolazione e protezione dei dati personali*, Milano, 2006, 993 ss.; I. A. CAGGIANO, *Il consenso al trattamento dei dati personali nel nuovo Regolamento europeo. Analisi giuridica e studi comportamentali*, in *Osserv. dir. civ. e comm.*, 2018, 67 ss. La dimensione sovranazionale della disciplina è assicurata da un ambito di applicazione territoriale che *ex art. 3 GDPR* trascende l'Unione Europea, mediante la previsione di una operatività che copre il trattamento dei dati personali degli interessati che si trovino nell'Unione, anche qualora effettuato da un titolare o da un responsabile che non è stabilito nell'Unione (come pure il trattamento anche fuori della UE da parte di un titolare o di un responsabile stabilito nell'Unione).

³⁹ R. D'ORAZIO, *Privacy by design e by default*, in V. D'ANTONIO, G. RICCIO, S. SICA, *op. cit.*, 81 ss.; E. LUCCHINI GUASTALLA, *Privacy e Data protection: principi generali*, in E. Tosi, *op. cit.*, 55 ss.; D. FARACE, *Privacy by design e privacy by default*, *ivi*, 485 ss.

realizzato in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, conservate separatamente e atte a garantire che i dati non siano attribuibili a una persona fisica identificata o identificabile.

La *privacy by design* costituisce un principio giuridico nel quale è racchiuso un paradigma suscettibile di essere esteso oltre i confini segnati dalla protezione dei dati personali: una disciplina che si avvale della tecnologia per disciplinare la tecnologia stessa e che, oltre ad apprestare una forma di tutela preventiva, modulabile in relazione al momento storico e allo stato delle conoscenze e delle applicazioni, recepisce il dato empirico senza farsene sovrastare, sembra in grado di realizzare una convergenza regolativa onde creare un auspicabile quanto necessario quadro uniforme a livello sovranazionale⁴⁰.

L'indicazione non è quella di estendere acriticamente a settori governati da altri principî – per la protezione di altri interessi – un precetto funzionale alla prevenzione di ben individuati e circoscritti rischi, o di ravvisarvi il riscontro compiuto e risolutivamente efficace per ogni situazione in cui l'innovazione tecnologica applicata alla finanza minacci interessi meritevoli di tutela, né tantomeno la scelta per un binomio inscindibile e autosufficiente *Fintech / Regtech*, quanto

⁴⁰ M. C. GAETA, *La protezione dei dati personali nell'Internet of Things: l'esempio dei veicoli autonomi*, in *Dir. informaz. e informatica*, 2018, 147 ss. (ivi 177) parla di tecno-regolamentazione. «La rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali. La portata della condivisione e della raccolta di dati personali è aumentata in modo significativo. La tecnologia attuale consente tanto alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività. Sempre più spesso, le persone fisiche rendono disponibili al pubblico su scala mondiale informazioni personali che le riguardano. La tecnologia ha trasformato l'economia e le relazioni sociali e dovrebbe facilitare ancora di più la libera circolazione dei dati personali all'interno dell'Unione e il loro trasferimento verso paesi terzi e organizzazioni internazionali, garantendo al tempo stesso un elevato livello di protezione dei dati personali. Tale evoluzione richiede un quadro più solido e coerente in materia di protezione dei dati nell'Unione, affiancato da efficaci misure di attuazione, data l'importanza di creare il clima di fiducia che consentirà lo sviluppo dell'economia digitale in tutto il mercato interno. È opportuno che le persone fisiche abbiano il controllo dei dati personali che le riguardano e che la certezza giuridica e operativa sia rafforzata tanto per le persone fisiche quanto per gli operatori economici e le autorità pubbliche». Così, efficacemente e con chiara consapevolezza del fattore tecnologico, i Considerando nn. 6-7 del GDPR.

piuttosto d'intendere la valorizzazione di un modello regolativo dotato di molti dei requisiti indispensabili ad una tutela efficiente e di un promettente grado di elasticità. Nel paradigma *by design* è ravvisabile un significativo rovesciamento di prospettiva nel rapporto tra norma e tecnica: non più la rincorsa a governare l'innovazione da parte del legislatore ma la necessaria, previa, conformità di ogni tecnologia innovativa ai dettami e agli obiettivi dell'ordinamento⁴¹. Le potenzialità espansive del principio di "protezione sin dalla progettazione" sono confermate dal suo riferirsi non solo alle misure tecniche concretamente adottate ma altresì (e ancor prima) agli strumenti e alle tecnologie utilizzate: a mente dell'art. 32, è necessario garantire un livello di sicurezza adeguato al rischio, onde la sicurezza del trattamento non deve essere minacciata dall'impiego di tecnologie che non siano a loro volta conformi ai medesimi standards di sicurezza⁴².

Tra le opzioni per «integrare le tutele nel trattamento» onde realizzare le finalità sottese all'adozione del Regolamento, la norma seleziona, sulla scorta del *Considerando* n. 78 e sia pure esemplificativamente, proprio i processi volti alla minimizzazione e alla pseudonimizzazione dei dati personali: nel primo senso, abilitando il titolare al trattamento dei soli dati dei quali abbia realmente bisogno per raggiungere le finalità divise; nel secondo, attuando modifiche e dissimulazioni atte a rendere non facilmente o non direttamente attribuibili dati sensibili ad una determinata persona fisica⁴³.

Lo *pseudonimato* si differenzia dall'anonimato in quanto il mascheramento dell'identità non è definitivo ma reversibile, consentendo l'identificazione del reale centro di interessi (coloro ai quali i dati personali si riferiscano ovvero le persone, fisiche o giuridiche, che abbiano concluso transazioni in criptovaluta, disponendone o ricevendone) grazie all'utilizzo di elementi ulteriori o «informazioni aggiuntive» con le quali superare la crittografia e associare le chiavi ad una – ed una sola, inequivocabile – identità. Le modalità tecniche di pseudonimizzazione non interrompono la

⁴¹ Cfr. G. SIMEONE, *Machine learning e tutela della privacy alla luce del GDPR*, in G. Alpa (a cura di), *Diritto e intelligenza artificiale*, cit., 288 ss. Cfr. pure M. SEGHESSIO, *Blockchain and Privacy*, in A. Borroni, *op. cit.*, 129 ss.

⁴² G. SIMEONE, *ibidem*.

⁴³ Sulle modalità tecniche di anonimizzazione e pseudonimizzazione dei dati si veda G. D'ACQUISTO, M. NALDI, *op. cit.*, 41 ss. e 117 ss.

concatenazione dei passaggi necessari per il collegamento tra dato e persona, solo ne rendono più o meno complessa e agevolmente ricostruibile l'identificazione. In altri termini «l'associazione biunivoca tra dato e persona non è modificata... e il dato pseudonimo, una volta impiegato in combinazione con tutti i mezzi necessari per effettuare la sostituzione di attributi a ritroso, è inequivocabilmente riferibile alla persona»⁴⁴.

Chiaramente, non ogni dilemma è sciolto, né ogni profilo critico, e neppure esorcizzata ogni minaccia che dalla tecnologia applicata alla finanza possa derivare. Si sono dianzi messe in luce le difficoltà operative e i meccanismi, essi pure tecnologici, di contrasto ad una affidabile re-identificazione: e non v'è dubbio che molta dell'efficacia dipenda dalla disponibilità e dalla facilità di utilizzo, anche in termini di costi e di tempi, delle misure con le quali risalire all'identità degli interessati o delle parti. Misure tecniche di contrasto – alla commissione di crimini o al trattamento illegittimo di dati – destinate ad evolvere insieme alla stessa tecnologia usata a supporto dei fenomeni contrastati, di cui saggiare la ragionevolezza (come sottolineato nel *Considerando* n. 26 del *GDPR*) e delle quali, a fini di prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo, dovrebbero potersi agevolmente avvalere le Unità Nazionali di Informazione Finanziaria, come prescritto dalla Quinta Direttiva UE⁴⁵.

Rimane sullo sfondo, tendenzialmente irrisolvibile, la tensione tra riservatezza e trasparenza, protezione dei dati personali e sicurezza generale, finalità privatistiche di tutela della persona da una parte, prevenzione dei reati e garanzia del sistema finanziario nel suo complesso dall'altra: in un orizzonte prospettico nel quale anche l'identità personale analogica è destinata fatalmente a sfumare verso l'identità digitale. Nello *pseudonimato* – mascheratura atta a rendere non immediatamente intellegibile la perdurante inequivoca corrispondenza tra dato e persona, reversibile perché temperata da adeguate modalità di identificazione a posteriori ove necessario –

⁴⁴ G. D'ACQUISTO, M. NALDI, *op. cit.*, 38.

⁴⁵ A.M. GAMBINO, C. BOMPRESZI, *Blockchain e protezione dei dati personali*, cit., 630, richiamano applicazioni in grado di impedire la moltiplicazione di identità digitali (account) a fronte di un'unica identità analogica (*Sovrin*, *Evernym*) e sistemi di autenticazione destinati a creare una ID, con i propri dati personali, da inserire in blockchain in modo sicuro e inaccessibile (*ShoCard*).

sembrano tuttavia poter convergere finalità di sicurezza e principi di privacy, senza che la salvaguardia dell'una annienti la difesa dell'altra e un insieme di interessi abbia a prevalere sistematicamente sull'altro.

Verosimilmente, il miglior funzionamento della misura tecnica (e del sotteso paradigma regolativo) potrebbe essere garantito dalla previsione della conservazione delle informazioni aggiuntive *off-chain*, rendendole tanto più sicure quanto più affidate a soggetti sottoposti a vigilanza e controllo e a sistemi di *compliance*, come si è visto per *exchangers* e *wallet providers*. In questa prospettiva è altrettanto innegabile che, a differenza delle *permissionless*, le *permissioned blockchain*, nelle quali un'entità o un gruppo di blocchi ha la prerogativa di consentire l'accesso al sistema, ammettendo nuovi nodi a contribuire, possano realizzare un significativo incremento del livello di identificazione (o quanto meno identificabilità) degli utenti⁴⁶.

Riconoscere esclusivamente la liceità dei sistemi a registro distribuito connotati quanto meno da una parziale centralizzazione gerarchica (*permissioned*, *consortium* o privati), ovvero legare sicurezza e riservatezza all'*off-chain* quando non addirittura alla tangibile materialità di dispositivi *off-line*, equivarrebbe tuttavia a negare i fenomeni, non già a disciplinarli.

L'innovazione tecnologica non si arresta e non arretra, e dischiude scenari inediti, taluni rassicuranti talaltri minacciosi: di certo ostici ed ostili se si pretenda di continuare ad interpretare il mondo con categorie adusate. «La rivelazione finale della fragilità di ogni cosa. Vecchie e spinose questioni si erano risolte in tenebre e nulla. L'ultimo esemplare di una cosa si porta con sé la categoria. Spegne la luce e scompare».⁴⁷

⁴⁶ A.M. GAMBINO, C. BOMPRESZI, *Blockchain e protezione dei dati personali*, cit., 627 ss. e 632 ss. Diversamente orientata F. FAINI, *Il diritto nella tecnica: tecnologie emergenti e nuove forme di regolazione* in *Federalismi.it*, 16, 2020, 79 ss.

⁴⁷ C. MC CARTHY, *La strada*, Einaudi, Torino, 2007, trad. M. Testa, 22.