Riciclaggio, autoriciclaggio (...ed altro ancora) nel tempo della moneta virtuale e della cybersicurezza[1]

di Giovanni Diotallevi

presidente di sezione della Corte di cassazione

Sommario: 1. Premessa. – 2. Le valute virtuali e i rischi connessi alla loro utilizzazione. – 3. Segue: in particolare le operazioni di riciclaggio e di autoriciclaggio. – 4. Segue: Le valute virtuali e la finalità di investimento. – 5. Segue: Gli acquisti in criptovaluta e la loro idoneità ad ostacolare l'individuazione della provenienza illecita del denaro nei reati di riciclaggio, impiego di denaro beni o utilità di provenienza illecita, di autoriciclaggio. Il reato di cui all'art. 166 TUF. – 6. Segue: Autoriciclaggio e il delitto di trasferimento fraudolento di valori. – 7. L'operazione di finanziamento del terrorismo: analogie e differenze rispetto all'operazione di riciclaggio (e autoriciclaggio). 8. Problemi in tema di oneri probatori; in particolare in relazione alla tracciabilità delle operazioni. – 9. Segue: Il controllo sulle modalità di raccolta delle prove da parte dell'autorità straniera: gli algoritmi utilizzati dall'A.G. – 10. Valutazioni conclusive (...assolutamente parziali e provvisorie).

1. Premessa

Il contrasto del riciclaggio di capitali illeciti, e dell'autoriciclaggio in particolare, nell'era digitale costituisce uno dei settori della disciplina penale dove lo sviluppo normativo è costantemente sollecitato da interventi sistematici del Legislatore sovranazionale[2], come quelli collegati alla natura ed estensione degli specifici reati presupposti (in particolare il riferimento va ai reati fiscali), all'ingresso nell'economia delle valute virtuali e alla natura dei beni interessati dalle operazioni di

[1] L'articolo costituisce la rielaborazione della relazione: "*La tracciabilità delle monete virtuali ai fini della configurabilità del delitto di autoriciclaggio"* svolta nel corso organizzato dalla S.S.M. -Struttura territoriale della formazione decentrata di Palermo, Agrigento e Caltanissetta il 20 e 21 settembre 2024, "*In memoria del giudice Rosario Livatino"*, in materia di: "*Intelligenza artificiale: sicurezza, trasparenza, conservazione e uso dei dati. Problematiche relative all'individuazione delle responsabilità penali e dei movimenti di denaro nel ciber spazio. L'informatizzazione del processo e la giustizia predittiva"*.

[2] A partire dal d.lgs. n. 195/2021 che ha modificato le norme incriminatrici in tema di riciclaggio (artt. 648-bis, 648-ter, 648-ter 1 c.p.), ampliando la platea dei reati presupposto anche ai reati colposi ed alla maggior parte dei reati contravvenzionali, più recentemente in data 19 giugno 2024, è stato pubblicato nella Gazzetta Ufficiale dell'Unione Europea il c.d. "AML Package", ovvero il pacchetto di riforma della disciplina dell'antiriciclaggio e del contrasto al finanziamento del terrorismo, composto dalla Direttiva (UE) 2024/1640 (c.d. VI Direttiva Antiriciclaggio), dal Regolamento (UE) 2024/1624 (Regolamento Antiriciclaggio) e dal Regolamento (UE) 2024/1620 (Regolamento AMLA). In particolare il Regolamento si prefigge l'obiettivo di garantire la tracciabilità dei trasferimenti di cripto attività, al fine di prevenire il riciclaggio di denaro, stoppando le transazioni sospette. In tal senso, infatti, il regolamento MiCA (Markets-in-Crypto-Assets Regulation) va ad introdurre un quadro giuridico completo ed armonico in tutta Europa, e riguarderà diverse attività come: l'emissione e la negoziazione di cripto-asset, l'autorizzazione e la vigilanza dei fornitori di servizi di cripto-asset e degli emittenti di token con riferimento ad asset e moneta elettronica, la protezione dei consumatori e la prevenzione degli abusi di mercato. Il testo concordato comprende misure contro la manipolazione del mercato (fondamentali sono le norme per prevenire non solo il riciclaggio di denaro, ma anche il finanziamento del terrorismo e altre attività criminali) ed estende ai trasferimenti di cripto attività la c.d. "travel rule", cioè la regola, comune in ambito antiriciclaggio, che prevede che le informazioni sull'origine e sul beneficiario finale dei cripto-asset "viaggino" con la transazione, e che queste siano conservate da entrambi i partecipanti al trasferimento. Ciò significa che chiunque effettui un trasferimento di cripto-asset dovrà fornire tali informazioni per garantire la tracciabilità delle transazioni. Tuttavia, le norme non si applicheranno ai trasferimenti da persona a persona effettuati senza l'intervento di un fornitore di servizi finanziari. Pertanto i trasferimenti diretti tra individui o tra fornitori di servizi di cripto-attività saranno esclusi dall'obbligo di fornire informazioni sull'origine e sul beneficiario finale della transazione. Inoltre alcuni trasferimenti di cripto-asset comportano specifici fattori di elevato rischio in tema di riciclaggio di denaro, finanziamento del terrorismo e altre attività criminali ed *"in particolare i trasferimenti relativi a prodotti, transazioni o tecnologie progettati per migliorare l'anonimato, compresi i mixer o i tumblers (non opera cioè solo con portafogli propri, ma utilizza, a sua volta, svariati strumenti di valuta elettronica, come se fosse un vero e proprio "fondo" di bitcoin.").*

riciclaggio e autoriciclaggio, al rapporto con la nozione di provento, alla natura transnazionale delle forme di più difficile interpretazione e ai rapporti con reati contigui, come la fattispecie di cui all'art. 512 bis c.p., nel quadro di un'analisi comparata estesa, quantomeno, al contesto europeo.

Si tratta, dunque di una materia particolarmente complessa perché richiede un approccio multilivello non solo tra i vari settori propriamente giuridici, ma anche dell'economia e della finanza; un dato che richiama la necessità di una analisi articolata rispetto alla prevenzione dei fenomeni di riciclaggio, autoriciclaggio e di finanziamento del terrorismo, in particolare, in vista dell'entrata in vigore del pacchetto AML dell'Unione Europea, alla regolamentazione dei mercati, sino ai presidi punitivi e agli strumenti investigativi applicabili per le più gravi manifestazioni di rottura della disciplina normativa.

L'incidenza che l'applicazione delle nuove tecnologie spiega sui sistemi di regolazione delle transazioni finanziarie, unitamente alle conseguenze che la trasformazione digitale innesca sui criteri della disciplina dell'antiriciclaggio, valorizza il valore specifico dell'attività di prevenzione, in particolare della Guardia di finanza e dell'UIF oltre che dell'EPPO e degli uffici requirenti nazionali nonché il ricorso alla cooperazione giudiziaria transnazionale in particolare, anche con riferimento all'adozione dei provvedimenti di congelamento e di confisca e al reciproco riconoscimento dei medesimi[3].

2. Le valute virtuali e i rischi connessi alla loro utilizzazione

Ogni valuta virtuale ha propri meccanismi di funzionamento; tuttavia, tali valute hanno una serie di caratteristiche comuni in quanto:

- sono create da un emittente privato (nel caso delle cc.dd. valute centralizzate) o, in via diffusa, da utenti che utilizzano software altamente sofisticati (nel caso delle cc.dd. valute decentralizzate);

- non sono fisicamente detenute dall'utente, ma sono movimentate attraverso un conto personalizzato noto come "portafoglio elettronico" (cd. *e-wallet*), che si può salvare sul proprio computer o su uno smartphone, o che può essere consultato via internet, al quale si accede grazie ad una password (questi portafogli elettronici sono generalmente software, sviluppati e forniti da appositi soggetti, i c.d. *wallet providers*; esistono poi delle piattaforme di scambio, che offrono il servizio di conversione delle valute virtuali convertibili in moneta legale;

- possono essere acquistate con moneta tradizionale su una piattaforma di scambio ovvero ricevute online direttamente da qualcuno che le possiede, per poi essere detenute su un "portafoglio elettronico": [4]

- i titolari dei portafogli elettronici e i soggetti coinvolti nelle transazioni rimangono generalmente anonimi;

- le transazioni tramite le quali vengono trasferite sono tecnicamente irreversibili[5].

---

[3] Si fa riferimento agli strumenti di cooperazione, conseguenti all'emanazione del regolamento (UE) 2023/2844 del Parlamento europeo e del Consiglio, del 13 dicembre 2023, relativo alla digitalizzazione della cooperazione giudiziaria e dell'accesso alla giustizia anche in materia penale transfrontaliera e recante la modifica di determinati atti nel settore della cooperazione giudiziaria, e alla Direttiva 2014/41/UE del Parlamento europeo e del Consiglio, del 3 aprile 2014, relativa all'ordine europeo di indagine penale (OEI) e il Regolamento (UE) 2018/1805 del Parlamento europeo e del Consiglio, del 14 novembre 2018, relativo al riconoscimento reciproco dei provvedimenti di congelamento e dei provvedimenti di confisca nonché al recentissimo d.lgs. 4 settembre 2024, n. 138, in G.U 1.10.2024 sulla Cybersicurezza in ordine al quale v. *amplius sub* § 9, pag. 43.

[4] Utilizzando questo portafoglio i titolari possono effettuare acquisti presso esercizi commerciali o persone fisiche che accettano le valute virtuali, effettuare rimesse in favore di altri soggetti titolari di portafogli di valute virtuali, nonché riconvertirle in moneta legale.

[5] La Banca d'Italia ha stimato che le valute virtuali siano oltre 400 nel mondo, e che molte di queste valute virtuali hanno smesso di operare poco dopo essere state lanciate, con rilevanti perdite per gli utilizzatori. Con la conseguenza che l'acquisto, il possesso o lo scambio di valute virtuali possono comportare rischi significativi, soprattutto per coloro che ne fanno uso, senza disporre di un'adeguata conoscenza del fenomeno e consapevolezza dei rischi connessi.

In Italia, l'acquisto, l'utilizzo e l'accettazione in pagamento delle valute virtuali devono allo stato ritenersi *attività lecite*: le parti sono *libere di obbligarsi* a corrispondere somme, anche non espresse in valute aventi corso legale.

Tuttavia, le attività di emissione di valuta virtuale, conversione di moneta legale in valute virtuali e viceversa e gestione dei relativi schemi operativi possono rappresentare, nell'ordinamento nazionale, la violazione di disposizioni normative, penalmente sanzionate, che riservano l'esercizio della relativa attività ai soli soggetti legittimati [6].

La giurisprudenza della Corte di Cassazione ha sottolineato che "*In tema di intermediazione finanziaria, la vendita "on line" di moneta virtuale, pubblicizzata quale forma di investimento per i risparmiatori, è attività soggetta agli adempimenti previsti dalla normativa in materia di strumenti finanziari di cui agli artt. 91 e seguenti del TUF, la cui omissione integra il reato previsto dall'art. 166, comma 1, lett. c), TUF*" (Sez. 2 , Sentenza n. 44378 del 26/10/2022; in senso conforme anche Cass. 26807/2020) [7].

La CONSOB, infatti, esercita i poteri previsti relativi alla tutela degli investitori nonché all'efficienza e alla trasparenza del mercato, del controllo societario e del mercato dei capitali, nel caso in cui la vendita di bitcoin venga reclamizzata come una vera e propria proposta di investimento, attività soggetta agli adempimenti di cui agli artt. 91 e seguenti TUF, la cui omissione integra pertanto la sussistenza del sopra ricordato reato di cui all'art. 166 comma 1 lett. c) TUF .

In assenza di obblighi informativi e di presidi di trasparenza tipizzati dal legislatore (fatta salva sempre la possibile applicazione della normativa protettiva in caso di intervento di intermediari finanziari nelle già ricordate transazioni e l'applicazione della normativa penalistica da ultimo menzionata), potrebbe risultare difficile reperire indicazioni affidabili per comprendere il funzionamento, i costi, il valore e i rischi di ciascun tipo di valuta virtuale.

L'acquisto, lo scambio e l'utilizzo di valute virtuali non sono assistiti da tutele legali e/o contrattuali analoghe a quelle che accompagnano le operazioni in valuta legale.

La Financial Action Task Force (FATF), preposta al contrasto del riciclaggio di denaro e del finanziamento del terrorismo, ha pubblicato un documento sull'argomento, che descrive le caratteristiche e gli attori coinvolti nei sistemi di valute virtuali.
L'Autorità Bancaria Europea (EBA) ha emanato un'avvertenza per i consumatori che utilizzano valute virtuali: in alcuni paesi esse sono state esplicitamente vietate; in altri sono state previste alcune forme di regolamentazione.

[6] V. gli artt. 130, 131 TUB per l'attività bancaria e l'attività di raccolta del risparmio; art. 131 ter TUB per la prestazione di servizi di pagamento; art. 166 TUF, per la prestazione di servizi di investimento.

[7] Nella sentenza n. 44378 /2022 è stato infatti precisato che, per quanto concerne i "soggetti che operano nell'ambito delle valute virtuali, si deve rilevare che per *exchanger* si intende il soggetto che gestisce le piattaforme *exchange,* intendendosi per *exchange* la piattaforma tecnologica che permette di scambiare questo prodotto finanziario, la cui funzione, quindi, è quella di poter permettere di effettuare l'acquisto e la vendita delle criptovalute e di realizzare un profitto; sono stati inclusi i "prestatori di servizi relativi all'utilizzo di valuta virtuale" tra i cc.dd. soggetti obbligati (art. 3, comma 5, lett. i), D.Lgs. n. 231/07) e la relativa imposizione di iscriversi in apposito registro tenuto presso l'OAM - Organismo competente in via esclusiva ed autonoma per la gestione degli Elenchi degli Agenti in attività finanziaria e dei Mediatori creditizi - con relativo obbligo di comunicazione al Ministero Economia e Finanze (art.17 bis, comma 8 bis, D.Lgs. n. 141/2010): con la IV e la V Direttiva UE Antiriciclaggio, recepite rispettivamente con il d.lgs. n. 90/2017 e con il d.lgs. n. 125/2019, sono stati previsti specifici obblighi nei confronti dell'exchanger (cambiavalute di bitcoin et similia, definiti come ogni persona fisica o giuridica che fornisce a terzi, a titolo professionale, anche online, servizi funzionali all'utilizzo, allo scambio, alla conservazione di valuta virtuale e alla loro conversione da, ovvero in, valute aventi corso legale o in rappresentazioni digitali di valore, ivi comprese quelle convertibili in altre valute virtuali nonché i servizi di emissione, offerta, trasferimento e compensazione e ogni altro servizio funzionale all'acquisizione, alla negoziazione o all'intermediazione nello scambio delle medesime valute, art. 1, comma 2, lett. ff, d.lgs. n. 231/2007) e del wallet provider (gestori di portafogli virtuali, definiti come 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, art. 1, comma 2, lett. ff bis)), entrambi inseriti nella categoria "altri operatori non finanziari".

Come già evidenziato le transazioni in valuta virtuale sono generalmente irreversibili, spesso non sono supportate da un contratto né da procedure di reclamo e le controparti sono anonime.[8]

L'accettazione di valute virtuali da parte dei fornitori di beni e servizi si basa sulla loro discrezionalità e/o su accordi che possono cessare in qualsiasi momento e senza alcun preavviso con grande aleatorietà del loro valore e della possibile utilizzazione delle somme detenute per scopi programmati.

In questo quadro l'aspetto che interessa più concretamente è quello relativo alla circostanza che la rete di valute virtuali può prestarsi a essere utilizzata per transazioni connesse ad attività criminali, incluso il riciclaggio di denaro dove, nonostante la visibilità delle transazioni in valuta, i titolari dei portafogli elettronici e, più in generale, le parti coinvolte possono, come sottolineato, rimanere anonimi. Ciò può rendere necessario l'intervento delle autorità per "chiudere" le piattaforme di scambio impedendo l'accesso o l'utilizzo di eventuali fondi custoditi presso di esse. E' questa la ragione per cui le valute virtuali non sono considerabili economicamente "valute" o "monete", ma ormai possono essere considerate "beni", in quanto cose che possono formare oggetto di diritti, secondo la definizione data dall'art. 810 cod. civ.[9]

La scelta del legislatore europeo di ritenere la valuta virtuale come un "bene", cui attribuire un valore specifico, appare assolutamente funzionale alla disciplina normativa dell'antiriciclaggio e dell'antiterrorismo, proprio perché il "bene" risulta tesaurizzabile e utilizzabile all'occasione come mezzo di scambio, nonostante la stessa valuta virtuale non abbia lo status giuridico di una "valuta" o di una "moneta" secondo gli ordinari parametri economico - finanziari.

Con la pubblicazione in Gazzetta Ufficiale della legge 28 giugno 2024, n. 90 recante «*Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici*», entrata in vigore il 17 luglio 2024, il legislatore ha inasprito la risposta sanzionatoria in teme di reati informatici anche nell'ottica di una attività di prevenzione rispetto alla consumazione di altre fattispecie come il riciclaggio e l'auto riciclaggio e altri aspetti concernenti la sicurezza pubblica.

Sono state introdotte modifiche al codice penale finalizzate a un inasprimento della risposta sanzionatoria in relazione ad alcuni reati, tra cui quelli di agli artt. 615-*ter* c.p. (accesso abusivo a un sistema informatico o telematico), 615-*quater* c.p. (detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici), 617-*bis* c.p. (detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni o conversazioni telegrafiche o telefoniche), 617-*quater* c.p. (intercettazione, impedimento o interruzione illecita di comunicazioni

---

[8] In ogni caso, la mancanza di definizioni, di standard legali e di obblighi informativi rende difficile provare in giudizio di aver subito un danno ingiusto. E' anche possibile che l'utilizzo o la conversione di valute virtuali siano soggetti a costi e commissioni non chiaramente indicati. Inoltre, l'emissione e la gestione di valute virtuali, compresa la conversione in moneta tradizionale, sono attività non soggette a vigilanza da parte della Banca d'Italia né di alcuna altra autorità in Italia. Peraltro, in caso di condotta fraudolenta, di fallimento o cessazione di attività delle piattaforme di scambio non esistono tutele normative specifiche atte a coprire le perdite subite. Analogamente, per le somme in valuta virtuale depositate presso terzi non operano i tradizionali strumenti di tutela, quali i sistemi di garanzia dei depositi, senza contare che la valuta virtuale archiviata nel "portafoglio elettronico" potrebbe andare persa a seguito di malfunzionamenti o attacchi informatici. Anche in caso di smarrimento della password del portafoglio elettronico la perdita potrebbe essere permanente, in quanto non esistono autorità centrali che registrano le password o ne emettono altre sostitutive (cfr. http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-keydefinitions-and-potential-aml-cft-risks.pdf).

[9] A questa definizione è giunto il legislatore europeo nella Direttiva (UE) 2018/843 del Parlamento europeo e del Consiglio del 30 maggio 2018 (c.d. V Direttiva antiriciclaggio) che ha modificato la Direttiva (UE) 2015/849 del Parlamento europeo e del Consiglio del 20 maggio 2015 relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo (cd. IV Direttiva antiriciclaggio).
Il legislatore europeo (art. 1 della V Direttiva antiriciclaggio che ha introdotto nell'elenco delle definizioni di cui all'art. 3, il punto n. 18) ha infatti definito le valute virtuali ai fini dell'uso delle stesse per operazioni di riciclaggio o finanziamento del terrorismo come la rappresentazione di un valore in forma digitale "che non è emessa o garantita da una banca centrale o da un ente pubblico, non è necessariamente legata a una valuta legalmente istituita, non possiede lo status giuridico di valuta o moneta, ma è accettata da persone fisiche e giuridiche come mezzo di scambio e può essere trasferita, memorizzata e scambiata elettronicamente".

informatiche o telematiche), 617-*quinquies* c.p. (detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche), 617-*sexies* c.p. (falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche).

Sono state poi aggiunte interpolazioni al codice di procedura penale tese a estendere alle fattispecie di criminalità informatica più gravi talune delle previsioni processuali riservate ai reati di maggiore allarme sociale. Gli interventi hanno riguardato, tra l'altro, la modifica dell'art. 51, comma 3-*quinquies*, c.p.p., con l'integrazione dell'elenco dei reati informatici rispetto a cui le funzioni di pubblico ministero in primo grado sono svolte dalla procura distrettuale[10].

---

[10] Le funzioni di pubblico ministero sono esercitate:
a) nelle indagini preliminari e nei procedimenti di primo grado, dai magistrati della procura della Repubblica presso il tribunale;
b) nei giudizi di impugnazione dai magistrati della procura generale presso la corte di appello o presso la corte di cassazione.
2. Nei casi di avocazione, le funzioni previste dal comma 1 lettera a) sono esercitate dai magistrati della procura generale presso la Corte di appello.
Nei casi di avocazione previsti dall'articolo 371 -bis, sono esercitate dai magistrati della Direzione nazionale antimafia e antiterrorismo.
3. Le funzioni previste dal comma 1 sono attribuite all'ufficio del pubblico ministero presso il giudice competente a norma del capo II del titolo I.
3 -bis. Quando si tratta dei procedimenti per i delitti, consumati o tentati, di cui agli articoli 416, sesto e settimo comma, 416, realizzato allo scopo di commettere taluno dei delitti di cui agli articoli 12, commi 1, 3 e 3 -ter , e 12 -bis del testo unico delle disposizioni concernenti la disciplina dell'immigrazione e norme sulla condizione dello straniero, di cui al decreto legislativo 25 luglio 1998, n. 286, 416, realizzato allo scopo di commettere delitti previsti dagli articoli 473 e 474, 517 -qua ter ,600, 601, 602, 416 -bis , 416 -ter , 452 -quaterdecies e 630 del codice penale, per i delitti commessi avvalendosi delle condizioni previste dal predetto articolo 416 -bis ovvero al fine di agevolare l'attività delle associazioni previste dallo stesso articolo, nonché per i delitti previsti dall'articolo 74 del testo unico approvato con decreto del Presidente della Repubblica 9 ottobre 1990, n. 309, dall'articolo 291 -quater del testo unico approvato con decreto del Presidente della Repubblica 23 gennaio 1973, n. 43, le funzioni indicate nel comma 1 lettera a) sono attribuite all'ufficio del pubblico ministero presso il tribunale del capoluogo del distretto nel cui ambito ha sede il giudice competente.
3 -ter. Nei casi previsti dal comma 3 -bis e dai commi 3 -quater e 3 -quinquies, se ne fa richiesta il procuratore distrettuale, il procuratore generale presso la corte di appello può, per giustificati motivi, disporre che le funzioni di pubblico ministero per il dibattimento siano esercitate da un magistrato designato dal procuratore della Repubblica presso il giudice competente.
3 -quater. Quando si tratta di procedimenti per i delitti consumati o tentati con finalità di terrorismo le funzioni indicate nel comma 1, lettera a) , sono attribuite all'ufficio del pubblico ministero presso il tribunale del capoluogo del distretto nel cui ambito ha sede il giudice competente.
3 -quinquies. Quando si tratta di procedimenti per i delitti, consumati o tentati, di cui agli articoli 414 -bis , 600 -bis , 600 -ter , 600 -quater , 600 -quater .1, 600 -quinquies , 609 -undecies , 615 -ter , 615 -quater , 617 -bis , 617 -ter , 617 -quater , 617 -quinquies , 617 -sexies , 635 -bis , 635 -ter , 635 -quater , 635 -quater .1, 635 -quinquies , 640 -ter e 640 -quinquies del codice penale, o per il delitto di cui all'articolo 1, comma 11, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, le funzioni indicate nel comma 1, lettera a) , del presente articolo sono attribuite all'ufficio del pubblico ministero presso il tribunale del capoluogo del distretto nel cui ambito ha sede il giudice competente.».
«Art. 406 (Proroga dei termini). — 1. Il pubblico ministero, prima della scadenza, può richiedere al giudice, quando le indagini sono complesse, la proroga del termine previsto dall'articolo 405. La richie sta contiene l'indicazione della notizia di reato e l'esposizione dei motivi che la giustificano.
2. La proroga può essere autorizzata per una sola volta e per un tempo non superiore a sei mesi.
2 -bis .
2 -ter .
3. La richiesta di proroga è notificata, a cura del giudice, con l'avviso della facoltà di presentare memorie entro cinque giorni dalla notificazione, alla persona sottoposta alle indagini nonché alla persona offesa dal reato che, nella notizia di reato o successivamente alla sua presentazione, abbia dichiarato di volere esserne informata. Il giudice provvede entro dieci giorni dalla scadenza del termine per la presenta zione delle memorie. 4. Il giudice autorizza la proroga del termine con ordinanza emessa in camera di consiglio senza intervento del pubblico ministero e dei difensori.
5. Qualora ritenga che allo stato degli atti non si debba con cedere la proroga, il giudice, entro il termine previsto dal comma 3 secondo periodo, fissa la data dell'udienza in camera di consiglio e ne fa notificare avviso

3. *Segue:* in particolare le operazioni di riciclaggio e di autoriciclaggio

Le operazioni di riciclaggio, o, *mutatis mutandis,* di autoriclaggio o di autoriciclaggio e riciclaggio in concorso[11] , vengono realizzate in genere da chi ha la necessità di nascondere la reale titolarità del

al pubblico ministero, alla persona sottoposta alle indagini nonché, nella ipotesi prevista dal comma 3, alla per sona offesa dal reato. Il procedimento si svolge nelle forme previste dall'articolo 127.
5 -bis . Le disposizioni dei commi 3, 4 e 5 non si applicano se si procede per taluno dei delitti indicati nell'articolo 51 comma 3 -bis e nell'articolo 407, comma 2, lettera a) , numeri 4), 7 -bis e 7 -ter) . In tali casi, il giudice provvede con ordinanza entro dieci giorni dalla presentazione della richiesta, dandone comunicazione al pubblico ministero.
6. Se non ritiene di respingere la richiesta di proroga, il giudice autorizza con ordinanza il pubblico ministero a proseguire le indagini.
7. Con l'ordinanza che respinge la richiesta di proroga, il giu
dice, se il termine per le indagini preliminari è già scaduto, fissa un termine non superiore a dieci giorni per la formulazione delle richieste del pubblico ministero a norma dell'articolo 405. 8. Gli atti di indagine compiuti dopo la presentazione della richiesta di proroga e prima della comunicazione del provvedimento del giudice sono comunque utilizzabili sempre che, nel caso di provvedi mento negativo, non siano successivi alla data di scadenza del termine originariamente previsto per le indagini.».
«Art. 407 (Termini di durata massima delle indagini preliminari).
— 1. Salvo quanto previsto all'articolo 393 comma 4, la durata delle indagini preliminari non può comunque superare diciotto mesi o, se si procede per una contravvenzione, un anno. 2. La durata massima è tuttavia di due anni se le indagini preliminari riguardano: a) i delitti appresso indicati:
1) delitti di cui agli articoli 285, 286, 416 -bis e 422 del co dice penale, 291 -ter , limitatamente alle ipotesi aggravate previste dalle lettere a) , d) ed e) del comma 2, e 291 -quater , comma 4, del testo unico approvato con decreto del Presidente della Repubblica 23 gennaio 1973, n. 43;
2) delitti consumati o tentati di cui agli articoli 575, 628, terzo comma, 629, secondo comma, e 630 dello stesso codice penale;
3) delitti commessi avvalendosi delle condizioni previste dall'articolo 416 -bis del codice penale ovvero al fine di agevolare l'attività delle associazioni previste dallo stesso articolo;
4) delitti commessi per finalità di terrorismo o di eversione dell'ordinamento costituzionale per i quali la legge stabilisce la pena della reclusione non inferiore nel minimo a cinque anni o nel massimo a dieci anni, nonché delitti di cui agli articoli 270, terzo comma e 306, secondo comma, del codice penale;
5) delitti di illegale fabbricazione, introduzione nello Stato, messa in vendita, cessione, detenzione e porto in luogo pubblico o aperto al pubblico di armi da guerra o tipo guerra o parti di esse, di esplosivi, di armi clandestine nonché di più armi comuni da sparo escluse quelle previste dall'articolo 2, comma terzo, della legge 18 aprile 1975, n. 110;
6) delitti di cui agli articoli 73, limitatamente alle ipotesi aggravate ai sensi dell'articolo 80, comma 2, e 74 del testo unico delle leggi in materia di disciplina degli stupefacenti e sostanze psicotrope, prevenzione, cura e riabilitazione dei relativi stati di tossicodipendenza, approvato con decreto del Presidente della Repubblica 9 ottobre 1990, n. 309, e successive modificazioni;
7) delitto di cui all'articolo 416 del codice penale nei casi in cui è obbligatorio l'arresto in flagranza;
7 -bis) dei delitti previsto dagli articoli 600, 600 -bis , primo comma, 600 -ter , primo e secondo comma, 601, 602, 609 -bis nelle ipotesi aggravate previste dall'articolo 609 -ter , 609 -quater , 609 -octies del codice penale, nonché dei delitti previsti dagli articoli 12, comma 3, e 12 -bis del testo unico di cui al decreto legislativo 25 luglio 1998, n. 286, e successive modificazioni;
7 -ter) delitti previsti dagli articoli 615 -ter , 615 -quater , 617 - ter , 617 -quater , 617 -quinquies , 617 -sexies , 635 -bis , 635 -ter , 635 -qua ter , 635 -quater .1 e 635 -quinquies del codice penale, quando il fatto è commesso in danno di sistemi informatici o telematici di interesse mili tare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico.
b) notizie di reato che rendono particolarmente complesse le investigazioni per la molteplicità di fatti tra loro collegati ovvero per l'elevato numero di persone sottoposte alle indagini o di persone offese;
c) indagini che richiedono il compimento di atti all'estero;
d) procedimenti in cui è indispensabile mantenere il collegamento tra più uffici del pubblico ministero a norma dell'articolo 371.
3. Salvo quanto previsto dall'articolo 415- bis, non possono essere utilizzati gli atti di indagine compiuti dopo la scadenza del termine per la conclusione delle indagini preliminari stabilito dalla legge o pro rogato dal giudice.

[11] Cass., Sez. 2 -, Sentenza n. 13795 del 07/03/2019 - 29/03/2019 , *CED* 275528 In tema di autoriciclaggio, l'ipotesi di non punibilità di cui all'art. 648-ter.1, comma quarto, cod. pen. è integrata soltanto nel caso in cui l'agente utilizzi o goda dei beni provento del delitto presupposto in modo diretto e senza compiere su di essi

bene, di comportarsi in modo tale da realizzare nel grado più elevato la diminuzione ovvero l'azzeramento del rischio, con comportamenti funzionali a eludere completamente o comunque in misura rilevante la possibilità che l'intero prezzo o la refurtiva, ancorché convertiti, siano intercettati e di nascondere l'origine criminale dei fondi utilizzati per acquistare una valuta virtuale o l'origine criminale della valuta stessa.

Una scelta favorita dalle ingenti somme che possono avere a disposizione le associazioni criminali e dal fatto che l'attività di riciclaggio e/o di autoriciclaggio, può attendere il momento propizio per la sua esecuzione, proprio perché il trascorrere del tempo scolora l'origine delittuosa del bene stesso[12].

---

alcuna operazione atta ad ostacolare concretamente l'identificazione della loro provenienza delittuosa.; in dottrina v. Apollonio Andrea, *La tipicità del delitto di autoriciclaggio: alcuni chiarimenti della Cassazione tesi alla piena effettività della norma*, in *CP* , 2019,2928;
In tema di autoriciclaggio, il soggetto che, non avendo concorso nel delitto-presupposto non colposo, ponga in essere la condotta tipica di autoriciclaggio o contribuisca alla realizzazione da parte dell'autore del reato - presupposto delle condotte indicate dall'art. 648-ter.1 cod.pen., risponde di riciclaggio e non di concorso nel delitto di autoriciclaggio essendo questo configurabile solo nei confronti dell'intraneus. (Sez. 2, Sentenza n. 17235 del 17/01/2018 Ud. (dep. 18/04/2018) Rv. 272652 – 01);
In tema di autoriciclaggio, il soggetto che, non avendo concorso nel delitto-presupposto non colposo, ponga in essere la condotta tipica di autoriciclaggio o contribuisca alla realizzazione da parte dell'autore del reato-presupposto delle condotte indicate dall'art. 648-ter.1 cod.pen., risponde di riciclaggio e non di concorso nel delitto di autoriciclaggio essendo quest'ultimo configurabile solo nei confronti dell' "intraneus". (Fattispecie in cui l'imputata aveva versato su un libretto di deposito di una cooperativa di consumo, e poi prelevato mediante assegni, denaro provento dell'attività concussiva attuata dal marito). (Sez. 6 - , Sentenza n. 3608 del 07/06/2018 Ud. (dep. 24/01/2019) Rv. 275288 – 01
Integra il reato di riciclaggio la condotta di colui che, non avendo concorso nel delitto presupposto non colposo, contribuisca alla realizzazione del delitto di autoriciclaggio da parte dell'autore del delitto-presupposto, in quanto il reato di cui all'art. 648-ter.1 cod. pen. è configurabile solo nei confronti dell'"intraneus". (Fattispecie in cui l'imputato, dopo la commissione, da parte di un terzo, del delitto di peculato di prodotti destinati alla distribuzione gratuita, secondo le norme dell'Unione europea, concorreva con il predetto ad ostacolare l'accertamento della provenienza delittuosa di tale merce che, dopo la sostituzione dei contrassegni identificativi, veniva reimmessa nei circuiti commerciali). (Sez. 2, Sentenza n. 16519 del 22/12/2020 Ud. (dep. 30/04/2021) Rv. 281596 – 01.

[12] Il reato di riciclaggio è stato introdotto nel nostro ordinamento dal d.l. 21 marzo 1978, n. 59 conv. nella I. 18 maggio 1978 n. 191, che inserisce nel codice penale l'art. 648-bis c.p. con la rubrica "Sostituzione di denaro o di valori provenienti da rapina aggravata o sequestro di persona a scopo di estorsione". Si trattava, come osservato dalla dottrina, di una tipica figura di reato a consumazione anticipata, con il quale venivano puniti gli atti diretti a sostituire denaro proveniente da quegli unici tre delitti individuati dal legislatore, non essendo necessario, ai fini della consumazione del reato, l'avvenuta effettiva sostituzione del denaro (cfr., Sez. II, n. 13155 del 15/4/1986, Ghezzi, Rv. 174381; Sez. II, n. 2851 del 5/12/1991, dep. 1992, Monteleone, Rv. 189493); in tale configurazione della fattispecie delittuosa, non era evidentemente possibile il tentativo. La figura di reato veniva successivamente riscritta con l'art. 23 della l. 19 marzo 1990, n. 55, da un lato, richiedendosi, ai fini della consumazione del reato, l'effettiva sostituzione del denaro, beni o altre utilità provenienti da un più ampio catalogo di delitti pur sempre predeterminato ex lege, non bastando il semplice compimento di atti diretti a sostituirlo e, da un altro lato, inserendo tra le condotte sanzionate, anche quella di ostacolo all'identificazione della provenienza delittuosa del bene. Pertanto, in adempimento agli obblighi derivanti per lo Stato italiano dall'adesione alla Convenzione sul riciclaggio, la ricerca, il sequestro e la confisca dei proventi di reato approvata nell'ambito del Consiglio d'Europa in data 8 novembre 1990, si perveniva alla formulazione della norma attualmente vigente. Essa risulta caratterizzata, in primo luogo, dal novero dei reati presupposto del riciclaggio di tutti i delitti non colposi ed in secondo luogo dal significativo ampliamento delle condotte "di ripulitura" concretamente sanzionabili, fino ad includervi tutte le operazioni volte ad ostacolare l'identificazione della provenienza delittuosa del denaro, dei beni o delle altre utilità oggetto del reato. Una completa ricostruzione della normativa che ha introdotto il delitto di riciclaggio e delle successive modifiche che ne hanno comportato la trasformazione da fattispecie a consumazione anticipata in reato rispetto al quale potrebbe essere configurabile il tentativo si rinviene in Sez. un., n. 25191 del 27/2/2014, Iavarazzo (in motivazione al par. 2, pagg. 10 e seguenti).
L'orientamento teso a negare in ogni caso la configurabilità, anche alla luce dell'attuale normativa, del tentativo di riciclaggio, si fonda, in realtà, su un apparente contrasto (Sez. 2, Sentenza n. 5505 del 22/10/2013 Ud. (dep. 04/02/2014, Rv. 258340) che, in termini solo assertivi, trae le proprie conclusioni dall'errato convincimento della presenza di un reato (ancora oggi) a consumazione prolungata: detto orientamento, ampiamente smentito da numerose sentenze sopra indicate, viene tralaticiamente ribadito da poche recenti pronunce (Sez. VII, n. 23887 del 2/5/2023, Vailatti, non mass.; Sez. II, n. 3517 del 1/12/2022, dep. 2023, Meli,

Le valute virtuali sono particolarmente funzionali allo sfruttamento in tal senso della loro natura perché sono anonime, o meglio, la titolarità delle valute virtuali non è evidente, in quanto il titolare si scherma dietro *nicknames* , anche se i passaggi della titolarità sono registrati su una stringa; rendono possibile una parcellizzazione del rischio, operando in maniera differenziata sull'incidenza dello stesso in base a variabili valutate in base alla condizione di operatività e alla qualità dell'interlocutore; chiunque può assumere la qualità di titolare del bene virtuale in ragione del loro libero trasferimento analogamente al denaro conta nte;la loro conservazione e memorizzazione non è di facile accesso e, considerato il numero di operazioni cui teoricamente possono essere sottoposti rendono molto difficoltosa la corretta ricostruzione della loro provenienza originaria, mentre l'utilizzazione dello strumento digitale scolora ulteriormente il "target" criminale di provenienza. Come già evidenziato chi si attiva per riciclare beni di provenienza delittuosa mette assolutamente in conto la possibilità della perdita totale o parziale del bene oggetto del riciclaggio o dell'autoriciclaggio e, nel caso delle valute virtuali, il rischio di perdita di valore della valuta medesima. Se si tratta di riciclare il prezzo di una attività corruttiva ovvero il profitto di una estorsione, ovvero denaro accumulato illecitamente e ulteriormente valorizzato rispetto all'iniziale investimento, la perdita eventuale del valore della valuta virtuale in cui il denaro di origine criminale è stato reinvestito appare, in larga parte, una evenienza riconducibile al "rischio di impresa" del disegno criminoso. L'obiettivo è infatti la cancellazione della natura criminale del "bene", perché sullo sfondo aleggia comunque il pericolo concreto di un provvedimento di sequestro ovvero di confisca[13].

---

non mass.). Fermo quanto precede, detto contrasto giurisprudenziale – per la verità più fittizio che reale – deve ritenersi superato e, comunque, privo di attualità.
Tenuto conto delle considerazioni che precedono, è stato affermato il seguente principio di diritto: "Il delitto di riciclaggio, introdotto dall'art. 3 d.l. n. 59 del 1978, convertito – in parte qua senza modifiche -nella I. n. 191 del 1978, che lo aveva inizialmente configurato come delitto a consumazione anticipata, come tale incompatibile con il tentativo, non ha, nella sua formulazione attualmente vigente, introdotta dall'art. 23 I. n. 55 del 1990 (e non mutata dagli interventi novellatori sopravvenuti), natura giuridica di delitto a consumazione anticipata, ed è, pertanto, compatibile con il tentativo".
Ciò considerato, ferma la configurabilità del tentativo di riciclaggio, nella fattispecie, la Corte territoriale ha correttamente ritenuto la ricorrenza di condotte idonee ad ostacolare l'accertamento della provenienza delittuosa dei beni in contestazione, riconoscendo come i reati in parola (tanti quanti gli originari beni di provenienza delittuosa delle attività di trasformazione e di trasferimento) fossero, nei confronti di entrambi i ricorrenti, da ritenersi consumati, alla luce delle evidenze riscontrate dagli operanti di polizia giudiziaria all'atto del loro intervento Sez. 2, Sentenza n. 6586 del 11/01/2024 Ud. (dep. 14/02/2024, Rv. 285909 – 01).
[13] La DIRETTIVA (UE) 2024/1260 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 24 aprile 2024
La DIRETTIVA (UE) 2024/1260 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 24 aprile 2024 riguardante il recupero e la confisca dei beni è funzionale a rendere più efficiente l'attuale quadro giuridico dell'Unione riguardante il reperimento e l'identificazione, il congelamento, la confisca e la gestione dei beni strumentali, dei proventi o dei beni, e gli uffici per il recupero dei beni, adesso composto dalla direttiva 2014/42/UE del Parlamento europeo e del Consiglio (, dalla decisione 2007/845/GAI del Consiglio (e dalla decisione quadro 2005/212/GAI del Consiglio.
Appare comune la consapevolezza che un sistema efficace di recupero dei beni richiede una concertazione di sforzi da parte di un'ampia gamma di autorità, tra cui le autorità di contrasto, comprese le autorità doganali, le autorità fiscali e le autorità preposte al recupero delle imposte, nella misura in cui siano competenti per il recupero dei beni, fino agli uffici per il recupero dei beni, le autorità giudiziarie e le autorità per la gestione dei beni, inclusi gli uffici per la gestione dei beni. Onde garantire un'azione coordinata da parte di tutte le autorità competenti, è necessario stabilire un approccio maggiormente strategico per il recupero dei beni e promuovere una maggiore cooperazione fra le autorità coinvolte, nonché ottenere un chiaro quadro di insieme dei risultati del recupero dei beni. È inoltre necessario garantire una cooperazione più stretta e più efficace tra gli uffici per il recupero dei beni e gli uffici per la gestione dei beni e i loro omologhi in altri Stati membri.
Sotto questi profili il legislatore europeo ha sottolineato la necessità rafforzare la capacità delle autorità competenti di privare i criminali dei proventi delle loro attività criminose stabilendo norme volte a potenziare le capacità di reperimento e di identificazione come pure di congelamento dei beni, a migliorare la gestione dei beni congelati e confiscati fino alla loro destinazione a seguito di un provvedimento definitivo di confisca.
E' stata sottolineata la necessità che una lotta efficiente contro la criminalità organizzata richiede che siano disponibili misure di congelamento e di confisca che interessino i profitti derivanti da tutti i reati in cui sono attivi gruppi della criminalità organizzata. Tali reati includono le sfere di criminalità di cui all'articolo 83, paragrafo 1, del trattato sul funzionamento dell'Unione europea (TFUE); tuttavia l'ambito di applicazione della presente direttiva dovrebbe riguardare anche tutti i reati armonizzati a livello di Unione, comprese le frodi che

La legislazione europea ha demandato alle autorità preposte (individuate nelle Financial Intelligence Unit (FIU) – o unità nazionali di informazione finanziaria (in Italia, la UIF) il monitoraggio circa l'uso delle valute virtuali, cioè l'analisi dei flussi da e verso le stesse provenienti dalle valute aventi corso legale, riconoscendo alle autorità nazionali la possibilità di richiedere i codici digitali delle singole valute virtuali agli snodi che detengono tali informazioni[14]. A questa disciplina è conseguito l'assoggettamento a vigilanza dei cc.dd. "prestatori di servizi di portafoglio digitale" cioè di quei soggetti che conservano le chiavi digitali private di accesso per conto dei propri clienti alla titolarità

---

ledono gli interessi finanziari dell'Unione, dato il crescente coinvolgimento dei gruppi di criminalità organizzata in tali reati. Nell'ambito di applicazione della direttiva dovrebbe inoltre rientrare la criminalità ambientale, che è una delle attività centrali dei gruppi di criminalità organizzata ed è spesso collegata al riciclaggio di denaro o interessa i rifiuti e i residui prodotti nel contesto della produzione e del traffico di droga. Il favoreggiamento dell'ingresso e del soggiorno illegali costituisce una delle ulteriori attività centrali dei gruppi di criminalità organizzata ed è solitamente collegato alla tratta di esseri umani.

Onde garantire l'efficace attuazione delle misure restrittive dell'Unione, è ritenuto necessario ampliare l'ambito di applicazione della presente direttiva ai reati contemplati dalla direttiva (UE) 2024/1226 del Parlamento europeo e del Consiglio (9).

E' stato ritenuto opportuno definire in senso ampio il concetto di «bene» che può essere sottoposto a congelamento e confisca, in modo tale da comprendere i documenti giuridici o gli strumenti, compreso il formato elettronico o digitale, che attestano un titolo o un diritto sui beni sottoposti a congelamento o confisca, compresi, ad esempio, strumenti finanziari, fondi fiduciari, o documenti che possono far sorgere diritti di credito e di norma si trovano in possesso della persona interessata dalle procedure in questione.

Viene sottolineata l'opportunità di definire in senso ampio il «provento di reato», al fine di includervi i proventi diretti delle attività criminali e tutti i vantaggi indiretti, compresi il reinvestimento o la trasformazione successivi di proventi diretti, in linea con le definizioni del regolamento (UE) 2018/1805 del Parlamento europeo e del Consiglio (10).

Per garantire che, ai fini di contrasto dei reati di natura transnazionale, in tutti gli Stati membri sia data sufficiente priorità alle indagini finanziarie, viene ritenuto necessario che le autorità competenti avviino il lavoro di reperimento dei beni dal momento in cui vi è il sospetto di attività criminali che possono generare considerevoli vantaggi economici.

Data la natura transnazionale delle finanze utilizzate dai gruppi di criminalità organizzata, lo scambio rapido di informazioni tra gli stati membri appare una precondizione necessaria per individuare beni strumentali e proventi di reato e altri beni posseduti o controllati da criminali.

Gli uffici per il recupero dei beni dovrebbero pertanto avere un accesso immediato e diretto a dati pertinenti quali informazioni su immobili, registri anagrafici nazionali, banche dati commerciali e banche dati dei veicoli, in aggiunta all'accesso alle informazioni sui conti bancari ai sensi della direttiva (UE) 2019/1153 del Parlamento europeo e del Consiglio (11) e alle informazioni sulla titolarità effettiva ai sensi della direttiva (UE) 2015/849 del Parlamento europeo e del Consiglio (12)

La confisca determina la privazione definitiva di un bene. La custodia di un bene può essere un prerequisito per la confisca ed è spesso essenziale per l'efficace esecuzione di un provvedimento di confisca. In questo caso il bene è custodito mediante congelamento.

La confisca estesa dovrebbe essere possibile quando un organo giurisdizionale è convinto che i beni in questione derivino da una condotta criminosa, senza che sia necessaria una condanna per tale condotta.

Considerando che le attività criminali possono arrecare gravi danni alle vittime, viene ritenuto essenziale tutelare i diritti di queste ultime, compresi i diritti al risarcimento e alla restituzione. Gli Stati membri dovrebbero pertanto adottare misure adeguate affinché i diritti delle vittime in materia di risarcimento e restituzione nei confronti della persona oggetto di una misura di confisca a seguito di un reato siano presi in considerazione nell'ambito del procedimento di reperimento, congelamento e confisca dei beni, anche nei casi di reati transfrontalieri.

Sotteso a questa direttiva appare chiaro il messaggio che il riutilizzo sociale dei beni confiscati invia alla società in generale sull'importanza di valori quali la giustizia e la legalità, riaffermando la prevalenza dello Stato di diritto nelle comunità più direttamente colpite dalla criminalità organizzata e rafforzando la resilienza di tali comunità contro l'infiltrazione criminale nel loro tessuto sociale ed economico, come osservato negli Stati membri che hanno già adottato tali misure di riutilizzo sociale.

La presente direttiva dovrebbe essere attuata lasciando impregiudicate le direttive 2010/64/UE (15), 2012/13/UE (16), 2012/29/UE (17), 2013/48/UE (18), 2014/60/UE (19), (UE) 2016/343 (20), (UE) 2016/800 (21) e (UE) 2016/1919 (22) del Parlamento europeo e del Consiglio.

[14] Infatti, l'VIII considerando della V Direttiva Antiriciclaggio ritiene che non vada vietato l'uso delle valute virtuali in assoluto.

delle singole quantità di valuta virtuale; in questo modo è stata disciplinata la detenzione delle valute virtuali, la memorizzazione (della titolarità e della quantità) ed il loro uso in termini di trasferibilità[15].

È stato riconosciuto, tuttavia, come l'utilizzo di tali snodi sia facoltativo e, quindi, non è esclusa la possibilità di un occultamento dell'utilizzo delle valute stesse o comunque è stata impedita la possibilità di intercettare la titolarità ed i trasferimenti delle valute virtuali in assenza dell'intervento di un prestatore di servizi di portafoglio digitale. È stato quindi previsto come i cc.dd. snodi, cioè i prestatori di servizi di portafoglio digitale debbano essere soggetti a registrazione[16]. La previsione non assoggetta a vigilanza preventiva tali soggetti, ma si limita a porre a carico degli stessi gli obblighi di adeguata verifica all'atto della registrazione digitale delle chiavi private relative alla titolarità della quantità "X" di valuta virtuale, la registrazione delle transazioni aventi ad oggetto la stessa, la conservazione delle informazioni e, l'eventuale invio di una segnalazione di operazioni e/o comportamenti sospetti. Infine, sono stati estesi gli obblighi di identificazione di coloro che richiedano la prestazione di servizi di cambio (ovviamente in parte digitale) tra valute virtuali e valute aventi corso legale e viceversa, come previsto per l'esercizio di ogni attività di cambiavalute, come pure gli obblighi di conservazione delle informazioni e scritture contabili e segnalazione all'ingrosso delle operazioni di conversione da e verso le singole valute virtuali[17].

4. *Segue:* Le valute virtuali e la finalità di investimento.

Il rapporto fra normativa primaria e normativa secondaria: ai fini della sussistenza del reato non assume rilevanza se:

- il sistema di blockchain e criptovalute utilizzato dal network utilizzato per la vendita on line non è disciplinato in Italia;

- sussista regolarità fiscale delle operazioni di vendita, la formalizzazione di esse tramite contratti il cui contenuto sia stato annotato su un registro informatico non alterabile, l'attribuzione agli utenti di un'identità digitale per l'acquisto dei token convertibili nella criptovaluta Bitcoin; tutto ciò in conformità con il decreto del Ministro dell'economia e delle finanze del 13 gennaio 2022.

---

[15] v. la nuova definizione sub n. 19 all'art. 3 della IV Direttiva Antiriciclaggio.

[16] cfr. nuovo testo dell'art. 47, Paragrafo 1, IV Direttiva Antiriciclaggio

[17] In occasione della riforma della disciplina antiriciclaggio, il legislatore italiano – nel dare attuazione alla IV Direttiva antiriciclaggio – è intervenuto, con il d.lgs. n. 90/2017, sulla disciplina contenuta nel d.lgs. n. 231/2007 introducendo nel nostro ordinamento la definizione di "valuta virtuale". In particolare, l'art. 1, comma 2, lett. qq), del d.lgs. n. 231/2007 ha definito la valuta virtuale come «la rappresentazione digitale di un valore, non emessa da una banca centrale o da un'autorità pubblica, non necessariamente collegata a una valuta avente corso legale, utilizzata come mezzo di scambio per l'acquisto di beni e servizi e trasferita, archiviata e negoziata elettronicamente».
Dal punto di vista della qualificazione giuridica, il legislatore non si è preoccupato di escludere espressamente, dalla predetta definizione, la presunta equiparazione fra valuta virtuale e moneta legale, evidentemente perché ha ritenuto che non sussistano i presupposti sui quali fondare la predetta assimilazione. D'altra parte, sotto il profilo funzionale, non solo la criptovaluta non ha efficacia liberatoria erga omnes (in quanto la sua accettazione come mezzo di pagamento è subordinata alla volontà della controparte) ma l'estrema fluttuazione delle sue quotazioni ne compromette la funzione di riserva di valore. La combinazione di queste due criticità finisce, altresì, per ostacolare l'utilizzo della valuta virtuale come unità di conto.
Dunque, la moneta virtuale non può essere assimilata alla valuta legale e ciò sembra confermato anche dalle modifiche apportate dal d.lgs. n. 90/2017 all'art. 17-bis (rubricato "Attività di cambiavalute") del d.lgs. n. 141/2010, recante la disciplina dei soggetti operanti nel settore finanziario; modifiche che consentono di distinguere, sotto il profilo operativo, le valute virtuali da quelle legali. Per finalità di contrasto al riciclaggio, il nuovo art. 17-bis ha esteso la disciplina prevista per i cambiavalute anche ai prestatori di servizi che operano con valute virtuali e, in più, ha stabilito che tali soggetti, per esercitare la propria attività sul territorio nazionale, devono iscriversi in una sezione speciale del registro tenuto dall'Organismo degli Agenti e dei Mediatori.

5. *Segue:* Gli acquisti in criptovaluta e la loro idoneità ad ostacolare l'individuazione della provenienza illecita del denaro nei reati di riciclaggio, impiego di denaro beni o utilità di provenienza illecita, di autoriciclaggio. Il reato di cui all'art. 166 TUF.

La valuta virtuale può essere utilizzata in forma d'investimento quando la speculazione consista nella conversione della prima in moneta legale e viceversa, in base al rapporto di cambio monetale legale/valuta virtuale praticato su piattaforme di scambio online[18].

A tale scopo si deve evidenziare che l'art. 1, comma 1, lett. t), T.U.F. definisce offerta al pubblico ogni comunicazione rivolta a persone, in qualsiasi forma e con qualsiasi mezzo, che presenti sufficienti informazioni sulle condizioni dell'offerta e dei prodotti finanziari offerti, così da mettere un investitore in grado di decidere di acquistare o di sottoscrivere tali prodotti finanziari, incluso il collocamento tramite soggetti abilitati. L'art. 67-ter del codice del consumo prevede che per servizio finanziario deve intendersi qualsiasi servizio di natura bancaria, creditizia, di pagamento, di investimento, di assicurazione o di previdenza individuale.

Pertanto, allo stato, può ritenersi il bitcoin un prodotto finanziario qualora acquistato con finalità d'investimento: la valuta virtuale, quando assume la funzione, e cioè la causa concreta, di strumento d'investimento e, quindi, di prodotto finanziario, va disciplinato con le norme in tema di intermediazione finanziaria (art. 94 ss. T.U.F.), le quali garantiscono attraverso una disciplina unitaria di diritto speciale la tutela dell'investimento medesimo.

Pertanto, chi eroghi detti servizi è tenuto ad un innalzamento degli obblighi informativi verso il consumatore, per consentire allo stesso di conoscere i contenuti dell'operazione economico-contrattuale e di maturare una scelta negoziale meditata[19].

In conclusione, quindi, è sbagliato attribuire al bitcoin o a qualsiasi criptovaluta la natura di moneta virtuale o di strumento finanziario[20], ma quello che conta è l'uso che se ne fa[21].

---

[18] Cass., Sez. 2 , Sentenza n. 13795 del 07/03/2019 Cc. (dep. 29/03/2019) Rv. 275528 – 01 in cui è stato affermato che in tema di autoriciclaggio, rientrano nel novero delle attività speculative contemplate dall'art. 648-ter.1, comma primo, cod. pen. anche il gioco d'azzardo e le scommesse, in quanto attività idonee a rendere non tracciabili i proventi del delitto presupposto e, dunque, tali da ostacolare l'identificazione della loro provenienza delittuosa. (In motivazione la Corte ha specificato che la portata del sintagma "attività speculativa", da intendersi quale investimento ad alto rischio, può essere estesa anche alle predette attività, considerato che il concetto di alea, caratteristico del gioco o della scommessa, non risulta ontologicamente diverso o inconciliabile con quello di rischio calcolabile). Si pensi alla puntata dello stesso importo sul bianco e sul nero.

[19] Il Sole 24 ore del 3 gennaio 2020, ha riportato uno studio della Consob relativo alla creazione di un quadro organico che permetta di investire nel mondo delle criptovalute, indirizzato quindi sulle offerte pubbliche e sugli operatori abilitati.

[20] V. G. Coscioni, *La moneta virtuale come strumento finanziario?* in *Gli abusi di mercato. Profili di connessione con i reati societari e riflessi sulla responsabilità amministrativa degli enti,* Scuola superiore della Magistratura, 20 -22 ottobre 2021, Roma, (Corso organizzato in collaborazione con la Scuola di Polizia economico – finanziaria della Guardia di finanza).

[21] Appare utile osservare che la Suprema Corte si è occupata di definire la *nozione* di identità digitale inserita dal legislatore del 2013 nel reato di frode informatica. Cass. Pen. sez. II, 13 marzo 2024, n. 1355 in cui è stato affermato, per definire il concetto di identità digitale, che "Anche le procedure di accesso mediante credenziali a sistemi informatici a gestione privatistica, quale i servizi di home banking o le piattaforme di vendita online rientrano nella nozione di identità digitale, poiché anch'essi individuano in modo esclusivo ed univoco una determinata persona attraverso numeri o lettere secondo una sequenza unica destinata ad essere utilizzata dal solo titolare o da soggetto da questi autorizzato.
Il caso. Il tribunale di Napoli condannava in primo grado l'imputato per il reato di riciclaggio (art. 648-bis c.p.) poiché colpevole di aver messo a disposizione di ignoti il proprio conto corrente ove era confluito denaro proveniente dai delitti di accesso abusivo ad un sistema informatico e frode informatica (artt. 612-ter c.p. e 640-ter c.p.). La Corte d'appello di Napoli, in parziale riforma della sentenza di primo grado, riqualificava il reato ai sensi dell'art. 640-ter c.p. Ricorre per cassazione l'imputato, deducendo violazione di legge e vizio di motivazione in ordine alla ritenuta sussistenza dell'aggravante di cui all'art. 640-ter, comma 3 c.p. (furto o indebito utilizzo di identità digitale). Secondo la difesa, le risultanze processuali non proverebbero la sussistenza del furto o dell'indebito utilizzo dell'identità digitale, poiché nel caso in esame ci si era serviti di una chiavetta elettronica in grado di comunicare il codice di accesso da utilizzare di volta in volta per effettuare gli accessi fraudolenti nel conto corrente della vittima.

Con riferimento ai profili giurisprudenziali occorre sottolineare che:

a) con la sentenza Sez. 2 -, n. 27228 del 15/09/2020 - 30/09/2020, *CED.* 279650 – 02, è stata sottolineato dalla Corte di cassazione come il prodotto, il profitto o il prezzo del reato non coincide con il denaro, i beni o le altre utilità provenienti dal reato presupposto, consistendo invece nei proventi conseguiti dall'impiego di questi ultimi in attività economiche, finanziarie, imprenditoriali o speculative (nella specie, un'attività di ristorazione di proprietà di una s.a.s. intestata ad un prestanome dell'indagato, sui conti della quale erano state riversate le somme provenienti dalle truffe e appropriazioni indebite contestate all'indagato medesimo).

In questo caso è stato affermato che il sequestro preventivo funzionale alla confisca del profitto del reato di cui all'art. 648-ter cod. pen., può riguardare una intera società e il relativo compendio aziendale quando sia riscontrabile un inquinamento dell'intera attività della stessa, così da rendere impossibile distinguere tra la parte lecita dei capitali e quella illecita. (Fattispecie in cui la Corte ha confermato il sequestro, disposto ai sensi dell'art. 648-quater cod. proc. pen., su tutti i beni, compresi quelli strumentali, di una s.a.s. formalmente intestata al figlio dell'indagato, sui conti della quale il padre aveva riversato i proventi di una serie di truffe e appropriazioni indebite).

b) Appare utile fare riferimento anche alla pronuncia della Corte di Cass., Sez.2, n. 44337 del 10 novembre 2021, Stanzani, n.m., relativa al sequestro probatorio di un sito che, secondo l'accusa, era da considerare corpo del reato e cosa pertinente al reato in quanto "strumento attraverso il quale vi sono la pubblicizzazione dell'attività illecita e l'offerta alla clientela, strumenti propedeutici alla messa in circolazione della moneta elettronica".

Su questo tema il profilo più rilevante è proprio quello relativo alla circostanza che la rete di valute virtuali può prestarsi a essere utilizzata per transazioni connesse ad attività criminali, incluso il riciclaggio e l'autoriciclaggio di denaro: pur essendo le transazioni in valuta virtuale visibili, infatti, i titolari dei portafogli elettronici e, più in generale, le parti coinvolte possono, come sottolineato in precedenza, generalmente rimanere anonimi. Ciò può rendere necessario l'intervento delle autorità per "chiudere" le piattaforme di scambio impedendo l'accesso o l'utilizzo di eventuali fondi custoditi presso di esse.

c) A tale proposito, la Corte di cassazione ha affermato che "*integra il delitto di autoriciclaggio la condotta di chi, in qualità di autore del delitto presupposto di truffa, impieghi le somme accreditategli dalla vittima trasferendole, con disposizione "on line", su un conto intestato alla piattaforma di scambio di "bitcoin" per il successivo acquisto di tale valuta, così realizzando l'investimento di profitti illeciti in operazioni finanziarie a fini speculativi, idonee a ostacolare la tracciabilità dell'origine delittuosa del denaro*" (Cass., Sez.2, 27023 del 07/07/2022, Miele, Rv. 283681)[22]

La sentenza va sottolineata perché affronta anche il problema della competenza territoriale. A tal fine la sentenza afferma che: "*Poiché il reato di autoriciclaggio si consuma nel momento in cui vengono poste in essere le condotte di impiego, sostituzione o trasformazione di beni costituenti l'oggetto materiale del delitto presupposto* (Cass. sez. 2, sent. n. 38838 del 04/07/2019 - dep. 20/09/2019 - Rv. 277098), *nel caso in esame il denaro proveniente dalla commissione delle truffe è stato utilizzato per l'acquisto di criptovalute tramite l'effettuazione di una serie di bonifici, partiti dal conto corrente acceso presso la banca on line Mediolanum, con sede in Basiglio, nel circondario di Milano, ed indirizzati ad una banca tedesca. La condotta finalizzata all'occultamento della provenienza delittuosa si è realizzata, quindi, nella prospettiva accusatoria, rilevante per la determinazione della competenza, con gli atti dispositivi (bonifici) con i quali le somme di provenienza illecita sono state impiegate per comprare moneta virtuale. Ciò che rileva, quindi, è il*

La Suprema Corte, con la pronuncia in commento, ha ritenuto il ricorso infondato, sposando quel principio ormai consolidato secondo cui, in tema di frode informatica la nozione di "identità digitale" che integra l'aggravante in oggetto, non presuppone una procedura di validazione adottata dalla P.A (SPID, CIE, firma digitale) ma trova applicazione anche nel caso di utilizzo di credenziali di accesso a sistemi informatici gestiti da privati (home banking e simili).

[22] Art. 648, c. 1.ter c.p."...chiunque, avendo commesso o concorso a commettere un delitto impiega, sostituisce, trasferisce, in attività economiche, finanziarie, imprenditoriali o speculative, il denaro, i beni o le altre utilità provenienti dalla commissione di tale delitto, in modo da ostacolare concretamente l'identificazione della loro provenienza delittuosa.

luogo di impiego del denaro (da provento delle truffe a prezzo di acquisto di bitcoin) ossia il conto corrente sul quale le somme sono confluite dalle persone offese, vittime dei raggiri, e destinate al mercato estero, con la conseguenza che, ai fini della competenza per territorio, occorre fare riferimento al Tribunale del luogo in cui si trova l'istituto bancario in cui l'agente ha aperto quel conto corrente ed ha operato da remoto, dando disposizioni per immettere nel circuito finanziario il capitale illegittimamente acquisto". Correttamente la competenza territoriale è stata attribuita al Tribunale di Milano, secondo la regola generale di cui all'art. 8, comma 1 cod. proc. pen.[23]

In sostanza veniva ribadito che:

- l'indicazione normativa ex art. 648 ter.1 cod. pen. delle attività (economiche, finanziarie, imprenditoriali e speculative) in cui il denaro, profitto del reato presupposto, può essere impiegato o trasferito, lungi dal rappresentare un elenco formale delle attività suddette, appare piuttosto diretta ad individuare delle macro aree, tutte accomunate dalla caratteristica dell'impiego finalizzato al conseguimento di un utile, con conseguente inquinamento del circuito economico, nel quale, vengono immessi denaro o altre utilità provenienti da delitto e delle quali il reo vuole rendere non più riconoscibile la loro provenienza delittuosa (in termini, in motivazione, par. 1.8.1, Cass. sez. 2, sent. n. 13795 del 07/03/2019 - dep 29/03/2019 - Rv. 275528);

- possono essere ricondotte nell'ambito della dizione di "attività speculativa" (della quale il legislatore, non a caso, non offre rigida definizione) molteplici attività e, in particolare, tutte quelle in cui il soggetto ricerca il raggiungimento di un utile, anche assumendosi il rischio di considerevoli perdite;

- le valute virtuali possono essere utilizzate per scopi diversi dal pagamento e comprendere prodotti di riserva di valore a fini di risparmio ed investimento (sul punto, il parere della BCE riportato a pag. 18 dell'ordinanza, recepito nella V direttiva UE antiriciclaggio 2018/843);

d) Sempre con riferimento alla determinazione della competenza è stato ritenuto che *"Il reato di riciclaggio si perfeziona con la realizzazione dell'effetto dissimulatorio conseguente alle condotte tipiche previste dall'art. 648-bis, comma primo, cod. pen., non essendo necessario che il compendio "ripulito" sia restituito a chi l'aveva movimentato, cosicché il mero trasporto materiale in altro luogo del bene riciclato esula dalla condotta tipica di trasferimento, da intendersi in senso esclusivamente giuridico di movimentazione dissimulatoria. (Fattispecie relativa al trasporto transfrontaliero di denaro oggetto di movimentazione e di occultamento in Svizzera, in cui la Corte ha dichiarato la competenza del giudice del luogo in cui era avvenuta la reintroduzione clandestina in Italia delle somme in contanti, idonea a occultare definitivamente le tracce dell'origine illecita del denaro, considerando "post factum" irrilevante il successivo trasferimento delle somme all'interno del territorio nazionale***)**. (Sez. I, Sentenza n. 2561 del 12/12/2022 - 20/01/2023, Rv. 283873 – 01).

e) Altra sentenza che si è occupata del rapporto tra autoriciclaggio e bitcoin è la n. 2868 del 2022 (Panfietti, n.m.), che tratta di un soggetto che, avendo commesso il reato di sfruttamento della prostituzione, faceva confluire somme su carte postepay intestate a prestanome, e da lì venivano effettuati bonifici verso società estere, che si occupavano poi dell'acquisto di criptovalute; in questo

[23] Il ricorrente (nel ricorso) ritiene che le operazioni in questione non avrebbero la finalità speculativa indicata nel capo d'imputazione e che, in ogni caso, le regole del mercato di riferimento non consentirebbero di nascondere l'identità dell'acquirente, essendo incentrate su criteri di trasparenza. Orbene, a prescindere che nel capo d'incolpazione provvisoria è ben individuata la condotta delittuosa rilevante ("avendo commesso i delitti di truffa aggravata di cui ai precedenti capi, impiegava e sostituiva in attività speculative e, in particolare, nell'acquisto di criptovalute il denaro preveniente dalla commissione di tali delitti in modo da ostacolarne concretamente l'identificazione della provenienza delittuosa; il tribunale aveva evidenziato che evidenziato che il ricorrente aveva provveduto a curare immediatamente il trasferimento di somme non appena accreditate - senza mai riscuoterle - attraverso disposizioni on line in favore di altro conto tedesco intestato alla piattaforma di scambio di bitcoin, per il successivo acquisto di valuta virtuale il cui impiego finale risulta ancora imprecisato, ponendo così in essere un investimento dei profitti illeciti in operazioni di natura finanziaria, idonee a ostacolare la tracciabilità e la ricostruzione della origine delittuosa del denaro. La moneta virtuale, secondo la condivisibile prospettazione del tribunale, basata su pertinenti richiami legislativi, giurisprudenziali e dottrinari, non può essere esclusa dall'ambito degli strumenti finanziari e speculativi ai fini di una corretta lettura dell'art. 648 ter.1 cod. pen.

caso è stato ritenuto che sia stato frapposto un serio ostacolo alla identificazione dell'agente come destinatario finale delle transazioni ed effettivo titolare di bitcoin acquistati non da lui, ma da società estere che fungevano da "exchanger" di criptovalute; d'altra parte ai fini dell'integrazione del reato di autoriciclaggio non occorre che l'agente ponga in essere una condotta di impiego, sostituzione o trasferimento del denaro, beni o altre utilità che comporti un assoluto impedimento alla identificazione della provenienza delittuosa degli stessi, essendo, al contrario, sufficiente una qualunque attività, concretamente idonea anche solo ad ostacolare gli accertamenti sulla loro provenienza (così Sez.2, n. 36121 del 24/05/2019, Rv. 276974).

Relativamente alla invocata tracciabilità dell'operazione di acquisto della criptovaluta, la Corte ha rilevato come la presenza di un c.d. registro digitale fosse, almeno nel caso di specie, sostanzialmente irrilevante. In questo caso non si è trattato di un acquisto diretto di Bitcoin da parte dell'indagato, ma di un trasferimento di somme di denaro a società estere successivamente incaricate di cambiare la valuta ricevuta in Bitcoin. L'indagato, dunque, non ha agito in autonomia ma si è servito di un intermediario specializzato, che si è interposto nella identificazione del denaro.

Peraltro, tali transazioni sono avvenute per il tramite di soggetti prestanome, titolari apparenti delle carte Postepay dalle quali partivano i bonifici in favore delle società exchanger. L'analisi della blockchain, perciò, non avrebbe comunque ricondotto al reale proprietario del denaro riciclato.

f) Ancora in tema di riciclaggio, ai fini della determinazione della competenza territoriale, il reato realizzato con condotte frammentarie e progressive, affidate a plurimi soggetti che apportino il loro contributo in tempi e luoghi diversi, deve considerarsi consumato ove si realizza il primo atto, ancorché costituente un segmento della condotta tipica. (Fattispecie in cui il luogo di consumazione del reato è stato individuato in quello in cui era avvenuta l'iniziale consegna del denaro di provenienza delittuosa, destinato ad essere dapprima trasferito in altri luoghi del territorio nazionale, quindi fatto espatriare per l'impiego in operazioni di investimento). (Sez. 2 , Sentenza n. 38105 del 08/04/2021 Ud. (dep. 25/10/2021) Rv. 282019 - 01[24]

[24] La sentenza ha fatto corretta applicazione, in tal senso, dell'insegnamento della giurisprudenza di legittimità secondo il quale «il delitto di riciclaggio, pur essendo a consumazione istantanea, è a forma libera e può anche atteggiarsi a reato eventualmente permanente quando il suo autore lo progetti e lo esegua con modalità frammentarie e progressive» (Sez. 2, n. 29611 del 27/04/2016, Bokossa, Rv. 267511; Sez. 2, n. 34511 del 29/04/2009, Raggio, Rv. 246561).
Rispetto a queste argomentazioni, i ricorrenti indugiano nel riproporre gli argomenti già delineati con i motivi di appello, volti a fornire una lettura alternativa dei fatti storici descritti nelle imputazioni, esaltando l'inidoneità della mera consegna del denaro avvenuta in Campolongo ad integrare il fatto tipico ex art. 648 bis cod. pen.; in tal modo, si isola quella che è stata l'operazione iniziale rispetto alle modalità descritte nell'imputazione, più complesse e articolate, attraverso le quali doveva essere realizzata l'attività di riciclaggio che richiedeva, quale prima fase, quella del recupero delle somme da riciclare dai nascondigli -ove erano state da tempo occultate con l'affidamento agli altri imputati, incaricati delle successive operazioni. Sempre nella medesima prospettiva, non colgono nel segno le censure che criticano l'ipotizzata connessione ex art. 12, lett. A) cod. proc. pen., distinguendo il concorso nel delitto di cui al capo A) ascritto al ricorrente, realizzatosi mediante le attività di investimento eseguite all'estero, dal concorso nel fatto di reato come descritto; ancora una volta i ricorrenti trascurano di considerare l'oggetto dell'imputazione come formulata, separano temporalmente le condotte, individuano luoghi differenti in cui furono eseguite le singole attività materiali succedutesi nel tempo, senza considerare che la forma di manifestazione del reato plurisoggettivo comprende anche ipotesi in cui il contributo dei singoli concorrenti può manifestarsi in luoghi e tempi diversi, ciò che non incide però nell'attribuzione del fatto come contestato e, conseguentemente, dell'individuazione del luogo in cui il fatto tipico si realizza. A questo riguardo, è stato affermato dalla giurisprudenza di legittimità, con espresso riguardo ai profili della competenza territoriale, che ove la realizzazione del fatto tipico (che, si ripete, nel caso sottoposto al giudizio della Corte territoriale è stato individuato nella prima consegna del denaro) sia conseguenza del concorso o della cooperazione tra più agenti, ovvero di condotte indipendenti avvinte da connessione ai sensi dell'art. 12, lett. a), cod. proc. pen., territorialmente competente è, alla stregua della regola prevista dall'art. 16, comma 2, cod. proc.pen., il giudice del luogo in cui si è consumato il reato, anche nel caso in cui detto luogo sia diverso da quelli nei quali sono state realizzate le azioni od omissioni dei concorrenti (Sez. 1, n. 38871 del 12/06/2019, G.i.p. Tribunale Palermo, Rv.276880 - 02). Si tratta in questo caso dell'applicazione più generale del c.d. criterio dell'ubiquità allargata in forza del quale, proprio per le caratteristiche della fattispecie di riciclaggio sopradescritta, è sufficiente che inizialmente sia stato posto in essere solo un frammento della condotta, il cui oggettivo rilievo appare idoneo per le sue modalità a configurare, apprezzare e collegare in modo inequivoco gli altri segmenti operativi realizzati successivamente,

g) Appare utile fare riferimento anche ad una sentenza del Tribunale di Milano del 5 aprile 2023, sui limiti all'emissione di moneta elettronica in assenza di autorizzazione della Banca d'Italia.

Il Tribunale ha preso le mosse ricordando come, ad avviso della Cassazione, "*la valuta virtuale deve essere considerata strumento di investimento perché consiste in un prodotto finanziario, per cui deve essere disciplinata con le norme in materia di intermediazione finanziaria e ciò a prescindere dalle modalità di pubblicizzazione adottate dall'offerente e dando rilievo all'elemento soggettivo del reato rappresentato dall'aspettativa di rendimento dell'investitore, piuttosto che all'elemento oggettivo costituito dalla causa (finanziaria o meno) dell'operazione*"[25].

Passando, invece, alla fattispecie di cui all'art. 132 bis TUB – che punisce l'abusivo esercizio di attività finanziaria nei confronti del pubblico – deve ritenersi ormai prevalente l'orientamento che considera la fattispecie incriminatrice integrata purché l'attività, anche se in concreto realizzata per una cerchia ristretta di destinatari, fosse rivolta ad un numero potenzialmente illimitato di soggetti e si fosse svolta professionalmente, ovvero in modo continuativo e non occasionale, non essendo invece necessario il perseguimento di uno scopo di lucro o, comunque, di un obiettivo di economicità, posto che "il carattere di professionalità non implica il perseguimento di uno scopo di lucro, o, quantomeno, di un obiettivo di economicità.(Cass., sez. V, 14 ottobre 2022, n. 39000; v. anche Cass. Pen. Sez. V, 22 marzo 2019, n. 12777).

6. *Segue*: Autoriciclaggio e il delitto di trasferimento fraudolento di valori

La giurisprudenza appare ormai prevalentemente orientata nel ritenere che il delitto di autoriciclaggio è in rapporto di specialità reciproca con quello di trasferimento fraudolento di valori, essendo accomunate le fattispecie dalla generica provenienza da delitto dei beni oggetto di trasferimento e dall'utilizzo di modalità dissimulatorie tese a rendere difficoltosa l'identificazione di detta provenienza, sicché, quando l'intestazione fittizia di un bene costituisca la principale modalità commissiva dell'autoriciclaggio, è configurabile solo quest'ultimo, più grave, delitto, in forza della clausola di riserva contenuta nell'art. 512-bis cod. pen. (Sez. 1 -, Sentenza n. 39489 del 22/06/2023 Ud. (dep. 28/09/2023) Rv. 285123 – 01).

In precedenza, era stato sottolineato che il delitto di riciclaggio, in quanto reato a forma libera e a formazione eventualmente progressiva, realizzabile anche con più atti finalizzati ad ostacolare

---

in Italia e poi all'estero; un movimento iniziale che ponendo in essere un iter modificativo della realtà concreta, contribuisce a realizzare il segmento finale cui ancorare il momento consumativo del reato. Alla luce delle suesposte considerazioni appaiono coerenti con queste valutazioni le modalità di individuazione della competenza territoriale affermata in sentenza. Cass., Sez. 2, Sentenza n. 38105 del 08/04/2021 - Ud. (dep. 25/10/2021), Rv. 282019 – 01.

[25] Passando ad analizzare gli aspetti più significativi degli artt. 131 bis TUB – "il testo letterale della prima disposizione sanziona chiunque emetta moneta elettronica in violazione dell'art. 114 bis e senza essere iscritto all'albo menzionato dagli artt. 13 e 114 bis del medesimo testo legislativo, mentre l'art. 132 punisce chiunque svolga nei confronti del pubblico una o più attività finanziarie previste dal TUB".
Quanto alla prima ipotesi, "la norma non fornisce particolari delucidazioni in relazione all'emissione di moneta elettronica: in un'ottica di offensività anticipata, potrebbe coincidere con il primo atto di emissione abusiva precedente la fase del caricamento del valore monetario su un determinato dispositivo oppure, ai fini dell'effettiva consumazione della fattispecie illecita, dovrebbe essere necessario attendere il completamento dell'operazione di caricamento con disponibilità della valuta economica".
Tuttavia, "sebbene in prima battuta, la norma potrebbe apparire come sintetica e poco espressiva, ad un'analisi più attenta della disposizione in esame, ponendo in connessione questa fattispecie con quelle immediatamente precedenti, si può notare come l'art. 131 bis punisca, a differenza delle altre aventi ad oggetto l'attività e la condotta di emissione, il singolo evento e, pertanto, la singola operazione di emissione abusiva".
Con riferimento poi al profilo psicologico, "questo deve individuarsi nel dolo generico da parte del soggetto agente, ovvero nella volontà e nella consapevolezza di emettere abusivamente e, quindi, senza i requisiti previsti dalla norma, moneta elettronica".
E' evidente – si legge nella decisione – "che la scelta del legislatore di recepire i dettami comunitari ha trovato il proprio fondamento nell'esigenza di attribuire un maggiore grado di strutturazione, di standardizzazione e di armonizzazione al mondo bancario e finanziario, al preciso scopo di ridurre gli episodi di abusivismo, in un'ottica di trasparenza, correttezza e sicurezza del mercato, della concorrenza e della clientela, anticipando, pertanto, la punibilità ad una fase ove la fattispecie illecita non ha ancora arrecato pregiudizio".

l'illecita provenienza del denaro, dei beni o delle altre utilità, assorbe il delitto di trasferimento fraudolento di valori in forza della clausola di riserva di cui all'art. 512-bis cod. pen. nel caso in cui quest'ultimo costituisca un segmento della più articolata condotta riciclatoria. (Sez. 2, Sentenza n. 38141 del 15/07/2022 - 10/10/2022 , CED 283677 – 01). In tal senso v. anche Sez. 2 , Sentenza n. 26902 del 31/05/2022 - 12/07/2022 , CED 283563 – 02) in cui è stato ritenuto non configurabile il delitto di trasferimento fraudolento di valori quando la finalità dell'agente è quella di agevolare la commissione del delitto di autoriciclaggio, in quanto tale finalità non rientra tra gli elementi costitutivi del delitto di cui all'art. 512-bis cod. pen.

7. *Segue:* L'operazione di finanziamento del terrorismo analogie e differenze rispetto all'operazione di riciclaggio (o autoriciclaggio)[26]

[26] La differenza tra riciclaggio (e auto riciclaggio) e finanziamento del terrorismo va sostanzialmente individuata nel fatto che l'attività di riciclaggio (e auto riciclaggio) consiste nella riutilizzazione di denaro frutto di attività illecite in attività legali. Il finanziamento del terrorismo prevede la raccolta o l'uso di fondi per finalità di terrorismo.
ESTRATTO:"Disciplinare per la rilevazione e comunicazione di operazioni sospette di riciclaggio e di finanziamento del terrorismo (art. 10 del Decreto Legislativo n. 231 del 21 novembre 2007 e ss.mm.ii.) del d.lgs. 231/2007 e ss.mm.ii"
Articolo 2. 1. Ai fini del presente disciplinare per:- "attività di riciclaggio", come precisato dall'art. 2, comma 4, del d.lgs. n. 231/2007 e ss.mm.ii, s'intende: a) la conversione o il trasferimento di beni, effettuati essendo a conoscenza del fatto che essi provengono da un'attività criminosa o da una partecipazione a tale attività, allo scopo di occultare o dissimulare l'origine illecita dei beni medesimi o di aiutare chiunque sia coinvolto in tale attività a sottrarsi alle conseguenze giuridiche delle proprie azioni; b) l'occultamento o la dissimulazione della reale natura, provenienza, ubicazione, disposizione, movimento, proprietà dei beni o dei diritti sugli stessi, effettuati essendo a conoscenza del fatto che tali beni provengono da un'attività criminosa o da una partecipazione a tale attività; c) l'acquisto, la detenzione o l'utilizzazione di beni essendo a conoscenza, al momento della loro ricezione, del fatto che tali beni provengono da un'attività criminosa o da una partecipazione a tale attività; d) la partecipazione ad uno degli atti di cui alle lettere a), b) e c) l'associazione per commettere tale atto, il tentativo di perpetrarlo, il fatto di aiutare, istigare o consigliare qualcuno a commetterlo o il fatto di agevolarne l'esecuzione; Il riciclaggio è considerato tale anche se le attività che hanno generato i beni da riciclare si sono svolte fuori dai confini nazionali;--"finanziamento del terrorismo", si intende qualsiasi attività diretta, con ogni mezzo, alla fornitura, alla raccolta, alla provvista, all'intermediazione, al deposito, alla custodia o all'erogazione, in qualunque modo realizzate, di fondi e risorse economiche, direttamente o indirettamente, in tutto o in parte, utilizzabili per il compimento di una o più condotte, con finalità di terrorismo secondo quanto previsto dalle leggi penali ciò indipendentemente dall'effettivo utilizzo dei fondi e delle risorse economiche per la commissione delle condotte anzidette (art. 2, comma 5, del d.lgs. 231/2007 e ss.mm.ii.); "Gestore", indica il Referente delle comunicazioni di operazioni sospette di riciclaggio e di finanziamento del terrorismo, nominato con provvedimento formale del Direttore Generale quale soggetto delegato a valutare ed effettuare le comunicazioni alla UIF, ai sensi dell'art. 11 delle Istruzioni UIF del 23 aprile 2018 (G.U. n. 269 del 19 novembre 2018) e dell'art. 6 del Decreto del Ministro dell'Interno 25 settembre 2015 (G.U. n. 233 del 7 ottobre 2015); "indicatori di anomalia", sono le fattispecie rappresentative di operatività ovvero di comportamenti anomali finalizzati ad agevolare la valutazione, da parte dei segnalanti, degli eventuali profili di sospetto di riciclaggio o di finanziamento del terrorismo; 2Documento: CI-GART-2023-02 Disciplinare Data 23/06/2023 Disciplinare per la rilevazione e comunicazione di operazioni sospette di riciclaggio e di finanziamento del terrorismo (art. 10 del Decreto Legislativo n. 231 del 21 novembre 2007 e ss.mm.ii.)----"operazione sospetta", si intende quella che per caratteristiche, entità, natura delle operazioni o qualsivoglia altra circostanza, conosciuta a ragione delle funzioni esercitate, tenuto conto anche della capacità economica e dell'attività svolta dal soggetto cui è riferita, induce a ritenere, sospettare o avere motivi ragionevoli per sospettare, in base agli elementi a disposizione del segnalante, che siano in corso o che siano state compiute o tentate operazioni di riciclaggio o di finanziamento al terrorismo o che comunque i fondi, indipendentemente dalla loro entità, provengano da attività criminosa (art. 35 d.lgs. 231/2007 e ss.mm.ii.); "segnalante", il personale appartenente alle diverse strutture dell'ASI (addetto all'istruttoria; Responsabile di Unità Organizzativa o il Responsabile del procedimento/Responsabile unico del progetto) che abbia rilevato l'operazione sospetta nell'ambito dei procedimenti/processi dell'ASI di cui all'art. 10, comma 1, del d.lgs. 231/2007 e ss.mm.ii; "soggetto cui è riferita l'operazione", si intende il soggetto (persona fisica o entità giuridica) che nell'ambito dei procedimenti/processi dell'ASI di cui all'art. 10, comma 1, del d.lgs. 231/2007 e ss.mm.ii, entra in relazione con l'ASI e riguardo al quale emergono elementi di sospetto di riciclaggio, di finanziamento del terrorismo o di provenienza da attività criminosa delle risorse economiche e finanziarie; "Titolare effettivo", si intende la persona fisica o le persone fisiche, diverse dal

Nell'ambito delle misure di contrasto del riciclaggio e dell'autoriciclaggio il Consiglio dell'Unione europea ha adottato, il 30 maggio 2024, un pacchetto di nuove norme tese a tutelare il sistema finanziario dell'UE dalle attività di riciclaggio e dalle attività destinate al finanziamento del terrorismo.

Con il nuovo intervento tutte le norme relative al settore privato saranno incluse in un nuovo regolamento immediatamente applicabile, mentre l'organizzazione delle autorità nazionali competenti per la lotta contro il riciclaggio e il contrasto del finanziamento del terrorismo (AML/CFT) verrà disciplinata da una direttiva.

Il regolamento ha la funzione di armonizzare in modo esaustivo le norme già esistenti con l'obiettivo di eliminare i contrasti interpretativi nell'applicazione della normative di antiriciclaggio e di contrasto del finanziamento del terrorismo ed estende le norme antiriciclaggio a nuovi soggetti obbligati, come la maggior parte degli operatori del settore delle cripto-attività, i soggetti che commerciano beni di lusso e le società e gli agenti nel settore del calcio professionistico. Stabilisce obblighi più stringenti sulle modalità di verifica delle attività interessate, disciplina I criteri per individuare la titolarità effettiva delle medesime e fissa un limite di 10 000 EUR per i pagamenti in contanti.

L'obiettivo è quello di adeguare l'organizzazione dei sistemi antiriciclaggio nazionali stabilendo norme chiare sulle modalità di collaborazione tra le unità di informazione finanziaria (FIU, gli organismi nazionali che raccolgono informazioni sulle attività finanziarie sospette o insolite negli Stati membri) e le autorità di vigilanza. Per questo è stata istituita a livello europeo una nuova Autorità per la lotta al riciclaggio e al finanziamento del terrorismo (AMLA), che avrà sede a Francoforte e inizierà ad operare a metà del 2025. L'Autorità avrà poteri di supervisione diretta e indiretta sui soggetti obbligati ad alto rischio nel settore finanziario, anche in ragione della ormai acquisita consapevolezza della natura transfrontaliera della criminalità finanziaria.

Una delle novità della nuova Autorità tesa a migliorare l'efficienza del quadro di collaborazione in materia di AML/CFT, è relativa alla creazione di un meccanismo integrato con le Autorità nazionali per garantire che i soggetti obbligati rispettino gli impegni assunti in materia di contrasto al riciclaggio e al finanziamento del terrorismo nel settore finanziario. L'AMLA avrà anche un ruolo di sostegno in relazione al settore non finanziario e coordinerà e sosterrà le FIU. Oltre ai poteri di supervisione e al fine di garantire l'applicazione coerente e uniforme della nuova discipilina, in caso di violazioni gravi, sistematiche o ripetute di obblighi direttamente applicabili, l'Autorità potrà applicare sanzioni pecuniarie ai soggetti obbligati preventivamente individuati.

La nuova direttiva antiriciclaggio prevede inoltre che gli Stati membri dell'UE rendano disponibili mediante un punto di accesso unico le informazioni provenienti da registri centralizzati dei conti bancari, e l'accesso ai dati dei titolari dei conti bancarii. Poiché la direttiva antiriciclaggio fornirà l'accesso al punto di accesso unico solo alle FIU, il Consiglio ha adottato inoltre una direttiva distinta per garantire che le autorità di contrasto nazionali possano accedere ai centralizzati dei conti bancari attraverso il punto di accesso unico. La direttiva prevede inoltre l'armonizzazione del formato degli estratti conto bancari. Tale accesso diretto e l'uso di formati armonizzati da parte delle banche costituiscono un ulteriore strumento anche in relazione alla possibilità di individuare e confiscare i proventi di reato.

Il regolamento antiriciclaggio si applicherà dopo tre anni la sua entrata in vigore. Gli Stati membri avranno due anni di tempo per recepire alcune parti della direttiva antiriciclaggio e tre anni per recepirne altre parti.

Ciò premesso, occorre considerare che i comportamenti, i presupposti e le finalità perseguite da chi pone in essere un'operazione di riciclaggio sono completamente diverse da chi intende realizzare un'operazione di finanziamento del terrorismo.

---

cliente, nell'interesse della quale o delle quali, in ultima istanza, il rapporto continuativo è istaurato, la prestazione professionale è resa o l'operazione è eseguita (art. 1, comma 2, lett. pp) del d.lgs. 231/2007); "UIF", indica l'Unità di Informazione Finanziaria per l'Italia istituita presso la Banca d'Italia dal d.lgs. 231/2007 e ss.mm.ii.

Chi ricicla persegue la fondamentale esigenza di nascondere la vera titolarità del bene, di diminuire il rischio che l'intero prezzo o la refurtiva, ancorché convertiti, siano intercettati e di nascondere, pertanto l'origine criminale dei fondi utilizzati per acquistare una valuta virtuale o l'origine criminale della valuta stessa. Avendo ingenti somme a disposizione, chi ricicla non ha esigenze e limiti temporali: anzi più il tempo passa, più dell'origine criminale si perde la memoria.

Chi ricicla non si cura dell'eventuale perdita di valore alla quale una determinata valuta virtuale potrebbe andare incontro. Non essendo valori guadagnati lecitamente (si pensi al prezzo della corruzione o di un fenomeno estorsivo), oppure essendo il frutto di illeciti il cui ritorno sull'investimento iniziale è moltiplicato per numeri importanti, un'eventuale perdita di valore è un'eventualità sopportabile e già valutata come possibile da chi abbia la mecessità di riciclare il bene.

Il riciclatore, infatti, non ragiona secondo criteri di economicità e logicità di un'operazione finanziaria, ma esattamente all'inverso, in quanto sarà disponibile a pagare un prezzo comunque pur di poter nascondere l'origine criminale dei fondi utilizzati per l'acquisto di una valuta virtuale, oppure la sua percezione. La possibilità che il prezzo del reato e ciò in cui è stato convertito siano confiscati, rende più conveniente l'accettazione del rischio, piuttosto che non eseguire l'operazione stessa.

Nel finanziamento del terrorismo, al quale possono essere equiparate tutte le situazioni in cui una valuta virtuale è utilizzata al fine di aggirare sanzioni internazionali e/o embarghi e/o divieti e sanzioni amministrative o giudiziarie l'utilizzo di una valuta virtuale risponde ad esigenze molto diverse.

Le singole operazioni di conversione e/o trasferimento non sono di grande ammontare**,** proprio per dissimulare lo scopo effettivo del ricorso alle valute virtuali; a ciò deve aggiungersi la considerazione che il supporto alle organizzazioni terroristiche, offerto da alcuni Stati o Paesi, avviene direttamente in natura (in genere attraverso l'acquisto di armi tramite triangolazioni internazionali), anche perché sotto il profilo logistico l'atto terroristico per essere portato a compimento può anche fare a meno di investimenti elevati, nell'ipotesi in cui un numero ristretto di soggetti partecipi all'organizzazione ed esecuzione dell'attentato. Le organizzazioni terroristiche e chi finanzia il terrorismo in genere non prestano particolare attenzione al fatto che le valute virtuali possano o meno mantenere immutato il valore nel tempo, in quanto lo scopo non è quello di tesaurizzare un valore, ma di spenderlo o di convertirlo il più presto possibile.

La valuta virtuale, dunque, nell'ambito del finanziamento del terrorismo, assume una funzione di intermediario di pagamento in un'economia illecita e parallela che risponde a logiche diverse da quelle di un soggetto che intenda riciclare. [27]

8) Problemi in tema di oneri probatori; in particolare in relazione alla tracciabilità delle operazioni

Il problema della prova, in relazione alla tracciabilità delle operazioni, pone anche quello della specializzazione delle conoscenze, oltre che giuridiche, informatiche e finanziarie. La digitalizzazione delle operazioni e la mancanza nell'ordinamento italiano di una disciplina unitaria in materia di digitalizzazione delle valute rende più difficile l'accertamento delle responsabilità.

Senza dubbio si tratta di un settore dove di frequente è necessario l'espletamento di consulenze tecniche in fase di indagine e, eventualmente, di perizie; nonché di rogatorie, in caso di operazioni transfrontaliere; di acquisizione di documenti e dati tecnici; è necessaria una grande sensibilizzazione verso la possibilità della cooperazione giudiziaria non solo fra stati ma attraverso

[27] La storia di Uquid, una compagnia con sede in Gibilterra che si occupa della conversione di bitcoin, rappresenta un esempio di come un'organizzazione possa avere possibili implicazioni in operazioni di riciclaggio: la societa` offre ai suoi utenti una carta prepagata VISA che può essere ricaricata direttamente con bitcoin, senza che siano rispettati tutti obblighi informativi necessari imposti affinché le forze dell'ordine possano intercettare capitali di dubbia provenienza. V. Giulia Maria Mainardi, *Le cripto valute come strumento di riciclaggio di capitali illeciti da parte delle organizzazioni terroristiche,* tesi Master in *Geopolitica della sicurezza*, Università studi Niccolò Cusano, 2018-2019.

contatti diretti tra autorità giudiziarie. In quest'ottica il ruolo delle EPPO, la procura europea, può assumere in concreto e rivelarsi un fattore decisivo per il contrasto della criminalità organizzata.

Ciò premesso ai fini della configurabilità del concorso nei reati, materialmente posti in essere da altri con l'uso di criptovalute, può ritenersi necessario un contributo, anche soltanto agevolatore, all'altrui attività di impiego illecito, e la prova di tale contributo, che può prescindere dalla dimostrazione della esistenza di un previo accordo tra i concorrenti, può consistere in un rafforzamento del proposito del correo o, in alternativa, in un apporto materiale efficiente alla condotta di questo, analogamente a quanto previsto dalla Suprema Corte in un caso di aggiotaggio manipolativo (Sez. 5, Sentenza n. 3971 del 16/07/2015 - dep. 29/01/2016 - Rv. 265864.Tale conclusione si rafforza considerando che il riciclaggio (come l'autoriciclaggio) è diventato un reato che può manifestarsi in modalità informatiche proprio con riferimento agli impieghi speculativi in criptovalute dei proventi illeciti; in questo caso è il profitto del reato che viene digitalizzato e le modalità realizzative del reato sono digitali.

Con riferimento agli oneri probatori e le modalità del controllo giurisdizionale, merita attenzione il caso di sussistenza di reati con caratteristiche transfrontaliere, nell'ipotesi in cui un O.E.I. abbia ad oggetto prove già in possesso dell'Autorità giudiziaria straniera; in questo caso occorre prendere in esame anche le due decisioni delle Sezioni Unite Cass. 23756/2024 e Cass. 23755/2024 in merito al caso dei c.d. criptofonini Sky ECC e alla decisione del 30 aprile 2024 con cui la Grande Sezione della Corte di giustizia dell'Unione Europea si è pronunciata in merito all'analoga vicenda dei messaggi criptati scambiati attraverso la piattaforma Encrochat.[28].

Nei casi affrontati dalle Sezioni Unite, si è trattato delle comunicazioni che le autorità giudiziarie francesi erano riuscite a sottrarre dai server della piattaforma Sky ECC attraverso apposite attività di "hacking", attività che sarebbero consistite sia nella raccolta in tempo reale di comunicazioni in corso di svolgimento, attraverso operazioni di intercettazione e di acquisizione di dati esterni alle comunicazioni tramite i tabulati, sia nella raccolta di comunicazioni già avvenute e conservate nei server (c.d. "dati freddi"), attraverso atti di perquisizione e sequestro.

Il problema, risolto con le due sentenze gemelle della Corte di cassazione del giugno scorso concerne la natura e le conseguenti garanzie procedimentali applicabili all'acquisizione delle conversazioni via chat intercorse fra alcuni esponenti di associazioni criminali dedite al traffico di stupefacenti attraverso piattaforme online di tipo criptato, che avevano loro consentito di comunicare in modo riservato mediante smartphone appositamente modificati.

Le Sezioni Unite hanno preso in esame il tema dell'impiego dell'OEI (Ordine di indagine europeo) ai fini della raccolta di prove già in possesso dell'autorità di esecuzione secondo quanto già espressamente previso sia dalla direttiva sia dal d.lgs. n. 108 del 2017

a) Le Sezioni Unite con riferimento alla natura delle operazioni istruttorie in questione, hanno ritenuto che le stesse non consistono in un'"acquisizione di documenti e dati informatici conservati all'estero" ai sensi dell'art. 234 bis c.p.p., disciplina "alternativa e incompatibile" rispetto a quella dettata in tema di OEI; infatti essa "prescinde" "da forme di collaborazione con l'autorità giudiziaria di altro Stato", laddove il Considerando 35 della direttiva qualifica l'OEI come prevalente su tutti gli altri pertinenti strumenti internazionali che dovessero concorrere in materia[29]. In presenza di un OEI, dunque, operano le garanzie che devono assistere la raccolta delle prove tramite questo strumento, in particolare, il principio di equivalenza, ai sensi del quale l'atto di indagine richiesto nell'OEI dovrebbe poter essere emesso "alle stesse condizioni in un caso interno analogo" e il principio di proporzionalità, il quale esige che le eventuali compressioni dei diritti fondamentali originate dalle attività istruttorie siano contenute nello stretto necessario, e comunque non intacchino i nuclei essenziali degli stessi. Le Sezioni Unite hanno valorizzato la disposizione di cui all'art. 78 disp. att. c.p.p., relativo all'acquisizione della "documentazione di atti di un procedimento penale compiuti da autorità giudiziaria straniera" in cui si prevede, al comma 1, che la documentazione in questione "può essere acquisita" nei procedimenti penali nazionali "a norma

[28] M. Daniele, La *mappa del controllo giurisdizionale quando l'OEI ha ad oggetto prove già in possesso dell'autorità straniera,* in *Sistema penale,* rivista on line, 17 luglio 2024

[29] Sentenze Sezioni Unite Cass. 23756/2024, Giorgi, § 6 , *CED 286589*; Cass. 23755/2024, Gjuzi, § 9 s, *CED* 286573 - 2.

dell'articolo 238 del codice": vale a dire, delle prescrizioni che, in ambito nazionale, regolano la circolazione delle prove da un procedimento penale ad un altro. Pertanto, in questi casi le sole regole probatorie rilevanti ai fini dell'acquisizione in Italia delle prove già raccolte all'estero sono quelle rinvenibili nell'art. 238 c.p.p., a cui l'art. 78 disp. att. rinvia; qualora le prove fossero state acquisite con le forme delle intercettazioni di comunicazioni, si deve fare riferimento all'art. 270 c.p.p., il quale, sebbene non espressamente richiamato, può ritenersi applicabile in virtù dei criteri desumibili dall' all'art. 78 disp. att. In conclusione, per l'emissione di un OEI finalizzato all'acquisizione di comunicazioni criptate già autonomamente raccolte all'estero, non deve ritenersi necessaria l'autorizzazione preventiva di un giudice dello Stato di emissione, proprio perché se la circolazione di prove del genere da un procedimento ad un altro avvenisse a livello nazionale, tale autorizzazione preventiva non servirebbe, in quanto non richiesta nè dall'art. 238, nè dall'art. 270 c.p.p. Una soluzione sostanzialmente condivisa anche dalla Corte di giustizia nel caso Encrochat[30]. In applicazione del principio di equivalenza, pertanto, la Corte di cassazione ritiene che pure il corrispondente OEI possa essere emesso direttamente da un pubblico ministero, anche quando le prove richieste fossero già state raccolte all'estero attraverso intercettazioni o acquisizione di tabulati[31]. Pertanto, un OEI finalizzato ad ottenere prove già raccolte dalle competenti autorità dello Stato di esecuzione non dovrebbe "essere adottato necessariamente da un giudice quando, in forza del diritto dello Stato di emissione, in un procedimento puramente interno a tale Stato, la raccolta iniziale di tali prove avrebbe dovuto essere ordinata da un giudice, ma competente ad ordinare l'acquisizione di dette prove è il pubblico ministero". È comunque previsto un controllo giurisdizionale posticipato in base all'obbligo di rispettare i diritti fondamentali nei limiti del principio di proporzionalità e all'esigenza di assicurare che agli atti istruttori richiesti nell'OEI siano applicabili "mezzi d'impugnazione equivalenti a quelli disponibili in un caso interno analogo", tali da permettere, nell'ambito dello Stato di emissione, di contestare le "ragioni di merito dell'emissione dell'OEI". Le Sezioni Unite hanno ritenuto corretto assegnare tale esame al giudice nazionale chiamato ad utilizzare le prove autonomamente raccolte all'estero e trasmesse tramite l'OEI: in particolare, al giudice di merito o al giudice chiamato ad applicare una misura cautelare, i quali conservano "integro il potere di valutare se vi siano i presupposti" per "ammettere" ed "utilizzare" tali prove ai fini delle decisioni di loro spettanza"[32]. L'art. 14 § 7 della direttiva, fa riferimento al rispetto dei "diritti della difesa" e delle "garanzie del giusto processo nel valutare le prove acquisite tramite l'OEI".

A livello nazionale, l'art. 36 del d.lgs. n. 108 del 2017, ripropone la regola prevista dall'art. 431 comma 1 lett. d c.p.p. per l'utilizzabilità delle prove raccolte tramite le rogatorie: sono ammissibili i "verbali degli atti" "assunti all'estero a seguito di ordine di indagine ai quali i difensori sono stati posti in grado di assistere e di esercitare le facoltà loro consentite dalla legge italiana".

Ciò premesso le Sezioni Unite prendono in esame due specifici requisiti di utilizzabilità:

a) quando vengano in gioco prove raccolte autonomamente all'estero tramite atti che, come le intercettazioni o l'acquisizione di tabulati, a livello nazionale richiederebbero l'autorizzazione preventiva di un giudice, la Corte di cassazione propone una condizione chiara: il fatto che l'acquisizione delle suddette prove fosse a suo tempo stata autorizzata ex ante da un giudice nello Stato di esecuzione. Questo presupposto, perlomeno nel caso esaminato dalla sentenza Giorgi, può ritenersi presente, se si considera che le comunicazioni criptate erano state acquisite a seguito di provvedimenti motivati emessi da *juges d'instruction* francesi. Inoltre, la sentenza Giorgi aggiunge che, qualora le comunicazioni fossero state autonomamente acquisite all'estero con la forma delle intercettazioni, sarebbe necessaria la loro rilevanza per l'accertamento di delitti per i quali è

[30] Grande Sezione della Corte di giustizia dell'Unione Europea, 30 aprile 2024 , Encrochat M.N., C-670/22
[31] Operazioni istruttorie che, a differenza delle perquisizioni e dei sequestri, a livello nazionale non potrebbero essere disposte direttamente dal pubblico ministero, ma necessiterebbero di una preventiva autorizzazione giurisdizionale.
La conclusione trova una conferma anche nella più sopra menzionata sentenza della Corte di giustizia relativa al caso Encrochat, dove i giudici della CGUE hanno sottolineato che il pubblico ministero figura tra i soggetti che, ai sensi dell'art. 2 lett. c della direttiva, possono costituire un'autorità di emissione dell'OEI. L'unica condizione è che l'organo di accusa sia competente, in un caso interno analogo, "ad ordinare un atto di indagine diretto alla trasmissione di prove già in possesso delle autorità nazionali competenti".
[32] Sentenza Gjuzi, § 9.4; sentenza Giorgi, § 12.4 cit:

obbligatorio l'arresto in flagranza, così come previsto dall'art. 270 comma 1 c.p.p. Qualora, poi, tali intercettazioni fossero state eseguite all'estero in rapporto ad indirizzi di comunicazione situati in Italia, opererebbe senz'altro l'obbligo di notifica delle operazioni alle competenti autorità italiane in forza degli artt. 31 della direttiva e 24 del d.lgs. n. 108 del 2017. In questi casi, le intercettazioni diverrebbero inutilizzabili qualora non fossero ammissibili in un caso interno analogo: per quanto concerne l'Italia, se fossero state disposte in rapporto a reati per i quali non sarebbero consentite secondo l'ordinamento interno. Secondo le Sezioni Unite, nelle vicende considerate, anche tali condizioni potevano dirsi rispettate, in quanto le accuse avevano ad oggetto il reato di associazione per delinquere finalizzata al traffico di stupefacenti. Appare evidente come la Suprema Corte abbia configurato il percorso motivazionale alla luce del principio di diritto in base al quale "l'utilizzabilità del contenuto di comunicazioni scambiate mediante criptofonini, già acquisite e decrittate dall'autorità giudiziaria estera in un procedimento penale pendente davanti ad essa, e trasmessa sulla base di Ordine Europeo di Indagine, deve essere esclusa se il giudice italiano rileva che il loro impiego determinerebbe una violazione dei diritti fondamentali". Il sistema dell'OEI è infatti ispirato al principio di "presunzione relativa" di conformità ai diritti fondamentali delle attività istruttorie svolte dalle autorità giudiziarie degli altri Stati dell'Unione per cui "l'onere di allegare e provare i fatti da cui inferire la violazione di diritti fondamentali grava sulla difesa, quando è questa a dedurre l'inutilizzabilità o l'invalidità di atti istruttori acquisiti dall'autorità giudiziaria italiana mediante OEI", principio applicato anche nel settore delle rogatorie, e in ogni caso riconducibile al principio generale vigente nell'ordinamento nazionale [33].

Il controllo sulle ragioni di merito dell'emissione dell'OEI è operato dal giudice nazionale chiamato ad utilizzare le prove, anche se già autonomamente raccolte all'estero, e non può fare a meno di una valutazione in ordine del rispetto dei presupposti di merito di emissione dell'OEI stabiliti dalla lex fori[34] anche per evitare che l'impiego dell'OEI ai fini della trasmissione di prove già autonomamente raccolte all'estero abbia l'effetto di eludere le condizioni previste dalla lex fori[35].

9. *Segue:* Il controllo sulle modalità di raccolta delle prove da parte dell'autorità straniera: *gli algoritmi utilizzati dall'A.G.*

Le Sezioni Unite, in questo caso, hanno affermato, che l'impossibilità per la difesa di conoscere gli algoritmi utilizzati dall'autorità giudiziaria straniera per la decriptazione delle comunicazioni "non determina, almeno in linea di principio, una violazione di diritti fondamentali". Se è vero, che la disponibilità di tale algoritmo è "funzionale al controllo di affidabilità del contenuto delle comunicazioni", deve però osservarsi che "il pericolo di alterazione dei dati non sussiste, salvo specifiche allegazioni di segno contrario, in quanto il contenuto di ciascun messaggio è inscindibilmente abbinato alla sua chiave di cifratura, per cui una chiave errata non ha alcuna possibilità di decriptarlo, anche solo parzialmente" [36]

Da ultimo appare opportuno accennare al disegno di legge, allo studio al Senato, in tema di Sequestro di dispositivi e sistemi informatici o telematici, memorie digitali, dati, informazioni,

---

[33] Considerazioni analoghe si trovano nella sentenza Encrochat della Corte di giustizia, (Corte giust., 30 aprile 2024, M.N., C-670/22),

[34] Il vaglio dovrebbe focalizzarsi sulle "ragioni" che l'OEI dovrebbe indicare: un adempimento previsto in generale dagli artt. 5 § 1 lett. b della direttiva e 30 lett. b del d.lgs. n. 108 del 2017, e che non potrebbe essere omesso solo perchè l'OEI abbia ad oggetto prove già in possesso dell'autorità di esecuzione.

[35] V. anche Corte giust., Gavanozov II, (Prima Sezione) 11 novembre 2021,cit., § 54.

[36] E' opportuno che le produzioni dei flussi comunicativi acquisiti con OIE siano corroborate, da parte del pubblico ministero, da una disamina analitica del procedimento penale originario nel quale tali dati sono stati acquisiti, delle procedure e delle tecniche utilizzate e dei provvedimenti autorizzativi. Un esempio significativo è rappresentato dall'ordinanza del Tribunale del Riesame di Reggio Calabria del 23/11/2023, la quale, decidendo sul rinvio della Cassazione di cui alla sentenza n. 44155/23 del 26/10/2023, ha nuovamente confermato l'ordinanza genetica, dando atto delle più articolate produzioni effettuate dal pubblico ministero, contenenti una rassegna organica e puntuale dei provvedimenti autorizzatori francesi, delle tecniche di intercettazione dei server, delle modalità di conservazione dei dati e della identificazione dei dati di rilievo per i procedimenti interni. Ne deriva anche la necessità di selezione corretta dei dati comunicativi per consentire alla autorità giudiziaria italiana di valutarne la pertinenzialità, completezza e utilità alle fattispecie oggetto dei procedimenti penali interni.

programmi, comunicazioni e corrispondenza informatica inviate e ricevute (nuovo art. 254-ter c.p.p.), il quale prevede che, nel corso delle indagini preliminari, il giudice per le indagini preliminari, a richiesta del pubblico ministero, disponga con decreto motivato il sequestro di dispositivi e sistemi informatici o telematici, o di memorie digitali, necessari per la prosecuzione delle indagini in relazione a circostanze e modalità dei fatti e nel rispetto del criterio di proporzione. Qualora il pubblico ministero, poi, intenda procedere al sequestro dei dati inerenti a comunicazioni, conversazioni o corrispondenza informatica inviate e ricevute (chat *et similia*), lo richiede al giudice per le indagini preliminari, che provvede con un distinto e ulteriore decreto motivato, disponendo il sequestro in presenza dei presupposti di cui al primo periodo e agli articoli 266, comma 1, e 267, comma 1, c.p.p. (come nelle intercettazioni). Inoltre, copia del decreto di sequestro è notificata all'avente diritto alla restituzione del dispositivo [...]. La riforma, anche in base ai lavori preparatori, non inciderebbe sulle acquisizioni di dati comunicativi delle piattaforme criptate in oggetto, nel senso di determinare la necessaria autorizzazione preventiva del GIP, e ciò sia per la disposizione transitoria, secondo la quale le norme in via di introduzione si applicano alle perquisizioni e ai sequestri la cui esecuzione ha avuto inizio in data successiva alla sua entrata in vigore, sia perché, nel caso in cui venga valorizzata l'interpretazione secondo la quale si è di fronte a un trasferimento di prove precostituite all'estero quand'anche l'atto sottostante fosse qualificato come intercettazione, lo stesso può essere adottato con un semplice provvedimento del pubblico ministero.

Con il D.Lgs. 7 dicembre 2023, n. 203 l'Italia, nell'ottica di una più intensa cooperazione giudiziaria relativa al contrasto all'accumulazione illecita di patrimoni, ha adeguato la normativa nazionale al regolamento (UE) 2018/1805 del Parlamento europeo e del Consiglio del 14 novembre 2018 relativo al riconoscimento reciproco dei provvedimenti di congelamento (sequestri) e di confisca[37].

Appare opportuno segnalare che nella G.U. n. 230 del 1° ottobre 2024 è stato pubblicato il d.lgs. 4 settembre 2024, n. 138 recante il «Recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE)

[37] Vi sono ricompresi la confisca diretta di cui all'art. 240 c.p., a cui devono essere aggiunte, aderendo al più recente indirizzo giurisprudenziale (Corte cost., 25/3/2015, n. 49, che analizza la questione con riferimento alla confisca urbanistica di cui all'art. 44D.P.R. 6 giugno 2001, n. 380, T.U. edilizia; Cass. pen., Sez. un., 26/6/2015, n. 31617), le confische disposte in caso di prescrizione del reato dopo la condanna di primo grado. La confisca c.d. "allargata" ex art. 240-bis c.p., rappresentando questa l'ipotesi di confisca di cui all'art. 5 della direttiva 2014/42/GAI. Tale inclusione potrebbe essere sostenuta, ma si deve tenere conto dei rilievi proposti dalla Corte costituzionale, in merito allo standard probatorio: infatti, la confisca di cui all'art. 5, nel prevedere in capo agli Stati poteri estesi di confisca, qualifica espressamente la circostanza della sproporzione come uno degli "elementi di prova" di cui il giudice può disporre per convincersi che i beni derivino da condotte criminose.
L'ipotesi di confisca, disciplinata dall'art. 240-bis c.p., dovrebbe rientrare nell'ambito di applicazione del Regolamento anche nel momento in cui venga prevista in un procedimento di esecuzione: questo profilo è confermato dalla previsione di cui all'art. 676 c.p.p. (le Sezioni unite, infatti, hanno affermato che non vi è una violazione del diritto alla difesa, costituzionalmente garantito dall'art. 24, comma 2, Cost., "perché tale diritto non è da intendersi in senso assoluto, ma va modulato secondo l'oggetto" (Cass. pen., Sez. Un., 17/7/2001, n. 29022). E questa possibilità, ad oggi, è anche confermata a seguito dell'introduzione del comma 1 dell'art. 183-quater D.Lgs. n. 271/1989 ad opera del D.Lgs. n. 21/2018, trattandosi, in ogni caso, di un "procedimento in materia penale", nell'accezione conforme al significato specificato al considerandum n. 13 del regolamento. Per quanto concerne la confisca di prevenzione e le critiche relative alla sua inclusione all'interno dell'ambito di applicazione dello strumento regolamentare, di cui al D.Lgs. n. 159/2011 deve essere considerato che il Regolamento richiede che il provvedimento di confisca, emesso dallo Stato che ne auspica il riconoscimento, rispetti le "garanzie della materia penale". Pertanto in base agli approdi più recenti della dottrina e della giurisprudenza, la ricomprensione della confisca di prevenzione disciplinata dal D.Lgs. n. 159/2011 all'interno dell'ambito di applicazione del Regolamento 1805/2018, deve ritenersi possibile anche alla luce del provvedimento della Corte EDU adottato nella vicenda Cavallotti (Corte EDU, Sez. I, 28/8/2023, Applicazione n. 29614/16). La circostanza che venga in rilievo il principio di stretta legalità, intesa sia come esistenza di una base legale, sia come direttiva di standard legislativi sufficientemente precisi, accessibili e prevedibili, con il divieto di applicazione del principio di retroattività , della proporzione, della necessità e della ragionevolezza della misura di prevenzione a fronte del ricorso sempre più ampio e generalizzato agli "strumenti più estremi della politica criminale" compreso il ne bis in idem, che impone la proporzionalità complessiva delle sanzioni irrogate, giustifica la risposta affermativa alla questione in esame.
In dottrina v. L. Della Ragione, *D.Lgs. 203/2023: l'Italia si adegua alla normativa europea in tema di congelamento e confisca,* in *Il Quotidiano Giuridico*, Rivista on line, 2024

n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148». Il d.lgs. n. 138/2024 stabilisce misure volte a garantire un livello elevato di sicurezza informatica su tutto il territorio italiano, contribuendo così ad incrementare il livello comune di sicurezza nell'Unione europea in ossequio alla direttiva (UE) 2022/2555, che ha obbligato gli stati membri dell'UE ad adottare strategie nazionali efficaci in materia di cybersicurezza proprio in base alla considerazione che «*la rapida trasformazione digitale e l'interconnessione della società [...] ha portato a un'espansione del panorama delle minacce informatiche, con nuove sfide che richiedono risposte adeguate, coordinate e innovative in tutti gli Stati membri*» (cons. n. 3)[38].

10. Valutazioni conclusive (...assolutamente parziali e provvisorie)

La realtà che si manifesta propone una grande sfida della cui importanza è necessario essere pienamente consapevoli, caratterizzata da una serie di elementi, alcuni sicuramente estranei alla giurisprudenza e alla legislazione fino a qualche anno fa, come i connotati innovativi della prova elettronica, la sua peculiare localizzazione e la necessità della sua conservazione, le fonti private (Internet Service Provider) da cui frequentemente nasce e presso cui è reperibile, la connotazione specificamente transnazionale del reato, nel cui ambito spesso assume rilievo probatorio, la necessità di strumenti investigativi di particolare sofisticazione tecnologica, la necessaria volatilità e durata limitata nel tempo[39]. Uno scenario che consegna all'interprete una nuova prospettiva sul diritto che fa riferimento all'interconnessione che si realizza fra i diversi ordinamenti nel tempo della legalità plurale, dove il principio di legalità, in materia penale, unitamente ai suoi corollari, riceve nuova linfa dal diritto sovranazionale, proprio in forza del collante derivante dagli stessi principi fondamentali, in tema di legalità, determinatezza e tassatività, in quanto la piattaforma multilivello delle fonti del diritto non conduce ad esiti contrastanti, e l'ottica dell'interlegalità comporta una precettività giuridica condivisa tra più ordinamenti[40]. Condizioni che strutturalmente richiedono approcci innovativi nell'esercizio della giurisdizione, adeguando i parametri concettuali e normativi all'ineludibile incremento dell'attività di cooperazione internazionale. Una sfida che, senza enfasi, va oltre i confini dei singoli Stati, per coinvolgere le istituzioni a tutti i livelli, a tutela del principio di legalità sostanziale e processuale all'interno di un "sistema di sistemi" complesso, che richiede allo stesso tempo una attività di interpretazione unitaria funzionale a un risultato di unità, completezza, coerenza in attuazione dei principi del giusto processo, sotto il profilo del rispetto del diritto di difesa e del contraddittorio e a tutela, alla fine, dei principi fondanti della nostra Democrazia costituzionale.

---

[38] In dettaglio il d.lgs. 4 settembre 2024, n. 138 sulla Cybersicurezza prevede:1) una Strategia nazionale di cybersicurezza; 2) l'integrazione del quadro di gestione delle crisi informatiche; 3) la conferma dell'Agenzia per la cybersicurezza nazionale quale Autorità nazionale competente NIS, punto di contatto unico NIS e Gruppo di intervento nazionale per la sicurezza informatica in caso di incidente in ambito nazionale; 4) la designazione dell'Agenzia per la cybersicurezza nazionale e del Ministero della difesa quali Autorità nazionali di gestione delle crisi informatiche su vasta scala; 5) l'individuazione di Autorità di settore NIS che collaborano con l'Agenzia per la cybersicurezza nazionale; 6) l'indicazione dei criteri per l'individuazione dei soggetti a cui si applica il decreto e la definizione dei relativi obblighi in materia di misure di gestione dei rischi per la sicurezza informatica e di notifica di incidente; 7) l'adozione di misure in materia di cooperazione e di condivisione delle informazioni ai fini dell'applicazione del decreto in oggetto (v. nota Sistema penale, riv. *on line* 9.10.2024).

[39] F S. Ragazzi-F. Spiezia, *Decifrare, acquisire e utilizzare le comunicazioni criptate in uso alla criminalità organizzata: uno sguardo europeo, in attesa del count-down italiano,* in sistemapenale.it, 26 febbraio 2024, f. 2, p. 223 s;

[40] Ci si consenta *ex plurimis* il riferimento a G. Diotallevi, *Il giusto processo e le garanzie del diritto di difesa nel sistema multilivello del diritto europeo,* in *CEDU e Ordinamento italiano, La giurisprudenza della CEDU e l'impatto nell'ordinamento interno,* a cura di Angela Di Stasi (2016- 2020), p. 368 e ss.
E. Scoditti, *Lo scenario dell'interlegalità,* in *Questione Giustizia,* Rivista on line, 22 aprile 2020.