ISSN 1121-1725

Pubblicazione trimestrale
Anno XXXI

3-4/2018

CEDAM

Rivista trimestrale di
Diritto penale dell'economia

edicolaprofessionale.com/RTDPE

Wolters Kluwer

Poste italiane s.p.a. - Spedizione in Abbonamento Postale - D.L. 353/2003 (conv. in L. 27/02/2004 n° 46) art. 1, comma 1 - DCB Milano
Pubblicazione trimestrale - Con I.P.

Lorenzo Picotti (*)
Prof. ordinario di diritto penale nell'Università di Verona

PROFILI PENALI DEL *CYBERLAUNDERING*: LE NUOVE TECNICHE DI RICICLAGGIO

Sommario: 1. Introduzione: oggetto e limiti dell'indagine. – 2. Definizione di *cyberlaundering* e forme di manifestazione del fenomeno. – 3. Crittografia, abuso dell'identità digitale ed anonimato quali «tecniche» caratteristiche dei comportamenti penalmente illeciti nel *Cyberspace.* – 4. Gli specifici profili penali del *cyberlaundering* come *cybercrime* in senso ampio. – 5. Sui «nuovi» reati presupposto ed i «nuovi» reati strumentali riconducibili al fenomeno del *cyberlaundering*. – 6. Osservazioni conclusive: prospettive di prevenzione e contrasto.

1. – Il tema del *cyberlaundering* è oggi particolarmente attuale ed interessante, perché incrocia due importanti profili di novità per il penalista: quello del riciclaggio, moderno "reato economico" caratterizzato da una preoccupante espansione e da incessanti fenomeni di evoluzione ed adattamento, nelle sue modalità di realizzazione ed estensione, alle nuove opportunità di natura tecnica, oltre che finanziaria, aperte dall'odierna società globalizzata; e quello dei *cybercrimes*, la cui evoluzione e non meno preoccupante espansione meritano da tempo specifica attenzione da parte di penalisti e studiosi, oltre che di organismi internazionali e forze di *law enforcement*, dato il crescente impatto che le nuove "tecnologie dell'informazione e della comunicazione" (c.d. TIC) hanno sull'incessante trasformazione e manifestazione delle più svariate attività penalmente illecite che si realizzano nel c.d. *Cyberspace* (1).

(*) Rielaborazione ed aggiornamento, con aggiunta di note, della relazione svolta al Convegno internazionale di studio per il XXX anno dalla fondazione della *Rivista trimestrale di diritto penale dell'economia*: "Trent'anni di diritto penale dell'economia. In memoria di Giuseppe Zuccalà" svoltosi a Verona il 20 e 21 ottobre 2017.

(1) Per un inquadramento generale sul significato e la rilevanza del *Cyberspace* nonché l'analisi e la classificazione dei *cybercrimes*, sia consentito rinviare a L. Picotti, *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in Id., (cur.), *Il diritto penale dell'informatica nell'epoca di Internet*, Cedam, Padova 2004, p. 21 s.; e, da ultimo, Id., *Diritto penale e tecnologie informatiche: una visione d'insieme*, in A. Cadoppi, S. Canestrari, A. Manna, M. Papa (cur.), *Cybercrime* (in corso di pubblicazione).

Il presente contributo si articola pertanto in tre parti: dopo la necessaria definizione e la sintetica illustrazione del fenomeno, che serviranno ad evidenziare il ruolo delle TIC ed in specie del *web* nella commissione dei reati di riciclaggio nelle diverse fasi in cui può scomporsi (§ 2), l'attenzione si concentrerà sui profili propriamente giuridico-penali del *cyberlaundering*, per analizzarne la sussumibilità in una pluralità di figure delittuose, che tenga conto delle sue diverse fasi e della possibilità di ricondurle sistematicamente alla categoria dei *cybercrimes* "in senso ampio" (§§ 3 e 4). Non si tratta soltanto di riconoscere il rilievo penale delle nuove modalità e tecniche di commissione di questi reati, bensì di evidenziare che la specifica potenzialità espansiva del fenomeno, nel contesto contemporaneo, porta a coinvolgere nuove tipologie di *reati-presupposto* ed a far emergere altresì una pluralità di "nuovi" *reati strumentali*, la cui commissione serve a soddisfare gli interessi (illeciti) al cui perseguimento è funzionale la complessa attività criminosa in esame (§ 5). In chiusura si accennerà alle attuali prospettive di prevenzione e contrasto, necessariamente aperte ad una dimensione sovranazionale, per non lasciare il "mondo cibernetico", in cui anche l'economia legale ed illegale è immersa, privo di un'efficiente regolazione giuridica, necessariamente affidata anche alle sanzioni penali (§ 6).

2. – Cosa s'intende per *cyberlaundering*?

Ai fini della presente indagine il concetto va in prima approssimazione inteso in senso ampio, in un'accezione criminologica, prima che giuridico-penale [2], quale *fenomeno* complesso che comprende l'insieme di tutte le attività illecite finalizzate a "ripulire" (letteralmente: "lavare") non solo il "denaro" (*moneylaundering*), ma più in generale i capitali, i beni, i valori o le altre "utilità" di provenienza delittuosa, ricorrendo a sistemi o mezzi elettronici o, meglio, "cibernetici", resi disponibili dalle TIC, che coinvolgono oggi soprattutto la "rete": vale a dire il *web* da intendersi in senso ampio, quale *Cyberspace* comprensivo sia di Internet, nella tradizionale dimensione del *world wide web* (www), che dei nuovi e diversi protocolli

---

[2] Sull'importanza di muovere, per un efficace approccio anche penalistico, dal riconoscimento della "dimensione" empirica ed economica del fenomeno, storicizzandone e valutandone l'impatto nella sua ampiezza, estensione globale ed evoluzione anche tecnica, cfr. – nella assai vasta produzione sul tema – E. CAPPA, D. CERQUA (cur.), *Il riciclaggio del denaro. Il fenomeno, il reato, le norme di contrasto*, Milano 2012, ed ivi in specie P. L. VIGNA, *Il fenomeno criminale*, p. 3 s.; D. MASCIANDRO, *Reati e riciclaggio: profili di analisi economica*, p. 15 s.; nonché F. BRUNI, D. MASCIANDRO (cur.), *Mercati finanziari e riciclaggio. L'Italia nello scenario internazionale*, Milano 1998.

di comunicazione, connessione e scambio oggi sviluppatisi a livello globale, fino al c.d. *deep* nonché *dark-web* (3).

In sintesi, le attività criminose oggetto d'esame sono specificamente quelle che possono dirsi – in tutto od in parte – commesse nel *Cyberspace*, configurando quindi dei *cybercrimes* (4).

Nel fenomeno del *cyberluandering*, non diversamente da quanto già emerso da tempo nell'analisi del *moneylaundering* inteso nella sua ampia nozione criminologica, possono distinguersi molteplici fasi: dalla "sostituzione", al "trasferimento" alle "altre operazioni che ostacolano l'identificazione della provenienza" (5). Attività e condotte non riducibili tutte entro la definizione giuridico-positiva del nostro delitto di "riciclaggio" di cui all'art. 648-*bis* c.p., comprendendo anche il "reinvestimento di capitali di provenienza illecita" (art. 648-*ter* c.p.) e il c.d. auto-riciclaggio (art. 648-*ter*.1 c.p.), nonché altri reati strumentali, accessori o comunque connessi, ai quali sono riconducibili ulteriori attività ed operazioni che realizzano o preparano le predette "fasi", idonee ad "occultare" la provenienza criminale ed a "convertire" o "far circolare" il denaro, i capitali, i beni, i valori, le utilità predette tramite strumenti di pagamento, accumulo, investimenti, scambi o trasferimenti di diversa natura od intestazione, capaci – in sintesi – di *trasformarne* il potere d'acquisto "potenziale", non direttamente od efficacemente spendibile sul mercato, in un potere d'acquisto "effettivo" nel

---

(3) *Dark web* (in italiano: *web* oscuro o rete oscura) è il termine che si usa per definire l'insieme delle *darknet* ("reti oscure") che si raggiungono via Internet solo attraverso specifici *software*, configurazioni e accessi autorizzativi, caratterizzate da contenuti in gran parte criptati, anziché gli usuali *browser* comunemente disponibili. Esso è in realtà soltanto una parte del *deep web*, che è tutta la enorme parte del *web* che non è indicizzata dai motori di ricerca, per cui sarebbe erroneo, come talora si confonde, utilizzare il termine *deep web* per riferirsi al (solo) *dark web*. Le *darknet* includono sia piccole reti *friend-to-friend* o *peer-to-peer*, come reti grandi e famose quali *Tor*, *Freenet* e *I2P*, in cui operano organizzazioni pubbliche e singoli individui. Alla DARKNET "Tor" si fa riferimento come *onionland* (terra della cipolla, in riferimento alla sua tecnica di anonimizzazione "*onion routing*" e al suo suffisso di dominio ".onion") (definizioni da *Wikipedia*, voce *Darkweb*).

(4) Sul passaggio dalla categoria dei *computer-crimes* a quella dei *cybercrimes*, nella dottrina penale italiana volendo cfr. già L. PICOTTI, *Introduzione* a Id. (cur.), *Il diritto penale dell'informatica,* cit., in specie p. VII. Per precisazioni sulle distinzioni fra reati informatici e reati cibernetici, sia consentito rinviare a L. PICOTTI, *Diritto penale e nuove tecnologie*, cit., in specie § 5.

(5) La tradizionale distinzione in tre fasi dell'attività di riciclaggio – *placement* (piazzamento materiale dei proventi es. dei contanti presso istituti bancari), *layering* (stratificazione tramite operazioni volte a separare il capitale dalla sua origine, ad es. spostandolo in paradisi *off shore*) ed *integration* (integrazione nei circuiti legali con investimenti leciti) – potrebbe essere ricondotta a quelle di "sostituzione", "trasferimento", "altre operazioni che ostacolano l'identificazione della provenienza".

sistema economico (legale e non), realizzando in concreto gli evidenti vantaggi competitivi derivanti dalla loro origine illecita.

Tra questi, oltre ad immediati profitti indebiti, si devono considerare, quali esiti pratici ed anzi spesso finalità del riciclaggio ampiamente inteso, anche le "infiltrazioni" nei gangli vitali dell'economia legale (e non) e persino della politica, mediante l'acquisizione dei poteri di gestione e di controllo di imprese, società, organismi, enti, amministrazioni, resa possibile proprio grazie ai cospicui mezzi illeciti resi disponibili, che facilitano (fra l'altro) corruzioni pubbliche e private su larga scala (6).

Il ventaglio di questo complesso di attività criminose è dunque assai ampio ed articolato, non riducendosi il fenomeno criminologico del *cyberlaundering* alla dimensione dei singoli reati già menzionati, ma dovendo piuttosto estendersi, a titolo esemplificativo, alla falsificazione di carte di credito o di pagamento, al loro utilizzo indebito, all'abuso (o "furto") di identità e di *account* nonché, più in generale, ad ogni sorta di operazioni nel *web*, specie in circuiti illeciti o non regolamentati, che possono integrare altresì reati bancari, societari, tributari ed in materia di mercati finanziari, oltre che violazioni ed irregolarità di natura amministrativa e disciplinare che vi siano connesse (7).

L'esempio più banale di *cyberlaundering* è l'utilizzo di una carta di pagamento elettronica "ricaricabile" (c.d. *smart card*), che consenta l'acquisto di beni o servizi, spendendo i proventi illeciti nel mercato legale, apparentemente "ripuliti" dal transito per detto mezzo di pagamento co-

---

(6) In argomento, sulle diverse fasi del fenomeno globalmente inteso, cfr. A. R. CASTALDO, M. NADDEO, *Il denaro sporco. Prevenzione e repressione nella lotta al riciclaggio*, Padova 2010, in specie p. 13 s. in cui si evidenzia il passaggio da un modello a due fasi (lavaggio: *money laundering*; e reimpiego: *recycling*) ad uno a tre fasi, più adeguato allo scenario odierno, vale a dire: a) il "piazzamento" o "collocamento" (c.d. *placement*), in cui si ha il materiale versamento dei proventi illeciti nel mercato, tramite istituzioni o intermediari finanziari od acquisto di beni; b) la "stratificazione" (c.d. *layering*), in cui si fornisce una copertura alla ricchezza proveniente dal reato "avvalendsi di un caleidoscopio di operazioni anche contemporanee, fra loro correlate e sempre mutevoli" (es. *wire transfer* di fondi, triangolazioni di società con sedi *off shore*, ricostruzioni simulate di *paper trials*); c) l'"integrazione" (c.d. *integration*) vale a dire la definitiva (re-)immissione nei circuiti economici legali dei proventi così "lavati" ed ormai indistinguibili da quelli di qualsiasi attività lecita, fatti transitare attraverso banche, societá assicurative, o di intermediazione accreditate, grossi studi legali o altri filtri ritenuti al di sopra di ogni sospetto. Con precipua attenzione ai profili tecnici v. altresì S. MULINARI, *Cyberlaundering. Riciclaggio di capitali, finanziamento del terrorismo e crimine organizzato nell'era digitale*, Milano 2003, p. 1 s.

(7) Sulla diversità di nozioni, ai fini penali ed ai fini amministrativi, si vedano i diversi contributi raccolti in A. MANNA (cur.), *Riciclaggio e reati connessi all'intermediazione mobiliare*, Torino 2000; sulla relativa disciplina di prevenzione cfr. ampiamente A. R. CASTALDO, M. NADDEO, *Il denaro sporco*, cit., p. 253 s.

mune, il cui valore viene reso disponibile con modalità idonee ad occultarne l'origine, ad es. tramite falsa identità del titolare o mediante "clonazioni" o manipolazioni informatiche, rapidamente eseguibili con programmi relativamente semplici, rinvenibili anche in siti *web* (ed in specie nel *dark web)*.

Le scommesse illegali ed i giochi d'azzardo in rete, oggi estremamente diffusi, rappresentano altre occasioni di riciclaggio – come lo era il "tradizionale" gioco al casinò, perlomeno prima che fosse oggetto di particolare regolamentazione da parte della disciplina antiriciclaggio – accanto a ben più sofisticate forme, per importi anche ingenti, di trasferimenti elettronici di fondi ed investimenti di ogni tipo, che prevedono passaggi e transazioni strumentali via *web*, capaci di rendere impossibile o molto difficile risalire alla loro origine od all'identità dei soggetti da cui realmente provengano od a cui siano destinati, grazie all'anonimato, alla crittografia, all'abuso dell'identità "digitale", cui direttamente od indirettamente si può ricorrere nel *Cyberspace*.

Se si cerca in Internet, anche senza necessità di scandagliare il menzionato *dark web*, si rinvengono offerte di "servizi finanziari" *off-shore* in grado di dare risultati immediati e riservati, ad esempio grazie ad acquisti di valori mobiliari o di immobili ovvero reinvestimenti di ogni natura in "tempo reale" – per lo più aventi collocazione od effetti in paesi o continenti diversi da quelli d'origine, possibilmente in paradisi fiscali, in cui i controlli siano assenti o poco efficaci – che permettono di occultare o comunque di far perdere subito le tracce, con una serie adeguata di movimentazioni o transazioni elettroniche, della provenienza (soggettiva od oggettiva) dei capitali, dei valori, delle "utilità" in tal modo *ripuliti* e resi quindi disponibili per l'impiego, la spendita od il consumo in altri circuiti, legali o non (8).

2.1. – Pur senza alcuna pretesa di esaustività, per un inquadramento dei mezzi e delle modalità *tecniche* che connotano oggi il fenomeno del *cyberlaundering* è utile considerare, ai fini dell'indagine giuridica – accanto alle attività di *diretto* rilievo economico e finanziario realizzabili nel *Cyberspace* nell'ampio mondo del commercio elettronico e dei possibili investimenti via *web*, ovvero ai menzionati giochi d'azzardo, nonché scommesse illegali *on-line* – soprattutto i moderni *mezzi di pagamento elettronici* la cui

(8) Per esemplificazioni "sperimentali" cfr. già A. SCARTEZZINI, *Il rischio di riciclaggio in Internet: alcune ipotesi di regolazione*, in L. PICOTTI (cur.), *Il diritto penale dell'informatica*, cit., p. 433 s.

marcata evoluzione e diversificazione li rende particolarmente interessanti alla luce dei più recenti sviluppi.

Si è appena fatto cenno alle *smart card*, o carte intelligenti, che sono alternative all'utilizzazione e circolazione di denaro contante. Proprio per limitarlo, l'utilizzo di carte di credito, di debito, di pagamento è anzi richiesto, se non addirittura reso obbligatorio in molti casi ed in un numero sempre maggiore di ordinamenti (9), dalla disciplina di prevenzione del riciclaggio e di altri reati, in specie fiscali. In linea di principio, infatti, l'utilizzo di tali "carte" consente di "tracciare" (elettronicamente) i passaggi di denaro ed i pagamenti anche minuti, rendendo individuabile la fonte delle somme spese e/o spendibili, ma solo in quanto siano da addebitare su un conto corrente riconducibile ad un soggetto identificato oppure "caricate" in anticipo tramite un *chip* in esse incorporato, che ne consenta la memorizzazione per un ammontare determinato, riferendosi a disponibilità, in linea di principio, parimenti identificabili. Però non solo è, di fatto, tecnicamente possibile manipolare ed anche duplicare o riprodurre abusivamente (c.d. clonazione) i *chip* tramite i quali sono elaborati e memorizzati i dati – sia identificativi della carta o del suo portatore, se nominale, sia relativi ai valori disponibili – e le operazioni effettuate, ma anche intervenire, senza diritto, sui programmi di gestione, ad es. per superare i limiti massimi prefissati, moltiplicando le possibilità di utilizzo, ovvero facendo apparire una diversa provenienza fittizia. E si possono anche sfruttare le carenze di controllo o le compiacenze nell'applicazione della disciplina preventiva antiriciclaggio al momento dell'emissione, veicolata da regole e prassi contrattuali con l'ente bancario o finanziario emittente, che può essere anche straniero od extracomunitario, e la cui violazione dovrebbe da questi enti essere prevenuta e, se del caso, segnalata, non essendo invece per lo più tecnicamente rilevabile dal beneficiario dei pagamenti così effettuati e ben più complessa o meno efficace da accertare *ex post*.

2.2. – Tornando più in specifico alle *smart card* ricaricabili, ad es., l'identificazione iniziale del titolare o del beneficiario, che deve avvenire al momento dell'emissione e consegna del documento (informatico) e della stipula del contratto che ne disciplina l'uso, può essere di fatto elusa, sia rilasciandola ad un rappresentante legale di una società o di un ente di comodo, per utilizzarne i dati "soggettivamente" fittizi nelle transazioni,

---

(9) In forza delle Convenzioni internazionali, delle Raccomandazioni del Gruppo GAFI e delle Direttive europee via via susseguitesi, su cui si tornerà.

sia occultando l'utilizzatore reale con un prestanome e con passaggi successivi, anche semplicemente consegnandola per l'uso ad un terzo non identificabile, ma fornito soltanto delle necessarie "credenziali informatiche" (codice identificativo, PIN, *password*), in modo da lasciare coperto da un anonimato "di fatto" il soggetto *realmente* autore o beneficiario della transazione, così da occultare le provenienze o le destinazioni *effettive* delle somme spese o messe in circolazione.

2.3. – Più in generale, è da tempo che lo stesso sistema bancario offre sempre più servizi *on-line* ai propri clienti (c.d. *on-line banking* od *home banking*), che danno possibilità di accesso e gestione diretta dei rapporti bancari e finanziari, in modalità interamente digitale ad opera dello stesso utente, che può sfruttare le caratteristiche di "ubiquità" ed immediatezza, rese disponibili e sempre più efficienti grazie ai moderni dispositivi portatili – quali *tablet, smartphone, mobile* in genere – ed alla accessibilità pressoché permanente alla rete: per cui grazie a semplici programmi od *app* "scaricabili" anche sui predetti dispositivi portatili, si può operare dall'ufficio, da casa, in viaggio, all'estero, da ogni luogo ed in ogni momento in cui la rete sia accessibile, od anche posticipando gli effetti a momenti successivi in cui lo diventi od in cui sia più opportuno conseguirli, frazionando così pagamenti e trasferimenti nel tempo e nello spazio, od individuando beneficiari o destinazioni di comodo, senza l'immediato controllo del personale dell'istituto bancario o finanziario, che dovrebbe effettuare le segnalazioni di "operazioni sospette".

2.4. – Ma in quest'imponente sviluppo tecnologico, che coinvolge e modifica necessariamente il comportamento degli operatori e degli utenti, occorre distinguere i moderni sistemi di pagamento mediante "moneta elettronica", necessariamente connessi ad un "emittente autorizzato" ed appoggiati ad un conto corrente bancario o ad una carta di credito o di pagamento, o comunque a fonti di alimentazione tradizionali della necessaria "provvista" (quali bonifici e trasferimenti di fondi, addebiti e prelievi di somme *on-line* consentiti dal titolare, che servono ad alimentare e "ricaricare" il credito disponibile, specie delle *smart card*), dai più inquietanti sistemi di pagamento "deregolamentati" e spesso senz'altro illegali, che si stanno impetuosamente diffondendo.

Si può muovere dal paradigmatico esempio del sistema *Paypal*, od altri analoghi, ormai diffusi a livello globale e divenuti (in linea di principio) compatibili con la disciplina bancaria anche europea, relativa alla c.d. moneta elettronica (*e-money*), giuridicamente definita dall'art. 2, punto

2), della direttiva 2009/110/CE [10], alle cui regolamentazioni tali sistemi di pagamento si sono adattati, essendo rispetto ad essi intervenuta anche la IV direttiva antiriciclaggio [11], attuata nel nostro ordinamento dal d.lgs.

---

[10] Cfr. l'art. 2, punto 2) che definisce «moneta elettronica» il "valore monetario memorizzato elettronicamente, ivi inclusa la memorizzazione magnetica, rappresentato da un credito nei confronti dell'emittente che sia emesso dietro ricevimento di fondi per effettuare operazioni di pagamento ai sensi dell'articolo 4, punto 5), della direttiva 2007/64/CE e che sia accettato da persone fisiche o giuridiche diverse dall'emittente di moneta elettronica".

[11] Il considerando 7 della menzionata direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo, che vale la pena riportare, recita: "L'utilizzo dei prodotti di moneta elettronica è sempre più considerato un sostitutivo dei conti bancari, il che, in aggiunta alle misure previste dalla direttiva 2009/110/CE del Parlamento europeo e del Consiglio, giustifica che essi siano assoggettati agli obblighi di prevenzione e contrasto del riciclaggio e della lotta al finanziamento del terrorismo (*Anti-Money Laundering/Combating the Financing of Terrorism*: AML/CFT). Tuttavia, in talune comprovate circostanze di rischio esiguo e a rigorose condizioni di mitigazione del rischio, *gli Stati membri dovrebbero poter esonerare i prodotti di moneta elettronica da determinate misure di adeguata verifica della clientela* [corsivo agg.], quali l'identificazione e la verifica del cliente e del titolare effettivo, ma non dal controllo delle operazioni o dei rapporti d'affari". In particolare, quando la moneta elettronica serva solo per l'acquisto di beni e servizi e l'importo memorizzato elettronicamente sia "sufficientemente basso" da impedire l'elusione sostanziale delle norme di prevenzione, gli Stati membri potrebbero esonerarne i soggetti altrimenti obbligati ed autorizzare comunque misure semplificate. In conformità a tali criteri, l'art 12 della direttiva prevede che "gli Stati membri possono consentire ai soggetti obbligati di non applicare determinate misure di adeguata verifica della clientela per la moneta elettronica, se sono rispettate tutte le condizioni [...] di mitigazione del rischio" specificamente elencate, che fanno riferimento anche a valori soglia importi successivamente modificati e ridotti dalla più recente direttiva (UE) 2018/843 del Parlamento e del Consiglio del 30 maggio 2018, che ha riformulato il citato art. 12 della direttiva 2015/849.

In ogni caso, per quanto concerne il nostro ordinamento, l'art. 17 d.lgs. 231/2007, modificato dall'art. 2 d.lgs. 90/2017, non è ricorso ad alcuno dei ridotti limiti di valore monetario contenuti nella stessa direttiva quale condizione per la deroga, così recitando: "Gli obblighi di adeguata verifica della clientela sono osservati altresì nei casi in cui le banche, gli istituti di moneta elettronica, gli istituti di pagamento e Poste Italiane S.p.A. agiscono da tramite o siano comunque parte nel trasferimento di denaro contante o titoli al portatore, in euro o valuta estera, effettuato a qualsiasi titolo tra soggetti diversi, di importo complessivamente *pari o superiore a 15.000 euro* [corsivi agg.]. (…) 6. Nella prestazione di servizi di pagamento e nell'emissione e distribuzione di *moneta elettronica* effettuate tramite agenti in attività finanziaria di cui all'articolo 3, comma 3, lettera c), ovvero tramite soggetti convenzionati e agenti di cui all'articolo 1,comma 2, lettera nn), le banche, Poste Italiane S.p.A., gli istituti di pagamento e gli istituti di moneta elettronica, ivi compresi quelli aventi sede centrale in altro Stato membro, nonché le succursali di questi ultimi, osservano gli obblighi di adeguata verifica della clientela *anche per le operazioni occasionali di importo inferiore a 15.000 euro* [corsivi agg.]". Sui possibili riflessi penali dell'estensione del novero delle "attività criminose" presupposto del riciclaggio, di cui alla IV direttiva 2015/849, cfr. gli spunti (riferiti in specie ai reati fiscali) di R.M. VADALÀ, *La provenienza illecita nel delitto di riciclaggio: possibili novità dalla quarta direttiva antiriciclaggio?* in questa *Rivista*, 2017, p. 234 s.

25 maggio 2017 n. 90, che ha a tal fine modificato in più punti il d.lgs. 21 novembre 2007, n. 231. E da ultimo, la V Direttiva del 2018 è nuovamente intervenuta in materia (12), peraltro con disposizioni cui in parte il legislatore italiano si è già "anticipatamente" conformato, proprio nella materia in esame, avendo a disposizione il relativo progetto (13).

Un account *Paypal* è facilmente attivabile in pochi minuti via Internet, senza alcun contatto fisico o personale con il fornitore del servizio, semplicemente fornendo un indirizzo e-mail ed un numero di cellulare: e consente l'immediata possibilità di effettuare o ricevere pagamenti nel *web*, senza previo deposito di valori o somme di denaro, né loro custodia da parte del prestatore del servizio, fermo solo il conteggio del "dare" ed "avere" (c.d. *balance*), che deve restare entro certi limiti di pareggio o sbilancio, alle condizioni e nei termini temporali contrattualmente prefissati. In tal modo, tutti i singoli movimenti, compresi investimenti di ogni tipo, pagamenti ad esempio in giochi d'azzardo o scommesse, scambi ed acquisiti anche illeciti, ecc., vengono direttamente ed immediatamente eseguiti *on line* dall'utente, superando od almeno posticipando le singole registrazioni e verifiche, operate invece dagli intermediari bancari tradizionali, fermo soltanto il *successivo* addebito o accredito delle somme movimentate sul conto corrente bancario o sulla carta di credito o di debito collegate, che avviene soltanto periodicamente o manualmente, allorché sia richiesto il saldo risultante dal *balance*, dipendente dall'insieme degli addebiti ed accrediti conseguenti alle operazioni che possono essere opportunamente programmate nell'entità e nei tempi. È evidente dunque la possibilità e rapidità di esecuzione in tempo reale di abusi ed operazioni di "piazzamento" ed anche "occultamento", specie se si creano ed utilizzano identità digitali fittizie o sottratte a terzi ignari, la cui ricostruzione *a posteriori* può essere estremamente complessa e risultare comunque tardiva.

2.5. – Ancor più articolato e particolarmente interessante, per il nostro tema, è soprattutto il nuovo fenomeno, emerso ormai anche all'attenzione

---

(12) Sulla direttiva (UE) 2018/843 del Parlamento europeo e del Consiglio del 30 maggio 2018, che modifica la direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo, per quanto qui di interesse, cfr. *infra* nel testo.

(13) Per uno sguardo d'insieme sul d.lgs. 90/2017ed i sui riflessi sulla normativa penale in materia, cfr. T. GIACOMETTI, O. FORENTI, *La nuova disciplina in materia di prevenzione del riciclaggio e di finanziamento del terrorismo (d.lgs. 25 maggio 2017, n. 90),* in *www.penalecontemporaneo.it* (4.7.2017).

dell'opinione pubblica e reso specificamente possibile dalle TIC e dal *web*, dei sistemi di pagamento tramite le c.d. valute virtuali, o "criptovalute", variamente denominate (dai più famosi *Bit-coin* ad *Ethereum*, ecc.), che prescindono cioè non solo dalla materiale circolazione del denaro, quale valore di scambio, ma anche dallo stesso sistema bancario e finanziario, cui invece si connettono pur sempre i servizi di pagamento elettronici e la moneta elettronica, di cui si è sopra detto.

I nuovi sistemi "deregolamentati" di pagamento che si sviluppano nel *Cyberspace* sono sorti *spontaneamente* ad opera di programmatori, produttori, utenti, spesso neppure precisamente identificati, e bypassano il ruolo essenziale di regolazione e controllo sulla moneta, che si esercita tramite l'autorità centrale (BCE, Banca d'Italia, ecc.) nella fase sia dell'emissione che della circolazione, nonché più in generale tramite i soggetti (banche ed altri intermediari finanziari), su cui si concentrano da tempo i formali obblighi antiriciclaggio, in specie d'identificazione ed adeguata verifica della clientela, oltre che di registrazione, segnalazione di operazioni sospette, e quant'altro.

Per le "criptovalute" non interviene alcun soggetto "emittente", che assuma il potere e la responsabilità giuridicamente riconosciuti della loro produzione, raccolta, accumulo e circolazione, essendo i valori espressi quali mezzi di pagamento o di scambio soltanto "virtuali" o, meglio, convenzionali, in quanto vengono (ampiamente) utilizzati ed accettati come tali dagli utenti nel *web*, e soprattutto nel menzionato *dark web*.

Non si tratta di un fenomeno *di per sé* illegale, anche se è prevalentemente sfruttato a fini illeciti di riciclaggio o svolgimento di attività criminose, quali estorsioni, corruzioni, traffici illeciti di ogni genere (dalla droga, alle armi, fino a quelli di persone e di organi).

Oggi vi è anzi un interesse crescente per tali nuovi sistemi di pagamento, dati i molteplici vantaggi che offrono, da parte delle stesse istituzioni bancarie, a livello europeo e mondiale (come dimostra un rapporto della BCE del 2012 ed una sentenza della stessa Corte di Giustizia del 2015, su cui si tornerà (14)), oltre che nazionale (come emerge da una specifica Risoluzione della nostra Agenzia delle Entrate del dicembre 2016, di cui appresso meglio si dirà (15)).

---

(14) CGUE 22.10.2015 C-264/14, su cui cfr. *infra*, nota 19.

(15) Risoluzione dell'Agenzia delle Entrate del 2.9.2016, n. 72, riguardante un interpello sul trattamento fiscale applicabile alle società che svolgono attività di servizi relativi a monete virtuali (*bitcoin*), su cui cfr. *infra*, nota 20.

E del resto, la direttiva (UE) 2018/843 del Parlamento europeo e del Consiglio del 30 maggio 2018, che modifica la direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo, facendosi espressamente carico di prevenire e contrastare l'emergente "*uso improprio per scopi criminali*" delle "criptovalute" (denominate "*valute virtuali*") (16), per l'anonimato che garantiscono alle operazioni loro tramite effettuate (considerando 9), amplia l'ambito di applicazione della disciplina antiriciclaggio già stabilito dalla direttiva 2015/849 anche ai "*prestatori di servizi* [...] *di cambio tra valute virtuali e valute aventi corso legale*" nonché di "*servizi di portafoglio digitale*" (considerando 8 ed art. 1) (17).

Le "criptovalute" sono in effetti ormai centinaia, o forse migliaia, essendo facilmente acquistabili nel *web* ed utilizzabili non solo per pagare o ricevere pagamenti, ma anche per investire, accumulare ed esportare capitali del tutto "virtuali" – il cui valore cioè non solo è espresso in formato esclusivamente digitale, ma ha fondamento soltanto convenzionale – che comunque consentono di effettuare transazioni ed acquisti, contrarre debiti ed ottenere crediti, produrre profitti finanziari e speculativi anche enormi: il tutto senza ricorrere a movimentazioni di denaro, monete o valute ufficiali, né apertura od utilizzo di conti corrente bancari, ovvero appoggio ad essi, né trasferimenti di comuni fondi finanziari o formali finanziamenti od anticipazioni, depositi, prelievi o mutui di tipo tradizionale, né tantomeno necessità di utilizzo di carte di credito o di debito, *smartcard* o altri "documenti" equivalenti emessi da istituti di credito o finanziari ed intestati a soggetti determinati.

I produttori originari delle "criptovalute" restano (o possono restare) celati ed anonimi, essendo soltanto creatori di algoritmi, che vengono poi utilizzati a catena per "estrarre" (da parte dei c.d. *miners*) "blocchi" di dati criptati, che incorporano o, meglio, rappresentano – soltanto *digitalmente* – valori economici solo convenzionalmente riconosciuti come tali da chi li usa,

---

(16) Ai sensi del nuovo numero 18) aggiunto all'art. 3 della direttiva 2015/849 dall'art. 1 della direttiva 2018/843, per "valuta virtuale" si intende "*una rappresentazione di valore 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*".

(17) Ai sensi del nuovo numero 19) aggiunto all'art. 3 della direttiva 2015/849 dall'art. 1 della direttiva 2018/843, per "prestatore di servizi di portafoglio digitale" si intende: "*un soggetto che fornisce servizi di salvaguardia di chiavi crittografiche private per conto dei propri clienti, al fine di detenere, memorizzare e trasferire valute virtuali*".

in un sistema del tutto decentralizzato di nodi di rete collegati (tramite sistemi *peer to peer*), non richiedenti alcuna connessione ad un *server* centrale, ma soltanto la condivisione dei dati stessi, tramite protocolli comuni. La sequenza necessaria di tali "blocchi" di dati criptati è tale, che consente ad ogni operatore – c.d. *miner* – di riconoscere, autenticare e convalidare il blocco precedente ed aggiungerne uno nuovo, se autorizzato tecnicamente dal sistema, allungando la catena di blocchi (per questo si parla di sistemi *Blockchain*, di per sé utilizzabili e sviluppati anche per altri fini, quali la tenuta di sistemi di registrazione cronologicamente certe, ecc.) (18).

Ogni blocco addizionale rinforza e convalida quelli precedenti. Ed il controllo della loro autenticità proviene così solo dalla rete, non da un intermediario o gestore centralizzato. Si crea in pratica un enorme archivio (o data base) nel *Cyberspace*, verificabile ed immodificabile per quanto riguarda la registrazione di ogni transazione ed attività già svolta, peraltro criptata e non riconducibile ad identità riconoscibili, che rappresenta l'unica garanzia del valore di scambio della stessa "criptovaluta", senza – come detto – che vi siano emittenti, né garanti, del relativo valore economico.

Il sistema in tal modo si estende, diffonde e regola solo in forza dei suoi codici tecnici, non giuridici, con un rischioso potenziale di inflazione, peraltro compensato dall'apprezzamento straordinario delle "valute" in questione, dato che l'estrattore di ogni nuovo "blocco" (o *miner*) ricava dalla sua attività un compenso commisurato in una percentuale o valore proporzionale all'attività, nei limiti consentiti dall'algoritmo, mentre i semplici utilizzatori (od *users*) di tali valute possono acquistarle su apposite piattaforme Internet, che li offrono a fronte di corrispettivi in denaro o servizi, oppure cedendo altri beni o servizi pagati a loro volta in "criptovaluta", da qualsivoglia contraente in rete. Oggi esistono numerose società ed imprese, con piattaforme o siti, che offrono nel *web* a qualsivoglia utente servizi legali di acquisto o vendita di *Bitcoin* o di altre "criptovalute" a titolo oneroso, la cui attività è stata oggetto della citata sentenza della Corte di Giustizia del 2015 (19) e della correlata Risoluzione della nostra

---

(18) Il meccanismo richiama da lontano l'architettura delle c.d. catene di Sant'Antonio, ma ovviamente ad un livello ben più sofisticato, in quanto ogni blocco contiene un marcatore temporale (*timestamp*) che serve ad evitare transazioni contemporanee, e l'*hash* (una funzione algoritmica informatica non invertibile, che mappa una stringa di lunghezza arbitraria in una stringa di lunghezza predefinita) del blocco precedente, collegando così univocamente insieme i blocchi della catena.

(19) CGUE 22.10.2015, C-264/14, di cui si riportano i passi di interesse: "§ 24. La valuta virtuale a flusso bidirezionale «bitcoin», che sarà cambiata contro valute tradizionali nel contesto di operazioni di cambio, non può essere qualificata come «bene materiale» ai

Agenzia delle Entrate del settembre 2016 ([20]), oltre che da ultimo della direttiva (UE) 2018/843, sopra citata.

È peculiare di questi sistemi di pagamento che tutti i dati siano, come detto, crittografati, per garantirne la sicurezza ed autenticità, ma così anche la assoluta riservatezza, grazie ad un sistema a chiavi asimmetriche, di cui ciascun detentore possiede la chiave privata a lui soltanto nota, che gli consente di disporre della "valuta" disponibile, e di operare con essa i pagamenti e le transazioni. Invece la chiave pubblica, associata alla critto-

---

sensi dell'articolo 14 della direttiva IVA, dato che, come rilevato dall'avvocato generale al paragrafo 17 delle sue conclusioni, questa valuta virtuale non ha altre finalità oltre a quella di un mezzo di pagamento. […]. § 26. Conseguentemente, le operazioni oggetto del procedimento principale, che consistono nel cambio di diversi mezzi di pagamento, non ricadono nella nozione di «cessione di beni», prevista da detto articolo 14 della direttiva. In questo contesto, tali operazioni costituiscono prestazioni di servizi ai sensi dell'articolo 24 della direttiva IVA. [...]. § 31. Occorre pertanto rispondere alla prima questione dichiarando che l'articolo 2, paragrafo 1, lettera c), della direttiva IVA va interpretato nel senso che costituiscano prestazioni di servizi effettuate a titolo oneroso, ai sensi di tale disposizione, operazioni, come quelle oggetto del procedimento principale, che consistono nel cambio di valuta tradizionale contro unità della valuta virtuale «bitcoin» e viceversa, effettuate a fronte del pagamento di una somma corrispondente al margine costituito dalla differenza tra, da una parte, il prezzo al quale l'operatore interessato acquista le valute e, dall'altra, il prezzo al quale le vende ai suoi clienti. […]. § 49. Orbene, le operazioni relative a valute non tradizionali, vale a dire diverse dalle monete con valore liberatorio in uno o più paesi, costituiscono operazioni finanziarie in quanto tali valute siano state accettate dalle parti di una transazione quale mezzo di pagamento alternativo ai mezzi di pagamento legali e non abbiano altre finalità oltre a quella di un mezzo di pagamento".

([20]) La Risoluzione è il primo tentativo da parte dell'Agenzia delle Entrate di dare un inquadramento nel sistema fiscale italiano alle monete virtuali, su queste basi: a. il *bitcoin* è un mezzo di pagamento alternativo alle monete aventi corso legale, operante esclusivamente per accettazione volontaria degli operatori, ovvero sul vincolo di fiducia tra soggetti che operano *peer-to-peer*, senza alcuna regolamentazione specifica né Autorità centrale; b. il *bitcoin* è, in particolare, una criptovaluta, in quanto ha natura digitale e si fonda su un sistema di crittografia algoritmica. Le monete virtuali hanno la medesima funzione di meri mezzi di pagamento, sicché anche le transazioni in *bitcoin* devono essere assoggettate al regime di esenzione ai fini IVA. Sul trattamento fiscale ai fini delle imposte dirette delle transazioni di cambio valuta, peraltro, il margine su prezzi vendita/acquisto costituisce "*materia imponibile soggetta ad ordinaria tassazione ai fini Ires (ed Irap)*". Quanto alla valorizzazione dei *bitcoin* eventualmente detenuti da una società a fine anno, questi vanno valutati fiscalmente al valore normale, da indentificarsi nella "*media delle quotazioni ufficiali rinvenibili sulle piattaforme* on line *in cui avvengono le compravendite di* bitcoin".In chiusura, la Risoluzione tocca un tema di primaria rilevanza, ritenendo che vada estesa già in via interpretativa (come poi è in effetti avvenuto tramite la direttiva) la portata della normativa antiriciclaggio alle transazioni in *bitcoin*. L'art. 11, comma 2, lett. *c*), d.lgs. n. 231/2007 estende infatti gli obblighi di *compliance* previsti per la categoria degli intermediari finanziari ai "*soggetti che esercitano professionalmente l'attività di cambiavalute, consistente nella negoziazione a pronti di mezzi di pagamento in valuta*".

grafia, viene comunicata alla parte o alle parti beneficiarie, che possono in tal modo ricevere i pagamenti od i trasferimenti di valori.

Il contenuto delle "criptovalute" è e resta dunque esclusivamente digitale, venendo esse semplicemente "archiviate" dal loro detentore in taccuini o "borsellini" elettronici (*wallet*), su *personal computer* o dispositivi portatili, come comuni file elettronici, non su *server*, né presso *provider* o terzi (salvo si voglia ricorrere ad appositi "prestatori di servizi di portafoglio digitale" di cui sopra si è detto). Pertanto, se da un lato sono sempre direttamente e liberamente disponibili e spendibili, senza nessun intervento necessario di altri soggetti, né dunque costo, per qualsivoglia operazione, salvi i limiti della disponibilità acquisita, dall'altro sono ben difficilmente rintracciabili, identificabili, sequestrabili, tantomeno confiscabili (se non "per equivalente"), salvo poter essere anche accidentalmente smarrite, cancellate o distrutte, ad es. da *malware* od a seguito di incidenti od attacchi informatici. Già si calcola che enormi valori siano andati perduti accidentalmente, ma potrebbero anche essere soltanto archiviati, senza che vi sia alcuna possibilità di accertare l'esistenza della massa effettivamente circolante o disponibile e presso chi sia "distribuita".

Per i peculiari vantaggi che offrono, le "criptovalute" hanno in ogni caso acquisito e mantengono costantemente una quotazione sui mercati *on-line*, espressa in valute tradizionali (quali euro, dollari, yen o remin, ecc.), con le quali possono *di fatto* essere scambiate, tramite le menzionate piattaforme, imprese o soggetti privati, che svolgono tali servizi nel *web*, assumendosi i relativi rischi, ma senza necessità di autorizzazioni od abilitazioni preventive, né ovviamente garanzia o controllo alcuno sui "tassi di cambio" (e provvigioni) applicabili.

In definitiva le "cripotovalute" prescindono da collegamenti vincolanti con il valore delle monete aventi corso legale e quindi non possiedono *di per sé* un valore di scambio ufficiale, giuridicamente garantito da istituti emittenti, che come detto non esistono, come è invece basilare nei sistemi di pagamento bancari e finanziari tradizionali, in cui sono regolati e controllati i flussi monetari.

La produzione e la circolazione delle "criptovalute" restano interamente affidate al susseguirsi degli interventi dei *miners*, che traggono vantaggio dalla produzione (od "estrazione" come viene chiamata in gergo) dei c.d. "blocchi" che si aggiungono incessantemente alla catena e ne assicurano, con l'estensione, anche la riproduzione ed esistenza come valore circolante, peraltro solo volontariamente e convenzionalmente accettato quale valore di scambio nelle transazioni con esse effettuate, come se

si trattasse di un baratto, non avendo di per sé i pagamenti così effettuati un effetto *giuridico* liberatorio.

Evidente è l'elevato livello di rischio di siffatti meccanismi, che si mantengono vivi per la loro continua estensione e diffusione, oggetto peraltro di incessanti attività speculative e, dunque, di possibili enormi "bolle", con oscillazioni di valore impressionanti (paradigmatico è l'incremento di valore dei *Bitcoin* di circa il 500% in un anno, con un crollo poi da 5000 euro a meno di 3000 in un solo giorno, e dopo una successiva risalita, un ulteriore caduta a circa 4000 euro di valore) (21).

Ai fini del tema del riciclaggio, va evidenziato che l'attrazione che offrono tali "criptovalute" nasce soprattutto dall'anonimato che garantiscono a chi le utilizza e dalla totale riservatezza che accompagna le singole operazioni con esse effettuate, oltre alla loro connaturata transnazionalità, immediatezza e flessibilità di utilizzo nel *Cyberspace*. Per cui esse circolano in prevalenza nel *dark web*, prestandosi, come anticipato, alle più disparate attività e transazioni illecite (traffici di droga, armi, medicinali, organi, prostituzione, estorsioni, investimenti speculativi di ogni genere), potendo essere accettate e scambiate in tempo reale e senza alcun vincolo o controllo in ogni parte del globo.

Insomma, è proprio l'estensione planetaria del mercato digitale e la mancanza di regolazione giuridica che ne assicura il successo ed il valore, pur estremamente fragile per l'altro rischio economico che vi è connaturato.

2.6. – Volendo sintetizzare, si può dire che si è ormai passati dall'utilizzo delle TIC e della rete quale mero "mezzo di trasmissione" e "circolazione" per effettuare trasferimenti di fondi, pagamenti, investimenti, ecc., alla dimensione interattiva e globale del *Cyberspace*, quale mondo che *produce* esso stesso nuovi e disparati servizi, funzioni e valori, nascenti dalla stessa globalità e varietà dei rapporti che vi si instaurano e vi si svolgono. L'utente diviene egli stesso operatore, che non solo può eseguire, quando e come vuole, operazioni economico-finanziarie e transazioni di ogni genere, effettuare pagamenti, incassare e trasferire crediti, aprire e chiudere *account* anche con differenti e molteplici profili identitari, ma anche "produrre", scegliere, acquisire e gestire in totale autonomia i valori

(21) La Stampa del 16.9.2017: "Il crollo è avvenuto dopo che la Banca Popolare della Cina ha dichiarato illegale la compravendita della criptovaluta. La situazione è peggiorata quando gli operatori hanno bloccato il trading. Per JP Morgan la "bolla" era scoppiata, anche se poi vi è stata invece una ripresa, seguita però da ulteriore caduta nell'autunno 2018.

di scambio e di investimento disponibili, che circolano, vengono accettati ed investiti ulteriormente, assumendosi interamente i relativi rischi.

Anche tale fenomeno dimostra che lo sviluppo della rete o, meglio, del *Cyberspace*, non è solo un fatto tecnologico, ma si correla ed interagisce strettamente con la rapida evoluzione dei rapporti sociali ed economici, nella nuova dimensione globale caratterizzata da un'estensione e da un'apertura straordinarie dei mercati e delle attività anche finanziarie, con una moltiplicazione di operazioni possibili, sia lecite, sia illecite, realizzabili nel *web*, coinvolgendo una pluralità sempre più estesa di soggetti, enti, imprese, organizzazioni, legali e non.

Il vantaggio è che si può più liberamente, immediatamente ed efficacemente operare nel *Cyberspace* rispetto a quanto è possibile fare tramite le tradizionali forme, modalità e strutture dell'economia c.d. reale, essendo in esso garantita la possibilità di sfruttare l'anonimato e la intrinseca transnazionalità, rapidità, flessibilità ed ubiquità di gestione (digitalizzata) di tutti i rapporti, che consentono la massima molteplicità di interazioni fra operatori e con il pubblico, divenuto potenzialmente mondiale, di consumatori, utenti, *partner*.

3. – Per quanto riguarda le ricadute sul tema specifico della rilevanza penale delle nuove "tecniche" di *cyberlaundering*, va evidenziato che i menzionati sviluppi aprono lo spazio ad una pluralità di comportamenti illeciti, che possono schematicamente suddividersi in due grandi gruppi: accanto all'uso indebito od alla forzatura di sistemi legali di pagamento ed investimento (ad es. tramite la manipolazione di *smart card* ovvero l'abuso di sistemi di pagamento o trasferimento di valori *on-line*, quali *Paypal*) emerge il sempre più massiccio ricorso ai sistemi extra-bancari e deregolamentati (rispetto alle discipline legali spesso diverse dei vari ordinamenti giuridici coinvolti) di raccolta, circolazione, investimento, scambio direttamente nel *Cyberspace* di somme, valori, crediti, "utilità", di cui risulta molto più difficile, se non impossibile, grazie soprattutto alle "criptovalute", tracciare l'origine e le successive movimentazioni, ed in ogni caso identificare con certezza e rapidità i soggetti effettivamente coinvolti ed interessati: sistemi che in contropartita presentano (come ogni circuito extralegale) ben più elevati rischi di instabilità e di volatilità dei valori in gioco.

Sul piano tecnico, più che di attività intrinsecamente ed originariamente illegali, si deve parlare di attività e servizi "a doppio uso": vale a dire non *di per sé* illecite, ma che *possono* essere e sono per lo più utilizzate a scopi illeciti, sistematicamente ed efficacemente, non solo occasionalmente.

Esemplificando si pensi alla *crittografia*, di cui sopra si è detto, quale caratteristica propria dei sistemi *Blockchain*, ed anche dei sistemi di *home banking* e *Paypal*, che riguardano la circolazione della c.d. moneta elettronica.

Da un lato la crittografia è giustificata ed anzi richiesta dalla necessità di garantire la sicurezza e la immodificabilità, oltre che la riservatezza, dei dati e delle operazioni finanziarie che si svolgono nel *web*, impedendo accessi ed interventi abusivi, manipolazioni od intercettazioni, legittime ed illegittime.

D'altro lato, però, la stessa crittografia è essenziale per mascherare, se non viene messa a disposizione la chiave di decriptazione, anche alle autorità di vigilanza ed alle forze investigative, oltre che ai terzi, il contenuto delle operazioni ed attività in questione, ed ancor più la reale identità dei soggetti che ne sono attori o beneficiari, creando problemi di non poco conto per tracciare – seppure *ex post* – l'effettiva movimentazione di capitali e valori ed identificare poi i titolari effettivi.

Si pensi così anche alla c.d. identità *digitale*, con cui cioè la singola persona, l'ente, l'impresa, viene identificata ed "accreditata" per operare nel *web*, che è giustamente oggetto della massima attenzione tecnica ed operativa nei diversi livelli ed ambiti in cui viene in rilievo [22].

Da un lato, essa è necessaria per attribuire e garantire al suo titolare l'imputazione corretta delle operazioni ed attività che svolge nel *Cyberspace*.

Dall'altro, però, può essere "abusata", sia da parte del legittimo titolare (ad es. facendone un uso in procedure non previste od oltre i limiti per cui sarebbe legittimato, soprattutto *moltiplicando* a piacimento le "identità" di cui può disporre nel *Cyberspace*), sia da parte di terzi (ad es. "sottraendola" del tutto illegittimamente al titolare od anche appropriandosene per un utilizzo ulteriore o diverso, rispetto a quello per cui era consentito l'uso da parte sua) ovvero addirittura essere del tutto "fittiziamente" creata (ad es. creando illegittimamente identità digitali "attribuite" a soggetti inesistenti). Non vi sono infatti meccanismi tecnici o procedure, che consentano di collegare univocamente ed inscindibilmente l'identità digitale con una sola persona fisica o giuridica determinata.

Il nostro codice penale, al comma 3 dell'art. 640 *ter* c.p., introdotto nel 2013 come ipotesi aggravata di frode informatica, parla – seppur impro-

---

[22] Sulla controversa identificazione di tale nozione sia sul piano tecnico, che sul piano giuridico, basti qui rinviare a G. MALGIERI, *La nuova fattispecie di "indebito utilizzo d'identità digitale": un problema interpretativo*, in *Riv. trim. dir. pen. cont.*, 2015 (2), p. 143 s.; ID., *Il furto di "identità digitale": una tutela patrimoniale della personalità*, in D. FALCINELLI, R. FLOR, S. MARCOLINI (a cura di), *La giustizia penale nella "rete"*, Milano, 2015, p. 37 ss.; e più di recente il contributo C. CRESCIOLI, *La tutela penale dell'identità digitale*, in *www.penalecontemporaneo.it*, 2018 (2), p. 265 s.

priamente sul piano del linguaggio giuridico – di "*furto o indebito utilizzo dell'identità digitale*", quale modalità tecnica che consente di "alterare" il funzionamento di un sistema informatico o di "intervenire senza diritto" su dati, informazioni o programmi: ma solo nella limitata prospettiva, traslata dallo schema della truffa comune, di "*procurare a sé o ad altri un ingiusto profitto con altrui danno*", vale a dire quale specifica modalità di causazione degli eventi consumativi di detto reato, laddove essa si dimostra invece capace di potenzialità realizzative ed utilizzazioni ben più articolate ed estese, in quanto può rendere non più tracciabili e, comunque, mascherare gli autori effettivi di operazioni, trasferimenti, pagamenti, ecc. ovvero i loro beneficiari.

Più di recente, la giurisprudenza ha applicato il delitto di "sostituzione di persona", di cui all'art. 494 c.p., ad un caso di sottrazione dell'identità digitale al di fuori del contesto del delitto di frode informatica [23], ma negli stretti limiti dei requisiti oggettivi (fra cui l'*induzione* di "*taluno in errore*") e soggettivi (il fine specifico di "*procurare a sé o ad altri un vantaggio o di recare ad altri un danno*") previsti dalla fattispecie, in ogni caso punita con l'esigua pena della reclusione fino ad un anno.

In breve: a fronte dell'intrinseco *anonimato* del denaro contante, contro la cui facilità di circolazione materiale, che prescinde dall'identificazione della sua provenienza eventualmente anche illecita (*pecunia non olet*), su cui si era appuntata – a partire dagli anni '90 del secolo scorso – e tuttora si appunta la disciplina antiriciclaggio, emerge oggi, in modo ben più insidioso, diversificato e penetrante, l'*anonimato* "di fatto" consentito dalle TIC nella circolazione di qualsivoglia valore, bene ed utilità nel *Cyberspace*. Anonimato che insieme ai sistemi di criptazione assume dimensioni e caratteristiche peculiari, riflettendo la pluralità e dinamicità degli sviluppi non solo delle TIC, ma anche della correlativa evoluzione dei rapporti economico-sociali nel *Cyberspace*, in cui ben maggiori sono le potenzialità di veloce circolazione, accumulazione, sostituzione, "ripulitura" di ricchezza illecita, al di là dei limiti fisici di spazio e di tempo, propri della circolazione delle monete e delle valute tradizionali. Per cui ben più ampi sono gli spazi di operatività e nel contempo di pericolosità per l'economia mondiale.

---

[23] Cfr. Cass. Sez. V, 8 giugno 2018 (dep. 19 luglio 2018), n. 33862; e già Cass. pen., sez. V, 23 aprile 2014, n. 25774 con nota di F. SANSOBRINO, *Creazione di un falso account, abusivo utilizzo dell'immagine di una terza persona e delitto di sostituzione di persona,* in *www.penalecontemporaneo.it* (30.9.2014).

A tale situazione, il diritto e le forze di *law enforcement* possono e devono parallelamente adeguarsi, a partire dal profilo tecnico, visto che la stessa tecnologia mette a disposizione strumenti di indagine, ricerca, tracciamento ed acquisizione delle prove c.d. elettroniche di straordinaria potenza e efficienza.

Il problema diventa dunque quello di adeguare la regolamentazione giuridica, penale e processuale, che gli Stati e l'Unione europea, accanto agli altri organismi internazionali, devono darsi, bilanciando le esigenze di sicurezza, prevenzione e repressione dei reati, con le garanzie della persona ed *in primis* con la *privacy* dei cittadini e degli utenti in genere nel *Cyberspace*.

4. – Venendo ad analizzare la specifica rilevanza giuridico-penale della costellazione di comportamenti sopra descritti, quali componenti delle diverse possibili fasi del complesso fenomeno del *cyberlaundering*, si deve innanzitutto ribadire che – alla luce dell'analisi svolta – non si è soltanto di fronte a nuove "modalità tecniche" di realizzazione dei delitti di riciclaggio, reimpiego ed autoriciclaggio, definiti dai citati artt. 648-*bis*, 648-*ter* e 648-*ter*.1 c.p. Muovendo da queste fattispecie, esse risultano già formulate con espressioni linguistiche ampie ed elastiche, che si prestano ad abbracciare in via ermeneutica, *de jure condito*, molteplici fasi od attività riconducibili ai fenomeni nuovi appena esaminati.

A livello interpretativo, infatti, le fattispecie predette possono ricomprendere molte di queste nuove modalità tecniche, che caratterizzano il *cyberlaundering*, dato che nelle espressioni "*sostituire*", "*trasferire*" o comunque "*compiere* altre *operazioni*" (...) "*in modo* da ostacolare *l'identificazione della loro provenienza*" (art. 648-*bis* c.p.; evidenz. agg.) rientrano sicuramente le condotte di cui si è parlato. In particolare l'elastica clausola di chiusura finale non richiede alcuna specifica modalità tecnica, né alcun univoco risultato finale, della condotta punibile, bastandone l'idoneità ad "*ostacolare*" l'identificazione della provenienza, sia oggettiva, che soggettiva, di valori ed "*utilità*", senza che occorra un'assoluta impossibilità, né che vi sia un vincolo definitorio alla materialità fisica degli oggetti della condotta stessa, estesi ben oltre l'ambito tradizionale del "*denaro*" o della moneta tradizionalmente intesa.

Non vi è, quindi, un problema di astratta tipizzazione, che richieda sul punto concrete modifiche normative.

E questa conclusione vale anche per il delitto di impiego di denaro, beni o utilità di provenienza illecita (art. 648-*ter* c.p.), in cui l'ambito assai ampio delle "*attività economiche e finanziarie*" cui deve farsi riferimento può certamente ricomprendere tutte quelle *on-line*, comprese le operazioni

di pagamento o trasferimento o scambio di valori di cui si è detto, anche mediante "criptovalute".

Quanto all'autoriciclaggio (art. 648-*ter*.1 c.p.), è anch'esso senz'altro concepibile *on line*, con le tecniche descritte, in quanto la fattispecie legale menziona sia l'impiego, che la sostituzione ed il trasferimento dei predetti oggetti "*in attività economiche, finanziarie, imprenditoriali o speculative*": rispetto ad esse vale quanto già detto per la sussunzione delle attività realizzabili nel *Cyberspace* sopra ricordate, con le varie tecniche descritte.

Ad es. se si opera attraverso un *gambling on line* illegale, si ha certamente un "*impiego*", in qualsiasi forma, dunque anche tramite pagamenti o trasferimenti elettronici del denaro o delle utilità di provenienza illecita via *web*, in un'attività che resta solo da stabilire se sia da qualificare come "*economica*" o "*speculativa*" (dovendosene escludere *prima facie* il carattere "*finanziario*" o "*imprenditoriale*") o se invece sia da considerare quale "*mera utilizzazione o* [...] *godimento personale*" per cui è prevista la non punibilità, ai sensi del controverso comma 4. Ma a ben vedere i problemi interpretativi che si pongono non sono diversi da quelli che si presentano con riferimento a corrispondenti condotte tradizionali nel mondo reale (nella fattispecie: di fronte all'impiego in un comune gioco d'azzardo), non essendo la formulazione tecnico-giuridica della fattispecie incriminatrice ad impedirne di per sé l'applicazione anche al *cyberlaundering*.

In conclusione, le fattispecie incriminatrici di cui agli artt. 648-*bis*, 648-*ter* e 648-*ter*.1 c.p. sono riconducibili alla categoria dei *cybercrime* o reati informatici "in senso lato", in quanto *possono* essere integrate (anche) da condotte che si realizzano *concretamente* con tecniche informatiche e, più precisamente, nel *Cyberspace*, senza che la loro punibilità dipenda dalla *specifica* previsione di *elementi* tecnici descritti dalla stessa fattispecie legale, che richiamino o rimandino espressamente e tassativamente alle TIC (24).

---

(24) Classico esempio della diversa categoria dei "reati informatici in senso stretto" è invece la menzionata frode informatica, di cui all'art. 640-*ter* c.p., come pure il più frequente delitto di accesso abusivo ad un sistema informatico o telematico (art. 615-*ter* c.p.), che sono inconcepibili senza ricorso alle TIC. Viceversa un esempio ricorrente della categoria dei "reati informatici in senso ampio" ed, in specie, dei *cybercrime*, è la c.d. diffamazione *online*, che si può certamente commettere nel *Cyberspace*, in quanto alla stregua della comune fattispecie delittuosa prevista dall'art. 595 c.p. la "*comunicazione con più persone*" di contenuti offensivi dell'onore o della reputazione altrui può essere realizzata (anche) con mezzi informatici o telematici: tanto che si ravvisa l'aggravante del ricorso a "*mezzi di pubblicità*" di cui al comma 3, quando si commetta su siti Internet accessibili ad un pubblico indeterminato (in argomento sia consentito il rinvio da ultimo a L. PICOTTI, *Diritto penale e tecnologie informatiche*, cit.).

Ma questo rilievo non significa che nella prassi non sia ben differente, sotto il profilo giuridico, oltre che criminologico, la commissione di un delitto in tutto od in parte nel *web* anziché (esclusivamente) nel mondo c.d. reale.

Se il *cyberlaundering* si consuma con comportamenti molto diversi da quelli dello spallone che porti la valigia di denaro contante oltre confine, sono evidenti i riflessi sulle questioni relative alla determinazione del luogo e del tempo della consumazione, ovvero delle prove (digitali) da acquisire, delle relative tecniche di ricerca e d'accertamento e delle corrispondenti garanzie processuali, ecc.

Quale concreto effetto giuridico, si potrà e dovrà altresì applicare, ai fatti di reato riconducibili al *cyberlaundering*, la Convenzione *Cybercrime* del 2001, il cui art. 14, par. 2, lett. b), prevede esplicitamente che ne siano oggetto tutti i crimini, comunque commessi, in tutto o in parte, *tramite* un sistema informatico (e dunque anche in Internet), pur se *non* rientrano tra quelli strettamente informatici, di cui alla lettera a), oggetto degli specifici obblighi d'incriminazione previsti nella prima parte della Convenzione stessa (artt. da 2 a 11) [25].

Del resto, tutte le misure processuali e le disposizioni relative alla cooperazione giudiziaria e di polizia fra gli Stati parte si estendono altresì a tutti gli *altri* ulteriori reati, per cui la raccolta di "prove elettroniche" si renda necessaria: con conseguente armonizzazione della disciplina relativa anche alla loro raccolta, conservazione, circolazione, validità (cfr. art. 14, par. 2, lett. c) Convenzione cit.). Per cui dovranno esservi compresi anche tutti i vari altri delitti, di cui ora ci si occuperà.

5. – La rilevanza penale dell'ampio fenomeno del *cyberlaundering* non può essere circoscritta, come detto, al ristretto novero dei delitti positivamente previsti nel nostro codice penale dagli artt. 648-*bis*, 648-*ter* e 648-*ter.*1.

Infatti, emergono "nuovi" reati presupposto e "nuovi" reati strumentali, da distinguere per la diversa posizione funzionale nell'ampia trama o catena del *cyberlaundering*. E senza pretesa alcuna di esaustività, basti in questa sede illustrare alcune delle ipotesi paradigmatiche, che possono venire in rilievo da ricondurre rispettivamente nella prima ovvero nella seconda categoria.

---

[25] In argomento sia consentito rinviare a L. PICOTTI, *La ratifica della Convenzione* Cybercrime *del Consiglio d'Europa. Profili di diritto penale sostanziale, in Dir. pen. proc.*, 2008, n. 6, p. 700 s.

5.1. *Nuovi reati presupposto* – Fra i primi si devono menzionare quelli ravvisabili nell'emblematico fenomeno del *phishing*, che a sua volta non delinea di per sé un singolo reato, ma un complesso insieme di comportamenti illeciti nel *Cyberspace*, che possono integrare una pluralità di reati cibernetici ed, infine, sfociare nel *cyberlaundering* (26).

Con il termine *phishing* si individua infatti quell'abuso di tecniche di *social engineering* con le quali l'autore induce la vittima (ad es. inviando una falsa e-mail che appaia provenire dall'istituto bancario presso cui è appoggiato un suo conto corrente gestibile *on line*) a fornire i propri dati riservati d'accesso ai servizi *home banking* (ID, PIN, PW: in pratica la sua "identità digitale"), poi abusivamente utilizzati per operare trasferimenti od operazioni a danno del titolare stesso, con ingiusto profitto degli autori o di terzi. Si possono configurare, in un tale fenomeno, frodi informatiche, in specie aggravate dal furto di identità digitale (*ex* art. 640-*ter*, comma 3, c.p.), truffe comuni (*ex* art. 640 c.p.), acquisizione e cessione illecite di password (*ex* art. 615-*quater* c.p.), accessi abusivi a sistemi informatici o telematici (*ex* art. 615-*ter*, c.p.) ed altri delitti che possono dunque tutti divenire reati-presupposto dei delitti di riciclaggio, ovvero di impiego od anche di autoriciclaggio, in quanto rappresentano la "fonte" illecita dei "proventi" che sono poi oggetto di detti ultimi delitti.

Al riguardo vi è un'ampia casistica giurisprudenziale, che ha ravvisato il delitto di riciclaggio a seguito di *phishing* (27), quale ultima fase dopo quella in cui si sono "pescate" le credenziali di accesso ai servizi *home banking* mediante artifizi, che possono integrare un'ipotesi di truffa comune *ex* art. 640 c.p., pur commessa nel *Cyberspace*, nell'esempio già menzionato di invio alla vittima di un'e-mail che la indirizza ad una pagina *web* contraffatta dell'istituto di credito, così da indurla realmente "*in errore*" e portarla ad immettervi le proprie credenziali, che poi il *phisher* "acquisisce" (cfr. art. 615-*quater* c.p.) ed "utilizza" per accedere abusivamente al sistema informatico della banca (art. 615-*ter* c.p.), tramite il quale opera infine il trasferimento abusivo di fondi della vittima stessa a favore di un conto corrente eventualmente intestato ad un terzo, il c.d. *financial manager*: soggetto che si presta ad un'apparente intermediazione finanziaria, acquisendo o trattenendo "provvigioni" per ogni trasferimento, che da

---

(26) Per una trattazione sistematica si veda R. FLOR, *Phishing, identity theft e identity abuse. Le prospettive applicative del diritto penale vigente*, in *Riv. it. dir. proc. pen.*, 2007, n. 2-3, p. 899 s.

(27) Cfr. in specie GUP Milano, 29.10.2008, in *Riv. giur. ec. az.*, 2009, n. 5, 111 s. con nota di R. FLOR; nonché Trib. Milano, 10.12.2007, *ivi*, 2008, n. 4, p. 97.

detto conto egli operi delle somme così ricevute, a favore del *phisher* o di terzi a lui collegati, normalmente su altri conti correnti all'estero, possibilmente in paesi non legati da Convenzioni di assistenza e cooperazione internazionale.

È quindi evidente che in questi ultimi trasferimenti possono ravvisarsi gli estremi del delitto di riciclaggio *ex* art. 648-*bis* c.p. commesso dal *financial manager*, che sia consapevole della provenienza illecita delle somme, mentre al *phisher* che vi concorra od operi esso stesso anche il trasferimento all'estero o ad altri conti del provento della truffa o della frode informatica o degli altri reati menzionati, commessi da lui o da suoi complici, dovrebbe applicarsi la fattispecie di autoriciclaggio (28), *ex* art. 648-*ter.*1 c.p.

Il problema cruciale per la giurisprudenza è legato all'accertamento del dolo in capo al *financial manager*, richiedente la consapevolezza della provenienza delittuosa delle somme ricevute e da trasferire. Applicando i principi espressi nella nota sentenza della Cassazione a Sezioni unite sul dolo della ricettazione (29), potrebbe bastare anche il dolo eventuale, riferibile all'elemento rappresentativo avente ad oggetto il delitto presupposto, purché l'accertamento vada al di là del mero "sospetto", che potrebbe già emergere dalla stranezza dell'incarico o dalla "provvigione" esagerata rispetto alla prestazione richiesta.

Un "nuovo" reato presupposto del *cyberlaundering* è anche la frode informatica, eventualmente aggravata dal furto dell'identità digitale (art. 640-*ter*, comma 3, c.p.), che al di là delle ipotesi di *phishing* appena menzionate, può ravvisarsi anche nelle condotte di "manipolazione" del *chip* di una *smart card* o dei relativi programmi di gestione (caricamento degli importi disponibili, conteggio degli addebiti, dati di identificazione del titolare, ecc.) (30). Infatti l'"*alterazione del funzionamento*" del sistema come pure ogni altro intervento "*senza diritto*" su dati e programmi, da cui consegua un ingiusto profitto con altrui danno, realizza il reato in que-

---

(28) Sul rischio che attraverso detta incriminazione si violi però il divieto di *bis in idem* sostanziale, cfr. per tutti F. CONSULICH, *La norma penale doppia.* Ne bis in idem sostanziale *e politiche di prevenzione generale: il banco di prova dell'autoriciclaggio*, in questa Rivista, 2015, p. 55 s.

(29) Cass. Sez. un., 26.11.2009 (dep. 30.3.2010), n. 12433, Nocera, con nota di G. ABBADESSA, *Ricettazione e dolo eventuale*, in *www.penalecontemporaneo* (20.12.2010).

(30) Secondo Cass., sez. II, 15.4.2011, n. 17748, in C.E.D. Cass., n. 250113, «la frode informatica *ex* art. 640-*ter* c.p. è prospettabile nel caso di avvenuto utilizzo di carte di credito, falsificate mediante modificazione della banda magnetica, grazie ad acquisizione illegittima dei codici di accesso segreti (PIN)», data la specifica condotta di abusiva penetrazione all'interno del sistema informatico bancario, con procurato profitto.

stione, che diviene "presupposto" del successivo trasferimento od impiego dei proventi illeciti così conseguiti.

5.2. *Nuovi reati strumentali* – Accanto all'emblematica individuazione di possibili reati informatici (in senso stretto ed in senso ampio), quali "nuovi" delitti-presupposto del *cyberlaundering*, emergono oggi anche nuovi reati informatici (in senso stretto ed in senso ampio) ad esso *strumentali*, seguendo una distinzione emersa nella giurisprudenza della Corte di Cassazione, che porta ad affermarne l'autonoma punibilità, non restando essi "assorbiti" nei delitti di riciclaggio, né costituendone delitti-presupposto.

Il caso da cui prende le mosse tale orientamento è quello dell'utilizzazione di carte già "clonate" per trasferire proventi di un riciclaggio: condotta in cui si sono ravvisati gli estremi del delitto di cui all'art. 55 d.lgs. 21 novembre 2007, oggi invero abrogato, ma contestualmente sostituito, in forza del d.lgs. 1° marzo 2018, n. 21, attuativo della c.d. riserva di codice, da quello, formulato in modo identico, di cui al nuovo art. 493-*ter* c.p. La fattispecie, rubricata "*indebito utilizzo e falsificazione di carte di credito e di pagamento*" e collocata fra i delitti di "falsità in atti" di cui al capo III del Titolo VII, dedicato ai delitti contro la fede pubblica, nel Libro II del codice penale, punisce "*chiunque, al fine di trarne profitto per sé o per altri,* indebitamente utilizza [evidenz. agg.]*, non essendone titolare, carte di credito o di pagamento, ovvero qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi*", nonché chi alteri o falsifichi dette carte ovvero le possieda, ceda od acquisisca.

Il delitto (a differenza della frode informatica, che si consuma con l'effettivo conseguimento del profitto con altrui danno) è stato dunque considerato mero "*strumento"* e non invece "presupposto" del delitto di riciclaggio commesso, perché la condotta di "*utilizzazione*" indebita, nella specie: delle carte di credito estero già clonate da terzi ignoti, da parte del rappresentante di una società, che se ne è servito per trasferire *loro tramite* le somme di provenienza illecita, a loro volta provento della manipolazione ("*alterazione*" o "*falsificazione*": queste sì condotte integranti il reato presupposto) delle carte stesse, su conti della società, ne ha "*occultato la provenienza*": per cui la predetta fattispecie di "*utilizzazione*" è stata considerata autonomamente punibile, seppur in continuazione (*ex* art. 81, comma 2, c.p.) con il delitto di riciclaggio, di cui all'art. 648-*bis* c.p. [31]

[31] Cass., sez. II, 24.10.2013, n. 47147.

In altri termini, la "clonazione illecita" delle carte di credito, avvenuta anteriormente ad opera di ignoti, va tenuta distinta dall'"*utilizzazione*" indebita successiva, da parte di altro soggetto, autonomamente punibile, che a sua volta se ne è servito per porre in essere quelle "*altre operazioni*" di trasferimento, idonee ad ostacolare l'individuazione della provenienza delittuosa del denaro, che ha integrato anche la fattispecie legale del riciclaggio ([32]).

In conclusione, sono concettualmente distinguibili i due reati "cibernetici" (od informatici, il primo in senso stretto, il secondo in senso ampio), rispettivamente di ricezione ed utilizzazione della carta di credito falsificata, per esserne già avvenuta la clonazione del *chip*, e di riciclaggio, operato via *web* con "operazioni di trasferimento all'estero".

Un'altra ipotesi di reato cibernetico (in senso lato), strumentale al *cyberlaundering*, può essere il menzionato "furto d'identità digitale", autonomamente punibile alla stregua della citata giurisprudenza che vi ravvisa la fattispecie di cui all'art. 494 c.p. ([33]) ; od anche quella dell'accesso abusivo ad un sistema informatico o telematico (art. 615-*ter* c.p.), che consenta la realizzazione di trasferimenti illeciti di denaro o fondi, tramite un sistema *home banking* cui si sia ottenuto indebito accesso.

6. – Dall'analisi svolta emerge che di fronte all'imponenza e rapidità d'evoluzione dei fenomeni riconducibili all'ampia costellazione del *cyberlaundering*, occorre un adeguamento degli strumenti di prevenzione e contrasto: ma non tanto sul piano della tipizzazione legale di nuove fattispecie penali, essendo già applicabili e sufficienti quelle in vigore, che si presentano in numero ampio e forse anzi sovrabbondante, al punto da creare piuttosto problemi di coordinamento o possibile concorso (di reati o di norme); quanto invece su quello della disciplina dei controlli preventivi ed, ancor più, degli strumenti d'indagine e della pratica processuale, rispetto a cui servono regole ed interventi più efficaci, da ricondurre alle tecniche più propriamente concepite od utilizzabili per contrastare i *cybercrime* e, più in generale, la criminalità che si manifesta nel *web*.

La Convenzione *Cybercrime* del 2001, come detto, è senz'altro fra gli strumenti già applicabili al *cyberlaundering*.

([32]) La Cassazione, nella sentenza citata alla precedente nota, conclude infatti che "nel caso di riciclaggio di carte di credito provenienti da delitto, perché rubate o clonate, l'indebita *utilizzazione* delle stesse noncostituisce il reato presupposto del riciclaggio, ma un reato *strumentale* alla commissione del riciclaggio medesimo, ai sensi dell'art. 55, comma 9, d.lgs. 21 novembre 2007, n. 231".

([33]) Cfr. Cass., sez. V, 8.6.2018 (dep. 19.7.2018), n. 33862.

Ma è necessaria la consapevolezza che ci si deve muovere nella specifica prospettiva del contrasto ai reati cibernetici (ampiamente intesi), utilizzando le norme che permettono la ricerca e l'acquisizione delle prove elettroniche, a partire dai dati di traffico, dai dati di log ed ogni altra informazione utile, disponibili anche presso gli *Internet Service Provider* (IPS), che hanno l'obbligo di fornirli.

Il coinvolgimento di questi soggetti, essenziali nel funzionamento e nella gestione del *web*, serve non solo per la ricerca e l'acquisizione delle menzionate tracce digitali, rispettando ovviamente i diritti di protezione della *privacy*, da bilanciare con le esigenze di sicurezza, prevenzione ed accertamento dei reati, ma altresì per implementare più efficacemente adeguate discipline di prevenzione e monitoraggio, fino ad oggi concepite con riferimento al settore bancario, finanziario, professionale.

Pur essendo espressamente esclusa dalla normativa vigente la possibilità di imporre agli IPS obblighi di "generale" sorveglianza sulla rete (cfr. art. 17 d.lgs. 9 aprile 2003, n. 70, che si conforma all'art. 15 della direttiva CE 2000/31), non potendo certamente essere trasformati in poliziotti del *web*, tuttavia gli obblighi di segnalazione e di cooperazione, compresi quelli relativi all'identificazione degli utenti, di cui al comma 2 del citato art. 17 d.lgs. 70/2003 possono senz'altro essere indirizzati al contrasto del rischio di riciclaggio ampiamente inteso, così da consentire alle autorità di vigilanza, investigative, giudiziarie di interfacciarsi efficacemente con questi operatori.

Si è visto che il *cyberlaundering* si realizza per lo più bypassando l'intervento di intermediari bancari e finanziari, grazie ai moderni sistemi digitalizzati di pagamento e di trasferimento fondi *on-line*, carte elettroniche, catene *peer to peer*, *blockchain*, con cui circolano e si accreditano fra il pubblico anche le "criptovalute", soprattutto nel *dark web*. Ma l'utilizzo di appropriati software, algoritmi e sistemi "intelligenti", consente di rintracciare condotte prodromiche e strumentali a movimentazioni di valori ed altre operazioni sospette, in specie riferibili a provenienze o destinazioni *off shore*, così da contribuire efficacemente al contrasto del *cyberlaundering*.

E del resto, la direttiva (UE) 2018/843 del Parlamento europeo e del Consiglio del 30 maggio 2018, che modifica la direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo, facendosi espressamente carico di prevenire e contrastare "*l'uso improprio per scopi criminali*" delle "criptovalute" (denominate "*valute virtuali*"), per l'anonimato che garantiscono alle operazioni loro tramite effettuate (considerando 9), amplia l'ambito di applicazione della disciplina antiriciclaggio già stabilito dalla direttiva 2015/849 anche ai "*prestatori di servizi* [...] *di cambio tra valute virtuali e valute aventi corso*

legale" nonché di "*servizi di portafoglio digitale*" (considerando 8 ed art. 1), nel contempo estendendo gli obblighi di utilizzare i "*mezzi di identificazione elettronica*" di cui al Regolamento (UE) 910/2014, che riguarda la cooperazione amministrativa in ambito fiscale (art. 1, n. 8, lettera a) direttiva 2018/843), dato che "*i più recenti sviluppi tecnici nel settore della digitalizzazione delle operazioni e dei pagamenti consentono una identificazione sicura elettronica o a distanza, che dovrebbero avere un riconoscimento a livello transnazionale*" (cfr. *considerando* (22) direttiva 2018/843).

D'altro lato, i reati riconducibili all'esaminato fenomeno del *cyberlaundering* possono rientrare anche nella categoria dei "reati transnazionali", di cui alla Convenzione di Palermo del 2000 contro la criminalità organizzata transnazionale, alla stregua della definizione che ne dà l'art. 3, secondo il quale si considerano tali quelli puniti "*con pena della reclusione non inferiore nel massimo a 4 anni, qualora sia coinvolto un gruppo criminale organizzato*", nonché siano commessi "*in più di uno Stato*" oppure siano commessi "*in uno Stato, ma una parte sostanziale della preparazione, pianificazione, direzione o controllo avvenga in un altro Stato*" od ancora siano commessi "*in uno Stato, ma in esso sia implicato un gruppo criminale organizzato impegnato in attività criminali in più di uno Stato*", od infine siano commessi "*in uno Stato ma abbia[no] effetti sostanziali in un altro Stato".* Ne consegue l'applicazione di tutti gli strumenti di cooperazione ed assistenza internazionali, anche ai fini della confisca dei proventi, previsti dalla Convenzione medesima, cui l'Italia ha dato attuazione con la l. 16 marzo 2006, n. 146.

Per vero, detta Convenzione individua altresì, all'art. 6, nel "riciclaggio dei proventi di reato" una delle specifiche incriminazioni che gli Stati aderenti devono prevedere, stabilendone i requisiti necessari per garantire un'adeguata armonizzazione internazionale. Tuttavia questi si riferiscono ancora, restrittivamente, a "beni" o "denaro" tradizionalmente intesi, ed anche le misure di prevenzione e segnalazione, da indirizzare agli istituti bancari e finanziari (art. 7), denotano una nozione del fenomeno ancora estranea alle tipologie tecnologicamente sviluppatesi negli anni più recenti, di cui si è sopra trattato.

Viceversa, la più recente direttiva UE 2018/1673 del Parlamento e del Consiglio del 23 ottobre 2018, sulla lotta al riciclaggio mediante il diritto penale, prevede espressamente, tra le "*attività criminose*" che configurano i fatti presupposto da cui derivano i proventi oggetto del reato di riciclaggio, quale definito dall'art. 3, anche la "*criminalità informatica*" (art. 2, n. 1, lettera v), "*compreso qualsiasi reato di cui alla direttiva 2013/40/UE*" contro gli attacchi informatici.

Questo significa che anche *altri* reati informatici (compresi quelli cibernetici, quindi), oltre all'accesso abusivo, all'intercettazione illecita, alle interferenze relative a sistemi ed a dati, alla produzione o disponibilità di strumenti per commettere reati, espressamente previsti dalla direttiva del 2013, possono rientrare in questa più ampia categoria (34), mentre la definizione dei "*beni*" che sono oggetto delle condotte costituenti riciclaggio comprende espressamente quelli "*di qualsiasi tipo, materiali o immateriali, mobili o immobili, tangibili o* intangibili*, e i documenti o gli strumenti giuridici in qualsiasi forma,* compresa quella elettronica o digitale*, che attestano il diritto di proprietà o altri diritti sui beni medesimi*" (art. 2, n. 2; evidenz. agg.).

Del resto emerge dai "considerando" che precedono le disposizioni normative della citata direttiva 2018/1673, che il legislatore europeo ha consapevolmente tenuto conto degli sviluppi anche tecnologici, che richiedono il superamento dell'ormai insufficiente definizione dei requisiti relativi alla configurazione del riciclaggio come reato, stabiliti dalla decisione quadro 2001/500/GAI ("considerando" 4). Ed espressamente dedica il "considerando" (6) all'"*uso delle valute virtuali*" che "*presenta nuovi rischi e sfide nella prospettiva della lotta al riciclaggio*": per cui, pur non essendovi alcuna specifica disposizione al riguardo, si rileva che "*gli Stati membri dovrebbero garantire che tali rischi siano affrontati in modo adeguato*". Rilievo che ha avuto evidente incidenza sulla ampia definizione – appena menzionata – dei "*beni*" che possono essere oggetto di riciclaggio.

Si aggiunga, infine, che la precedente direttiva UE 2017/1371, relativa alla lotta contro la frode che lede gli interessi finanziari dell'Unione europea, già prevede una specifica punizione del riciclaggio che lede tali interessi finanziari (35), per cui è ora stabilita la competenza della neo istituita Procura Europea (36).

---

(34) Sulla nozione di "criminalità informatica" che compare (anche) nell'art. 83, par. 1, TFUE, per individuare una delle sfere di criminalità grave e transnazionale rispetto a cui è stabilita la competenza penale (concorrente) dell'Unione europea, sia consentito rinviare a L. Picotti, *La nozione di "criminalità informatica" e la sua rilevanza per le competenze penali europee*, in questa *Rivista,* 2011, n. 4, p. 827 s.

(35) Art. 4 direttiva 2017/1371/UE del 5 settembre 2017, che rimanda (ancora) alla definizione del reato di riciclaggio di denaro di cui all'art. 1, par.3, della direttiva (UE) 2015/849, non coincidente con quella di cui all'art. 3 della direttiva 2018/1673: per cui l'art. 1, par. 2, di quest'ultima, per evitare sovrapposizioni definitorie, esclude la propria applicazione "al riciclaggio riguardante beni derivanti da reati che ledono gli interessi finanziari dell'Unione, che resta soggetto alle norme specifiche stabilite dalla Direttiva (UE) 2017/1371".

(36) La competenza dell'EPPO viene determinata attraverso il rinvio alla direttiva (UE) 2017/1371 sulla protezione degli interessi finanziari dell'Unione ("la direttiva PIF") e comprende quindi tutti i reati lesivi di tali interessi, nonché quelli di partecipazione ad un'orga-

In definitiva, vi sono tutti i presupposti perché queste nuove ed articolate discipline, di diritto sostanziale ed ancor più processuale, si applichino efficacemente e tempestivamente per combattere il complesso fenomeno del *cyberlaundering*, non potendo restare il *Cyberspace* un mondo "senza diritto", e dovendo anzi intervenirvi efficacemente anche il diritto penale, quando, come nel campo in esame, è indispensabile combattere fenomeni di così grande portata, alla cui evoluzione anche tecnologica esso deve necessariamente adeguarsi.

Altrimenti vorrebbe dire accettare che il mondo di oggi, ed ancor più il mondo futuro, siano lasciati alla giungla dei meri rapporti di forza, dominati da gruppi criminali, con buona pace di ogni regolata convivenza sociale.

ZUSAMMENFASSUNG: *Das Thema "Cyberlaundering" ist sehr aktuell und interessant, weil es sich mit zwei neuen Forschungsgebieten überschneidet: zum einen mit dem der Geldwäscherei, einem modernen "Wirtschaftsdelikt", das sich rasant verbreitet und in den neuen technologischen und finanztechnischen Mitteln einer globalen Gesellschaft immer wieder Ansätze zur Weiterentwicklung und zur Anpassung findet; zum anderen berührt es den Problemkreis der sog. Cybercrimes, deren Verbreitung und Fortentwicklung seit einiger Zeit vermehrte Aufmerksamkeit in der Strafrechtspraxis und -lehre wie auch von Seiten internationaler Organismen und Strafverfolgungskräften erfährt, dies angesichts des steigenden Einflusses, den moderne Informations- und Kommunikationstechnologien (sog. TIC) auf das Auftreten und die kontinuierliche Weiterentwicklung der unterschiedlichsten kriminellen Handlungen im sog. Cyberspace ausüben. Der Beitrag gliedert sich in drei Teile. Eingangs wird das Phänomen des Cyberlaunderings illustriert, und dabei die wichtige Rolle aufgezeigt, die die TIC bei der Verübung von Geldwäschereistraftaten im Internet und im Dark Web spielen. In der Folge wendet sich der Autor den rein strafrechtlichen Aspekten des Cyberlaunderings zu und zeigt, wie dieses Phänomen verschiedene Straftatbestände verwirklichen kann, die systematisch unter dem Sammelbegriff Cybercrime "im weiteren Sinne" vereinbar sind, wodurch sein besonderes Expansionspoten-*

---

nizzazione criminale (di cui alla decisione quadro 2008/841/GAI), quando l'attività dell'organizzazione criminale sia incentrata sulla commissione dei reati PIF. A titolo di competenza c.d. "ancillare", l'EPPO potrà inoltre procedere nei confronti di qualsiasi altro reato "indissolubilmente legato" ad un reato PIF, sia pur solo a determinate condizioni individuate dal regolamento, in particolare per ciò che riguarda la maggior gravità del reato PIF rispetto a quello connesso.

tial hervorgehoben wird, das immer neue Arten von vorausgesetzten Straftatbeständen einbezieht und zugleich eine Vielzahl von instrumentellen Verbrechen notwendig macht, die der Befriedigung der (illegalen) Interessen dienen, auf die die hier behandelte, komplexe kriminelle Tätigkeit ausgerichtet ist. Abschließend gewährt der Autor einen Ausblick auf gewisse Präventiv- und Repressivmaßnahmen, die notwendigerweise in einen übernationalen Rahmen zu stellen sind, damit der "Cyberspace" eine effiziente juristische und strafrechtliche Regulierung in diesem Bereich erfahren kann.

ABSTRACT: *The issue of Cyberlaundering is particularly topical and interesting, as it crosses two aspects of novelty: money laundering, as a modern "economic crime" characterized by a worrisome expansion and unceasing evolution and adaptation, in its modalities of perpetration, to the new technical and financial opportunities which are gradually disclosing in today's globalised society; and Cybercrimes, whose extension and evolution long deserve the specific attention of criminal lawyers and scholars, other than that of international bodies and law enforcement agencies, giving the growing impact that the new "information and communication technologies" (ICT) have on the unceasing transformation and manifestation of the most disparate criminal activities in the so-called Cyberspace. This contribution is structured in three parts. First, we will illustrate the phenomenon of Cyberlaudering, characterised by the important role of ICT in the web and the dark web in the commission of money-laundering offences. Then the focus switches to the legal-penal aspects of Cyberlaundering, as we will analyse the various offences in which it can manifest itself, to be included in the category of Cybercrimes "broadly considered", so as to emphasise its expansive capability, which brings to involve new types of predicate crimes and to uncover a number of instrumental crimes, functional to the satisfaction of (illicit) interests, at which the complex criminal activity is aimed. In closing, we will indicate perspectives of prevention and contrast to be necessarily framed in a supranational dimension to pursue the objective of not to deprive the "cyber world" of an efficient legal and penal regulation in such sector.*