

Vendita di società “ready made” ed obblighi di verifica della clientela nella disciplina sulla prevenzione di riciclaggio e finanziamento del terrorismo: contrasto all’anonimato e valute virtuali

di Pietro Maria Sabella

Title: Selling of “Ready made” companies and customers due diligence provisions in the normative on prevention of money laundering and terrorism financing purposes: new instruments to fight anonymity through the use of virtual currencies

Keywords: “Ready made” company; Money laundering; Virtual currency.

1. – Con la decisione del 17 gennaio 2018, la Prima Sezione della Corte di Giustizia dell’Unione Europea è intervenuta, su rinvio pregiudiziale, ex art. 267 TFUE, promosso da parte della Corte Suprema amministrativa della Repubblica Ceca (Nejvyšší správní soud) sull’interpretazione di alcune disposizioni della Direttiva 2005/60/CE in materia di prevenzione dell’uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e finanziamento del terrorismo.

In particolare, la domanda veniva presentata nell’ambito di una controversia sorta fra la società *Corporate Companies s.r.o.* ed il Ministero delle Finanze (*Ministerstvo financí CR*) riguardo all’osservanza, da parte dell’ente suddetto degli obblighi previsti dalla normativa nazionale posti in recepimento della Direttiva del 2005.

La pronuncia appare da subito di particolare interesse poiché chiarisce quali siano i soggetti privati, operanti all’interno dell’Unione Europea, ad essere destinatari delle misure di prevenzione volte ad ostacolare la commissione di fatti di riciclaggio e di finanziamento del terrorismo, poste dalla c.d. “Terza Direttiva anti-riciclaggio” del 2005 e a quali forme di controllo essi possano essere sottoposti dalle autorità nazionali a tutela dell’integrità del sistema finanziario europeo (sul tema, la CGUE è intervenuta con *sentenza del 10 marzo 2016, causa C- 235/14, Safe Interenvios, SA contro Liberbank, SA e a., sentenza del 25 aprile 2013, causa C-212/13, Jyske Bank Gibraltar Ltd contro Administración del Estado*).

Nel caso di specie, il giudice del rinvio domandava se l’art. 2, par. 1, punto 3, lett. c), da considerarsi in combinato disposto con l’art. 3, punto 7, lett. a) della Direttiva 2005/60/CE, trasposta nell’ordinamento ceco con la legge n. 253/2008, dovesse essere interpretato nel senso che, fra i soggetti destinatari della norma, potessero rientrare anche quelle persone giuridiche, la cui attività commerciale principale consista nella vendita di società appositamente costituite in assenza di alcuna preventiva richiesta di acquisto da parte di un cliente.

In poche parole, a differenza di quanto già statuito con la causa *C-212/13*, la questione di diritto concerneva l’ipotesi se il controllo sulla cessione di quote societarie ed

altri benefici economici dovesse essere svolto anche in assenza della preventiva identificazione del soggetto beneficiario.

Sul punto, infatti, la *Corporate Companies s.r.o.* riteneva di non rientrare nell'ambito applicativo delle norme sopra citate proprio in relazione al fatto che essa si limitava a costituire delle società c.d. "ready-made", già iscritte nel registro delle imprese ma prive di un acquirente e dunque non ancora in grado di svolgere alcuna reale attività economica.

Già prima del rinvio pregiudiziale, con sentenza del 25 maggio 2016, il Městský soud v Praze (Corte regionale di Praga capitale) confermava che la *Corporate Companies* rientrasse nell'ambito di applicazione dell'articolo 2, paragrafo 1, lettera h), punto 1, della legge sulla prevenzione del riciclaggio di denaro.

Il giudice ceco sottolineava che la suddetta disposizione si applicasse a tutte le persone che, nell'ambito della loro attività professionale, costituissero persone giuridiche per i loro clienti, a prescindere dal fatto che ciò avvenisse su richiesta del cliente o che le persone giuridiche fossero costituite al fine di essere integrate in un portafoglio di offerte per futuri clienti potenziali.

Successivamente, la *Corporate Companies* proponeva ricorso innanzi alla Corte di Cassazione della Repubblica ceca avverso la summenzionata decisione, continuando ad affermare che l'attività da essa esercitata, consistente nella creazione di società per sé stessa e a proprie spese, non potesse far rientrare la stessa fra i soggetti obbligati ai sensi dell'art. 2, par. 1, lett. h), punto 1 della legge ceca sulla prevenzione del riciclaggio, in quanto tali operazioni non avvenivano né su richiesta di specifici clienti né a favore di prestanomi.

La Corte di Cassazione sospendeva così il giudizio rinviando, *ex art. 267 TFUE*, la questione alla CGUE.

Nel confrontare il caso specie e la legislazione ceca alla lettera ed alla *ratio* della Direttiva 2005/60/CE, la Corte europea precisava come, ai fini dell'applicazione dell'art. 3, punto 7, lett. a) della Direttiva 2005/60/CE, fosse del tutto irrilevante per l'applicazione della norma la circostanza che una società del genere, come la *Corporate Companies s.r.o.*, costituisse persone giuridiche con finalità di lucro in vista di una successiva cessione ad un cliente non ancora identificato.

E ciò sulla base del fatto che questa disposizione non operi alcun tipo di distinzione fra il caso in cui la cessione avvenga successivamente all'identificazione del cliente beneficiario o in precedenza. Del resto, come verrà successivamente osservato, in nessun modo la Terza Direttiva anti-riciclaggio lascia desumere che il legislatore europeo abbia optato per escludere dall'ambito di applicazione di detto articolo le persone giuridiche che svolgano un'attività commerciale come quella praticata dalla società ceca.

Per questo motivo, la Prima Sezione della Corte di Giustizia confermava che l'art. 2, par. 1, punto 3, lett. c) da leggersi in combinato disposto con l'art. 3, punto 7, lett. a) della Direttiva 2005/60/CE, andasse interpretato nel senso che fra i soggetti destinatari dell'obbligo di verifica rientrano anche quei soggetti, come quello del caso di specie, la cui attività commerciale consiste nel vendere società da esso stesso costituite, senza alcuna previa richiesta da parte di propri potenziali clienti, al fine di essere successivamente vendute mediante la cessione delle quote che tale soggetto detenga nel capitale dell'ente.

2. – Per comprendere adesso le ragioni che hanno condotto la CGUE a tale statuizione, può essere utile esaminare la *ratio* della Direttiva 2005/60/CE, e in generale della normativa antiterrorismo e antiriciclaggio, peraltro, recentemente superata dalla c.d. "Quarta Direttiva Anti-riciclaggio", 849/2015/UE, del 20 maggio del 2015, che ha ancor più contribuito ad intensificare le misure specificatamente rivolte al contrasto dell'uso del sistema finanziario europeo ai fini di riciclaggio e di finanziamento del terrorismo ed al quale l'ordinamento nazionale italiano si è recentemente conformato con il d.lgs. n. 90/2017 (cfr. A. Rossi, *Prevenzione del riciclaggio e finanziamento del terrorismo: finalità e novità normative*, in *Dir. Pen. e proc.*, 2018, 25 e ss; R.M. Vadalà, *La provenienza illecita nel*

delitto di riciclaggio: possibili novità dalla IV direttiva autoriciclaggio?, in *Riv. Trim. dir. pen. ec.*, 2017, 391 e ss; V. Aragona, *Il contrasto al finanziamento del terrorismo*, in www.dirittopenalecontemporaneo.it, 1 giugno 2017;).

In primo luogo, occorre ricordare come il fenomeno del terrorismo internazionale rappresenti oggi un elemento di forte e costante espansione del diritto penale contemporaneo (si veda V. Militello, *Terrorismo e sistema penale*, in *Riv. Trim. dir. pen. cont.*, 2016, 4 e ss.) che tende ad esprimersi secondo un approccio *multilivello ed integrato*, caratterizzato, appunto, dall’intervento costante della legislazione internazionale, europea e nazionale.

A partire dagli attacchi alle Torri Gemelle del 2001, come noto, si è assistito ad un affastellamento della normativa in materia di prevenzione e contrasto al terrorismo internazionale che ha fatto emergere contraddizioni ma che ha condotto anche a notevoli risultati.

Infatti, da un lato, si è acuito il rischio di un ritorno al diritto penale del nemico e dell’autore (F. Fasani, *Terrorismo islamico e diritto penale*, Padova, 2016; R. Bartoli, *Lotta al terrorismo internazionale. Tra diritto penale del nemico, jus in bello del criminale e annientamento del nemico assoluto*, Torino, 2008; M. Donini, *Il diritto penale di fronte al “nemico”*, in *Cass. Pen.*, 2006, 737 e ss; F. Palazzo, *Contrasto al terrorismo, diritto penale del nemico e principi fondamentali*, in *Quest. Giust.*, 2006, 674 e ss;) anche a fronte dell’impiego di una tecnica di legislazione improntata su di un’eccessiva anticipazione della tutela per comportamenti prodromici alla realizzazione di fatti di reato: esempi specifici possono essere tratti dalla criminalizzazione delle condotte di “addestramento” e c.d. “auto-addestramento” con finalità di terrorismo, disciplinati nel codice penale italiano all’art. 270-*quinquies* c.p.

Peraltro, recentemente, la realizzazione di attività di riciclaggio e di finanziamento del terrorismo mediante l’impiego di mezzi informatici (c.d. cybercrimes “in senso ampio”, L. Picotti, *La nozione di criminalità informatica e la sua rilevanza per le competenze penali europee*, in *Riv. Trim. dir. pen. ec.*, 2011, 827 e ss) ha indotto, come per esempio accaduto in Italia, all’impiego di captatori informatici, quali il *Trojan horse*; si tratta infatti di strumenti impiegati quali mezzi di ricerca della prova che, ingerendosi profondamente nella vita privata degli indiziati, mettono in luce profili di potenziale contrasto fra le esigenze investigative e di repressione dei reati con la tutela della *privacy* e della riservatezza, salvaguardati sia a livello costituzionale che convenzionale (nella giurisprudenza CGUE, recentemente *sentenza del 21 dicembre 2016, causa C-203/15, Tele 2 Sverige AB c. Post-och telestyrelsen*).

Ecco che, in un certo senso, oggi si assiste ad un’attività normativa che cerca di adeguarsi alla “perenne emergenza” causata dalla imprevedibilità del fenomeno terroristico e che si snoda fra eccessi di tutela e conflittualità con i diritti fondamentali.

Dall’altro lato, invece è necessario evidenziare come, sia con la Direttiva 2005/60/CE, che con altre più recenti, quali la summenzionata Direttiva 849/2015/UE o la Direttiva Antiterrorismo 2017/541/UE (si veda sul punto, S. Santini, *L’Unione Europea compie un nuovo passo nel cammino della lotta al terrorismo: una prima lettura della Direttiva 2017/541*, in *Dir. Pen. cont.*, 2017, 13 e ss;), nonché con le Direttive 2017/1371/UE (c.d. Direttiva PIF, sul punto E. Basile, *Brevi note sulla nuova Direttiva PIF. Luci ed ombre del processo di integrazione europea in materia penale*, in www.penalecontemporaneo.it, 12 dicembre 2017;) in materia di contrasto alle frodi che ledono gli interessi finanziari UE e la Direttiva 2016/1148/UE (c.d. Direttiva NIS), sulla prevenzione del cybercrime condivisa dai Paesi UE, sia stato costruito un impianto legislativo composito e articolato, che agendo su piani diversi, appare, almeno sulla carta, in grado di prevenire condotte di finanziamento e di arricchimento illecito della criminalità organizzata e terroristica.

E tutto ciò nella consapevolezza da parte del legislatore europeo che i traffici illeciti avvengono su scala globale ed attraverso l’impiego dei mezzi informatici in internet e nel *dark web*.

Allo stesso modo, negli ultimi anni, è stato compreso – e la Direttiva 2005/60/CE ne è un chiaro esempio, come il finanziamento del terrorismo sia un fenomeno criminoso interdipendente dalla realizzazione di altri gravi reati, quali il riciclaggio, l'auto-riciclaggio ed i reati tributari.

Vi è una florida letteratura che evidenzia la continuità tra criminalità economica e criminalità organizzata, tanto che è possibile affermare come esse cooperino per l'ottenimento di una pluralità di fini condivisi, il cui raggiungimento è consentito attraverso un'organizzazione ed una razionalizzazione delle risorse economiche ed umane congiunto (si veda U. Savona, *Economia e criminalità*, in *Scienze soc.*, Vol IX, Roma, 2001, 97). Si registrano, peraltro, casi di vera e propria sovrapposizione fra le attività delle organizzazioni criminali con finalità di terrorismo e il crimine economico tanto da potere parlare di consorzierie criminali transnazionali che riescono a fornire servizi economici su scala globale ed in modo anche apparentemente lecito.

Per queste ragioni le preoccupazioni per la tutela del sistema finanziario europeo si sono acute al punto da indurre le istituzioni europee a predisporre strumenti normativi complessi finalizzati anche a salvaguardare la concorrenza e la trasparenza nel mercato, anche attraverso l'armonizzazione delle tecniche di prevenzione e repressione delle condotte di riciclaggio.

Del resto, la libera circolazione di merci, capitali, servizi e persone all'interno del mercato libero non può che essere garantita se non attraverso un efficace monitoraggio della circolazione delle finanze e delle transazioni economiche.

Ecco perché prima la Direttiva 2005/60/CE e successivamente la nuova Direttiva 849/2015/UE hanno obbligato gli stati membri ad intervenire per evitare che «i flussi di denaro illegali possano danneggiare l'integrità, la stabilità e la reputazione del settore finanziario e minacciare il mercato interno dell'Unione e lo sviluppo internazionale» (Considerando 1).

Ciò al fine di evitare di mettere in grave pericolo la «solidità, l'integrità e la stabilità degli istituti finanziari e di credito, nonché la fiducia nel sistema» (Considerando 2).

Dalla prospettiva del penalista va però fin da ora evidenziato come i concetti di "solidità", "integrità", "corretto funzionamento", "reputazione" e "stabilità del sistema finanziario", non possano, *prima facie*, essere identificati quali veri e propri beni giuridici costituzionalmente rilevanti, idonei a ricevere una protezione penale, ma più che altro quali "meri" obiettivi di politica economica protetti dalla sanzione punitiva.

In un certo qual modo, dunque, si è assistito così ad una evoluzione del modello tradizionale del diritto penale e, in generale, sanzionatorio che, al fine di garantire la tutela di una pluralità di interessi giuridici di dimensione collettiva e transnazionale, - rispetto ai quali il diritto penale tradizionale appare inefficace -, si sviluppa in modo frammentario e segmentato fra codici, leggi speciali e normative europee che necessitano così del costante intervento delle Corti nazionali ed europee per assicurarne una dimensione unitaria su tutto il territorio dell'UE nonché il rispetto dei principi costituzionali e convenzionali dei Paesi membri.

3. – In questo contesto, la Direttiva 2005/60/CE rappresentava già, al momento della sua adozione, il frutto di un approccio moderno al contrasto all'approvvigionamento di risorse economiche e finanziarie da parte del terrorismo internazionale ed al compimento di attività di riciclaggio (in questo senso, A. Balsamo, *La destinazione delle somme di denaro fa scattare il finanziamento del terrore*, in *Guida al diritto – Diritto Comunitario ed internazionale*, 2006, 37) per tre ragioni fondamentali.

La prima è che con questa direttiva il legislatore europeo ha disciplinato il finanziamento al terrorismo ed il riciclaggio di proventi illeciti in modo del tutto autonomo e non quale appendice del più ampio fenomeno del reato associativo con finalità di terrorismo, fondato su ragioni para-ideologiche e che si manifesta tendenzialmente mediante la realizzazione di attacchi e atti di violenza su vasta scala (cfr. M. Levi,

Combating the financing of Terrorism. A history and Assesent of the control of “threat finance”, in The British journal of Criminology, 2010, 650 e ss;).

La seconda attiene al fatto che non è più contemplato quale presupposto del finanziamento l’elemento soggettivo della volontà di finanziare le associazioni criminali per la realizzazione di specifici atti di terrorismo, contenuto invece nella Convenzione di New York del 1999; nel quadro legislativo europeo, infatti, la condotta di finanziamento si configura anche indipendentemente dalla partecipazione psicologica dell’autore del reato alla realizzazione successiva di attacchi. Fin dai primi interventi legislativi in materia (decisione del Consiglio n. 931/2001 e decisione del Consiglio n. 475/2002), la disciplina del finanziamento del terrorismo ha potuto così avere una propria autonomia ed identità giuridica (diversamente, come visto, da quanto accaduto in un primo momento nelle Convenzioni internazionali, sul punto, W. Allen, *The war against terrorism financing*, in *Journal of money laundering control*, 2003, 306 e ss;).

La terza è conseguenza del fatto che la Direttiva comunitaria, recependo le indicazioni del GAFI (sul punto, C. Di Gregorio – G. Mainolfi, *Le transazioni finanziarie sospette: controlli e adempimenti*, Roma, 2004;), che aveva evidenziato le forti interconnessioni tra riciclaggio di denaro e altre risorse economiche e foraggiamento delle imprese terroristiche, si caratterizza per avere quale punto qualificante il controllo preventivo e capillare dei traffici e degli scambi commerciali e finanziari attraverso un’adeguata verifica da parte di enti, persone giuridiche e professionisti nei confronti della propria clientela.

Infatti, i soggetti indicati dall’art. 2 della Direttiva del 2005, come qualificati dall’art. 3, sono chiamati ad identificare la propria clientela trascrivendo ed archiviando tutta una serie di informazioni specifiche, come esito di un’adeguata verifica, tutte le volte in cui:

- instaurano rapporti di affari;
- eseguono transazioni occasionali il cui importo sia pari o superiore a 15.000,00 Euro, indipendentemente dal fatto che siano effettuate con un’operazione unica o con diverse operazioni che appaiono collegate;
- vi sia un sospetto di riciclaggio o di finanziamento del terrorismo e indipendentemente da qualsiasi deroga, esenzione o soglia applicabile; (si precisa come la giurisprudenza della CGUE, sentenza 10 marzo 2016, causa C-235/14, *Safe Interenvios SA c. Liberbank Sa e a.* abbia affermato che la Direttiva 2005/60/CE non osta a che la normativa dei Paesi membri possa prevedere strumenti di controllo più pregnanti attivabili anche quando il sospetto di riciclaggio non sia ancora sorto);
- vi siano dubbi sulla veridicità o sull’adeguatezza dei dati precedentemente ottenuti ai fini dell’identificazione del cliente.

Gli obblighi di verifica vengono ulteriormente incrementati in presenza di situazioni che, per loro natura, potrebbero presentare un rischio più elevato di riciclaggio o di finanziamento del terrorismo. Un caso esemplificativo si ha in tutte le ipotesi in cui il cliente non sia fisicamente presente per l’identificazione; in questa evenienza la direttiva impone ai soggetti obbligati misure specifiche per scongiurare la commissione di illeciti connessi ad un rischio più elevato attraverso l’applicazione di misure volte a:

- garantire l’accertamento dell’identità del cliente tramite documenti, dati o informazioni supplementari;
- adottare misure ulteriori per la verifica o la certificazione dei documenti forniti o richiedere una certificazione di conferma di un ente creditizio o finanziario soggetto alla presente direttiva;
- garantire che il primo pagamento relativo all’operazione sia effettuato tramite un conto intestato al cliente presso un ente creditizio.

La seconda ipotesi che richiede misure specifiche e più rigide riguarda i casi in cui le operazioni o i rapporti di affari vengano posti in essere con persone “politicamente esposte” (art. 13, par. 4, della direttiva del 2005; termine mutuato dalle raccomandazioni

del GAFI, cfr. T. Persio Porzia, *Il valore “condizionante” delle raccomandazioni del GAFI tra soft law e vocazione prescrittiva*, in *Cass. Pen.*, 2015, 2064 e ss;) residenti in un altro stato membro o in un paese terzo. In particolare, rispetto a questi individui, ai soggetti obbligati incombe l’obbligo di attivarsi per adottare ogni misura adeguata per stabilire l’origine del patrimonio e dei fondi impegnati nel rapporto d’affari o nell’operazione.

Tali previsioni normative evidenziano come il legislatore europeo abbia avvertito l’esigenza di identificare tutti coloro che vengano coinvolti in operazioni economiche e transazioni finanziarie realizzate dai soggetti destinatari della Direttiva, agli artt. 2 e 3, in loro favore ed indipendentemente dal tipologia dell’affare o dello scopo al quale esso sia diretto.

E ciò proprio in considerazione del fatto che la vera prevenzione possa essere efficacemente ottenuta solo tramite l’apposizione di strumenti normativi con una capacità deterrente tale da porsi quale barriera immediata per l’ingresso di proventi illeciti nel libero mercato europeo.

In questo, la precedente legislazione in materia, contenuta nella Direttiva 91/308/CE, abrogata nel 2005, risultava avere una scarsa applicazione in quanto si limitava a prevedere solo alcune indicazioni generali in merito alle procedure da applicare nell’identificazione dei soggetti beneficiari da parte di persone giuridiche e professionisti.

Invece, con la terza direttiva antiriciclaggio l’adeguata verifica, per il professionista e per la persona giuridica che operi nel mercato, consiste in un obbligo effettivo che non ha ad oggetto la semplice identificazione della clientela ma contempla un procedimento complesso volto a conoscere il titolare effettivo dell’operazione, ad ottenere informazioni e svolgere un controllo costante sul rapporto d’affari; attività che comprende anche la conoscenza dell’origine dei fondi e delle risorse economiche prima che esse vengano impiegate nell’operazione.

Tant’è vero che per l’art. 9 della Direttiva 2005/60/CE, la verifica deve avvenire prima dell’instaurazione del rapporto di affari, dell’esecuzione della transazione o, in via residuale, in ogni momento ritenuto opportuno.

Dunque, si pone già un vincolo di controllo in un momento antecedente allo svolgimento dell’operazione economica proprio al fine di tutelare, in via preventiva ed efficace, la solidità e l’integrità del sistema finanziario in tutte le fasi in cui esso possa essere messo a repentaglio (precedentemente ne conferma la finalità preventiva *sentenza 4 maggio 2017, causa C-17/16, Oussama El Dakkak c. Administration des douanes et des droits indirects*).

Per questa principale ragione, nel caso di specie, viene affermato come la costituzione di una cosiddetta società “*ready made*” rappresenti, di per sé, un’operazione idonea alla realizzazione tanto di attività di riciclaggio di proventi illeciti quanto del finanziamento del terrorismo. Ed infatti, la possibilità di acquistare un ente già iscritto presso il registro delle imprese e con il capitale interamente versato mediante la semplice sottoscrizione di un contratto di compravendita anche *online* è, in realtà, il metodo più rapido e proficuo per assicurarsi l’ingresso nel mercato con l’impiego di risorse illecite.

La società “*ready made*” è dunque un ente già perfettamente costituito, “pronto all’uso” da parte di qualunque soggetto voglia intraprendere un’attività commerciale in un dato mercato e per tale ragione esso può rappresentare uno strumento adeguato per dissimulare e trasferire risorse ottenute illegalmente o per finanziare indirettamente il terrorismo. Ecco che l’identificazione del cliente costituisce un passaggio necessario e fondamentale per prevenire tali attività, in quanto il controllo sulla creazione di una struttura aziendale siffatta risulta essere la prima vera barriera per dissuadere tutti coloro che intendano utilizzare un ente per ripulire denaro e altri proventi illeciti.

I rischi connessi al compimento di attività di riciclaggio e di finanziamento del terrorismo non si presentano, pertanto, solo nel caso in cui una società venga costituita a monte per conto o a nome di un terzo, ma anche e forse soprattutto nel momento in cui essa, anche se costituita per *incertam personam*, venga poi ceduta ad un cliente successivamente acquisito mediante il trasferimento, a favore di quest’ultimo, delle quote

detenute nel capitale della società suddetta.

Senza considerare che la costituzione e la vendita di società “ready made” da parte di persone giuridiche collegate ed operanti in Paesi UE ed extra UE può occultare altresì, come anticipato, fenomeni di evasione fiscale e di frode IVA, fortemente lesive degli interessi finanziari dell’UE, nonché, come visto, di riciclaggio il cui provento illecito derivi proprio dal compimento illeciti tributari quali delitti presupposto (sul rapporto tra delitti tributari e riciclaggio, *ex multis*, R. Cordeiro Guerra, *Reati fiscali e riciclaggio*, in *Riv. Dir. trib.*, 2013, 116 e ss; G. Izzo, *La frode fiscale quale possibile presupposto del riciclaggio*, in *Il fisco*, 1996, 5291 e ss;).

Del resto, l’acquisto di una società “ready made” può essere indicativo di un’anomalia nella vita commerciale di un ente; spesso, infatti, queste società precostituite vengono impiegate quali vere e proprie “cartiere” (sul tema *ex multis*, I. Caraccioli, *La responsabilità penale dei c.d. “buffers” (o “filtri”) nelle frodi carosello in materia di Iva: gli orientamenti della giurisprudenza*, in *Riv. Dir. Trib.*, 2014; 3; G. Salcuni, *Il “giro dei diritti”: fra frode fiscale, transfer pricing e tax saving*, in *Riv. Trim. dir. pen. ec.*, 2013, 523 e ss; F. Tesauro, *In tema di frode carosello e sanzioni*, in *Giur. It.*, 2013, 2166;) per chiari scopi di evasione fiscale nel breve termine o di riciclaggio di alcuni capitali, destinate successivamente alla chiusura al momento di adempiere agli obblighi dichiarativi e fiscali.

Queste aziende fittizie, in secondo luogo, vengono sovente impiegate per abbattere i costi dell’ente acquirente mediante la produzione di documentazione falsa dichiarata in fatture emesse per prestazioni inesistenti con la conseguenza di produrre un ragguardevole profitto a seguito dell’omesso versamento dell’IVA.

Non v’è dubbio quindi che la mancata collocazione fra i soggetti destinatari degli obblighi di verifica della clientela derivanti dalla Direttiva del 2005 degli operatori che forniscono società “ready made”, idonee a riciclare prontamente denaro sporco, frodare l’IVA o finanziare la criminalità transnazionale, avrebbe rappresentato un chiaro *vulnus* allo spirito e allo scopo della suddetta disciplina europea.

Pertanto, le argomentazioni della CGUE, al di là delle tecniche interpretative sviluppate, possono dirsi condivisibili. Escludere dall’alveo applicativo dell’art. 3, punto 7, lett. a) della direttiva 2005/60/CE, i soggetti che offrono servizi commerciali di vendita di società “ready made”, significherebbe favorire l’anonimato degli acquirenti delle società precostituite nonché l’elusione della prima barriera posta dal legislatore europeo per impedire l’uso di enti commerciali per fini di riciclaggio o di finanziamento del terrorismo. In altri termini, afferma la CGUE «un’interpretazione siffatta dell’art. 3, punto 7, lett. a), della direttiva 2005/60 favorirebbe, in definitiva, ciò che la direttiva 2005/60 mira proprio ad evitare».

4. – Il problema della pericolosità dell’anonimato nelle transazioni finanziarie e commerciali risulta essere oggi ancora centrale tanto più in considerazione del fatto che, in molti casi, esse vengono realizzate mediante l’impiego delle criptovalute, oggetto di costanti riflessioni e dibattiti che si muovono fra esigenze di regolamentazione e spinte innovative.

Ecco che può essere ora utile analizzare tale problematica alla luce dei nuovi strumenti di prevenzione e contrasto al finanziamento del terrorismo ed al riciclaggio di proventi illeciti.

Come è noto, infatti, le transazioni che avvengono con l’uso delle monete digitali e, in particolare, attraverso i c.d. *bitcoins* (cfr. R. Bocchini, *Lo sviluppo della moneta virtuale: primi tentativi di inquadramento e disciplina tra prospettive economiche e giuridiche*, in *Diritto dell’informazione e dell’informatica*, 2017, 27 e ss; R. Razzante, *“Bitcoin” e monete digitali. Problematiche giuridiche*, in *Gnosis*, 2014, 106 e ss; N. Passerelli, *Bitcoin e antiriciclaggio*, in www.sicurezzanazionale.gov.it, 15 novembre 2016; N. Vardi, *“Criptovalute” e dintorni: alcune considerazioni sulla natura giuridica del “Bitcoin”*, in *Rivista dell’informazione e dell’informatica*, 2015, 443 e ss;) garantiscono una scarsa tracciabilità da parte

dell'amministrazione finanziaria e della polizia giudiziaria, divenendo così il nuovo strumento principe nel compimento di attività di riciclaggio e di finanziamento illecito del terrorismo e della criminalità organizzata, oltre che di evasione fiscale.

Lo stesso *bitcoin*, definito quale nuovo “contante digitale” (N. Passerelli, *Bitcoin e antiriciclaggio*, cit., 2;) è contemporaneamente un sistema di pagamento ed una moneta (così si è espressa anche la CGUE, *sentenza del 22 ottobre 2015, causa C-264/14, Skatterverket c. David Hedqvist*). Essendo una rappresentazione digitale di valore (vedi Art. 1, Direttiva 849/2015/UE), gestita elettronicamente, e indipendentemente da intermediari finanziari, banche o altri istituti di credito, può dar facilmente luogo a operazioni di riciclaggio e di finanziamento del terrorismo in quanto appare, per sua natura, idonea a dissimulare il reale oggetto del trasferimento realizzato nel web, luogo virtuale in cui, come anticipato, i controlli da parte degli istituti e degli enti deputati al monitoraggio delle transazioni sono ancora più difficili ed incerti.

Se poi consideriamo quanto può avvenire all'interno del *deep web*, ed in particolare nel *dark web*, ovvero in quella parte dell'internet nascosta, poco conosciuta o normalmente non frequentata, poiché decisamente inaccessibile, i sistemi di prevenzione si mostrano ancora più fragili.

Esso è del resto un luogo in cui gli *hackers* provenienti da tutto il mondo comunicano attraverso il sistema *peer to peer*, per cui risulta particolarmente complicato tracciare le transazioni finanziarie e prevenire, in generale, la commissione di illeciti.

In pratica, il nuovo sistema virtual-finanziario fondato sul *bitcoin* pone chiare difficoltà per il legislatore nazionale ed europeo così chiamato a disciplinare i rischi che derivano dall'anonimato, o meglio dallo “pseudo-anonimato” delle transazioni; infatti, ogni soggetto titolare di un account *bitcoin* è garantito sulla totale riservatezza della propria identità e dell'oggetto delle transazioni compiute (S. Nakamoto, *Bitcoin, a peer-to-peer electronic cash system*, in www.bitcoin.org, 2008). Recentemente, peraltro, da uno dei più recenti rapporti del GAFI (Rapporto GAFI, *Virtual currencies Key definitions and potential AML/CFT risks*, in www.fatf-gafi.org, 2014) sono emersi alcuni fra gli espedienti illeciti impiegati per occultare l'origine della transazione, quali il collegamento della transazione ad un indirizzo diverso dal reale attraverso il meccanismo del *tumbler*, o l'utilizzo del browser *T.O.R.* che consente, fra l'altro, l'accesso al *deep web* (si veda N. Passarelli, *Bitcoin e antiriciclaggio*, cit., 14; S. Capaccioli, *Riciclaggio, antiriciclaggio e bitcoin*, in *Il Fisco*, 2014, 4562 e ss;).

Sebbene ogni transazione che avvenga mediante l'uso delle criptovalute sia registrata in un *distributed ledger*, ovvero in un libro contabile digitale, di pubblico dominio, accessibile da chiunque per risalire ai soggetti titolari degli account mediante l'impiego delle nuove tecnologie di criptazione e decriptazione di *blockchain*, va evidenziato come l'algoritmo matematico con il quale coincide la catena delle transazioni, non solo è alquanto ardua da decifrare, ma soprattutto non garantisce la riconducibilità delle operazioni ad una ben definita persona fisica o giuridica (cfr. L. La Rocca, *La prevenzione del riciclaggio e del finanziamento del terrorismo nelle nuove forme di pagamento. Focus sulle valute virtuali*, in *Analisi giuridica dell'economia*, 2015, 201 e ss; S. Capaccioli, *Riciclaggio, antiriciclaggio e bitcoin*, in *Il Fisco*, 2014, 4562) .

Inoltre, esistono alcuni soggetti che svolgono un'attività di intermediazione tra il mondo reale della moneta ad uso corrente e quello virtuale delle criptovalute. In particolare, vi sono ruoli, come quello del *virtual currency exchanger*, che effettua operazioni di scambio delle valute virtuali in valute con corso legale o il c.d. *wallet provider* (cfr. G.P. Accinni, *Profili di rilevanza penale delle criptovalute nella riforma della disciplina antiriciclaggio 2017*, in *Arch. Pen.*, 2018, 27 e ss;), il quale fornisce all'utente un portafoglio elettronico per conservare e trasferire la moneta virtuale, che proprio in ragione dell'attività praticata possono concorrere nel delitto di riciclaggio con l'autore del reato-presupposto e contribuire considerevolmente a minacciare l'integrità del sistema finanziario dell'UE che le Direttive 2005/60/CE e 2015/849/UE tendono a preservare.

Sebbene il contributo di questi soggetti appaia eventuale, in quanto il *bitcoin*,

profitto illecito del reato presupposto, non deve necessariamente essere re-immesso nel circuito economico reale, ben potendo continuare a circolare nel mondo virtuale o essere scambiato con ulteriori criptovalute che non necessitano poi del contributo degli *exchangers* per essere introdotti nel circuito legale (sulle operazioni di cambio fra *bitcoin* e moneta reale, nella giurisprudenza CGUE si veda *sentenza 22 ottobre 2015, causa C- 264/14, Skatteverket c. Davide Hedqvist*), è innegabile come questi soggetti possano diventare i veri e propri responsabili dell’efficacia della normativa antiriciclaggio, poiché essi risultano essere gli unici in grado di accertare l’identità dell’utente che utilizza il *bitcoin* prima che questo compia ulteriori operazioni o attivi un account diverso.

Nulla dunque esclude che, per esempio, società “ready made” possano essere acquisite anche con criptovaluta o con proventi derivanti dal riciclaggio *online* della moneta digitale.

Ecco perché gli obblighi di verifica sulla provenienza dei fondi e sull’identità degli acquirenti devono essere capillari e coinvolgere non solo le nuove figure degli *exchangers* e dei *wallet providers*, ma ogni soggetto operante nel mercato in grado di immettere nel mercato nuove risorse economiche.

5. – Sul punto, quindi, può essere utile evidenziare quali siano gli ultimi provvedimenti normativi adottati a livello europeo per integrare e migliorare il sistema di prevenzione del riciclaggio e del finanziamento del terrorismo, mediante l’imposizione di obblighi di verifica in capo ad imprese e professionisti operanti all’interno dell’UE.

In particolare, già nel 2012, il GAFI, con le raccomandazioni 24 e 25 aveva inquadrato le proprie riflessioni sugli abusi del diritto (*ex multis*, F. Gallo, *La nuova frontiera dell’abuso del diritto in materia fiscale*, in *Rass. Trib.*, 1315 e ss;) compiuti con l’utilizzo di società fittizie o “schermo”, fra le quali possono sicuramente rientrare, per alcuni profili, anche le società “ready made”, il cui acquisto, celato dall’anonimato dell’identità del cliente e dei fondi, può integrare, come anticipato, gravi ipotesi di riciclaggio o di finanziamento del terrorismo, nonché di frodi IVA ed evasione fiscale.

In questo contesto, solo la trasparenza degli assetti societari e la conoscenza degli effettivi titolari degli enti costituiti e ceduti possono assicurare un adeguato meccanismo per inibire l’occultamento di risorse economiche (O. Salvini, *Il contrasto all’abuso del sistema finanziario per scopi di riciclaggio e finanziamento del terrorismo: la IV Direttiva (EU) 2015/849, tra coordinamento e cooperazione*, in *Riv. it. Dir. e proc. Pen.*, 2016, 147 e ss; R. Razzante, *La quarta direttiva contro il riciclaggio: spunti per una nuova regolamentazione italiana del fenomeno*, in www.magistraturaindipendente.it, 2015;).

Decisivo, dunque, risulta ancora una volta essere il ruolo degli intermediari, persone fisiche e giuridiche, nell’adempimento degli obblighi di verifica della clientela anche per le prestazioni rese *online*.

Tuttavia, sebbene la formulazione originaria della Direttiva 2015/849/UE, che raccoglie alcune indicazioni del GAFI, abbia rafforzato il sistema di prevenzione degli illeciti lesivi degli interessi finanziari dell’Unione Europea, prevedendo fra i reati gravi la cui perpetrazione configura “attività criminosa” anche i reati fiscali relativi a imposte dirette e indirette, puniti con una certa pena, (la direttiva invita gli stati membri ad armonizzare la nozione di reato fiscale a livello europeo tramite un costante scambio di informazioni da parte delle *Financial Information Units*), non ha però previsto particolari modifiche in relazione ai soggetti destinatari della stessa.

Anzi, per un certo verso, ne è stato delimitato l’ambito di applicazione, conferendo agli stati membri la facoltà di escludere i soggetti che esercitino in modo occasionale o, su scala molto limitata, attività finanziarie con rischio di riciclaggio e di finanziamento del terrorismo molto basso (art. 2, par. 3), purché tali attività siano limitate in termini assoluti e a livello di singola operazione ed abbiano il carattere dell’accessorietà e siano direttamente collegate all’attività principale, essendo prestate solamente a favore dei clienti della stessa.

Un passo in avanti è stato però compiuto con riferimento alle modalità con cui

effettuare le verifiche che sono fondate su criteri più stringenti circa l'identificazione del cliente e la provenienza dei fondi e la con l'adozione, all'interno di ogni stato membro, di un registro centrale esterno alle società all'interno del quale trasferire i dati raccolti (artt. 30 e 31 della Direttiva 2015/849/UE).

Il pregio della Direttiva del 2015, in poche parole, è l'aver messo in luce la necessità che le misure di prevenzione, fra le quali rientrano gli obblighi di verifica della clientela, svelino il mascheramento di fondi provenienti da forme gravi di criminalità e dalla raccolta di beni o di denaro a scopo di finanziamento del terrorismo mediante un approccio che sia fondato sul riconoscimento e l'identificazione del "rischio"; agli operatori del mercato viene chiesto di porre in essere processi di verifica basati sull'evidenza fattuale, al fine di individuare in modo più efficace i rischi di riciclaggio di finanziamento del terrorismo.

Le modifiche più rilevanti rispetto alla categoria di soggetti destinatari dell'obbligo di verifica della clientela e di riduzione dei rischi derivanti dall'impiego delle *virtual coins* e dalle operazioni compiute nel totale anonimato sono giunte soltanto negli anni successivi ed, in particolare, nel 2016 (L. Starola, *Contrasto al finanziamento del terrorismo, all'elusione fiscale internazionale e al riciclaggio*, in *Corr. Trib.*, 2016, 2630;) e, successivamente nell'aprile del 2018 con l'approvazione della proposta della Commissione da parte del Parlamento Europeo .

Infatti, con la precipua finalità di contrastare il finanziamento del terrorismo, in primo luogo, la Commissione Europea ha adottato, il 5 luglio 2016, una proposta di modifica della Direttiva 849/2015, nonché della Direttiva 2009/101/CE, in materia di coordinamento delle norme aventi ad oggetto la pubblicità delle società.

Essa ha previsto l'introduzione, entro il 1° gennaio 2017, di disposizioni volte a neutralizzare i rischi di finanziamento del terrorismo legate proprio all'impiego delle valute virtuali ed i rischi derivanti dagli strumenti di pagamento anonimi, nonché il rafforzamento dei poteri delle *Financial Intelligence Units (FIU)* e la promozione di una maggiore cooperazione fra le stesse. (A. Rossi, *Prevenzione del riciclaggio e finanziamento del terrorismo: finalità e novità normative*, cit. 28; in particolare sulle *FIU*, si veda il *Rapporto annuale di informazione finanziaria per l'Italia, n. 9, anno 2017*, con commento di A. Di Lernia, *Il rapporto dell'unità di informazione finanziaria per l'Italia per l'anno 2016*, in www.penalecontemporaneo.it, 10 ottobre 2017;).

Sono previste, peraltro, anche disposizioni che mirano a promuovere una maggiore trasparenza fiscale ed una più efficace lotta all'evasione fiscale ed al riciclaggio, attraverso la totale accessibilità ai registri dei beneficiari effettivi e la pubblicizzazione di alcune informazioni in essi contenute riferite sia a società che a *trusts*; l'interconnessione dei registri nazionali per agevolare la cooperazione tra gli stati membri; l'estensione delle informazioni a disposizione delle autorità degli stati membri che vigilano sulle attività di riciclaggio ed un controllo più stringente sulle operazioni compiute con soggetti residenti in Paesi extra UE.

Grazie alla proposta della Commissione Europea, tutti i prestatori di servizi che operano *online* e con le valute digitali, in particolare gli *exchangers*, i *money transfers* e i *wallet providers*, saranno chiamati ad adempiere agli specifici vincoli di adeguata verifica della clientela in occasione dell'instaurazione di un rapporto o del conferimento dell'incarico, finanche in presenza di un'operazione occasionale. L'*escamotage* suggerito dalla Commissione consentirà di imporre l'obbligo nei confronti di qualunque tipologia di soggetto privato operante sul mercato, a prescindere dalla qualificazione data dall'art. 3 della Direttiva, almeno tutte le volte in cui la transazione e l'investimento sia fatto in criptovalute o con strumenti che generino un rischio di anonimato.

Infine, una misura particolarmente innovativa ha ad oggetto l'abbassamento della soglia richiesta per potere procedere all'identificazione del titolare effettivo di un ente. La proposta della Commissione Europa, infatti, vuole ridurla dal 25% al 10% in modo da potere far emergere il numero delle entità commerciali "non reali", che non svolgono alcuna attività, essendo esse normalmente entità di intermediazione, costituite con lo scopo di separare alcuni beni e redditi da quelli del titolare effettivo per fini di risparmio

fiscale. In questo modo, verrà garantito un controllo più approfondito anche rispetto alle società “ready made”, che, come già affermato, vengono frequentemente acquistate proprio per trasferire capitali da un ente all’altro solo per fini elusivi e non per l’esercizio di attività di impresa.

Complessivamente, dunque, lo scopo specifico dell’emendamento della Commissione Europea è quello di approntare sistemi di prevenzione in grado di affrontare il problema, ormai a tutti noto, della smaterializzazione del denaro e del reddito, alla base del quale fundamentalmente vi è l’interesse della persona fisica e giuridica di pianificare il proprio carico fiscale e di collocare le proprie risorse economiche in Paesi diversi da quello di residenza in modo elusivo o fraudolento.

Ecco che l’esatta e corretta identificazione della clientela diventa un presupposto fondamentale per ridurre i rischi. E dal momento che la maggior parte delle attività di intermediazione finanziaria e di investimento è posta in essere da persone giuridiche, il processo di armonizzazione europeo dovrebbe fondarsi anche su un riavvicinamento delle legislazioni in materia di responsabilità da reato degli enti (in particolare sulla responsabilità degli enti e terrorismo, si veda R. Sabia, *Delitti di terrorismo e responsabilità da reato degli enti tra legalità ed esigenze di effettività*, in *Riv. Trim. dir. pen. cont.*, 2017, 208 e ss;) in modo che non solo si possa agire adeguatamente sul piano della repressione dell’illecito ma che si possa soprattutto condividere una strategia di prevenzione rispetto all’ingresso nel mercato di risorse economiche illecite gestite dalle imprese stesse e provenienti, in particolare, da Paesi extra UE.

Dopo l’approvazione della proposta della Commissione Europea del 2016 da parte del Parlamento Europeo, avvenuta il 19 aprile 2018, il 14 maggio scorso, il Consiglio ha adottato una Direttiva che rafforza la prevenzione del riciclaggio di denaro sporco e di finanziamento del terrorismo (www.consilium.europa.eu).

In particolare, al fine di garantire «la maggiore trasparenza delle operazioni finanziarie, delle società e degli altri soggetti giuridici, nonché dei trusts e degli istituti giuridici aventi assetto o funzioni affini a quelli dei trusts, allo scopo di migliorare l’attuale quadro di prevenzione e di contrastare più efficacemente il finanziamento del terrorismo» (Considerando 2), ed al fine di combattere l’anonimato e di distinguere correttamente fra le valute virtuali e la moneta elettronica (Considerando 10) e di garantire così la trasparenza nel mercato e la fiducia degli investitori, fra le altre cose, i prestatori di servizio delle valute virtuali saranno equiparati alle banche e agli altri intermediari finanziari, venendo così chiamati ad applicare controlli di *due diligence* e di adeguata verifica della clientela per porre un freno al regime di anonimato associato alle transazioni economico-finanziarie realizzate *online*.

L’ambito di applicazione della direttiva è esteso a tutte le forme di servizi di consulenza fiscale, alle agenzie di locazione, ai commercianti d’arte, ai prestatori di servizi di portafogli elettronici e a quelli di cambio valuta virtuale.

In questo modo, sono ampliate le misure per l’identificazione delle società “cartiere” e “fantasma” e per tracciare i flussi finanziari diretti ad alimentare atti di terrorismo nel territorio europeo. Di fatto, si tratta della prima regolamentazione organica in tema di criptovalute.

6. – Così intervenendo, ancora una volta, le istituzioni europee stanno contribuendo allo sviluppo di un *diritto penale europeo* fundamentalmente imperniato sulla salvaguardia degli interessi finanziari comunitari mediante tecniche di tutela che agiscono più sul piano della prevenzione che della repressione e che tendono ad inibire l’approvvigionamento di risorse illecite da parte della criminalità organizzata transazionale, a volte, anche a scapito della tutela della privacy o della manifestazione di altre libertà fondamentali.

In questo contesto, dunque, non si dovrà attendere molto prima di potere analizzare nuovi arresti della giurisprudenza europea sui confini applicativi di un diritto europeo “della prevenzione da rischio di reato” che sembra trovare sempre di più le proprie radici

nell'art. 325 TFUE, concentrato sulla primaria tutela degli interessi finanziari.

Tuttavia, sarà proprio nel *metodo dialogico* (I. Rivera, *L'Europa dei giudici e dei diritti. Questioni di metodo dialogico*, in www.federalismi.it, 2014, 26 e ss;) di confronto attuato dalle Corti nazionali ed europee, ed in particolare, dalla Corte EDU, che sarà possibile influire sulla costruzione di un sistema disciplinare multilivello ed integrato in materia penale più avanzato, che possa rispondere all'esigenza di tutelare in via primaria non solo, appunto, gli interessi finanziari, ma anche altri interessi collettivi e del singolo, consacrati nella Carta di Nizza o nella Convenzione di Strasburgo sui diritti dell'uomo, fondamentali per un' Europa dal volto "umano e solidale".