

Rivista
di Diritto Bancario

dottrina
e giurisprudenza
commentata

Estratto dal n. 5/2018

La disciplina antiriciclaggio alla
prova del processo di digitaliz-
zazione dei pagamenti

Alberto Urbani

ISSN: 2279-9737

 DIRITTOBANCARIO

Direzione scientifica:

Filippo Sartori, Stefano Ambrosini, Sandro Amorosino, Filippo Annunziata, Sido Bonfatti, Francesco Capriglione, Alfonso Castiello d'Antonio, Paoloefisio Corrias, Fulvio Cortese, Matteo De Poli, Raffaele Di Raimo, Aldo Angelo Dolmetta, Alberto Gallarati, Gian Luca Greco, Ugo Patroni Griffi, Bruno Inzitari, Marco Lamandini, Raffaele Lener, Paola Lucantoni, Alberto Lupoi, Daniele Maffei, Ugo Malvagna, Luca Mandrioli, Rainer Masera, Alessandro Melchionda, Roberto Natoli, Elisabetta Piras, Maddalena Rabitti, Giuseppe Santoni, Maddalena Semeraro, Antonella Sciarrone Alibrandi, Francesco Tesauo

Direzione esecutiva:

Alberto Gallarati, Paola Lucantoni, Luca Mandrioli, Elisabetta Piras, Francesco Quarta, Maddalena Semeraro

Comitato editoriale:

Francesco Albertini, Francesco Autelitano, Stefano Daprà, Eugenia Macchiavello, Massimo Mazzola, Manila Orlando, Carlo Mignone, Edoardo Rulli, Stefania Stanca

La disciplina antiriciclaggio alla prova del processo di digitalizzazione dei pagamenti*

1. L'opportunità di un riesame critico della legislazione antiriciclaggio alla luce della sua esperienza applicativa

Sia nell'ordinamento italiano che nell'ambito dell'Unione Europea, la legislazione antiriciclaggio si avvicina ormai rapidamente al traguardo dei trent'anni di esperienza applicativa. Già questo giustificherebbe una verifica attenta e ragionata sull'efficacia e sull'efficienza dell'impianto regolamentare adottato e dunque, di riflesso, sulla coerenza sul piano fattuale tra obiettivi attesi e risultati raggiunti. Come si sa, sul tema le opinioni non sono del tutto univoche¹, non fosse altro che per l'evidente ragione che tale valutazione richiederebbe una impossibile analisi controfattuale delle dimensioni del fenomeno contrastato in assenza di una regolamentazione in materia o per effetto di una disciplina diversa. Anche solo leggendo i rapporti annuali dell'Unità di Informazione Finanziaria², a me pare tuttavia che i risultati conseguiti possano essere considerati più che positivi e che quindi a conti fatti, come si usa dire, il gioco abbia valso la candela.

Ciò però non esime, ovviamente, dall'opportunità di una attenta e ponderata valutazione della disciplina di prevenzione e contrasto del riciclaggio e del finanziamento del terrorismo anche alla luce delle profonde modifiche morfologiche ed operative che hanno contrassegnato in questi lunghi anni l'ambiente nel quale i diversi soggetti destinatari delle prescrizioni in materia svolgono la loro attività. Come si sa, tanto il legislatore sovranazionale quanto quello interno hanno attuato una costante opera di adeguamento

* Il presente scritto riproduce, con l'aggiunta di note bibliografiche, la relazione tenuta al convegno su *I servizi di pagamento nell'era della digitalizzazione: innovazione tecnologica, esigenze della clientela e regolazione* svoltosi a Taormina il 15 e 16 febbraio 2018 e sarà pubblicato anche nel volume che ne raccoglierà gli atti.

¹ Per informazioni, anche di tipo quantitativo, si veda ad es. l'ultima *Relazione* al Ministro dell'economia e delle finanze per l'anno 2016, predisposta dal COMITATO DI SICUREZZA FINANZIARIA, *Valutazione delle attività di prevenzione del riciclaggio e del finanziamento del terrorismo*, Roma, 2017; in chiave critica, v. le pertinenti osservazioni di F. DI VIZIO, *Risultati seri e tematiche vive dell'antiriciclaggio*, in *Papers dell'Osservatorio sulle crisi di impresa*, luglio 2014, www.osservatorio-oci.org; più in generale, per un'impostazione metodologica della questione, cfr. invece, per tutti, A.R. CASTALDO, M. NADDEO, *Il denaro sporco. Prevenzione e repressione nella lotta al riciclaggio*, Padova, 2010, p. 45 ss.

² Da ultimo, *Rapporto Annuale dell'Unità di Informazione Finanziaria* per l'anno 2016, Roma, 2017, reperibile sul sito istituzione dell'UIF e presentato con una *Relazione* accompagnatoria dal Direttore dell'Unità, C. CLEMENTE, il 3 luglio 2017.

della disciplina agli scenari operativi che si andavano evolvendo, ma il rischio concreto che le tecniche impiegate dalle organizzazioni criminali per occultare la circolazione della ricchezza progrediscano più rapidamente degli strumenti normativi atti a contrastarle è concreto e assai insidioso, sicché non risultano affatto eccessivi "tagliandi" della normativa di settore, anche ravvicinati nel tempo, atti a promuoverne la costante efficacia.

2. Le sfide precipue poste dal processo di digitalizzazione dei pagamenti

In questa prospettiva, il processo di digitalizzazione dei pagamenti, oggetto di questo convegno, può rappresentare un banco di prova di indubbia utilità, non fosse altro che per la poliedricità del fenomeno, in sé considerato, e per la rapidità dei cambiamenti che lo caratterizzano.

Che l'avvento e la diffusione delle tecnologie informatiche abbiano disclosed alle organizzazioni criminali nuovi validi canali per il riciclaggio del denaro illecito è un dato noto ed acclarato da diverso tempo: lo spallone ha ceduto il posto al *trader* digitale, il corriere con la valigetta colma di banconote al tecnico informatico specializzato in transazioni finanziarie³. Già da diversi anni è stato evidenziato come le nuove tecnologie si presentino agli occhi della criminalità economica come molto promettenti in ragione di una serie articolata di fattori concomitanti: per la velocità delle transazioni, che consente di effettuare una pluralità di operazioni in un brevissimo arco temporale; per la facilità di impiego e per i costi molto ridotti che le caratterizzano; per la riservatezza che molto spesso continuano ad assicurare, comunque sicuramente maggiore di quella offerta dai canali bancari e finanziari internazionali; per il parallelo processo di terziarizzazione delle stesse organizzazioni criminali, o quanto meno di quelle di più alto livello; infine, non ultimo, per la sostanziale anarchia che caratterizza *internet* e, più in generale, il mondo virtuale⁴.

Tali fattori sono ulteriormente accentuati proprio quando le tecnologie in parola fanno il loro ingresso nel settore dei mezzi di pagamento, dal momento che in questi casi lo strumento informatico non solo *entra in contatto*, ma addirittura – almeno in una certa misura – *si sostituisce* nelle funzioni a quel bene così particolare e delicato che è la moneta, centro stesso del sistema economico: emblematico il caso della moneta elettronica⁵, tant'è che ad un certo punto del percorso evolutivo della disciplina antiriciclaggio⁶ tale

³ In argomento v. già G. POMANTE, *Internet e criminalità*, Torino, 1999, p. 228.

⁴ Sul punto, sia consentito un rinvio a A. URBANI, *Disciplina antiriciclaggio e ordinamento del credito*, Padova, 2005, p. 39 ss.

⁵ In tema v. ancora A. URBANI, *op. cit.*, p. 44 ss.

⁶ Ossia con il varo del D.Lgs. 21 novembre 2007, n. 231, il quale sin dal testo originario accolse continui riferimenti alla moneta elettronica ed inserì gli istituti di

strumento ed i soggetti che, oltre alle banche, lo possono emettere hanno fatto il loro ingresso nella normativa di settore.

Di qui, come detto, l'interesse per un riesame critico della legislazione in materia dallo specifico angolo di osservazione della sua applicazione al vasto e sempre più articolato ambito dei servizi e degli strumenti di pagamento in forma digitalizzata.

3. Pagamenti in forma digitalizzata e prescrizioni antiriciclaggio: a proposito di obblighi di segnalazione di operazioni sospette e di adeguata verifica della clientela

Entrando dunque nel merito delle nostre riflessioni, un primo ordine di considerazioni può partire guardando l'impianto generale dei presidi antiriciclaggio per come consegnato dalla nostra legislazione domestica. Questo, come noto, a partire dal 2007 è imperniato sui quattro pilastri fondamentali degli obblighi di adeguata verifica della clientela, degli obblighi di registrazione (oggi tramutatisi in obblighi di conservazione, dopo le modifiche al D.Lgs. n. 231/2007 recentemente apportate dal D.Lgs. n. 90/2017, di attuazione della Quarta direttiva (UE) 2015/849), degli obblighi di segnalazione di operazione sospetta e, infine, delle limitazioni all'uso del contante e dei titoli al portatore.

Paradossalmente, il profilo da sempre e a buon titolo considerato come il più delicato e problematico, ossia l'*obbligo di segnalare un'operazione sospetta* di riciclaggio o di finanziamento del terrorismo, se osservato con riguardo specifico ai pagamenti digitalizzati non sembra porre questioni peculiari, diverse cioè da quelle comuni agli altri ambiti nei quali è articolata la disciplina o da quelle proprie dell'obbligo di segnalazione in sé considerato. In fondo, sin dall'ormai lontana L. n. 197/1991 gli operatori sono stati invitati a scorgere eventuali profili anomali in un trasferimento di denaro con riguardo non soltanto a chi materialmente richiede quell'operazione ma soprattutto, e prima ancora, guardando al soggetto cui l'operazione stessa è riferita, come richiedeva l'art. 3 di quella legge⁷: il vaglio critico dell'operazione anche nei confronti di chi non entra fisicamente in contatto con l'addetto del soggetto tenuto all'eventuale segnalazione è pertanto, da sempre, nel DNA della normativa in materia. Anzi, guardando alle tecnologie informatiche dall'opposto punto di vista delle autorità amministrative in materia di antiriciclaggio e degli organi investigativi, al contrario tali strumenti possono

moneta elettronica tra i soggetti destinatari della disciplina antiriciclaggio (cfr. art. 11, co. 1, lett. c)).

⁷ Sul punto, v. infatti già M. COMPORI, *Identificazione della clientela, segnalazione di operazioni sospette di riciclaggio e tutela della riservatezza*, in *Il riciclaggio del denaro nella legislazione civile e penale*, a cura di C.G. Corvese e V. Santoro, Milano, 1996, p. 395.

costituire un alleato fondamentale nel contrasto dell'economia criminale, sol che si pensi ad esempio agli algoritmi assai sofisticati che coadiuvano nel far emergere possibili profili di anomalia nei rapporti o nelle transazioni finanziarie.

È invece a partire dagli adempimenti connessi all'*adeguata verifica della clientela* che la digitalizzazione dei pagamenti pone difficoltà pratiche speciali. In questo caso, infatti, la distanza fisica tra chi avvia un rapporto o chiede un'operazione e colui che deve procedere alla verifica frappone un ostacolo intrinseco alle esigenze di certezza in ordine alla effettiva identità del cliente, più che all'acquisizione e alla valutazione di informazioni sullo scopo e sulla natura del rapporto continuativo e al controllo costante del rapporto con i clienti, dal momento che questi ultimi, in fondo, almeno in una certa misura restano invece possibili anche a distanza.

Non è un caso, dunque, che fino alla recente novella di attuazione della Quarta direttiva antiriciclaggio l'art. 19 del D.Lgs. n. 231/2007 prescrivesse che l'identificazione e la verifica dell'identità del cliente dovesse avvenire «*in presenza del cliente*», mentre la possibilità di una identificazione a distanza era desumibile soltanto in via indiretta dall'art. 28, nel momento in cui questo imponeva, in tal caso, obblighi di verifica rafforzati; norme apposite, inoltre, erano dettate in ipotesi di esecuzione degli obblighi in parola da parte di terzi (artt. 29-35, vecchio testo)⁸.

L'attuale testo dell'art. 19 del decreto antiriciclaggio non rivoluziona il quadro normativo previgente, ma apre espressamente alla possibilità di adempiere agli obblighi di adeguata verifica «*anche senza la presenza fisica del cliente*», ancorché la regola di partenza resti, come in passato, che «*l'identificazione del cliente e del titolare effettivo è svolta in presenza del medesimo cliente ovvero dell'esecutore*». La maggiore e specifica attenzione all'assolvimento a distanza degli obblighi in questione è tuttavia attestata dall'elencazione articolata e puntuale di casi nei quali ciò può avvenire, tutti contrassegnati dal comun denominatore della *certezza* circa i dati raccolti, come nell'ipotesi in cui, ad esempio, il cliente sia in possesso di un'identità digitale caratterizzata dal livello massimo di sicurezza ai sensi del Codice dell'amministrazione digitale (D.Lgs. 7 marzo 2005, n. 82). Fermo restando inoltre che restano in vigore, per quanto aggiornate, le disposizioni riguardanti l'esecuzione degli obblighi di adeguata verifica da parte dei terzi (ora artt. 26-30, D.Lgs. n. 231/2007), anche dal versante degli obblighi di verifica rafforzata la riforma dimostra una maggiore attenzione ai rischi derivanti dal ricorso alle nuove tecnologie, come si può desumere, tra gli altri, dai riferimenti alle situazioni nelle quali i «*prodotti o [le] operazioni [...] potrebbero favorire*

⁸ In argomento, v. ampiamente C. RUGGIERO, *La nuova disciplina dell'antiriciclaggio dopo il d.lg. 21 novembre 2007, n. 231*, Torino, 2008, p. 113 ss.

*l'anonimato» e, ancor più, ai «rapporti continuativi, prestazioni professionali od operazioni occasionali a distanza non assistiti da adeguati meccanismi e procedure di riconoscimento» e ai «prodotti e pratiche commerciali di nuova generazione, compresi i meccanismi innovativi di distribuzione e l'uso di tecnologie innovative o in evoluzione per prodotti nuovi o preesistenti»⁹. Di tal modo, il rischio derivante dal ricorso con finalità illecite a strumenti di pagamento in forma digitale certo non è scongiurato, né oggettivamente sarebbe possibile eluderlo del tutto se non vietando *tout court* l'applicazione delle nuove tecnologie ai sistemi di pagamento, con scelta che sarebbe però non solo anacronistica, ma soprattutto dannosa per l'intera economia; ciò nonostante, lo sforzo aggiuntivo apertamente richiesto agli operatori nel momento in cui si avvalgono di strumenti digitali per prestare servizi di pagamento sembra costituire un buon punto di equilibrio tra esigenze di celerità nei processi per il trasferimento di somme di denaro e istanze di preservazione di tali strumenti dall'uso per finalità vietate dall'ordinamento.*

Tutte queste indicazioni trovano ora un seguito nei recentissimi «*Orientamenti definitivi*» che l'EBA ha diramato poco più di un mese fa – e precisamente il 4 gennaio scorso –, con i quali ha cercato di definire i fattori che gli enti creditizi e gli istituti finanziari dovrebbero prendere in considerazione nel valutare i rischi di riciclaggio e finanziamento del terrorismo¹⁰. Questi orientamenti contengono avvertenze anche in merito all'assolvimento a distanza degli obblighi di adeguata verifica della clientela, che si pongono in piena linea di continuità con le norme di rango primario che abbiamo appena richiamato; le autorità competenti e le imprese coinvolte sono invitate a conformarsi a questi orientamenti – alcuni qualificati come «settoriali» perché rivolti a specifiche categorie di destinatari – entro il prossimo 26 giugno.

4. (Segue) ... nonché di conservazione e di limitazioni nell'uso del contante e di titoli al portatore

Nell'assetto normativo in vigore fino al luglio dello scorso anno l'imposizione di obblighi di adeguata verifica della clientela era strettamente correlato agli ulteriori *obblighi di registrazione* dei dati raccolti in un archivio unico informatico, che ciascuno dei destinatari dell'adempimento in questione era tenuto ad istituire (art. 37, D.Lgs. n. 231/2007, vecchio testo). Come si è avuto modo di accennare, l'attuazione della Quarta direttiva ha portato alla sostituzione di questi adempimenti con meri *obblighi di conservazione* dei

documenti, dei dati e delle informazioni raccolte, secondo quanto oggi stabilito dall'art. 31 del decreto antiriciclaggio.

Per quanto riguarda l'ambito dei sistemi di pagamento per via digitale, al pari degli obblighi di segnalazione di operazioni sospette il cambio di impostazione non dà adito a questioni particolari. Soltanto, in via ben più generale, può forse valere la pena di evidenziare come, sopprimendo gli obblighi di «registrazione», sia venuta meno la necessaria istituzione e tenuta dell'archivio unico informatico (fatto salvo un periodo transitorio che sta per scadere il 31 marzo 2018), tant'è che ora l'art. 34, co. 3, del D.Lgs. n. 231/2007 si limita a demandare alle Autorità di vigilanza di settore la valutazione circa l'opportunità («*possono*») di adottare disposizioni specifiche per la conservazione e l'utilizzo dei dati e delle informazioni relativi ai clienti, «*contenuti in archivi informatizzati, ivi compresi quelli già istituiti presso i soggetti rispettivamente vigilati, alla data di entrata in vigore del presente articolo*». Al riguardo, una recentissima comunicazione della Banca d'Italia¹¹ ha precisato che il proprio Provvedimento datato 3 aprile 2013 recante «*Disposizioni attuative per la tenuta dell'Archivio Unico Informatico e per le modalità semplificate di registrazione di cui al [previgente] articolo 37, commi 7 e 8, del decreto legislativo 21 novembre 2007, n. 231*» non è più in vigore, ma che poiché la legge continua a prevedere obblighi di conservazione dei dati per l'assolvimento degli adempimenti antiriciclaggio attribuendo alla stessa Banca d'Italia il potere di emanare norme attuative in materia, «*in attesa di tale intervento*», l'utilizzo – si noti – «*su base volontaria*» dell'Archivio Unico Informatico «*costituisce modalità idonea ad assolvere a questi obblighi*».

Si tratta di una evidente delegificazione – o se si preferisce di un'amministrativizzazione – della specifica materia, che onestamente può destare qualche preoccupazione se si tiene conto che la standardizzazione prima imposta dalla normativa secondaria in ordine ai contenuti e alle modalità di tenuta dell'archivio era considerata funzionale alla celerità della sua consultazione da parte degli organi investigativi. Forse, nella direzione prescelta, ha militato la constatazione che, nella prassi, l'accesso «diretto» agli archivi unici informatici è stato sin qui piuttosto infrequente, dal momento che il ricco patrimonio informativo messo a disposizione dall'Anagrafe tributaria ha indotto a preferire almeno in prima istanza quest'ultimo strumento.

Detto per inciso, la stessa Comunicazione della Banca d'Italia ha chiarito invece che il proprio, importante, provvedimento del 10 marzo 2011 contenente «*Disposizioni attuative in materia di organizzazione, procedure e controlli interni volti a prevenire l'utilizzo degli intermediari e degli altri soggetti che svolgono attività finanziaria a fini di riciclaggio e di finanziamento del*

¹¹ Cfr. *Comunicazione della Banca d'Italia in materia di obblighi antiriciclaggio per gli intermediari bancari e finanziari*, in data 9 febbraio 2018, pubblicata sul sito istituzionale dell'Organo di vigilanza.

⁹ V. L. LA ROCCA, *La prevenzione del riciclaggio e del finanziamento del terrorismo nelle nuove forme di pagamento. Focus sulle valute virtuali*, in *Analisi giur. econ.*, 2015, p. 201 ss.

¹⁰ Cfr. EUROPEAN BANKING AUTHORITY, *Orientamenti relativi ai fattori di rischio*, doc. JC 2017 37 del 4 gennaio 2018.

terrorismo” «è in linea generale compatibile con il nuovo quadro normativo primario ed è pertanto applicabile».

Resta infine da considerare il fronte delle *limitazioni all'uso del contante e dei titoli al portatore*, oggi come in passato disciplinato dall'art. 49 del decreto.

È noto come, sin dalla loro introduzione, tali limitazioni fossero preordinate prioritariamente a canalizzare i trasferimenti di denaro contante (cui, per intuitibili ragioni, erano accostati alcuni tra i più diffusi titoli al portatore) nell'alveo di intermediari abilitati, di modo che, in sinergia con gli obblighi di identificazione della clientela e soprattutto di registrazione delle operazioni, fosse possibile mantenere traccia dei flussi di circolazione di queste principali e tradizionali fonti di ricchezza¹². Di riflesso, per svariati motivi (non tutti connessi con obiettivi di contrasto del riciclaggio di denaro di provenienza illecita o di finanziamento del terrorismo) ne è scaturito al contempo l'auspicio per una maggiore diffusione di modalità di pagamento alternative, *in primis* carte di debito e carte di credito, in altri Paesi molto più impiegate che in Italia. Nonostante i progressi compiuti in questa direzione, grazie anche all'affermazione sul mercato di carte prepagate, molta strada resta ancora da percorrere per colmare il divario che ancora persiste al confronto con altre aree dell'Unione Europea.

Senonché, a ben considerare, nella prospettiva che ci riguarda gli strumenti di pagamento alternativi al denaro contante e ai tradizionali titoli cambiari presentano al tempo stesso vantaggi e rischi intrinseci. Se è vero infatti che in linea di massima il denaro “elettronico” garantisce una maggiore tracciabilità rispetto alla banconota o anche alla cambiale o all'assegno, l'esperienza attesta purtroppo che il ricorso alle carte di pagamento in sostituzione del denaro contante può essere funzionale all'impiego da parte di soggetti diversi dal titolare formale dello strumento oppure finalizzato all'organizzazione logistica di attentati terroristici, come ad esempio nel caso tragico della strage sul lungomare di Nizza¹³.

¹² Sul punto, v. ad es. P. COSTANZO, *La disciplina comunitaria: dalla direttiva 91/308/CEE alla direttiva 2001/97/CE*, in *Profili internazionali dell'attività di prevenzione e contrasto del riciclaggio di capitali illeciti*, a cura dell'Ufficio Italiano dei Cambi, Roma, 2004, p. 84.

¹³ Tale rischio è stato opportunamente segnalato anche dal direttore dell'UIF, C. CLEMENTE, nel corso dell'audizione dinanzi alla VI^a Commissione Finanze della Camera dei Deputati il 19 aprile 2016, *Money transfer e prevenzione del riciclaggio e di finanziamento del terrorismo*, p. 19 del documento. Per l'osservazione che le nuove strategie terroristiche, specie quelle di stampo *jihadista*, tendono a privilegiare iniziative autonome individuali o di piccoli gruppi informali, le quali, proprio per le loro caratteristiche intrinseche, necessitano di risorse finanziarie modeste che possono dunque transitare anche per il tramite di strumenti di pagamento elettronico di larga

Tale ambivalenza¹⁴ merita naturalmente attenta e prudente considerazione, sì da fare in modo che la graduale ed *auspicabile* progressiva sostituzione del denaro contante con nuovi strumenti digitali di pagamento non si traduca anche in agevolazione di operazioni gravemente illecite da parte di organizzazioni criminali o di singoli individui, specie grazie al facile paravento del possibile anonimato.

5. Evoluzione dei sistemi di pagamento ed evoluzione del perimetro applicativo del D.Lgs. n. 231/2007

Il riesame critico dello strumentario approntato dalla legislazione antiriciclaggio nelle sue quattro articolazioni fondamentali alla luce dei processi in atto di digitalizzazione dei pagamenti deve tuttavia essere accompagnato, quanto meno, da un secondo filone di indagine, incentrato sulla valutazione del perimetro applicativo della normativa materia sotto il profilo soggettivo e dunque, di riflesso, anche sulle attività monitorate.

Se è vero infatti che una disciplina in questo settore che si proponga di risultare efficace non può prescindere dal coinvolgimento di tutti quei soggetti che, in ragione dell'attività esercitata, a vario titolo hanno a che fare con il denaro o con beni di particolare valore, occorre altresì evitare con molta attenzione il rischio di un'estensione non ragionata di prescrizioni antiriciclaggio concepite per un determinato settore di attività ad altri affatto diversi. L'esperienza maturata al riguardo con il D.Lgs. n. 374/1999, quando il nostro ordinamento anticipò almeno in parte la scelta, che di lì a breve sarebbe stata compiuta dalla Seconda direttiva del 2001, di rendere applicabili le misure in materia anche a soggetti diversi dalle banche e dagli intermediari finanziari per i quali erano state originariamente elaborate, generando incertezze e difficoltà pratiche ad esempio nei riguardi delle agenzie di affari in mediazione immobiliare o dei fabbricanti o commercianti di oggetti preziosi¹⁵, ci deve avvertire della inopportunità del ricorso maldestro ad una tecnica legislativa che potremmo definire del “copia e incolla”.

diffusione e quindi difficilmente tracciabili in via preventiva, v. A. URBANI, A. MINTO, *La Quarta direttiva europea in materia di antiriciclaggio, tra luci, ombre e prospettive*, in *Dir. banca merc. fin.*, 2017, I, p. 126.

¹⁴ Per certi versi indirettamente attestata anche dal fatto che l'innalzamento della soglia massima di utilizzo del denaro contante, di cui oggi all'art. 40, co. 1, del D.Lgs. n. 231/2007, è stato talvolta motivato con esigenze di rilancio dell'economia nazionale, quasi che tali limitazioni rappresentassero una sorta di palla al piede dello sviluppo economico della Nazione: sul punto v. infatti le critiche di A. MINTO, *Le “canne al vento” della disciplina antiriciclaggio: brevi riflessioni a margine di alcune disposizioni del d.l. n. 78/2010*, in *Dir. banca merc. fin.*, 2010, I, p. 151.

¹⁵ Sul punto v. ancora, ampiamente, A. URBANI, *op. cit.*, p. 227 ss.

Ciò premesso, è indubitabile però che la nascita e la diffusione di strumenti innovativi di pagamento, offerti non più soltanto da banche ma altresì da nuove tipologie di operatori, richiede una costante opera di aggiornamento della disciplina antiriciclaggio anche sotto il profilo soggettivo, al fine di evitare che tali operatori, se non sottoposti a prescrizioni in materia di efficacia pari a quelle da tempo in vigore per gli intermediari più tradizionali, possano essere facilmente preferiti a questi ultimi per porre in essere operazioni illecite.

Al riguardo, appare emblematico il caso dei *money transfer*, efficacemente illustrato un paio d'anni fa dal Direttore dell'Unità di Informazione Finanziaria in occasione di un'audizione davanti alla VI^a Commissione Finanze della Camera dei Deputati¹⁶. Si tratta, come noto, di soggetti che offrono il servizio di rimessa di denaro – specie all'estero – *senza l'apertura di conti di pagamento intestati al pagatore o al beneficiario* (cfr. art. 1, co. 1, lett. n), del D.Lgs. 20 gennaio 2010, n. 11). La rischiosità intrinseca in chiave antiriciclaggio del servizio offerto, dovuto proprio all'assenza di un conto retrostante, ha opportunamente indotto il legislatore a mantenere a 1.000 euro la soglia di utilizzo del contante da utilizzare per la rimessa, in luogo degli attuali 3.000 euro che costituiscono il limite di importo di carattere generale (cfr. art. 49, co. 2, D.Lgs. n. 231/2007).

La questione centrale e probabilmente più delicata¹⁷ attiene alla circostanza che per lo svolgimento dell'attività gli intermediari sono soliti avvalersi di una rete distributiva affidata ad agenti, coordinati in un c.d. «punto di contatto centrale» e sottoposti ad una regolamentazione differente a seconda che operino per un intermediario italiano o per uno avente la sede legale in un altro Stato membro dell'Unione Europea¹⁸: solo nel primo caso, infatti, gli agenti sono tenuti all'iscrizione nell'elenco tenuto dall'Organismo degli Agenti e dei Mediatori (OAM), mentre nell'altro, in omaggio alla regola generale dell'*home country control*, sono applicabili le norme del Paese d'origine, spesso più blande di quelle italiane. Per di più, prima della recente riforma, se invece di fruire della libertà di insediamento questi intermediari avessero scelto di operare in regime di libera prestazione di servizi, nessuna prescrizione antiriciclaggio nazionale sarebbe stata loro applicabile. Ne è derivato un prevedibile processo di arbitraggio normativo, tant'è che in soli tre anni, dal 2012 al 2015, gli istituti di pagamento italiani esercenti il servizio di *money*

transfer calarono drasticamente da 19 a 9 ma per converso, alla fine del 2015, quelli comunitari si attestarono a ben 270, di cui 36 operanti attraverso una rete di agenti¹⁹.

Soprattutto, però, una serrata “campagna ispettiva” condotta dalla UIF sempre nello stesso anno fece emergere, in materia antiriciclaggio, diffuse carenze organizzative di tali intermediari e frequenti irregolarità, evidenziando in particolar modo come la rete distributiva rappresentasse il vero punto debole per l'attività in discorso, tanto più nel caso di agenti plurimandatari: si pensi, ad esempio, alla possibilità di frazionare in modo artificioso un'operazione rivolgendosi contemporaneamente a più agenti, alle rimesse frazionate ma contestuali da parte di più ordinanti, al ricorso da parte dell'agente di collaboratori non noti all'istituto di pagamento fruitori delle chiavi di accesso attribuite all'agente.

Di qui l'intervento, assai opportuno, operato in materia dal D.Lgs. n. 90/2017, il quale ha inciso su più punti del decreto antiriciclaggio ma soprattutto vi ha introdotto per la prima volta, in un Capo autonomo, disposizioni specifiche per i soggetti convenzionati e gli agenti di prestatori di servizi di pagamento e di istituti di moneta elettronica (cfr. artt. 43-45). In particolare, la riforma ha valorizzato il ruolo del punto di contatto centrale, ora da istituirsi anche da parte degli intermediari beneficiari della libera prestazione di servizi. Il punto di contatto centrale è espressamente indicato dall'art. 43, co. 3, del D.Lgs. n. 231/2007 come la struttura organizzativa attraverso la quale gli istituti di pagamento e gli IMEL assolvono agli obblighi in materia antiriciclaggio, con il presumibile risultato di aver reso più stringente ed effettivo per l'intera rete distributiva l'assolvimento dell'insieme degli obblighi antiriciclaggio.

Si tratta di un esempio virtuoso, tra gli altri possibili, sia di adattamento del quadro normativo all'evoluzione della platea di soggetti che popolano l'industria dei servizi di pagamento, sia di risposta alle criticità delle disposizioni previgenti emerse in sede applicativa e nell'ambito delle attività di vigilanza oltre che di indagine da parte delle autorità preposte.

¹⁹ È interessante osservare come secondo i dati al 31 dicembre 2017 ricavabili dalla *Relazione annuale sulle attività svolte nel 2017* dell'Organismo degli agenti e dei mediatori (OAM), mentre il numero degli istituti di pagamento italiani esercenti il servizio di *money transfer* è rimasto pressoché inalterato rispetto a due anni prima (8 invece di 9), viceversa il numero di quelli comunitari è improvvisamente precipitato a 16 (13 dei quali si avvalgono di agenti): tale brusca contrazione sembra indirettamente attestare che le recenti modifiche introdotte in attuazione della Quarta direttiva, di cui subito si dirà nel testo, paiono aver raggiunto l'obiettivo di una maggiore equiparazione tra istituti di pagamento italiani e istituti di pagamento comunitari quanto alla disciplina antiriciclaggio applicabile nel nostro Paese, stemperando pertanto in modo deciso i negativi fenomeni di arbitraggio normativo sopra segnalati.

¹⁶ Cfr. C. CLEMENTE, *doc. cit.*

¹⁷ Non a caso, il problema è ben rimarcato dagli orientamenti settoriali riguardanti i soggetti che offrono servizi di rimessa di denaro emanati dall'EBA, cit., Tit. III, Cap. 4, p. 49 ss.

¹⁸ In chiave informativa, v. M. PALANA, *Il riciclaggio nell'ambito dell'attività degli «agenti money transfer»*, in http://www.diritto.it/system/docs/30025/original/Money_transfer-Riciclaggio.pdf.

Certo, il progresso tecnologico incalzante e la dinamicità dei mercati finanziari convergono nel rendere sempre più arduo il mantenimento di standard normativi coerenti con un quadro operativo in cambiamento continuo. Se come si è appena visto sono state da poco implementate nuove regole riguardanti l'attività di *money transfer*, subito la realtà pone all'attenzione, ad esempio, l'ingresso nel mercato di nuove tipologie di operatori, quali ad esempio Circle, le cui piattaforme di *instant payment* consentono agli utenti di trasferire istantaneamente e in modo gratuito somme di denaro con una facilità paragonabile all'invio di un sms, avvalendosi della tecnologia *blockchain*.

6. (Segue) In particolare, “fintech” e criptovalute

Il mondo della c.d. *fintech* rappresenta in effetti una sfida che ci attende non soltanto in un prossimo futuro, bensì già nell'immediato, anche in chiave di contrasto del riciclaggio di denaro e di finanziamento del terrorismo. Ciò, ovviamente, a partire da quel magma composito costituito dalle c.d. criptovalute, le quali in realtà, più che come e vere e proprie “valute”²⁰, almeno in

²⁰ Sul punto v. le chiare osservazioni di M. MANCINI, *Valute virtuali e bitcoin*, in *Analisi giur. econ.*, 2015, p. 122 ss.; per una diversa impostazione v. però M. PASSARRETTA, *Bitcoin: il leading case italiano*, in *Banca borsa tit. cred.*, 2017, II, p. 475, nonché, sulla scorta di una distinzione concettuale tra «valuta» e «moneta», N. VARDI, “*Criptovalute*” e dintorni: *alcune considerazioni sulla natura giuridica dei bitcoin*, in *Dir. informaz. e informatica*, 2015, p. 446.

La questione testé accennata è complessa e, in tutta evidenza, travalica l'ambito e le finalità delle nostre riflessioni, quanto meno perché implicherebbe un ulteriore approfondimento circa il rapporto tra la nozione di «moneta» e quella di «denaro», in chiave nazionale anche alla luce dell'art. 1277 c.c. e del ricco dibattito sviluppatosi nel corso del tempo attorno alla categoria delle obbligazioni pecuniarie. Ad ogni modo, può sinteticamente osservarsi come l'orientamento dottrinale da ultimo riferito si ponga sulla scia di un'autorevole e nota opinione per la quale è la base consensuale dei suoi utilizzatori a rendere qualificabile una moneta come tale (cfr. A. NUSBAUM, *Money in the law national and international*, Brooklin, 1950, p. 5 ss.), sicché le nuove c.d. valute virtuali risulterebbero inquadrabili nello schema delle monete complementari o alternative, come infatti assume esplicitamente N. VARDI, *op. cit.*, p. 448; sembra implicitamente accogliere tale impostazione anche S. CAPACCIOLI, *Criptovalute e bitcoin: un'analisi giuridica*, Milano, 2015, p. 114, che la ritiene «una nuova forma di moneta». Al riguardo, risultano tuttavia ancora attuali le parole di un insigne Maestro quale T. ASCARELLI, che seppure ovviamente condizionato da un contesto reale assai diverso da quello odierno, già ne *La moneta. Considerazioni di diritto privato*, Padova, 1928, p. 121, così avvertiva: «In realtà, mentre il semplice concetto di danaro implica una determinata qualifica di alcuni oggetti senza alcun carattere normativo tanto che come abbiamo visto detta attribuzione è frutto di una semplice pratica di fatto e non di una consuetudine, il concetto di valuta ha un implicito carattere normativo, sì che la sua determinazione non può trovare la sua fonte

un primo momento si sono proposte come mezzi di pagamento²¹, collocandosi dunque in una posizione di contiguità funzionale con gli altri mezzi di pagamento, tanto più quelli digitalizzati.

Non a caso, come noto, *bitcoin* e le altre c.d. valute virtuali stanno suscitando ovunque una preoccupata attenzione da parte delle pubbliche autorità, sia per i rischi che derivano dalla loro promanazione extrastatuale che ne preclude il governo con i tradizionali strumenti di politica monetaria²², sia per l'elevato grado di rischio specie per i consumatori che può derivare dal loro utilizzo²³, sia proprio per il loro potenziale agevole impiego per finalità illecite, grazie al sostanziale anonimato garantito dalla *blockchain* quanto meno nelle fasi “intermedie” della circolazione²⁴. In pratica, seppure *mutatis mutandis*, si ripropongono pertanto problemi poi non così lontani da quelli, noti e consolidati, sollevati dall'impiego dei titoli al portatore, con l'ovvia “aggravante” che nel caso delle criptovalute non sono di certo allo stato immaginabili presidi

se non in una fonte di diritto e non in una semplice pratica di fatto: ciò vale tanto per gli oggetti in astratto, per le monete che rispondono a detta caratteristica, quanto per la singola moneta, il singolo pezzo. Difatti è lo Stato quello che legislativamente determina (contrariamente appunto a quanto ha luogo in tema di denaro) le monete che nel proprio ordinamento debbono venire considerate come valuta». In tale prospettiva pertanto, come si dice nel testo, almeno nel loro stadio originario le c.d. valute (o, se si preferisce, monete) virtuali paiono piuttosto essersi proposte come funzionalmente analoghe ad altri mezzi di pagamento digitalizzati. Solo il futuro saprà dirci se, per scelte degli ordinamenti valutari nazionali ancorché presumibilmente inserite nel contesto di accordi internazionali, queste evolveranno in vere e proprie valute.

²¹ Così, in una questione interpretativa di carattere fiscale, Corte Giust. Eur., 22 ottobre 2015, causa C-264/14, in *Foro it.*, 2015, IV, c. 513 ss. Secondo Trib. Verona, 24 gennaio 2017, in *Banca borsa tit. cred.*, 2017, II, p. 467 ss., con nota di M. PASSARRETTA, *cit.* – a quanto consta, prima pronuncia giurisprudenziale italiana sull'argomento – le valute virtuali andrebbero invece considerate alla stregua di strumenti finanziari.

²² V. R. SCALCIONE, *Gli interventi delle autorità di vigilanza in materia di schemi di valute virtuali*, in *Analisi giur. econ.*, 2015, p. 139 ss.

²³ Sul punto specifico, v. da ultimo l'Avviso diramato congiuntamente dall'Autorità Bancaria Europea (EBA), dall'Autorità Europea degli Strumenti Finanziari e dei Mercati (ESMA) e dall'Autorità Europea delle Assicurazioni e delle Pensioni (EIOPA) sui rischi delle valute virtuali, fatto proprio anche dalla Banca d'Italia con una *Avvertenza* pubblicata sul proprio sito istituzionale il 19 marzo 2018 ma già preceduto da un'altra *Avvertenza* datata 30 gennaio 2015. In argomento, v. anche S. CAPACCIOLI, *op. cit.*, p. 45 ss.

²⁴ V. ad es., in argomento, G. CARAMIGNOLI, I. DI PIETRO, *Il fenomeno Bitcoin: moneta “virtuale” con effetti “reali” sull'economia*, in *Riv. Guardia Fin.*, 2013, p. 1731 ss., partic. p. 1744 ss.

preventivi corrispondenti al divieto di emettere assegni privi dell'indicazione del beneficiario e della clausola di non trasferibilità.

Di fronte a rischi siffatti, non può dunque che essere salutata con estremo favore la scelta, compiuta dal legislatore nazionale in occasione della riforma del 2017, di anticipare previsioni contenute nella Proposta di Quinta direttiva antiriciclaggio²⁵ – a quanto consta in fase di stallo in sede europea – tese ad avviare un percorso di applicazione di misure in materia anche alle criptovalute e a talune categorie di soggetti che concorrono al loro impiego. Viene così fornita, per la prima volta, una definizione di «*valuta virtuale*»²⁶ ma, soprattutto, si estendono gli obblighi antiriciclaggio sia alle piattaforme di cambio di valute virtuali (c.d. *exchanger*) sia ai prestatori di servizi di portafoglio digitale (c.d. *custodial wallet*), accomunati sotto il nuovo sintagma «*prestatori di servizi relativi all'utilizzo di valuta virtuale*», intesi come «*ogni persona fisica o giuridica che fornisce a terzi, a titolo professionale, servizi funzionali all'utilizzo, allo scambio, alla conservazione di valuta virtuale a alla loro conversione da ovvero in valute aventi corso legale*»²⁷ e adesso tenuti, tra l'altro, all'iscrizione in una sezione speciale del registro dei cambiavalute di cui all'art. 17-*bis* del D.Lgs. n. 141/2010 (cfr. il co. 8-*bis* della stessa disposizione). Il novellato art. 3, co. 5, del D.Lgs. n. 231/2007, ora, alla lett. *i*) indica pertanto proprio costoro tra i soggetti obbligati al rispetto delle disposizioni che ci occupano, ancorché tale previsione risulti esplicitamente limitata «*allo svolgimento dell'attività di conversione di valute virtuali da ovvero in valute aventi corso forzoso*». In pratica, si è dunque adottato un approccio forzatamente “minimalista” ma comunque saggiamente pragmatico, dal momento che, nell'impossibilità almeno per il momento di tener traccia dei passaggi dei trasferimenti di criptovalute intermedi tra la prima conversione da una valuta legale e l'ultimo cambio di segno opposto, si è deciso quanto meno di censire gli estremi, ossia i momenti di contatto tra il circuito della moneta avente corso forzoso e quello della moneta virtuale. Almeno un primo, emblematico passo è stato dunque compiuto.

È interessante notare come la bozza di decreto ministeriale²⁸ previsto dall'art. 17-*bis*, co. 8-*bis*, del D.Lgs. n. 141/2010 (introdotto anche questo dal provvedimento di attuazione della Quarta direttiva), il quale dovrà stabilire le modalità e la tempistica con cui i prestatori di servizi relativi all'utilizzo di

²⁵ Com/2016/450/Final.

²⁶ Secondo l'art. 1, co. 2, lett. *qq*), del D.Lgs. n. 231/2007, per “*valuta virtuale*” si intende «*la rappresentazione digitale di valore, non emessa da una banca centrale o da un'autorità pubblica, non necessariamente collegata a una valuta avente corso legale, utilizzata come mezzo di scambio per l'acquisto di beni e servizi e trasferita, archiviata e negoziata elettronicamente*».

²⁷ Così l'art. 1, co. 2, lett. *ff*), del D.Lgs. n. 231/2007.

²⁸ Rimasta in pubblica consultazione fino al 16 febbraio scorso.

valuta virtuale saranno tenuti a comunicare al Ministero dell'economia e delle finanze la propria operatività sul territorio nazionale, all'art. 2 estenda curiosamente la propria portata applicativa anche agli «*operatori commerciali che accettano valuta virtuale quale corrispettivo di qualsivoglia prestazione avente ad oggetto beni, servizi o altre utilità*». Osservato incidentalmente che questa prospettata estensione non sembra supportata a livello di normativa primaria non solo dal D.Lgs. n. 141/2010²⁹ ma nemmeno dal D.Lgs. n. 231/2007, nel merito essa lascia tuttavia intravedere, in positivo, il comprensibile intento di stringere ulteriormente le maglie attorno alle criptovalute avviando forme di monitoraggio – e dunque di larvata supervisione – nei confronti di chi, pur non operando nel mondo della “finanza” intesa anche nella sua accezione più ampia, si presta alla diffusione di questi strumenti accettandoli in pagamento e dunque ne favorisce indirettamente l'utilità e, di riflesso, l'appetibilità.

7. Le capacità di adeguamento tempestivo della disciplina in materia al mutato contesto operativo, tra costanti e nuove istanze emergenti

Ancora una volta, pertanto, e come già ripetutamente avvenuto nei decenni passati, la legislazione antiriciclaggio italiana è riuscita a dimostrarsi sollecita e reattiva nella risposta a nuove esigenze poste dall'evoluzione dell'industria finanziaria, anticipando soluzioni che probabilmente saranno presto accolte anche a livello sovranazionale.

In effetti, ripercorrendo in modo diacronico l'evoluzione della disciplina di casa nostra in materia, sembra di poter scorgere alcune costanti. La capacità di percorrere i tempi rispetto ai provvedimenti dell'Unione Europea è, sin dagli albori, una di queste. Se si ricorda però che una delle scelte lungimiranti compiute dalla legislazione del 1991 riguardò l'avvio di forme di supervisione pubblica anche nei confronti di intermediari prima mai vigilati (si tratta della norme oggi confluite nel Titolo V del Testo unico bancario) per evitare che l'imposizione di prescrizioni antiriciclaggio ai soli intermediari già vigilati potesse vanificare gli sforzi nel contrasto dell'economia criminale che si stavano compiendo, è facile scorgere oggi nell'impegno di aggiornamento della normativa alla luce dell'evoluzione in chiave digitale del sistema dei pagamenti una ulteriore e interessante analogia.

Insomma: si può quanto meno dire che, in materia di lotta al riciclaggio e al finanziamento del terrorismo, il guanto della sfida lanciato dal processo di

²⁹ Si tratta – ricordiamo per inciso – del decreto legislativo di attuazione della direttiva 2008/48/CE relativa ai contratti di credito ai consumatori e recante altresì modifiche a Titolo VI del Testo unico bancario in merito alla disciplina dei soggetti operanti nel settore finanziario, degli agenti in attività finanziaria e dei mediatori creditizi.

digitalizzazione dei pagamenti sia stato raccolto dal regolatore o dai regolatori.

Rivista
di Diritto Bancario | dottrina
e giurisprudenza
commentata