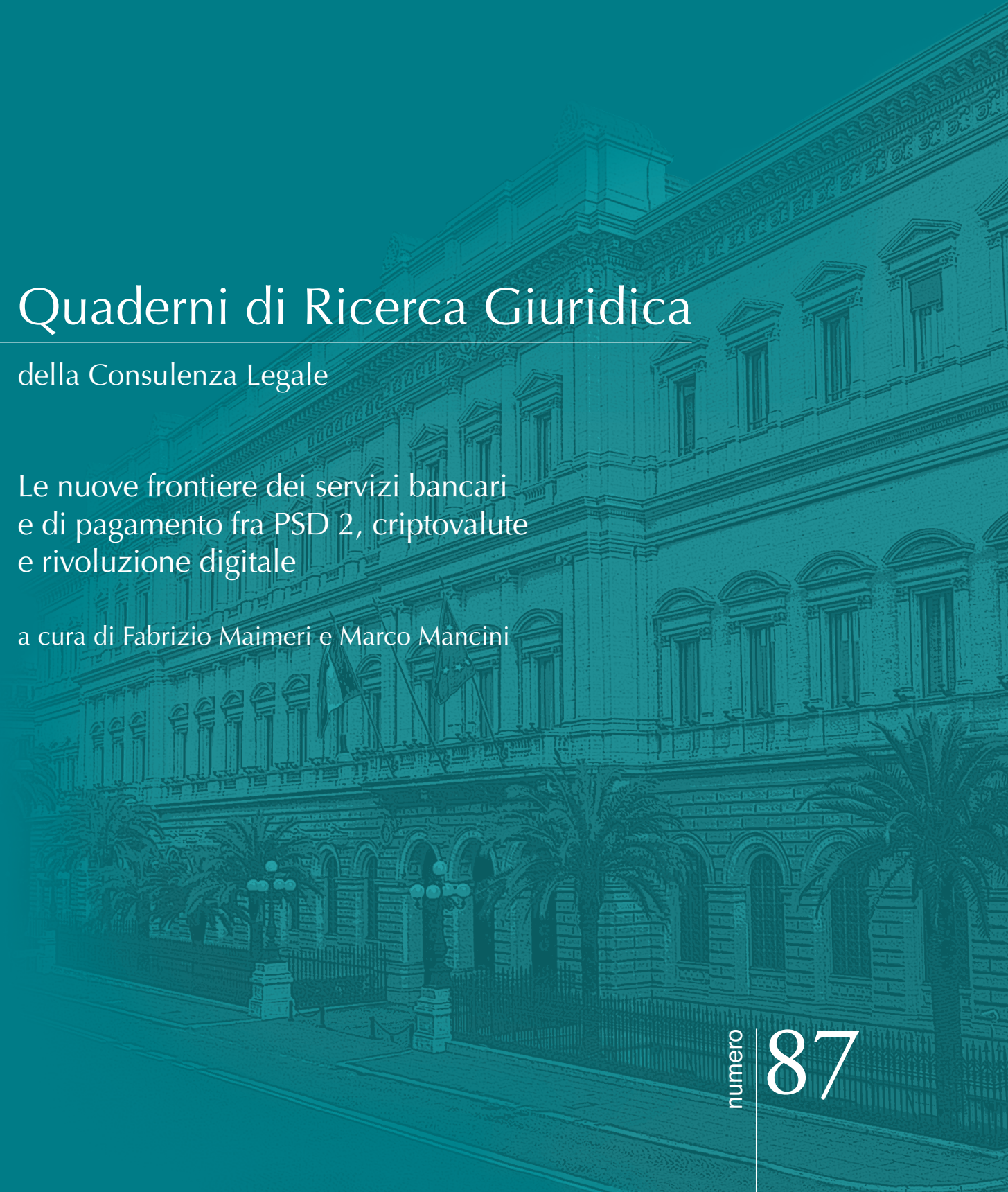
BANCA D'ITALIA
EUROSISTEMA

Quaderni di Ricerca Giuridica

della Consulenza Legale

Le nuove frontiere dei servizi bancari e di pagamento fra PSD 2, criptovalute e rivoluzione digitale

a cura di Fabrizio Maimeri e Marco Mancini



numero 87

settembre 2019

BANCA D'ITALIA
EUROSISTEMA

Quaderni di Ricerca Giuridica

della Consulenza Legale

Le nuove frontiere dei servizi bancari e di pagamento fra PSD2, criptovalute e rivoluzione digitale

a cura di Fabrizio Maimeri e Marco Mancini

Numero 87 – Settembre 2019

Nei Quaderni di Ricerca giuridica, curati dal Servizio Consulenza Legale, sono pubblicati gli studi condotti dagli avvocati della Banca d'Italia e da altri ricercatori interni ed esterni all'Istituto. La collana ha ad oggetto l'analisi giuridica di tematiche legate alle funzioni istituzionali o comunque di specifico interesse per la Banca d'Italia.

I lavori sono selezionati da un apposito Comitato editoriale, che tiene conto, tra l'altro, dell'originalità del contributo, della chiarezza espositiva, della coerenza dell'iter logico seguito e della completezza della trattazione. I "Quaderni" riflettono esclusivamente le opinioni dei singoli autori e non intendono, quindi, rappresentare posizioni ufficiali della Banca d'Italia.

ISSN: 0394-3097 (print)
ISSN: 2281-4779 (online)

Grafica e stampa a cura della Divisione Editoria e stampa della Banca d'Italia

SOMMARIO

Introduzione

Fabrizio Maimeri e Marco Mancini

Negli anni recenti il mondo dei servizi di pagamento e dei servizi bancari e finanziari è stato interessato da importanti cambiamenti, in parte indotti da interventi normativi, in parte originati dall'incessante sviluppo dell'innovazione tecnologica.

Sotto il profilo normativo, le principali cause del cambiamento sono rappresentate dalla seconda direttiva europea relativa ai servizi di pagamento nel mercato interno n. 2015/2366/UE del 25 novembre 2015 (c.d. PSD2), recepita nel nostro ordinamento dal decreto legislativo 15 dicembre 2017, n. 218, e dal regolamento UE 2015/751, che disciplina l'applicazione delle commissioni interbancarie ai pagamenti effettuati con strumenti basati sull'uso delle carte.

Si tratta di un pacchetto di norme di diversa caratura che non si limita ad ammodernare la precedente versione della direttiva PSD, ma la estende ed arricchisce verso nuovi scenari.

Il principale contenuto innovativo del complesso intervento normativo europeo risiede soprattutto nell'aver consentito di prestare servizi di pagamento a valere sul conto corrente bancario anche a prestatori diversi (cc.dd. *Third Party Providers*) rispetto a quello presso cui è radicato il conto, configurando in tal modo come un'*essential facility* quello che era stato sinora uno dei più riservati ed esclusivi rapporti contrattuali.

Parallelamente alle novità introdotte dal Legislatore europeo, la rivoluzione digitale applicata all'ambito delle attività finanziarie (*Fintech*) cui abbiamo assistito negli ultimi anni ha aperto nuove prospettive di sviluppo che potrebbero modificare radicalmente la tradizionale conformazione dei servizi di pagamento e, più in generale, dei servizi bancari e finanziari.

L'introduzione della tecnologia *blockchain*, che agevola la circolazione di beni *peer to peer* permettendo di verificare la legittimità del proprio titolo d'acquisto sulla base di un registro digitale distribuito fra gli stessi utenti, ha già reso possibile la diffusione a livello planetario delle valute virtuali o criptovalute e, nel prossimo futuro, potrebbe rendere inutile l'uso di registri centralizzati gestiti da autorità riconosciute e regolamentate.

Del pari, l'innovazione tecnologica ha ormai dato vita a piattaforme informatiche evolute in grado di consentire l'incontro diretto fra le esigenze dei soggetti che hanno liquidità in eccesso e soggetti alla ricerca di finanziamenti, con modalità tali da determinare in prospettiva una potenziale disintermediazione dalle relative attività delle banche e degli altri prestatori di servizi abilitati.

Una concausa della nuova conformazione dei servizi bancari, finanziari e di pagamento può forse ravvisarsi anche nell'inasprimento delle regole cui, a seguito della grande crisi finanziaria, sono state sottoposte le banche e gli altri soggetti abilitati alla prestazione di servizi di pagamento, che ha sicuramente concorso a determinare la contrazione del margine di redditività delle relative attività imprenditoriali. L'innalzamento dei requisiti patrimoniali e, più in generale, il crescente rigore delle regole poste a presidio dell'esercizio dell'attività

bancaria, finanziaria e di pagamento e il conseguente calo della redditività da essi indotto rischiano di innescare un meccanismo centrifugo, oggi reso possibile dalla disponibilità delle nuove tecnologie, che potrebbe spingere parte dei servizi bancari, finanziari e di pagamento verso nuovi soggetti e nuove modalità di esercizio meno o affatto regolamentate.

Quindi, sintetizzando, mentre la PSD2 amplia la gamma dei servizi di pagamento, legittimando – con il consenso del cliente – i prestatori abilitati a fornirli anche a valere su conti correnti bancari cui sono estranei, i nuovi scenari tecnologici da un lato favoriscono l'ingresso sul mercato di nuovi strumenti di scambio privati, che presentano alcune affinità con la moneta, dall'altro rendono possibili nuove modalità di circolazione dei valori mobiliari e di prestazione dei servizi bancari, finanziari e di pagamento, che prescindono dall'intermediazione dei soggetti abilitati, delle controparti centrali e, persino, delle stesse banche centrali.

La complessiva evoluzione del contesto dei servizi bancari, finanziari e di pagamento apre nuove sfide e pone delicati interrogativi in ordine alla natura giuridica dei nuovi strumenti di scambio e alla necessaria evoluzione delle modalità di vigilanza, delle forme di tutela dei clienti e del controllo dei rischi che potrebbero ingenerarsi.

Il presente studio, integrato da quindici contributi e condotto in sinergia dalla Consulenza legale della Banca d'Italia e da esponenti accademici e ricercatori esperti della materia, si propone di offrire un primo quadro ricostruttivo delle molteplici novità, che caratterizzano l'odierno assetto e le future prospettive dei servizi di pagamento e, più in generale, dei servizi bancari e finanziari.

Il punto di partenza dell'indagine consiste nel catalogare le novità principali della PSD2 e le loro possibili conseguenze applicative: si tratta di un assetto legislativo che da poco tempo è operativo (e non ancora del tutto) e del quale quindi si possono prefigurare gli esiti piuttosto che valutarli.

Il contributo di Porta ripercorre analiticamente l'iter normativo che ha condotto dalla direttiva alla normativa di recepimento, in particolare soffermandosi sul regime di "*operatività in esenzione*", sugli orientamenti dell'European Banking Authority (EBA) in ordine alle condizioni per beneficiare dell'esenzione dal meccanismo di emergenza (c.d. "*fall-back exemption*"), sulle modifiche in tema di trasparenza e correttezza dei rapporti con la clientela (a cominciare dalla *Strong Customer Authentication*). Uno sguardo d'insieme, sintetico ma completo, che dà conto delle molteplici finalità dell'intervento del legislatore europeo, che possono individuarsi nella competitività tra strumenti di pagamento, nell'accresciuta armonizzazione normativa e nell'incremento della sicurezza degli strumenti utilizzati.

Come già sottolineato in apertura, una delle novità più importanti della PSD2 consiste nella individuazione di due nuovi servizi e di due intermediari abilitati a svolgerli: il *"servizio di disposizione di ordine di pagamento", in forza del quale si "dispone l'ordine di pagamento su richiesta dell'utente*

di servizi di pagamento relativamente a un conto di pagamento detenuto presso un altro prestatore di servizi di pagamento" (PIS*: payment initiation service); e il "servizio di informazione sui conti", "servizio online che fornisce informazioni consolidate relativamente a uno o più conti di pagamento detenuti dall'utente di servizi di pagamento presso un altro prestatore di servizi di pagamento o presso più prestatori di servizi di pagamento" (*AIS*: account information service*). Il prestatore di entrambi i servizi deve operare su un conto online acceso presso un altro prestatore di servizi di pagamento, al quale compete amministrare e gestire il conto per il medesimo cliente (cd. prestatore di servizi di pagamento di radicamento del conto). È evidente la necessità che, per fornire siffatti servizi, siano potenziati, come la direttiva prevede, i presidi di sicurezza informatica dei pagamenti elettronici e il monitoraggio delle frodi, attribuendo all'EBA la competenza per la definizione di standard tecnici di comunicazione sicura tra i *Third Party Providers* e i prestatori di radicamento del conto. Di tutto ciò e dei complessi meccanismi di funzionamento e di processo di queste attività dà conto il contributo di Profeta, la quale si intrattiene con dovizia e dettaglio circa i profili di vigilanza sui fornitori dei servizi: e ciò avendo riguardo sia alla norma nazionale primaria, sia alle istruzioni della Banca d'Italia, sia alla valutazione complessiva di efficienza ed efficacia che il plesso normativo è in grado di assicurare.

Completa il saggio di Profeta un'appendice curata da Mastropaolo, che si intrattiene su uno specifico ma non marginale argomento: la presenza di una pluralità di intermediari nella catena del valore relativa alla prestazione di servizi di disposizione di ordine di pagamento o di informazione sui conti rende complessa l'attribuzione a ciascun soggetto degli obblighi previsti dalla normativa in materia di contrasto del riciclaggio e del finanziamento del terrorismo di cui al d.lgs. n. 231/2007, come modificato dal d.lgs. n. 90/2017. Di qui l'emersione di questioni specifiche, di cui si rilevano gli ambiti e si prefigurano le soluzioni.

Si è già accennato alla circostanza che insieme alla PSD2 è stato approvato un pacchetto di disposizioni relativo alle commissioni interbancarie: il problema non è nuovo, tutt'altro; ha avuto negli anni soluzioni differenziate, con interventi delle autorità di concorrenza nazionali e comunitarie, con approcci né definitivi né coerenti. L'ipotesi perseguita consiste nel fissare una misura massima delle *interchange fees* per le operazioni su carte, stabilita in modo diversificato, ponendo così la parola fine a molte delle tematiche fino ad oggi ampiamente discusse, ma facendone peraltro sorgere altre a seguito dell'approccio dirigistico prescelto, come i primi commentatori non hanno mancato di segnalare. Il lavoro di Maimeri esamina le varie indicazioni, non "scommette" sulla soluzione prescelta e cautamente lascia al mercato e alla esperienza applicativa futura la possibilità di superare o meno le obiezioni che sono state sollevate in proposito e che vengono partitamente analizzate.

Sempre nell'ottica dei costi, l'art. 3 della direttiva stabilisce un divieto generalizzato per il beneficiario/esercente di imporre spese aggiuntive, rispetto al costo del bene o del servizio, in relazione all'utilizzo di strumenti di pagamento: anche a questo riguardo è stato assunto un atteggiamento deciso, pervenendo alla

eliminazione delle deroghe al c.d. divieto di *surcharge* in precedenza possibili. Sui profili consumeristici e concorrenziali della questione e sulle possibili conseguenze attese della nuova soluzione discorre il saggio di Broggiato.

Le considerazioni fin qui elaborate dagli autori consentono di ampliare la prospettiva dell'indagine, aprendo il discorso agli effetti sul mercato delle novità introdotte partendo proprio dai due tipi di prodotti di cui si è occupato il lavoro di Profeta. Gammaldi e Iacomini si soffermano anzitutto sulla verifica della misura e del modo in cui sul settore dei servizi di pagamento incideranno le modalità specifiche nella prestazione dei nuovi servizi, soprattutto nell'ottica dei rapporti fra *Third Party Providers* e correntisti non più però solo nella logica della trasparenza e della sicurezza, bensì in quella più vasta dell'affidabilità che il mercato potrà ritenere di attribuire a questo settore di attività. In particolare, l'accesso ai conti disintegra le modalità finora consuete di acquisizione, conservazione, utilizzo dei dati relativi ai conti e questa situazione sollecita le Autorità (l'EBA nel fissare i requisiti di sicurezza, la Banca d'Italia nel verificarne il rispetto) a studiare un approccio certamente diverso rispetto al passato, non più replicabile.

E proprio alle delicate (anche per le notizie di stampa recenti) tematiche evocate dal contributo di Gammaldi e Iacomini si collega quello di Menzella, dedicato ai *Big data* e alla loro gestione. Se *knowledge is power*; se attraverso i servizi di pagamento (e non solo) si organizzano piattaforme che raccolgono una grande quantità di dati della clientela, è evidente la loro influenza sulle dinamiche competitive, sull'innovazione e sulla posizione degli utenti finali, tanto sotto il profilo dell'accesso a beni e servizi di consumo, a informazioni e notizie rilevanti, quanto con riferimento alla rilevanza della selettività degli algoritmi nella determinazione delle scelte. Tutto regolare e ineludibile, sembra, per il travolgente accrescersi della tecnologia e delle sue applicazioni. Ma altrettanto ineludibile appare la tendenza (doverosa) verso un *trade off* (soddisfacente se non ottimale) tra il valore commerciale dell'informazione e il rispetto di diritti individuali e collettivi fondamentali, quali la privacy, la tutela della concorrenza e le garanzie del pluralismo informativo. Di qui l'analisi, interessante e "di frontiera", di Menzella, la quale dimostra la stretta interconnessione tra la diffusione dei pagamenti in formato digitale, in particolare mediante la rete mobile, e i molteplici usi cui si prestano in tale ambito i *Big data* raccolti mediante i flussi telematici collegati ai pagamenti. La conclusione è che l'obiettivo del *trade-off* è ancora da conseguire, poiché, se la rivoluzione digitale in atto mette in discussione i paradigmi giuridici che finora hanno guidato la disciplina dei diversi fenomeni connessi all'uso dei *Big data*, ciò si riverbera sì sulle tecniche di controllo, ma prima ancora sul disegno del quadro delle regole che salvaguardi l'interesse pubblico garantendo un adeguato equilibrio tra opportunità e rischi del processo innovativo: in questa prospettiva, a livello europeo e più oltre, c'è ancora molta strada da fare per addivenire a un regime chiaro, con prescrizioni certe e uniformi, con tutele garantite in modo efficace dei vari interessi in gioco.

Parlando di rivoluzione digitale, non poteva l'indagine non aprirsi a quello che costituisce da qualche anno l'elemento più innovativo e dirompente nel

mondo dell'informatica, vale a dire il *blockchain* che, insieme alle piattaforme informatiche e agli algoritmi, costituisce la triade dalla quale si dipartono le diverse esperienze che si chiamano monete virtuali, transazioni di pagamento *peer to peer,* operazioni di raccolta (si pensi al *crowfunding*) e di impiego (il *peer to peer lending*), e così via, fino a comporsi in quel nuovo paradigma di *open banking* che costituisce la sfida di questi anni e di quelli a venire.

Si è allora adottata una ricostruzione tecnico-operativa di questo mondo di simboli, parole, concetti, espressioni matematiche chiedendo a Garavaglia di fissare in modo chiaro ma tecnicamente attrezzato terminologie e nozioni, in un saggio che servisse a fornire la cognizione degli elementi di base del discorso che si stava intraprendendo. E l'interesse sta proprio, si crede, nell'aver racchiuso in un numero ristretto di pagine l'abc basico dell'argomento, gli sviluppi potenziali e realizzati, fino a tracciare, nelle ultime righe, uno scenario che sembra futuribile ma che è solo prossimo.

Entrati con cognizione di causa e pertinenza di concetti e vocabolario, nel sistema della *blockchain*, l'indagine si indirizza verso l'ambito di utilizzo più frequente e sensibile di siffatto meccanismo, vale a dire alle criptovalute. Il saggio di Moliterni affronta, in un discorso sistematico che interconnette i diversi profili, la nozione di moneta, di moneta elettronica e di moneta virtuale, per valutarne similitudini e differenze ma, soprattutto, per verificare se l'ultima sia funzionalmente assimilabile alla prima, laddove assolva la finalità di mezzo di scambio, accettato dalle parti. L'altro tema interconnesso e di grandissimo rilievo consiste nelle modalità di scambio delle criptovalute, ovvero nella valutazione di servizi di pagamento fondati non sulle regole e sul controllo di una banca centrale, ma sulla fiducia degli operatori e su registri (formati attraverso *blockchain*) attraverso i quali, *peer to peer*, si perfezionano le transazioni. Si tratta di uno snodo cruciale: sistemi come quello delle criptovalute in tanto esistono in quanto alternativi a quelli istituzionali fondati su monete legali/statali (con controparti centrali, controlli continui, sanzioni, autorità); occorre valutare se tali sistemi siano di per sé idonei a garantire il pubblico interesse o se non occorra, a tal fine, prefigurare una qualche modalità di controllo, che non potrebbe essere certo quella che l'esperienza finora seguita ha prodotto. E qui la prospettiva si fa davvero stimolante, dovendosi discutere degli stessi principi fondanti del sistema dei pagamenti come finora conosciuto.

Affrontato il tema delle criptovalute nelle sue complessive valenze sistemiche e nelle problematiche strutturali, seguono una serie di saggi che ne completano e ne approfondiscono l'analisi sotto diversi profili.

Il lavoro di De Giorgi si sofferma sulla nozione di criptovaluta desumibile dalla disciplina nazionale antiriciclaggio (che a quella europea si ispira) per osservare come essa però non sciolga i dubbi sulla natura giuridica della stessa, limitandosi piuttosto a prescrivere regole confinate ai settori specifici della prevenzione del riciclaggio e del terrorismo, dettando una disciplina attinente non tanto all'oggetto – ossia alla valuta virtuale – quanto ai soggetti che prestano servizi in tale valuta. Questi ultimi, analogamente a coloro che svolgono attività

di cambiavalute, devono possedere determinati requisiti in tema di cittadinanza o sede, sono tenuti a effettuare una specifica comunicazione, vengono iscritti in una speciale sezione del registro tenuto dall'OAM e devono assolvere a taluni obblighi ex d.lgs. n. 231/2007. Prescrizioni specifiche, ma che ancora non consentono di definire quand'è che si sia in presenza di una valuta virtuale.

Restano in ogni caso senza risposta gli interrogativi su chi debba fissare la nozione di criptovaluta e su chi debba vigilarne l'utilizzo, posto il carattere universale degli scambi di cui essa è oggetto. Su questo problema si intrattiene il saggio di Ruccia il quale, dopo aver fornito un'ampia ricostruzione della posizione delle autorità nazionali dei singoli stati europei, ritiene soluzione percorribile quella di una stretta collaborazione fra le autorità di ogni paese, giacché ogni altra alternativa rischierebbe di apparire lenta e farraginosa di fronte a un fenomeno assai mutevole.

Che le transazioni in criptovalute, per le caratteristiche "liberal" che presentano, possano essere utilizzate per scopi illeciti, quali il riciclaggio e il finanziamento del terrorismo internazionale, è fatto noto, sul quale anche le autorità nazionali ed europee hanno emanato qualche "avviso di pericolo". Lo studio di Mastropaolo delinea efficacemente le modalità con le quali questo utilizzo indebito può realizzarsi e il riferimento alla normativa attuale (quella cui anche De Giorgi si riferiva nel suo lavoro) non è sufficiente a evitare questo rischio.

Ai profili tributari del trattamento delle operazioni in criptovalute è dedicato il saggio di Conte, la quale pone a confronto le determinazioni della normativa antiriciclaggio con quelle dei provvedimenti emanati dall'amministrazione finanziaria, confronto da cui nasce una sorta di "cortocircuito". Infatti, la Corte di Giustizia UE ha stabilito che le criptovalute non sono assimilabili a valute "legali" ma vanno considerate come mezzi di pagamento; in questo senso si è orientato anche il legislatore italiano con la definizione di "valuta virtuale" introdotta dalle modifiche alla normativa antiriciclaggio. L'amministrazione finanziaria nazionale invece – con la risoluzione n. 72/E del 2016 e l'interpello n. 956-39/2018 della Direzione Regione Lombardia del 2018 – ha affermato che le valute virtuali, ai fini fiscali, vanno assimilate alle valute estere. Ne deriva che la definizione di moneta virtuale non è solo un'esigenza sistematica, ma una necessità operativa quotidiana che il regulator (comunque individuato) è chiamato celermente a fornire.

Si è detto che il percorso iniziato con le modifiche alla PSD, passando per la configurazione di un nuovo e più articolato diritto dei pagamenti, declinato anche nell'ottica della moneta virtuale, si conclude, nella logica della "rivoluzione digitale", sul modo stesso di fare banca e finanza: e in due specifici saggi vengono affrontati entrambi questi profili.

Il contributo di Bellino, riferito al profilo bancario, conduce anzitutto all'analisi dettagliata del fenomeno del *lending based crowdfunding,* diffusamente noto come *peer-to-peer lending* (P2P *lending*), che, per ora, non è oggetto di regolamentazione in Italia. Dalla definizione del fenomeno fornita dall'EBA emerge con evidenza il ruolo della piattaforma, luogo virtuale tramite il quale

l'utente in *deficit* può rivolgersi direttamente al pubblico al fine di ottenere la concessione di un finanziamento. Siamo ovviamente nel campo di una concessione di credito fondata su un'istruttoria effettuata su algoritmi e nel solco della disintermediazione creditizia. Parimenti nel solco della disintermediazione creditizia viene ricondotta l'attività delle piattaforme che prestano il servizio di *invoice trading*, che permette alle imprese di ottenere rapidamente liquidità a fronte della cessione, tramite la piattaforma, di crediti risultanti da fatture emesse nei confronti dei propri clienti. Sul versante complementare, le piattaforme di P2P lending comportano forme di intermediazione delle attività di raccolta di risparmio, che, seppure non integrano l'attività di raccolta riservata alle banche, comunque generano un fenomeno più o meno ampio di spiazzamento del mercato. A differenza di quanto accade per il P2P lending, l'attività di *equity crowdfunding* è stata oggetto di un precoce intervento da parte del legislatore italiano che, primo in Unione Europea, ha regolato il fenomeno con il d.l. n. 179/2012, convertito in legge n. 212/2012. Dalla complessiva esposizione, dall'evidenziazione delle questioni ancora aperte, dall'elaborazione di ipotesi di soluzione, emerge un panorama certo destinato ad ampliarsi ma tutt'altro che scevro da rischi.

L'illustrazione degli effetti della rivoluzione digitale si completa con il saggio di Lucantoni, dedicato all'impatto delle nuove tecnologie sul mondo della finanza: *trading on line*, *robo-advisor* ed *equity crowdfunding* i servizi oggetto di studio, sia per definirne i contorni, sia per verificarne le modalità di svolgimento (algoritmi e piattaforme ancora una volta in primo piano), sia per prefigurare l'evoluzione dei controlli. L'attenzione del regolatore deve concentrarsi su uno dei pericoli maggiori – e comuni a questi tre strumenti – consistente nella correttezza del codice con il quale la piattaforma è stata realizzata al fine di garantire gli utilizzatori contro errori improvvisi o pericolosi malfunzionamenti, affrontando il tema del tipo di controllo da svolgere (*ex post* o *ex ante*) e da chi debba essere svolto (dal regolatore o dal cliente). Escluso il cliente per l'evidente complessità e l'elevato tecnicismo di simili controlli e rinviando al saggio citato per specifiche ipotesi di soluzione, non v'è dubbio che lo scenario complessivo tracciato con il Fintech obbliga il *regulator* a ripensare gli strumenti tradizionali di tutela degli investitori e del mercato, poiché molti dei presidi oggi vigenti (fra cui quello della trasparenza) potrebbero presto rivelarsi inefficaci. Il progressivo venir meno del ruolo degli intermediari, sostituiti da piattaforme e algoritmi impone un cambiamento strutturale che, per semplificare, dovrebbe rendere possibile il controllo e la verifica (*ex post* o *ex ante* si vedrà) dell'algoritmo utilizzato dalle piattaforme.

Lo svolgersi della ricerca secondo le linee sopra riassunte ha dato evidenza a profili di rischio in parte tradizionali e in parte del tutto nuovi e diversi rispetto al passato, sicché è parso opportuno concludere il Quaderno con il saggio di Porzio e Sampagnaro, che illustra questi nuovi pericoli, ne delinea i contenuti, li alloca nella filiera dei prodotti e ne immagina le possibili salvaguardie. Un lavoro predittivo, specifico su fattispecie oggetto di studio nei precedenti saggi, che riesce a dare contenuto e visibilità a un processo irreversibile che però deve essere tempestivamente gestito: occorre infatti evitare di procedere senza una

corretta individuazione dei pericoli da affrontare e di gestire senza strumenti adatti le conseguenze negative di cambiamenti già in atto.

Dato conto del percorso e delle finalità della ricerca si ritengono utili ancora poche precisazioni.

1. La circolarità delle tematiche trattate ha comportato che degli stessi argomenti parlassero più autori con accenti, angolazioni, stili diversi. Poiché si ritiene che la pluralità delle voci sia un valore aggiunto per qualsiasi ricerca, i curatori hanno favorito la discussione fra gli autori, ma hanno scelto di non entrare nell'argomentare di ciascun contributo. Si sono limitati a inserire dei richiami di coordinamento in nota, per favorire il lettore che voglia meglio orientarsi sui singoli temi e sulle varie trattazioni degli stessi.

2. Il diritto dell'economia per pervenire a risultati soddisfacenti deve giovarsi di letture economiche e del contributo di esperti della scienza economica in senso lato. Nella ricerca si è tentato di perseguire questa via, sia scegliendo giuristi che avessero una propensione all'approfondimento dei dati economici, sia invitando a partecipare studiosi dell'economia. L'approccio interdisciplinare è la cifra per affrontare i temi di cui al presente Quaderno.

3. Il tema trattato e le sue implicazioni diversificate in vari aspetti, l'assenza, salva qualche rara eccezione, di precedenti contributi giuridici di vasto profilo e di ricostruzioni sistematiche, l'evoluzione continua di fatti e normative di vario livello, renderebbero segno di presunzione pensare di elaborare un lavoro definitivo. Si è inteso soltanto ricostruire nel modo più completo possibile i problemi giuridici rilevati; fornirne un'esauriente illustrazione; fare il punto sullo stato dell'arte riguardo a un tema sfuggente e di difficile approccio. Insomma, un lavoro sicuramente compiuto in sé, ma auspicabilmente destinato a fornire spunti per ulteriori approfondimenti, magari su argomenti specifici. Tuttavia, quando è stato possibile, non si è mancato di proporre soluzioni, indicare linee di indirizzo, caldeggiare e auspicare orientamenti: perché, nella logica della collana, si ritiene che il "*diritto vivente*" sia appannaggio non solo della giurisprudenza, ma anche della dottrina, quando essa si misura con la concretezza dell'agire giuridico.

4. L'individuazione dei temi da trattare e del percorso da seguire è stato il primo problema che i curatori si sono trovati ad affrontare. In quella sede, propedeutica ma decisiva per la realizzazione del lavoro, sono stati preziosi i suggerimenti e le indicazioni di Pierfrancesco Bartolomucci che qui cordialmente si ringrazia.

Fabrizio Maimeri Marco Mancini

Obiettivi e strumenti della PSD2

Fabio Porta

1. Introduzione – 2. Profili evolutivi dei sistemi e dei servizi di pagamento nei Paesi dell'Unione – 2.1 Criticità del progetto SEPA – 3. La Direttiva 2007/64/CE del Parlamento Europeo e del Consiglio del 13 novembre 2007 relativa ai servizi di pagamento nel mercato interno (PSD1) – 3.1 L'evoluzione del mercato dei servizi di pagamento sotto la vigenza della PSD1 e le lacune emerse verso la completa armonizzazione – 4. Il recepimento della PSD2 e la normativa attuativa della European Banking Authority (EBA): recenti novità nazionali ed europee – 5. Il procedimento di regolamentazione secondaria della Banca d'Italia – 5.1 Il Provvedimento di attuazione dell'articolo 2, comma 4-bis, d.lgs. n. 11/2010, concernente il nuovo regime di "operatività in esenzione" nell'ambito della disciplina dei servizi di pagamento – 5.2 La Comunicazione della Banca d'Italia del 24 gennaio 2019 relativa agli agenti che distribuiscono servizi di pagamento – 5.3 I documenti di consultazione predisposti dalla Banca d'Italia per recepire gli Orientamenti dell'EBA sulle misure di sicurezza per i rischi operativi e di sicurezza dei servizi di pagamento e in materia di segnalazione dei gravi incidenti – 5.4 Gli Orientamenti dell'EBA sulle condizioni per beneficiare dell'esenzione dal meccanismo di emergenza (c.d. "fall-back exemption") e la comunicazione della Banca d'Italia del 4 gennaio 2019 – 5.5 Le modifiche alle disposizioni in materia di "Trasparenza delle operazioni e dei servizi bancari e finanziari. Correttezza delle relazioni tra intermediari e clienti"

1. Introduzione

L'innovazione tecnologica offre soluzioni in grado di facilitare i pagamenti, agevola il superamento delle tradizionali resistenze al cambiamento per molte fasce della popolazione favorendo processi di inclusione finanziaria.

In Europa, in materia di servizi di pagamento, il *trend* di sostituzione del contante con strumenti innovativi ha registrato, negli ultimi anni, una rilevante accelerazione grazie al potenziamento delle infrastrutture di rete e all'avvento delle nuove tecnologie digitali applicate in campo finanziario (le cc.dd. *fintech*)[1]; ciò ha favorito l'evolversi di processi consolidati e l'offerta di nuovi servizi anche da parte di operatori non finanziari[2].

In questo contesto, caratterizzato dall'ampliamento dell'offerta di soluzioni digitali per i pagamenti e da modalità innovative per la generazione di valore all'interno della filiera delle transazioni elettroniche, i servizi di pagamento hanno trovato nel mercato dell'Unione una rinnovata regolamentazione ad opera della Direttiva 2015/2366/UE (PSD2) – che ha abrogato la precedente PSD1 (2007/64/CE) – entrata in vigore il 13 gennaio 2016 e recepita nel nostro ordinamento il 13 gennaio 2018 con la pubblicazione sulla Gazzetta Ufficiale del d.lgs. n. 218/2017.

La PSD2 amplia l'ambito di applicazione delle disposizioni in materia di servizi di pagamento (c.d. *positive scope*), modifica i requisiti di fondi propri imposti agli istituti di pagamento e di moneta elettronica, introduce nuovi servizi di pagamento, rafforza i presidi a fronte dei rischi operativi e di sicurezza delle transazioni. La Direttiva è implementata da regolamenti di esecuzione della Commissione europea – direttamente applicabili ai destinatari – e orientamenti dell'European Banking Authority (EBA)[3].

Il presente contributo intende fornire un inquadramento generale delle principali novità introdotte dalla PSD2 alla luce delle istanze emerse nel mercato dei servizi di pagamento a fronte dell'evoluzione normativa degli ultimi anni.

2. Profili evolutivi dei sistemi e dei servizi di pagamento nei Paesi dell'Unione

L'introduzione dell'euro ha determinato una radicale trasformazione dei sistemi di pagamento dei Paesi dell'Unione che hanno abbandonato le

---

[1] Con il termine inglese *FinTech* ci si riferisce alla *Financial Technology*, ossia all'offerta di servizi di finanziamento, di pagamento, di investimento e di consulenza ad alta intensità tecnologica, che comportano forti spinte innovative nel mercato dei servizi finanziari. Sul tema, cfr. European Central Bank and Banca d'Italia joint conference, *Digital transformation of the retail payments ecosystem*, Intervento del Governatore della Banca d'Italia Ignazio Visco, Roma, 30 novembre 2017.

[2] D. Girompini D. (2018), *PSD2 e Open Banking. Nuovi modelli di business e ruolo delle banche*, in *Bancaria*, 2018, fasc.1, p. 70.

[3] Per una disamina degli atti normativi di secondo livello emanati in attuazione della PSD2, cfr. http://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money.

valute nazionali; tale processo ha interessato, con modalità e tempi diversi, i *sistemi* che regolano le transazioni interbancarie e quelli concernenti i pagamenti disposti dalla clientela al dettaglio[4]. Con riferimento ai primi, le banche centrali dell'area dell'euro hanno realizzato un sistema di pagamento integrato per il regolamento delle operazioni di politica monetaria e delle transazioni interbancarie in euro (*Trans-European Automated Real-Time Gross Settlement Express Transfer* – "TARGET", "TARGET2"), grazie al quale, sotto il profilo monetario, si è avuto l'immediato allineamento dei tassi a breve dei prestiti interbancari e si è facilitata la conduzione di una politica unitaria più efficace. Diversamente, i sistemi di pagamento al dettaglio hanno continuato a operare su base nazionale, sicché il grado di segmentazione nell'offerta dei servizi di pagamento alla clientela è rimasto per molto tempo ancorato a quello preesistente all'introduzione dell'euro. Con l'intento di superare gli ostacoli all'integrazione dei mercati dei pagamenti dell'Eurosistema, a dicembre del 2001 la Commissione europea ha emanato un Regolamento[5] che, intervenendo sulle condizioni dell'offerta, ha imposto agli intermediari di uniformare la misura delle commissioni applicate, sia sui bonifici transfrontalieri al dettaglio in euro sia su quelli domestici. Nel contempo sono state create le basi per la definizione di un quadro giuridico unitario dei pagamenti in euro.

In tale contesto la Commissione e il Sistema europeo delle banche centrali (SEBC) hanno promosso il progetto *Single Euro Payments Area* (SEPA) volto a modificare la struttura del mercato dei pagamenti.

La SEPA ha ricondotto l'esecuzione e la ricezione dei pagamenti in euro a regole, procedure operative e prassi di mercato omogenee[6], agendo principalmente su due leve fortemente interconnesse: (i) definizione di schemi di pagamento utilizzabili in modo uniforme in tutta l'area ("*SEPA for instruments*"); (ii) adeguamento delle infrastrutture per la compensazione e il regolamento dei pagamenti con l'obiettivo di assicurare la *raggiungibilità* di tutte le potenziali controparti europee ("*SEPA for infrastructures*").

Nel 2002 l'industria bancaria europea ha promosso la creazione del Consiglio europeo per i pagamenti (*European Payments Council – EPC*),

---

[4] L'euro è stato adottato all'inizio del 1999 per le transazioni eseguite nei mercati monetari e finanziari e per il regolamento delle transazioni interbancarie; all'inizio del 2002 per l'esecuzione dei pagamenti al dettaglio e come valuta unica a corso legale.

[5] Regolamento (CE) n. 2560/2001 del Parlamento europeo e del Consiglio del 19 dicembre 2001 relativo ai pagamenti transfrontalieri in euro.

[6] Il progetto SEPA comprende i ventotto paesi dell'Unione e i tre paesi dello Spazio Economico Europeo (Islanda, Norvegia e Liechtenstein), oltre a Svizzera e Principato di Monaco. Il progetto ha inteso favorire lo sviluppo di strumenti elettronici flessibili – alternativi a quelli cartacei – integrabili con canali innovativi di vendita di beni e servizi (*mobile shops ed e-commerce*).

responsabile della realizzazione del progetto SEPA[7]. Negli anni successivi l'EPC ha definito gli standard per gli strumenti di pagamento armonizzati, segnatamente: il quadro di riferimento per i pagamenti con carte (*SEPA card framework*) e per le infrastrutture di regolamento; gli "schemi" per i bonifici (*SEPA credit transfer*) e gli addebiti diretti (*SEPA direct debit*)[8].

2.1 Criticità del progetto SEPA

L'adeguamento agli standard SEPA si è rivelato, tuttavia, insoddisfacente principalmente a causa di due fattori. In primo luogo, la fase cruciale del progetto SEPA è coincisa con l'intensificarsi della crisi finanziaria, per effetto della quale sono state ridotte le risorse da destinare agli investimenti di riconversione e innovazione delle linee di attività da parte degli operatori del settore; in secondo luogo, le preesistenti infrastrutture nazionali sono rimaste operative[9]. A ciò deve aggiungersi che la definizione di accordi e alleanze tra i soggetti operanti dal lato dell'offerta a livello europeo è risultata frenata dalla difficoltà di individuare sedi di dialogo rappresentative delle diverse esigenze, non limitate alla partecipazione degli operatori bancari, bensì estese ad attori della PSD, quali gli istituti di pagamento e i fornitori dei servizi tecnologici e di rete (tra i quali gli operatori delle telecomunicazioni), chiamati a svolgere un ruolo importante in un mercato ampio e tecnologicamente più avanzato[10].

Per dare ulteriore impulso alla migrazione verso i nuovi strumenti di pagamento armonizzati, nel 2009 la Commissione europea ha definito una

---

[7] Nel 2010 è stato costituito il *SEPA* Council, co-presieduto dalla Commissione europea e dalla Banca Centrale Europea, per favorire un assetto efficace di *governance* del progetto. Al SEPA Council hanno partecipato in misura paritetica rappresentanti della domanda (consumatori e imprese) e dell'offerta (banche e altri prestatori di servizi di pagamento). A fine 2013 l'Euro Retail Payments Board (ERPB), presieduto dalla BCE, ha sostituito il SEPA Council con un mandato più ampio e una partecipazione maggiormente articolata dei diversi *stakeholders*.

[8] Come opportunamente osservato: "*In an increasingly digital world, technology and consumer needs change rapidly. The European Payments Council regularly updates its schemes (Rulebook) in order to adapt and remain at the forefront of payments technology. The payment schemes are updated every two years to reflect market needs and evolutions in the technical standards developed by international standards bodies, such as the International Organization for Standardization. This evolution is guided through a transparent change-management process, open to all stakeholders*" (EPC -https://www.europeanpaymentscouncil.eu/what-we-do/sepa-payment-scheme-management/evolution-schemes).

[9] Alla fine del 2011 gli indicatori SEPA pubblicati periodicamente dall'Eurosistema hanno evidenziato un forte ritardo nella migrazione, limitata al venti per cento dei bonifici e a una percentuale irrilevante dei RID. Un miglioramento si è registrato, invece, per il passaggio delle carte munite di microchip, come previsto dal *SEPA card framework*.

[10] Per un'analisi delle ragioni di mercato che hanno ostacolato la realizzazione della SEPA, cfr. J. Bott, *The Single Euro Payments Area: New AlliancesRequired to Tip the Market*, in *ECRI Research Report*, n.10, July 2009.

roadmap della SEPA[11]. Le difficoltà di realizzazione del programma hanno tuttavia indotto la Commissione, di concerto con l'Eurosistema, a fissare un termine ultimo per la dismissione delle procedure nazionali (1° febbraio 2014 per i paesi dell'Area Euro e 31 ottobre 2016 per gli altri), affidando alle istituzioni la guida del progetto, originariamente appannaggio del mercato[12]; in relazione a tale ultimo aspetto è stato posto in capo agli Stati Membri l'onere di individuare le "autorità competenti" nazionali responsabili per la migrazione. In Italia tale ruolo è stato affidato alla Banca d'Italia[13].

3. La Direttiva 2007/64/CE del Parlamento Europeo e del Consiglio del 13 novembre 2007 relativa ai servizi di pagamento nel mercato interno (PSD1)

La realizzazione della SEPA è stata accompagnata dalla definizione di una cornice normativa che, nella comunanza di finalità, ha modificato la struttura dei pagamenti al dettaglio in Europa mediante l'approvazione della Direttiva 2007/64/CE sui servizi di pagamento nel mercato interno (*Payment Services Directive*).

La PSD ha definito un quadro giuridico comune per gli Stati Membri dell'Unione, vincolando i Paesi a modificare il proprio ordinamento per rendere

---

[11] Commission of the European Communities, Bruxelles, 10.9.2009, COM (2009) 471 final, p. 3, in cui si afferma: «*To make the Single Euro Payments Area (SEPA) a success, strong committment by all actors concerned is required.* (...) *WhileSEPA is primarily market driven, some uncertainty can only be resolved with the aid of the public authorities. Action is needed now by all stakeholders*» (https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0471:FIN:EN:PDF).

[12] Il "Regolamento (UE) N. 260/2012 del Parlamento Europeo e del Consiglio del 14 marzo 2012" (cd. Reg. end-date) ha stabilito i requisiti tecnici e commerciali per i bonifici e gli addebiti diretti in euro e modificato il regolamento (CE) n. 924/2009, fissando la data ultima per la migrazione ai SCT e SDD al 1° febbraio 2014 per i paesi dell'Area Euro, ovvero al 31 ottobre 2016 per i paesi non Area Euro; il provvedimento in parola ha conferito agli Stati membri il compito di individuare le "autorità competenti" nazionali responsabili per la migrazione. Con successivo Regolamento (UE) N. 248/2014 del Parlamento Europeo e del Consiglio del 26 febbraio 2014 – che ha modificato il regolamento UE n. 260/2012 per quanto riguarda la migrazione ai bonifici e agli addebiti diretti a livello di Unione – è stato previsto un periodo di transizione di sei mesi (fino al 1° agosto 2014), durante il quale i pagamenti in formato domestico potevano essere accettati senza l'applicazione di sanzioni, pur restando in vigore la data del 1° febbraio 2014 per il completamento della migrazione alla SEPA.

[13] Quale Autorità competente per la migrazione alla SEPA, la Banca d'Italia ha emanato un Provvedimento (recante istruzioni applicative del Regolamento n. 260/2012 del Parlamento europeo e del Consiglio) che compendia le indicazioni utili per la gestione della migrazione. La Banca d'Italia si è altresì impegnata in un'ampia azione divulgativa volta a favorire l'assimilazione delle novità da introdurre sia attraverso pubblicazioni, sia mediante incontri con tutte le parti interessate (prestatori di servizi di pagamento, infrastrutture, Pubblica Amministrazione, imprese e consumatori).

uniformi i servizi di pagamento e ampliare la gamma dei prestatori[14]. Essa ha condiviso con la SEPA gli obiettivi di favorire l'innovazione e la concorrenza nell'offerta dei servizi di pagamento, fissando regole armonizzate a livello europeo per l'esecuzione dei pagamenti più efficienti (bonifici, addebiti diretti, carte di pagamento) rispetto a quelli tradizionali cartacei (contante e assegni). La Direttiva ha introdotto una nuova categoria di operatori autorizzati (gli istituti di pagamento – IP) in concorrenza con le banche, ha ampliato le forme di tutela della clientela e ha precisato i diritti e gli obblighi delle parti nell'esecuzione di operazioni di pagamento[15].

Nel nostro ordinamento la Direttiva 2007/64/CE è stata recepita con il d.lgs. n. 11/2010 e la modifica del Testo Unico Bancario. Nel nuovo *corpus* normativo talune previsioni (diritti e obblighi delle parti) ricalcano integralmente la Direttiva; per altre (IP e tutela della clientela dei servizi di pagamento) si è optato per la soluzione basata sulla definizione di principi generali di fonte primaria rimandando alla regolamentazione secondaria della Banca d'Italia i contenuti di dettaglio[16].

---

[14] In relazione al primo aspetto, la Direttiva indica tempi certi e uniformi per il completamento dell'operazione di pagamento, accresce la trasparenza vietando forme di tariffazione implicita, rafforza la tutela dell'utente rendendo il medesimo maggiormente informato e consapevole del rapporto in essere con l'intermediario, accresce la responsabilità diretta del prestatore di servizi nei confronti del cliente. Con riguardo al secondo aspetto, la Direttiva introduce una nuova figura di intermediario finanziario specializzato nell'offerta di servizi di pagamento (l'istituto di pagamento), assoggettando il prestatore a un regime prudenziale specifico; agli istituti di pagamento viene consentita, altresì, l'offerta combinata di attività non finanziarie.

[15] Su tali profili, N. De Giorgi e M.I. Vangelisti, *La funzione di sorveglianza sul sistema dei pagamenti in Italia. Il provvedimento della Banca d'Italia del 18.9.2012 sui sistemi di pagamento al dettaglio,* Banca d'Italia, Quaderni di ricerca giuridica della consulenza legale, Banca d'Italia, n. 77, Roma, settembre 2014.

[16] Nel Testo Unico Bancario è stata disciplinata la riserva di attività dei servizi di pagamento in modo conforme alla normativa comunitaria; istituita la nuova categoria di intermediari vigilati (gli istituti di pagamento); attribuiti alla Banca d'Italia poteri di vigilanza regolamentare, informativa e ispettiva; regolate le procedure sanzionatorie e di gestione delle crisi. La disciplina è stata completata con l'adozione della normativa secondaria di competenza della Banca d'Italia che – in stretta aderenza con quanto richiesto dalla Direttiva – riproduce lo schema di regolamentazione e controlli vigente per gli altri intermediari soggetti a vigilanza prudenziale, nel rispetto del principio di proporzionalità. La possibilità, riconosciuta agli IP esercenti anche attività non finanziarie ("ibridi commerciali"), di concedere credito alla clientela con scadenza entro i dodici mesi e di detenere conti intestati ai clienti – sebbene in connessione alla prestazione di servizi di pagamento – ha rappresentato un elemento di forte innovazione per il sistema finanziario italiano, caratterizzato, fino ad allora, da una riserva in favore di banche e di intermediari finanziari per l'attività di erogazione del credito e da una riserva in favore di banche ed IMEL per la detenzione di conti della clientela. Gli IP operano direttamente nei confronti del pubblico e possono, ove autorizzati alla prestazione dello specifico servizio: emettere strumenti di pagamento, tra i quali le carte di credito, anche con modalità *revolving*; detenere conti intestati ai clienti ("conti di pagamento"), sui quali i medesimi possono, tra l'altro, disporre operazioni di conferimento e prelevamento di somme, bonifici o addebiti diretti; erogare credito con durata non superiore ai dodici mesi, a condizione che sia strumentale alla prestazione di servizi di pagamento; effettuare servizi di trasferimento fondi e di rimesse di denaro. A differenza di quanto previsto per la generalità degli intermediari vigilati, gli IP possono esercitare anche attività non finanziarie, non essendo per essi previsto l'obbligo di esclusività dell'oggetto sociale ma solo quello di costituire un apposito patrimonio destinato per la prestazione dei servizi di pagamento.

Al regime di vigilanza prudenziale della Banca d'Italia è stata affiancata la funzione di sorveglianza sul sistema dei pagamenti prevista dall'art. 146 t.u.b., con riguardo al regolare funzionamento, all'affidabilità e all'efficienza del sistema medesimo e alla tutela degli utenti di servizi di pagamento. Nel t.u.b. sono state, altresì, rafforzate le norme a tutela dell'utente dei servizi di pagamento, volte ad assicurare la trasparenza delle condizioni contrattuali e a prevedere obblighi informativi lungo tutto l'arco dello svolgimento del rapporto (fase precontrattuale, stipula del contratto, fase successiva al ricevimento o all'esecuzione dell'ordine di pagamento). In attuazione di tali disposizioni, la Banca d'Italia ha adottato norme secondarie che hanno integrato gli obblighi informativi sui servizi di pagamento con quelli relativi ai rimanenti prodotti disciplinati dal t.u.b., in modo da preservare l'omogeneità e la coerenza del quadro normativo in materia di trasparenza.

Per gli intermediari finanziari operanti nei servizi di pagamento al momento della riforma, la prosecuzione dell'attività è stata condizionata alla previa trasformazione in IP e alla conseguente iscrizione nel relativo albo.

3.1 L'evoluzione del mercato dei servizi di pagamento sotto la vigenza della PSD1 e le lacune emerse verso la completa armonizzazione

La Direttiva 2007/64/CE ha dato impulso irreversibile a una più accentuata dinamica concorrenziale nel comparto dei servizi di pagamento *retail* in Europa, aperto anche agli intermediari non bancari (quali gli Istituti di Pagamento e gli Istituti di Moneta Elettronica); in relazione a questi ultimi, considerata la loro limitata operatività, sono stati previsti requisiti meno stringenti rispetto alle banche. Il dinamismo del mercato è stato sospinto anche dalla massiccia diffusione di dispositivi ad alto contenuto tecnologico, quali *smartphones* e *tablets*, che hanno consentito l'accesso digitale a un numero sempre maggiore di funzioni[17].

L'incalzare della tecnologia e i rapidi cambiamenti del mercato hanno rappresentato, per altro verso, elementi ostativi alla completa armonizzazione del sistema. All'interno dei confini nazionali si sono rivelate frammentate aree importanti, riguardanti i pagamenti effettuati con carte di credito, carte di debito, nuovi mezzi di pagamento che utilizzano la rete Internet e i menzionati

---

[17] Sulla materia, cfr. Camera dei Deputati, VI Commissione (Finanze), Indagine conoscitiva sulle tematiche relative all'impatto della tecnologia finanziaria sul settore finanziario, creditizio e assicurativo, Audizione del Vice Direttore Generale della Banca d'Italia Fabio Panetta (Roma, 29 novembre 2017), pp. 7 e 8; v. G. D'Agostino e P. Munafò, *Prefazione alla collana dedicata al FinTech*, CONSOB, *Quaderni Fintech*, n. 1, marzo 2018. In proposito, non si è mancato di osservare che "*The emergence of mobile telephony, the ubiquity of the internet, availability of high-speed computing, advances in cryptography, and innovations in machine learning could all combine to enable rapid changes in finance – just as they are in other areas of the economy*": M. Carney, *The Promise of FinTech – Something New Under the Sun ?*, *Speech given by Governor of the Bank of England, Chair of the Financial Stability Board, Deutsche Bundesbank G20 conference on* "*Digitising finance, financial inclusion and financial literacy*", Wiesbaden, Germania, 25.1.2017, p. 3.

dispositivi mobili. Alcune criticità connesse con la pratica implementazione della PSD sono derivate dalla difficoltà di far convergere verso soluzioni comuni strutture ordinamentali e procedurali fortemente differenziate tra i Paesi dell'Unione[18]. Inoltre, taluni servizi nel settore delle "IT" emersi nella prassi operativa, successivamente all'adozione della PSD1, sono risultati privi di specifica regolamentazione; in alcuni Stati membri ciò ha suscitato preoccupazioni in tema di sicurezza, protezione dei dati e responsabilità, pur considerando i potenziali benefici generati da tali servizi e prestatori.

L'insieme di questi fattori ha condotto nel 2015 a una rivisitazione sostanziale del quadro normativo europeo in materia di pagamenti mediante l'introduzione di due provvedimenti: la (nuova) Direttiva UE n. 2015/2366 sui servizi di pagamento nel mercato interno (altrimenti nota come PSD2, entrata in vigore a gennaio del 2016, da recepire negli Stati membri entro il 13 gennaio 2018)[19] e il *Regolamento* sulle carte di pagamento (Regolamento UE n. 2015/751 – *Interchange Fee Regulation* – entrato in vigore a giugno 2015)[20].

---

[18] Nel nostro Paese, l'esperienza applicativa maturata nei due anni successivi al recepimento della PSD ha sollecitato un intervento legislativo – sotto forma di "correttivo" al decreto legislativo n. 11/2010, ad opera del d.lgs. 14 dicembre 2010, n. 218 – per apportare talune modifiche e integrazioni alla disciplina. I fattori alla base di detto intervento sono principalmente ascrivibili all'evoluzione del quadro normativo applicabile a soggetti regolamentati (gli intermediari finanziari), molto vicini per operatività e dimensioni agli istituti di pagamento, all'emersione di problematiche applicative che hanno richiesto una soluzione normativa *ad hoc* nonché alla necessità di migliorare la formulazione di alcune disposizioni che hanno sollevato dubbi interpretativi.

[19] Per un'analisi dei lavori preparatori che hanno condotto all'emanazione della PSD2, cfr.: Commissione Europea, *Proposta di direttiva del Parlamento Europeo e del Consiglio, relativa ai servizi di pagamento nel mercato interno, Bruxelles, 24.7.2013*, COM(2013) 547 final 2013/0264 (COD), p. 13.; *Commission Staff WorkingDocument. Impact Assessment*, documento di accompagnamento alla proposta della futura PSD2, Brussels, 24.7.2013, SWD(2013) 288 final, volume 2/2, p. 137; Direttiva 2014/65/UE del Parlamento europeo e del Consiglio del 15 maggio 2014 relativa ai mercati degli strumenti finanziari e che modifica la Direttiva 2002/92/CE e la Direttiva 2011/61/UE.

[20] Rispetto a entrambi i provvedimenti, il ruolo di autorità competente per la definizione della regolamentazione secondaria (linee guida e standard tecnici regolamentari) è stato affidato alla European Banking Authority (EBA). La PSD2 rappresenta solo l'ultimo di una serie di interventi di derivazione comunitaria in tema di servizi di pagamento; in proposito si richiamano: Regolamento (CE) n. 1781/2006, che dispone che i prestatori di servizi di pagamento comunichino i dati informativi relativi all'ordinante lungo tutta la catena di pagamento, al fine di prevenire, investigare e individuare i casi di riciclaggio di denaro e di finanziamento al terrorismo; Direttiva 2007/64/CE (PSD1), che istituisce un quadro giuridico armonizzato per pagamenti più rapidi e semplici in tutta l'Unione Europea, creando maggiore concorrenza nei sistemi di pagamento, favorendo le economie di scala e rendendo più agevole l'attuazione della *Single Euro Payments Area(SEPA)*; Regolamento (CE) n. 924/2009 relativo ai pagamenti transfrontalieri, applicato a tutti i pagamenti elaborati elettronicamente e finalizzato ad eliminare le differenze nelle commissioni applicate agli utenti di servizi di pagamento per i pagamenti nazionali e transfrontalieri in euro all'interno del territorio UE; Direttiva 2009/110/CE sulla moneta elettronica, che istituisce il quadro giuridico per l'emissione e il rimborso di moneta elettronica e allinea il regime prudenziale per gli istituti di moneta elettronica ai requisiti applicabili agli istituti di pagamento; Regolamento UE n. 260/2012, che stabilisce termini per la migrazione dei bonifici e addebiti diretti paneuropei e sostituisce i programmi nazionali per i pagamenti domestici e transfrontalieri in euro all'interno dell'UE.

La Direttiva n. 2015/2366 amplia il campo di applicazione del *corpus* di norme giuridiche armonizzate sui servizi di pagamento precedentemente definito dalla PSD1. In particolare, riconduce nella speciale cornice giuridica UE della materia specifici ambiti operativi che, sebbene in parte affini o comunque connessi ad attività già regolamentate ai sensi della PSD1, erano rimasti esclusi dall'elenco dei "servizi di pagamento" oggetto di riserva a favore di soggetti autorizzati e, per tale motivo, estranei alla relativa disciplina e vigilanza di settore[21].

La nuova disciplina ridefinisce l'assetto regolamentare dei servizi di pagamento nel mercato interno dell'UE, con il preminente obiettivo di facilitare l'innovazione, la competizione, l'efficienza e la sicurezza delle transazioni. L'impatto dell'intervento interessa l'intero settore dei servizi finanziari, intesi in senso ampio, ivi inclusi quelli bancari e assicurativi.

Tra i principali obiettivi del complessivo intervento vi è quello di consentire agli utenti di servizi di pagamento nel mercato interno dell'UE di beneficiare di un paniere più ampio di servizi maggiormente efficienti, garantendo elevati standard di sicurezza per l'utilizzo di dispositivi elettronici, piattaforme e canali di comunicazione a distanza[22].

Particolare importanza assumono le disposizioni che disciplinano l'accesso aperto e condiviso ai conti di pagamento per la fruizione e la prestazione di servizi di pagamento innovativi "*Internet based*"[23]. L'ottica è tutelare gli utenti e per tale via garantire il regolare e affidabile funzionamento del sistema dei pagamenti nel suo complesso[24].

---

[21] La PSD2 ridefinisce l'elenco delle "attività commerciali" che nel mercato interno dell'UE costituiscono "servizi di pagamento" oggetto di riserva, stabilendo un innovativo *framework* giuridico armonizzato per lo sviluppo, tra l'altro, di uno o più mercati di nuovi servizi connessi a conti di pagamento, ovvero basati sui medesimi. Rispetto al corrispondente "allegato" della PSD1, quello aggiornato di cui alla PSD2 annovera i servizi di "disposizione di ordine di pagamento" e di "informazione sui conti" (cfr. nn. 7 e 8 dell'Allegato I della PSD2). Nel medesimo elenco non compare, invece, il servizio di cui al n. 7 dell'allegato della PSD1 concernente l'"*esecuzione di operazioni di pagamento ove il consenso del pagatore ad eseguire l'operazione di pagamento sia dato mediante un dispositivo di telecomunicazione, digitale o informatico e il pagamento sia effettuato all'operatore del sistema o della rete di telecomunicazioni o digitale o informatica che agisce esclusivamente come intermediario tra l'utente di servizi di pagamento e il fornitore di beni e servizi*".

[22] Commissione Europea (2017), *Payment Services Directive (PSD2): Regulatory Technical Standards (RTS) enabling consumers to benefit from safer and more innovative electronic payments*, Brussels, 27 November.

[23] Sulla rilevanza centrale del "conto di pagamento" nel quadro normativo della PSD2, va sottolineato che già in sede di recepimento della disciplina domestica della PSD1 era stato segnalato come le innovazioni normative introdotte dal d.lgs. 11/2010 ruotassero "*in larga misura sulla previsione del "conto di pagamento" e sul considerare fra i servizi di pagamento tutte le operazioni di gestione dello stesso, oltre all'acquisizione di strumenti di pagamento e all'esecuzione di pagamenti attraverso dispositivi di comunicazione*", P. Marullo Reedtz, *Commento sub art 1, comma 1, lett. b), l) e n)* d.lgs. 11/2010, in Aa.Vv., *La nuova disciplina dei servizi di pagamento*, a cura di M. Mancini, M. Rispoli Farina, V. Santoro, A. Sciarrone Alibrandi, O. Troiano, Torino, 2011, p. 9.

[24] Considerando (95), PSD2.

In materia di sicurezza, la PSD2 stabilisce regole di principio, affidando alla European Banking Authority (EBA) il compito di definire la normativa di dettaglio. Il processo di normazione dell'EBA in questo campo ha previsto quattro distinti interventi da completarsi entro gennaio 2018: i *Regulatory Technical Standards* (RTS) in tema di autenticazione forte e comunicazione sicura; le *Guidelines* in tema di *reporting* degli incidenti gravi di sicurezza; le *Guidelines* sui rischi operativi e di sicurezza dei PSP; le *Guidelines* in tema di reporting delle frodi[25].

La revisione della PSD risponde, dunque, alle fondamentali esigenze di: risolvere alcuni problemi legati alla scarsa armonizzazione con cui diverse disposizioni sono state recepite a livello domestico, contribuendo a fenomeni di arbitraggio regolamentare e incertezza giuridica; rafforzare la cooperazione tra le diverse autorità nazionali coinvolte nella supervisione di istituti di pagamento (IP) operanti a livello transnazionale, con l'obiettivo di assicurare condizioni di parità concorrenziale agli operatori e maggiori tutele agli utenti in tutta l'Unione; sostenere lo sviluppo del commercio elettronico, regolamentando i nuovi servizi che si vanno diffondendo per agevolare i pagamenti su Internet (servizi di iniziazione del pagamento e di aggregazione delle informazioni sui conti)[26] e irrobustendo le disposizioni in materia di sicurezza.

Dal punto di vista dei contenuti, la PSD2 introduce novità significative, fra cui: una più dettagliata lista di esenzioni per delimitarne l'applicazione ed evitare abusi; la possibilità di derogare all'impianto di regole previste per l'offerta di servizi di pagamento, a fronte di operazioni con un profilo di rischio limitato. La disciplina statuisce, altresì, un criterio quantitativo per escludere dal perimetro applicativo servizi relativi all'acquisto di beni digitali o biglietti elettronici tramite credito telefonico, di importo contenuto nel limite di euro 50,00 per transazione e per un valore mensile complessivo non superiore a euro 300,00.

L'ambito di applicazione della direttiva – e delle relative tutele a favore degli utenti dei servizi di pagamento – viene esteso a operazioni in valute *extra* UE, ovvero a transazioni nelle quali uno dei prestatori di servizi di pagamento sia insediato all'estero (previsione, peraltro, già introdotta nel nostro ordinamento in occasione del recepimento della PSD1).

---

[25] I mandati PSD2 conferiti all'EBA in tema di sicurezza e frodi sono i seguenti: *RTS on strong customer authentication and secure communication* (art. 98, PSD2 – Commission Delegated Regulation (EU) 2018/389), pubblicati a marzo 2018 (applicazione 14 settembre 2019); *Guidelines on fraud data reporting* (art. 96), pubblicate a luglio 2018; *Guidelines on major incident reporting* (art. 96), pubblicate a luglio 2017; *Guidelines on operational and security risk management* (art. 95), pubblicate a dicembre 2017.

[26] Il servizio di iniziazione del pagamento (*Payment Initiation*) consente di disporre ordini di pagamento nell'ambito di transazioni di *e-commerce*, mediante reindirizzamento del pagatore sul proprio conto di *internet banking*, effettuato da un *provider* diverso dalla banca che gestisce il conto; il servizio di informazioni sul conto (*Account Information*) aggrega le informazioni relative a più conti detenuti dallo stesso cliente ed è anch'esso fornito da un soggetto diverso rispetto all'intermediario presso il quale è detenuto il conto del cliente.

Sono ampliati i poteri delle Autorità dello Stato membro ospitante nei casi di prestazione di servizi di pagamento su base transfrontaliera, in particolare quando un IP operi tramite agenti in uno Stato membro diverso da quello in cui è registrato[27].

Sotto il profilo soggettivo, la PSD2 riconosce il ruolo dei nuovi operatori del settore (*Third Party Services Providers* - TPP) nel fornire soluzioni altamente innovative, basate sull'accesso ai conti della clientela[28], specializzati nella prestazione – previa autorizzazione o registrazione, a seconda dei casi – di nuovi servizi di pagamento, sottoposti alla disciplina e alla vigilanza di settore. In seno ai TPP la direttiva distingue due sottocategorie di prestatori (PSP), a seconda dei servizi erogati di "*disposizione di ordine di pagam*ento" (*Payment Initiation Services Providers* – Pisp – di cui all'art. 4, punto 19, PSD2)[29], ovvero di "*informazione sui conti*" (*Account Information Service Providers* – Aisp – di cui all'art. 4, punto 17, PSD2)[30].

I servizi erogati dai Pisp postulano il necessario collegamento a *conti di pagamento* detenuti presso Pisp diversi da quelli che forniscono i servizi in parola; ciò spiega, verosimilmente, il motivo per cui il legislatore europeo abbia incluso la figura del Pisp "*di radicamento del conto*", quale soggetto che "fornisce" o "amministra" un conto di pagamento per un pagatore (art. 4, punto 18). Diversamente, il servizio di *informazione sui conti*, materialmente non investe atti configurabili come realizzatori o attivatori di trasferimenti, prelievi, ritiri di fondi o altre operazioni attinenti a pagamenti. Sicché, nella specie, l'attrazione delle regole di statuto speciale riferibili a detta operatività trovano collocazione nell'ambito della disciplina dei servizi di pagamento, per la sola circostanza che le informazioni cui il servizio accede sono contenute nei conti di pagamento accessibili on line.

Per l'offerta dei nuovi servizi di iniziazione di ordini di pagamento e di informazioni sui conti di pagamento, vengono definite le procedure di autorizzazione e registrazione nonché i requisiti e il regime di responsabilità. Pur trattandosi di servizi ancora poco diffusi in alcuni paesi, come l'Italia, l'intervento del legislatore crea le condizioni per una maggiore concorrenza nel

---

[27] In particolare, vi è la possibilità di richiedere un intervento della European Banking Authority (EBA) per contrasti con l'autorità dello Stato membro di origine nonché di ottenere informazioni direttamente dall'IP e di adottare misure di carattere precauzionale in caso di seria minaccia agli interessi degli utenti. È inoltre possibile costituire un punto di contatto centrale nel caso in cui l'IP si avvalga di più agenti per facilitare i controlli su reti tipicamente composte da un elevato numero di piccoli operatori.

[28] cfr. P. Valcke, N. Vandezande, N. Van deVelde, *The evolution of third party payment providers and cryptocurrencies under the EU's upcoming PSD2 and AMLD4*, in *Swift institute working paperno. 2015-001*, 2015, p. 45 ss., i quali pure evidenziano come ciò rappresenti uno dei "*key developments since the adoption of the original Payment Services Directive*" (p. 15).

[29] Rientrano in tale categoria di TPP quei PSPs che prestano un servizio che consiste essenzialmente nel disporre, su richiesta e per conto di un utente del servizio stesso, un "ordine di pagamento" relativamente a un "conto di pagamento" detenuto però dal cliente di tale servizio presso un altro PSP che "fornisce" e "amministra" il conto di pagamento in questione.

[30] Sul tema cfr. il contributo di V. Profeta in questo *Quaderno*.

settore dei pagamenti per l'*e-commerce*, ad oggi in prevalenza basati sull'utilizzo delle carte.

Con l'obiettivo di rafforzare le tutele e la fiducia degli utenti nei servizi di pagamento digitali, la PSD2 introduce requisiti di sicurezza a più livelli[31]: regole stringenti per l'autenticazione delle transazioni; requisiti per la gestione dei rischi di sicurezza dei PSPs da valutare in fase di autorizzazione e nell'operatività corrente; requisiti specifici per la comunicazione sicura tra gli operatori, inclusi i nuovi prestatori di servizi di accesso ai conti; obblighi di segnalazione degli incidenti e di condivisione delle informazioni tra le autorità[32].

Il *Regolamento* sulle carte (IFR) – in linea con le *policy* della PSD2 – mira ad armonizzare le regole sui pagamenti con carta nell'Unione, aumentare la trasparenza, consentire una maggiore scelta all'utente a costi più contenuti. In relazione a tale ultimo aspetto, il provvedimento fissa limiti massimi – cogenti dal 9 dicembre 2015 – per le commissioni interbancarie pagate dalla banca dell'esercente a favore dell'emittente della carta nelle seguenti misure: 0,3% del

---

[31] Numerose disposizioni sono state introdotte con l'obiettivo di rafforzare la sicurezza dei pagamenti elettronici a fronte del crescente sviluppo delle transazioni *online*. In particolare: l'obbligo di autenticazione forte del cliente e delle transazioni per le operazioni via Internet; l'adozione di misure di sicurezza adeguate per tutelare la riservatezza e l'integrità delle credenziali di sicurezza personalizzate degli utenti; l'utilizzo di standard aperti per la comunicazione sicura tra prestatori di servizi di pagamento; gli obblighi di *reporting* all'Autorità competente dei gravi incidenti di sicurezza.

[32] Con l'introduzione della PSD2 il legislatore europeo ha riconosciuto e disciplinato modelli di servizio di tipo "Fintech" basati sull'accesso di terze parti ai conti della clientela. Questo nuovo sviluppo, che apre la disponibilità degli archivi aziendali a un novero potenzialmente ampio di operatori, non può non suscitare preoccupazioni in ordine ai rischi per la sicurezza connessi con l'utilizzo delle credenziali di accesso ai conti bancari. Per gestire tali rischi, come innanzi illustrato, la direttiva definisce un ampio set di requisiti, applicabili a tutti gli attori del nuovo ecosistema e articolato su quattro pilastri: l'autenticazione forte della clientela, la gestione del rischio IT a livello aziendale, il reporting obbligatorio degli incidenti, la comunicazione sicura tra gli operatori sfruttando tecnologie tipiche del mondo internet come le Application Programming Interfaces (API). In particolare, il rafforzamento dei presidi di sicurezza passa attraverso l'intervento di soggetti terzi, tra cui i gestori delle "applicazioni" informatiche - presenti sui dispositivi mobili (laptops, Smartphones, tablets) - utilizzate dai fruitori dei servizi di pagamento per l'esecuzione delle transazioni on line. Appare pertanto lecito interrogarsi sulla reale tenuta del sistema di sicurezza delineato dalla PSD2 e sulla capacità dello stesso di realizzare in pieno gli obiettivi perseguiti dalla normativa – primo fra tutti il rafforzamento delle tutele e della fiducia degli utenti nei servizi di pagamento digitali – che potrebbero essere vulnerati dal coinvolgimento di soggetti terzi, non necessariamente tenuti a standard tecnici specifici; lacune in tale ambito potrebbero infatti minare la tenuta del sistema e ricadere sugli intermediari, non in grado di intervenire sul livello di sicurezza adottato dagli operatori in parola. L'affidabilità dei singoli operatori costituisce infatti una precondizione per la resilienza del circuito dei pagamenti interbancari, per il quale essi fungono da punti di accesso (c.d. *endpoints*) ma di cui possono rappresentare un punto di debolezza in grado, nei casi estremi, di compromettere la fiducia nell'integrità dell'intero sistema fino a incepparne il funzionamento (in argomento, cfr. ITASEC19, Terza Conferenza Italiana sulla Cyber Security, *Sicurezza, privacy, normative: come farli coesistere in ambito Fintech?*, Intervento del Capo del Dipartimento Mercati e sistemi di pagamento della Banca d'Italia, Paolo Marullo Reedtz, Pisa, 14 febbraio 2019).

valore della transazione per le carte di credito; 0,2% del valore della transazione per le carte di debito e prepagate[33].

4. Il recepimento della PSD2 e la normativa attuativa della European Banking Authority (EBA): recenti novità nazionali ed europee

A far data dal 13 gennaio 2018 la PSD1 è stata abrogata e i riferimenti alla stessa devono intendersi di diritto relativi alla nuova direttiva (art. 114, PSD2). Dalla medesima data gli Stati Membri applicano le misure nazionali necessarie per conformarsi alla nuova normativa (art. 115, PSD2). In deroga a tale termine generale è stata fissata una scadenza differita per l'applicazione delle disposizioni sulle novellate "misure di sicurezza", che prescrivono ai "Prestatori di Servizi di Pagamento" (PSPs) l'utilizzo di meccanismi di c.d. "autenticazione forte del cliente" (*Strong CustomerAuthentication* – SCA) e di "standard aperti di comunicazione comuni e sicuri" (*Common and Secure Open Standards of Communication* – CSC)[34] nell'ambito delle comunicazioni telematiche – sia tra intermediari sia tra intermediari e clienti – relative alla esecuzione di diversi servizi e operazioni[35].

Nello specifico, gli Stati Membri sono tenuti all'applicazione delle citate "misure di sicurezza" decorsi diciotto mesi dall'entrata in vigore delle "Norme Tecniche di Regolamentazione" (c.d. *Regulatory Technical Standards*) previste ai sensi dell'art. 98 della PSD2, da adottarsi altresì da parte della Commissione Europea mediante regolamento delegato, conformemente agli artt. 10-14 del Regolamento (UE) n. 1093/2010 (cfr. art. 115, par. 4, PSD2). In tal guisa, oltre

---

[33] Il Regolamento sulle carte contiene ulteriori previsioni che hanno l'obiettivo di aumentare la trasparenza e le possibilità di scelta degli utenti tra le diverse tipologie di strumenti e servizi. Le principali novità (in vigore da giugno del 2016) riguardano: l'obbligo di separatezza contabile, organizzativa e decisionale tra le funzioni di gestione dei circuiti e l'infrastruttura che ne elabora le transazioni (*processing*) per ridurre i fenomeni di tariffazione aggregata dei servizi, aumentare la trasparenza delle tariffe applicate e accrescere la competizione nel mercato dei servizi di *processing* delle carte; la rimozione delle restrizioni territoriali al regime di emissione delle carte e convenzionamento degli esercenti; la trasparenza dei contratti e la limitazione delle condizioni "a pacchetto" per gli esercenti; le limitazioni alle regole di circuito che obbligano gli esercenti ad accettare tutte le carte; l'ampliamento delle possibilità di adottare soluzioni che permettano di selezionare i prodotti più efficienti sia per l'esercente sia per l'utente.

[34] La definizione delle "misure di sicurezza" e di un quadro giuridico chiaro e armonizzato al riguardo ha un rilievo preminente nell'ottica di sviluppo di un mercato sicuro, ordinato, efficiente, tecnologicamente neutro e concorrenziale della prestazione di innovativi servizi digitali e a distanza, non solo strettamente di pagamento, bensì finanziari in senso ampio, dove il ruolo dei PSPs potrebbe evolvere anche in quello di "piattaforma" per l'offerta di ulteriori e diversi prodotti e servizi finanziari da parte delle imprese a ciò autorizzate; in questo senso, cfr. D. Girompini, *PSD2 e Open Banking*, op. cit., p. 70.

[35] Si tratta dei servizi e delle operazioni di cui agli artt. 65, 66, 67 e 97 della PSD2: a) «conferma della disponibilità di fondi» sul conto di pagamento del pagatore per l'esecuzione di una operazione di pagamento basata su carta (c.d. *confirmation on availability of funds o fund checking*); b) "disposizione di ordine di pagamento" (*payment initiation*); c) "informazione sui conti" (*account information*); d) "autenticazione forte del cliente" (o SCA) laddove il pagatore effettui determinate operazioni (ossia quando: accede al suo conto di pagamento *online*; dispone un'operazione di pagamento elettronico; opera tramite un canale a distanza che può comportare un rischio di frode nei pagamenti o altri abusi).

a consentire di pervenire ad un elevato grado di standardizzazione a livello UE su aspetti che influenzano la struttura e le dinamiche di funzionamento di diversi mercati rilevanti, si è dato modo agli operatori di organizzarsi per essere *compliant* con tali nuovi standard armonizzati.

Il Regolamento delegato, adottato dalla Commissione Europea il 27 novembre 2017, reca le norme in materia di autenticazione forte del cliente e di standard aperti di comunicazione comuni e sicuri, applicabili dal 14 settembre 2019, ad eccezione dei par. 3 e 5 dell'art. 30, concernente taluni obblighi in materia di "interfacce di accesso" a sistemi informatici, cogenti dal 14 marzo 2019.

Orbene, a livello nazionale, il 13 gennaio 2018 è entrato in vigore il decreto legislativo 15 dicembre 2017 n. 218, con il quale è stata recepita nel nostro ordinamento la seconda Direttiva sui servizi di pagamento (UE n. 2015/2366)[36] e data attuazione ad alcune disposizioni del Regolamento (UE) n. 2015/751, relativo alle commissioni interbancarie sulle operazioni di pagamento basate su carta (IFR).

In ordine alle disposizioni di dettaglio, la Banca d'Italia ha avviato i lavori preparatori della disciplina di propria competenza curando, *inter alia*, l'aggiornamento delle disposizioni di vigilanza che riguardano i prestatori di servizi di pagamento (PSP) e di quelle in materia di trasparenza delle condizioni contrattuali e correttezza delle relazioni tra intermediari e clienti.

Rientra nella competenza della Banca d'Italia la definizione degli aspetti procedurali per l'autorizzazione dei prestatori e l'esercizio delle attività di controllo anche nei confronti dei *Third Party Providers*, categoria che, come innanzi evidenziato, ascrive i prestatori di servizi di disposizione di ordine di pagamento (PIS) e di informazione sui conti (AIS).

In parallelo con il recepimento a livello nazionale, il percorso di attuazione della PSD2 è proseguito in Europa con la finalizzazione delle linee guida e degli standard regolamentari affidata all'European Banking Authority (EBA). In particolare, la Direttiva ha conferito all'EBA il compito di sviluppare "*Regulatory Technical Standard*" (RTS) e "*Guidelines*" (GL) riguardanti principalmente tre ambiti: coordinamento tra le autorità competenti *home* e *host*; armonizzazione dei processi di autorizzazione degli istituti di pagamento; sicurezza dei pagamenti. Sotto quest'ultimo aspetto, il pacchetto normativo si compone di: i) RTS in tema di autenticazione forte e comunicazione sicura, la cui versione definitiva è stata pubblicata a marzo 2018 e troverà applicazione a far data dal 14 settembre 2019[37]; ii) *Guidelines* in tema di *reporting* degli incidenti gravi di sicurezza e *Guidelines*

---

[36] Le disposizioni europee sono state recepite attraverso il decreto legislativo 15 dicembre 2017 n. 218, il quale ha apportato le opportune modifiche al d.lgs. 1 settembre 1993 n. 385 (t.u.b.) e al d.lgs. 27 gennaio 2010, n. 11.

[37] Regolamento delegato (UE) 2018/389 della Commissione del 27 novembre 2017, che integra la direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione per l'autenticazione forte del cliente e gli standard aperti di comunicazione comuni e sicuri. Ai sensi dell'art. 38 il regolamento è entrato in vigore il giorno successivo a quello di pubblicazione nella Gazzetta ufficiale dell'Unione europea, avvenuta il 13 marzo 2018.

sui rischi operativi e di sicurezza dei PSP, pubblicate a inizio 2018; iii) *Guidelines* in tema di *reporting* delle frodi, sottoposte a consultazione pubblica nel corso del 2017 e pubblicate a luglio 2018[38].

Dal 13 gennaio 2018 la Direttiva PSD2 relativa ai servizi di pagamento nel mercato interno si applica negli Stati membri dell'Unione Europea; sicché i nuovi "servizi di pagamento", al pari di quelli tradizionalmente noti, a far tempo dalla predetta data di recepimento soggiacciono alla normativa di settore.

Alcune disposizioni tecniche, dettate dagli RTS, saranno cogenti dal 14 settembre 2019[39]. Tuttavia, a far data dal 14 marzo 2019, ai prestatori di servizi di pagamento è stato richiesto di approntare alcune delle misure tecniche ed informatiche funzionali all'erogazione dei servizi in questione, informandone le Autorità di Vigilanza.

Al fine di dare attuazione al nuovo quadro normativo, la Banca d'Italia ha posto in pubblica consultazione specifici provvedimenti, successivamente adottati ovvero in corso di emanazione.

---

[38] In tema di sicurezza il settore finanziario è interessato, altresì, dall'entrata in vigore di due provvedimenti di più ampio respiro: Regolamento UE 2016/679 sul trattamento dei dati personali (*General Data Protection Regulation* – GDPR), cogente da maggio 2018; Direttiva UE 2016/1148 sulla sicurezza delle reti e dei sistemi informativi (Direttiva NIS – *Network e Information Security*), recepita a livello nazionale a maggio 2018. In entrambi i casi sono previsti obblighi di segnalazione di incidenti informatici e specifici requisiti di sicurezza, verosimilmente estesi anche a operatori bancari e finanziari in quanto gestori di dati ai sensi della GDPR o operatori di servizi essenziali ai sensi della Direttiva NIS.

[39] La seconda direttiva sui servizi di pagamento (PSD2) e la connessa normativa attuativa fissano al 14 settembre 2019 la scadenza per l'adozione obbligatoria, da parte delle banche e degli altri prestatori di servizi di pagamento, di sistemi di autenticazione forte dei clienti, basati sull'utilizzo di almeno due fattori (es. password, impronta biometrica, certificato su smartphone, ecc.) per consentire alla clientela di effettuare in piena sicurezza l'accesso ai conti on line e l'esecuzione dei pagamenti elettronici. In considerazione della complessità degli adeguamenti, particolarmente rilevanti nel campo dei pagamenti online con carta, e della necessità di un coinvolgimento attivo degli utenti, il 21 giugno 2019 la European Banking Authority (EBA) ha riconosciuto alle autorità nazionali la possibilità di concedere ulteriore tempo, rispetto al 14 settembre, per consentire il completamento degli interventi e l'adozione dei nuovi strumenti di autenticazione da parte di tutti i clienti, con esclusivo riferimento alla suddetta categoria di pagamenti. Con comunicato stampa del 1° agosto 2019 la Banca d'Italia, all'esito di incontri tenuti con i principali operatori interessati (banche, circuiti di carte, centri servizi, associazioni di categoria degli utenti) anche nell'ambito di apposite riunioni del Comitato Pagamenti Italia, ha ritenuto che una migrazione graduale potesse ridurre fortemente i rischi di disservizi nei pagamenti online con carta, evitando soluzioni di continuità delle transazioni in settori economici vitali come il commercio elettronico. L'Istituto ha pertanto deciso di concedere una proroga per un periodo limitato, sulla base del termine massimo che sarà definito dall'EBA e successivamente comunicato al mercato. Ai fini della proroga è stato posto in capo agli intermediari l'obbligo di presentare un dettagliato piano di migrazione, comprensivo delle iniziative di comunicazione e di preparazione della clientela, sia lato esercenti, sia lato titolari di carte. Durante il periodo di migrazione i pagamenti effettuati senza autenticazione forte potranno continuare a essere inviati e accettati secondo le attuali modalità, avendo tuttavia presente l'immediata applicabilità delle regole di imputazione delle responsabilità, in caso di frodi, alle transazioni prive dei requisiti di sicurezza richiesti dalla normativa (cfr. https://www.bancaditalia.it/media/comunicati/documenti/2019-02/CS_01082019_a_f.pdf.).

5. Il procedimento di regolamentazione secondaria della Banca d'Italia

Il procedimento di regolamentazione secondaria è articolato e allo stato non è ancora terminato.

In data 11 luglio 2018 la Banca d'Italia ha posto in pubblica consultazione due documenti atti a modificare le disposizioni in materia di "*Trasparenza delle operazioni e dei servizi bancari e finanziari. Correttezza delle relazioni tra intermediari e clienti*" nonché le disposizioni di "*vigilanza per gli istituti di pagamento e gli istituti di moneta elettronica*".

Nelle more dell'emanazione dei testi definitivi, in data 11 ottobre 2018 l'Autorità ha emanato il Provvedimento di attuazione dell'art. 2, comma 4-*bis*, del d.lgs. n. 11/2010, che ha recepito il nuovo regime di "operatività in esenzione" rispetto alla disciplina dei servizi di pagamento.

Il 4 gennaio 2019 la Banca d'Italia ha diramato una *Comunicazione* al sistema in materia di accesso ai conti di pagamento, avente ad oggetto le *istruzioni* rivolte ai prestatori di servizi di pagamento con radicamento dei conti *online* per chiedere all'Autorità di Vigilanza di beneficiare dell'esenzione dall'obbligo di realizzare una specifica interfaccia alternativa volta a garantire l'accesso ai conti (c.d. "procedura di *contingency"* o "*fall-back solution*"), ai sensi dell'articolo 33 paragrafo 6 del Regolamento delegato (UE) 2018/389 della Commissione del 27 novembre 2017, che integra la direttiva PSD2 per quanto riguarda le norme tecniche di regolamentazione per l'autenticazione forte del cliente e gli standard aperti di comunicazione comuni e sicuri (RTS).

Il 9 gennaio 2019 la Banca d'Italia ha avviato un'ulteriore consultazione pubblica al fine di recepire all'interno della circolare n. 285/2013 – recante "Disposizioni di Vigilanza per le banche" – alcuni degli Orientamenti dell'European Banking Authority in materia.

Con comunicazione del 24 gennaio 2019, la Banca d'Italia ha fornito agli istituti di pagamento e agli istituti di moneta elettronica le istruzioni per la compilazione di una nuova segnalazione (con decorrenza dall'11 febbraio 2019) in materia di distribuzione di servizi di pagamento da parte di agenti.

Si espongono di seguito i tratti salienti degli interventi in rassegna.

5.1 Il Provvedimento di attuazione dell'articolo 2, comma 4-bis, d.lgs. n. 11/2010, concernente il nuovo regime di "operatività in esenzione" nell'ambito della disciplina dei servizi di pagamento

Come noto, la PSD2 ha ampliato l'ambito di applicazione soggettivo della normativa in materia di pagamenti, introducendo nuovi professionisti abilitati a prestare tipologie più moderne di servizi di pagamento; ha disciplinato il c.d. "*negative scope*", escludendo dall'ambito di applicazione alcuni servizi e operazioni

di pagamento al ricorrere di determinate condizioni. In particolare, la Direttiva ha escluso la possibilità per gli operatori di beneficiare di un'esenzione dal regime di prestazione dei servizi di pagamento senza consultare l'Autorità, prevedendo, a mente dell'articolo 37, l'obbligo di notifica all'Autorità di Vigilanza per i prestatori di servizi che emettono strumenti a spendibilità limitata e per gli operatori di reti o di servizi di comunicazione elettronica. Tale obbligo è stato espressamente recepito a livello nazionale nell'articolo 2, comma 4-*bis*, del d.lgs. n. 11/2010, introdotto dal d.lgs. n. 218/2017; le modalità e i termini per l'invio delle informazioni sono state specificate mediante Provvedimento della Banca d'Italia dell'11 ottobre 2018.

La notifica alla Banca d'Italia deve essere effettuata: la prima volta, per i prestatori di servizi basati su strumenti a spendibilità limitata entro il 30 aprile dell'anno successivo a quello di riferimento dell'operatività, e per i fornitori di reti o servizi di comunicazione elettronica entro centoventi giorni dalla chiusura contabile dell'esercizio, ai fini dell'iscrizione in una specifica sezione dell'albo degli istituti di pagamento, con l'indicazione delle informazioni utili all'Autorità per valutare l'attività svolta dall'operatore, utilizzando gli appositi schemi allegati al Provvedimento; in caso di aggiornamento o variazione delle informazioni comunicate nella precedente comunicazione; con cadenza annuale, relativamente a informazioni di carattere quantitativo.

Ciò posto, accertata la sussistenza delle condizioni per l'operatività in regime di esenzione, gli intermediari interessati devono essere iscritti in apposita sezione dell'albo degli istituti di pagamento. A tal fine, come prima notifica, i soggetti che prestano servizi basati su strumenti a spendibilità limitata, sussistendo le condizioni richieste, e i fornitori di reti o servizi di comunicazione elettronica devono comunicare alla Banca d'Italia, rispettivamente entro il 30 aprile 2019 e entro centoventi giorni dalla chiusura contabile dell'esercizio, le informazioni richieste riferite al periodo intercorrente tra l'1gennaio e il 31 dicembre 2018.

La Banca d'Italia, dal canto suo, è tenuta a notificare all'EBA i nominativi dei soggetti iscritti nell'albo e una descrizione dell'attività da questi svolta, ai fini della iscrizione degli stessi in un registro centrale europeo in materia.

5.2 La Comunicazione della Banca d'Italia del 24 gennaio 2019 relativa agli agenti che distribuiscono servizi di pagamento

In data 24 gennaio 2019, la Banca d'Italia ha pubblicato una *Comunicazione* recante: "*Nuova segnalazione degli agenti che distribuiscono servizi di pagamento. Istruzioni per gli istituti di pagamento e gli istituti di moneta elettronica italiani*". Il documento espone le modalità di compilazione e trasmissione della segnalazione da parte di istituti di pagamento e istituti di moneta elettronica, degli agenti in attività finanziaria iscritti nell'elenco dell'OAM, ai sensi dell'art. 128-*quater*, comma 2 e 6, t.u.b., con i quali gli Istituti medesimi hanno stipulato accordi di distribuzione per la promozione e la conclusione di contratti relativi alla prestazione di servizi di pagamento in Italia. Gli Istituti devono utilizzare tale procedura (denominata

"*GIAVA-Agenti*") al fine di comunicare il conferimento e la cessazione dei mandati relativi ad accordi di distribuzione, tempestivamente e comunque non oltre quindici giorni dall'evento. A far data dall'11 febbraio 2019, la segnalazione sostituisce l'invio all'Autorità di Vigilanza dei messaggi di posta elettronica previsti dalla *Comunicazione* della Banca d'Italia del 3 ottobre 2012 (c.d. "*Segnalazione Agenti SdP – Istruzioni*"), da intendersi abrogata dall'8 febbraio 2019. Le informazioni relative ad agenti e relativi accordi di distribuzione in essere alla data di avvio della nuova procedura, già acquisite dalla Banca d'Italia secondo le vecchie modalità, sono rese disponibili agli Istituti negli archivi del nuovo sistema.

5.3 I documenti di consultazione predisposti dalla Banca d'Italia per recepire gli Orientamenti dell'EBA sulle misure di sicurezza per i rischi operativi e di sicurezza dei servizi di pagamento e in materia di segnalazione dei gravi incidenti

In data 9 gennaio 2019 Banca d'Italia ha avviato una consultazione pubblica volta a recepire nell'ordinamento nazionale alcuni Orientamenti emanati da EBA ai sensi della PSD2.

Un primo provvedimento indica le modifiche e integrazioni da apportare alla Circolare n. 285/2013 ("Disposizioni di Vigilanza per le Banche"), segnatamente ai Capitoli 4 ("Sistema informativo") e 5 ("Continuità operativa") del Titolo IV, Parte Prima, al fine di recepire nell'ordinamento nazionale gli Orientamenti EBA del 19 dicembre 2017 in materia di segnalazione dei gravi incidenti nonché quelli del 12 gennaio 2018 sulle misure di sicurezza per i rischi operativi e per la sicurezza dei servizi di pagamento. Le modifiche alla normativa interna sono strettamente vincolate a fronte dell'elevato livello di dettaglio delle previsioni europee che lasciano limitati spazi di discrezionalità alle Autorità nazionali. Pertanto, dal documento della Banca d'Italia si evince che la normativa di prossima emanazione recepirà integralmente detti Orientamenti mediante rinvii nei Capitoli 4 e 5; peraltro, la Banca d'Italia precisa che le disposizioni di Vigilanza, ai citati capitoli, sono già ampiamente coerenti con quanto previsto dagli Orientamenti. Gli interventi proposti non fanno altro che operare dei raccordi tra gli obblighi già vigenti e quelli introdotti dall'EBA.

Nel dettaglio, il *framework* di cui agli Orientamenti EBA recepiti in tema di misure di sicurezza per i rischi operativi e per la sicurezza dei servizi di pagamento si compone di alcune novità, che si illustrano di seguito.

Innanzitutto, i prestatori di servizi di pagamento devono gestire i rischi operativi e di sicurezza secondo un livello di dettaglio proporzionato alle dimensioni, natura, scopo, complessità e rischiosità dei servizi di pagamento prestati, definendo un *framework per la gestione dei rischi* operativi e di sicurezza derivanti dall'inadeguatezza o dalla mancanza di processi interni, ovvero da eventi esogeni che hanno, o potrebbero avere, un effetto negativo sulla disponibilità, integrità e riservatezza dei sistemi che impiegano le tecnologie dell'informazione e della comunicazione e/o delle informazioni utilizzate per la prestazione dei servizi di

pagamento. Pertanto il *framework* per la gestione dei rischi dovrebbe: comprendere un esauriente documento relativo alla politica di sicurezza; essere coerente con la propensione al rischio del prestatore di servizi di pagamento; definire e attribuire i ruoli e le responsabilità fondamentali e le linee di riporto gerarchico necessarie per rafforzare le misure di sicurezza e gestire i rischi operativi e di sicurezza; stabilire le procedure e i sistemi necessari per individuare, misurare, monitorare e gestire la gamma di rischi derivanti dalle attività connesse ai servizi di pagamento.

A tal fine, i prestatori di servizi di pagamento devono, tra l'altro: definire e aggiornare periodicamente le funzioni aziendali, le risorse informatiche e i processi, classificati sotto il profilo della criticità, nonché rivedere periodicamente gli scenari di rischio e le relative misure preventive; definire criteri e soglie appropriati per la classificazione di un evento come "incidente operativo o di sicurezza", per tale intendendosi il singolo evento o serie di eventi collegati, non pianificati dal prestatore di servizi di pagamento che ha, o probabilmente avrà, un impatto negativo sull'integrità, la disponibilità, la riservatezza, l'autenticità, la continuità dei servizi relativi ai pagamenti; introdurre indicatori di pre-allerta che consentano l'individuazione rapida di incidenti operativi o di sicurezza; definire una procedura per la segnalazione ai preposti organi apicali degli incidenti operativi o di sicurezza nonché dei reclami dei clienti in materia di sicurezza; gestire le risorse informatiche e i sistemi informatici che devono essere in grado di garantire continuità operativa per limitare le perdite in caso di gravi interruzioni, rilevanti per il loro impatto sull'operatività sotto il profilo quantitativo e qualitativo nonché per le loro possibili ripercussioni.

In secondo luogo, i prestatori di servizi di pagamento, in caso di avvenuto grave incidente operativo o di sicurezza, devono sottoporre all'Autorità di Vigilanza un rapporto iniziale sull'incidente, entro quattro ore dalla rilevazione dell'errore, nonché un ulteriore rapporto finale contenente l'analisi delle cause che hanno originato l'incidente. A tal riguardo, la Banca d'Italia non ha esercitato la discrezionalità lasciata alle Autorità di Vigilanza nazionali che consentirebbe agli intermediari di delegare ad un terzo l'invio di tale comunicazione, confermando l'impostazione attualmente prevista per i gravi incidenti di sicurezza informatica per il complesso di attività e servizi bancari, in base alla quale le banche effettuano direttamente una comunicazione all'Autorità di Vigilanza.

5.4 Gli Orientamenti dell'EBA sulle condizioni per beneficiare dell'esenzione dal meccanismo di emergenza (c.d. "fall-back exemption") e la comunicazione della Banca d'Italia del 4 gennaio 2019

Il sistema bancario europeo è impegnato nelle attività di adeguamento al Regolamento dell'European Banking Authority (EBA) n. 389 del 27 novembre 2017, emanato ai sensi della PSD2. Tale provvedimento prescrive le regole tecniche standard (RTS) per la comunicazione sicura, tramite interfacce dedicate (API – *Application Programming Interface*), tra le banche di radicamento dei conti di pagamento on line e i prestatori di servizi di disposizione di ordini di

pagamento, di informazione sui conti e di conferma di disponibilità fondi (TPP). In tale ambito il Regolamento ha fissato al 14 settembre 2019 il termine entro il quale gli intermediari dovranno rendere disponibili le API ai prestatori dei citati servizi di pagamento, conformemente alle regole previste.

In questo contesto l'EBA, nell'ottica di mitigare i potenziali rischi derivanti da ipotesi di indisponibilità tecnica delle API, ha autorizzato le terze parti (art. 33, par. 4, Reg., cit.) a utilizzare, in caso di indisponibilità non programmata dell'interfaccia dedicata e guasto dei sistemi, l'interfaccia messa a disposizione degli utenti dei servizi, fino a che non venga ripristinato l'adeguato livello di disponibilità e prestazioni dell'interfaccia dedicata (*fall-back solution*). L'EBA ha tuttavia stabilito (art. 33, par. 6) che le competenti autorità nazionali possono esonerare gli intermediari di radicamento di conti dall'obbligo di mettere a disposizione, nei casi innanzi esposti, l'interfaccia dell'utente, purché l'interfaccia dedicata soddisfi determinati requisiti e condizioni di sicurezza da implementare e testare prima del termine per l'adeguamento[40]. A tal fine l'EBA ha disposto nei confronti degli intermediari di radicamento dei conti l'obbligo di: i) misurare – su base giornaliera – il livello di funzionamento o malfunzionamento delle interfacce attraverso appositi *key performance indicators*; ii) pubblicare statistiche trimestrali sulle prestazioni delle interfacce, dedicate e dell'utente, allo scopo di consentire alle terze parti e all'utente di raffrontare i livelli di servizio di ciascuna delle due tipologie di interfacce; iii) sottoporre le interfacce dedicate e gli indicatori di *perfomance* ad attività di *stress testing*; iv) implementare le interfacce che non creino ostacoli alle terze parti, con particolare riguardo ai sistemi di autenticazione; v) rendere disponibile, almeno sei mesi prima del termine per l'adeguamento, un dispositivo di prova della connessione e del funzionamento, al fine di consentire alle terze parti autorizzate di testare il *software* e le applicazioni utilizzati; vi) consentire alle terze parti, nella fase di implementazione, l'utilizzo per almeno tre mesi; vii) verificare che gli eventuali problemi relativi all'interfaccia dedicata siano stati risolti senza ingiustificati ritardi; viii) implementare le interfacce in ambiente di produzione entro l'1 giugno 2019[41].

---

[40] Le condizioni per l'esenzione specificate all'articolo 33, par. 6 del Reg. n. 389/2017 (RTS) sono dettagliate negli orientamenti dell'EBA, *Guidelines on the exemption from the contingency mechanism under the RTS on SCA and CSC*, pubblicate il 4 dicembre 2018.

[41] A gennaio 2019, l'EBA ha istituito un gruppo di lavoro (WG) sulle API, composto da trenta persone in rappresentanza degli ASPSP, terze parti (TPP), schemi API e altri partecipanti al mercato. L'obiettivo del gruppo è quello di facilitare la preparazione del settore per lo standard tecnico di regolamentazione (RTS) su *Strong Customer Authentication e Common Secure Communication* nonché supportare lo sviluppo di «*high-performing and customer-focused APIs under PSD2*». Su queste tematiche, in data 1 e 26 aprile 2016, l'EBA ha pubblicato due documenti contenenti i chiarimenti forniti dalla medesima autorità su questioni sollevate dal proprio gruppo di lavoro (WG-GR) concernenti gli artt. 30, ss. del Regolamento delegato (UE) 2018/389 della Commissione (RTS su SCA&CSC; cfr. https://eba.europa.eu/documents/10180/2545547/issues+iv+-+vii+as+raised+by+eba+wg-api.pdf; https://eba.europa.eu/documents/10180/2545547/issues+viii+to+xiii+raised+by+the+eba+wg+on+apis+.pdf).

Ebbene, il 4 gennaio 2019, la Banca d'Italia ha diramato una nota al sistema in materia di acceso ai conti di pagamento[42] che, in conformità dei predetti Orientamenti EBA del 4 dicembre 2018, reca le "istruzioni" sulle condizioni per beneficiare dell'esenzione dal meccanismo di emergenza (*procedura di contingency o "fall-back solution*") a norma dell'articolo 33, par. 6, RTS, inserendo gli opportuni riferimenti alla procedura riservata ai prestatori di servizi di pagamento con radicamento dei conti on line.

In particolare, tale *Comunicazione* indica le tempistiche, le istruzioni operative e la modulistica per richiedere l'esonero in esame, riportando le informazioni che tutti i prestatori di servizi di pagamento che detengono conti accessibili *online* (*Account Servicing Payment Service Providers* o ASPSP) devono comunicare per attestare il rispetto delle predette condizioni di sicurezza. Nello specifico, è stato previsto che gli ASPSP comunichino alla Banca d'Italia: i) entro il 14 marzo 2019 (Modulo "Informazioni sull'interfaccia dedicata") un primo set di informazioni generali, quali livello di servizio, disponibilità e prestazione delle interfacce, piano di pubblicazione delle statistiche sulle *performance*, procedure di autenticazione, procedure di risoluzione di eventuali problemi[43]; ii) entro il 14 giugno 2019 (Modulo "Informazioni sui *test* e sugli *stress test*") i risultati dei *test* effettuati con il dispositivo di prova nonché quelli emersi dalle attività di *stress testing* effettuate anche in sede di collaudo; iii) entro il termine ordinatorio dell'1 agosto 2019 (Modulo "Utilizzo delle interfacce dedicate") i risultati dell'utilizzo intensivo della piattaforma da parte delle terze parti nonché l'esito delle modalità di utilizzo delle piattaforme in ambiente di produzione dall'1 giugno 2019 fino al momento della comunicazione (informazione quest'ultima che costituisce atto formale di presentazione dell'istanza di esonero); iv) entro i primi giorni di settembre 2019, solo qualora vi siano differenze significative rispetto a quanto comunicato entro l'1 agosto precedente, eventuali evidenze integrative sull'utilizzo delle piattaforme.

In caso di adesione a "soluzioni cooperative" sorvegliate ai sensi dell'art. 146 t.u.b., viene evidenziato che la comunicazione da trasmettersi entro il 14 marzo 2019 assolve, altresì, all'obbligo della comunicazione preventiva a Banca d'Italia prevista dalla normativa sulle esternalizzazioni di Funzioni Operative

---

[42] cfr. Banca D'Italia, *Comunicazione della Banca d'Italia in materia di accesso ai conti di pagamento (previsto dalla Direttiva PSD2): istruzioni per l'esenzione dall'obbligo di realizzare la procedura di* contingency *("*fall-back solution*")*, 4 gennaio 2019.

[43] Come evidenziato *infra*, l'art. 33, par. 6, RTS, pone in capo ai prestatori di servizi di pagamento con radicamento dei conti on line l'obbligo di predisporre, entro il 14 settembre 2019, un'interfaccia di accesso per consentire ai TTPs di svolgere la propria attività. Tale obbligo, volto ad assicurare l'utilizzo di un canale sicuro di autenticazione e comunicazione tra il prestatore di servizi di pagamento con radicamento dei conti on line e le Terze Parti, è soddisfatto, alternativamente, attraverso: la realizzazione *ex novo* di una interfaccia dedicata all'accesso delle terze parti; l'adattamento dell'interfaccia utilizzata dal prestatore di servizi di pagamento con radicamento dei conti on line per l'autenticazione e la comunicazione con i propri clienti. In caso di adozione dell'interfaccia dedicata, si rende necessario assicurare alle terze parti l'accesso ai conti attraverso l'interfaccia utilizzata per i clienti, in caso di indisponibilità o prestazioni inadeguate dell'interfaccia dedicata (c.d. soluzione di *fall back* o "*fall-back option*").

Importanti (FOI), restando in capo agli intermediari l'onere di trasmettere, insieme alle predette informazioni, un'analisi dei rischi, sempre a condizione che la piattaforma abbia confermato di aver proceduto alla comunicazione preventiva di esternalizzazione FOI.

5.5 Le modifiche alle disposizioni in materia di "Trasparenza delle operazioni e dei servizi bancari e finanziari. Correttezza delle relazioni tra intermediari e clienti"

Il 19 marzo 2019 la Banca d'Italia ha emanato un provvedimento con il quale sono state apportate modifiche alle disposizioni in materia di "*Trasparenza delle operazioni e dei servizi bancari e finanziari. Correttezza delle relazioni tra intermediari e clienti*" adottato il 29 luglio 2009, come successivamente modificato.

L'intervento si è reso necessario per adeguare la disciplina nazionale al nuovo quadro normativo europeo riferito a vari ambiti di competenza e, in particolare: alla trasparenza dei servizi di pagamento (sezione VI), in attuazione della direttiva 2015/2366/UE relativa ai servizi di pagamento nel mercato interno e delle disposizioni del capo II-*bis*, titolo VI, del Testo Unico Bancario (TUB); all'informativa precontrattuale sugli indici di riferimento utilizzati nelle operazioni di credito immobiliare ai consumatori e credito ai consumatori (sezione VI-*bis*, par. 5.2, e sezione VII, par. 4), in attuazione delle disposizioni della direttiva 2014/17/UE (*Mortgage Credit Directive*, MCD) e della direttiva 2008/48/CE (*Consumer Credit Directive*, CCD), come modificate dal Regolamento 2016/1011/UE (c.d. Regolamento *Benchmark*); alle politiche e prassi di remunerazione per il personale preposto all'offerta dei prodotti bancari e per i terzi addetti alla rete di vendita (sezione XI, par. 2-*quater*), in attuazione degli Orientamenti dell'Autorità Bancaria Europea (*European Banking Authority* – EBA), concernenti le politiche e prassi di remunerazione relative alla vendita e alla fornitura di servizi bancari al dettaglio; alla gestione dei reclami (sezione XI, par. 3), in attuazione degli Orientamenti del *Joint Committee* delle Autorità Europee di Vigilanza (*European Supervisory Authorities* – ESAs) sulla gestione dei reclami per il settore degli strumenti finanziari e per il settore bancario. Alcune modifiche sono state volte altresì a recepire buone prassi rilevate nell'esercizio dell'attività di controllo[44].

Le modifiche di cui sopra si applicano a partire dal 1° luglio 2019, ad eccezione: delle variazioni alla sezione VI, che – per finalità di coordinamento con la disciplina in materia di conti di pagamento, di attuazione della direttiva 2014/92/UE (*Payment Accounts Directive*, c.d. PAD) – si applicheranno

---

[44] In dettaglio, le modifiche riguardano: la sezione I, paragrafi 2 e 4; la sezione II, paragrafo 2; la sezione VI; la sezione VI-*bis*, paragrafi 2 e 5; la sezione VII, paragrafi 2 e 4; la sezione VIII, paragrafo 2; la sezione X; la sezione XI, paragrafi 1, 2, 2-*bis*, 2-*quater* e 3; l'Allegato 3.

dal 1° gennaio 2020[45]; della modifica alla sezione XI, paragrafo 3, avente ad oggetto i tempi massimi di risposta ai reclami, che – per finalità di coordinamento con la disciplina in materia di presentazione dei ricorsi all'Arbitro Bancario Finanziario – si applicherà a partire dalla data che sarà indicata nel provvedimento di adozione delle modifiche alle disposizioni della Banca d'Italia sui sistemi di risoluzione stragiudiziale delle controversie in materia di operazioni e servizi bancari e finanziari. Fino a tale data, i tempi massimi di risposta alle istanze dei clienti restano non superiori a trenta giorni dalla ricezione del reclamo. Le politiche di remunerazione, rese conformi a quanto previsto dalla sezione XI, paragrafo 2-*quater*, del provvedimento sono sottoposte, al più tardi, all'approvazione dell'assemblea convocata per l'approvazione del bilancio relativo all'esercizio 2019.

Per quanto qui di stretto interesse, di seguito si evidenziano i contenuti salienti degli interventi mirati adottati dalla Banca d'Italia per completare l'adeguamento al quadro normativo europeo inerenti – relativamente ai profili di trasparenza – l'informazione precontrattuale (sez. VI, § 4), le comunicazioni alla clientela (sez. VI, § 6) e la gestione dei reclami (sez. XI, § 3).

In ordine al primo aspetto, le informazioni da fornire ai clienti prima della conclusione del contratto sono integrate con i dati aggiuntivi previsti dalla PSD2. In proposito rilevano, a titolo esemplificativo, le informazioni concernenti gli strumenti di pagamento basati su carta *multimarchio in co-badging*[46] (§ 4.4.1., lett. b), la procedura di sicurezza da seguire per comunicare i rischi di frode nei pagamenti (lett. e), la possibilità di presentare reclami al prestatore di servizi di pagamento (lett. g).

Vengono inoltre regolati gli obblighi informativi che fanno capo ai prestatori dei nuovi servizi di pagamento previsti dalla PSD2 (i.e., servizi di disposizione di ordini di pagamento e servizi di informazione sui conti),

---

[45] La Banca d'Italia ha tenuto in debita considerazione l'esigenza di realizzare – per quanto possibile – in un unico momento le modifiche alle Disposizioni di trasparenza, evitando una pluralità di interventi ravvicinati. L'aggiornamento in rassegna dà attuazione a vari indirizzi europei (direttiva PSD2; linee guida EBA sulla remunerazione del personale preposto all'offerta dei prodotti bancari e dei terzi addetti alla rete di vendita; linee guida delle ESAs sulla gestione dei reclami; Regolamento *Benchmark*). Alfine di coordinare le modifiche alla sezione VI in materia di trasparenza dei servizi di pagamento con quelle da apportare alla medesima sezione per dare attuazione alla direttiva PAD in tema di conti di pagamento (oggetto di separata consultazione pubblica), l'atto di emanazione del 19 marzo 2019 prevede che le modifiche in commento si applicheranno a partire dalla data che sarà indicata in un successivo provvedimento della Banca d'Italia (sul punto, cfr. Banca d'Italia, "*resoconto consultazione*", https://www.bancaditalia.it/compiti/vigilanza/normativa/consultazioni/2018/direttiva-2015-366ue/Resoconto_consultazione.pdf). Con atto di emanazione del 19 giugno 2019, la Banca d'Italia ha dato attuazione alla direttiva 2014/92/UE (*Payment Account Directive*) e al capo II-*ter*, titolo VI, t.u.b., in materia di conti di pagamento offerti a o sottoscritti da consumatori. Tali ultime modifiche si applicano dal 1° gennaio 2020. A partire da questa stessa data sono cogenti anche le modifiche alla sezione VI – attuative della direttiva 2015/2366/UE (PSD2) – apportate con il citato provvedimento del 19 marzo 2019 (cfr. https://www.bancaditalia.it/compiti/vigilanza/normativa/archivio-norme/disposizioni/trasparenza_operazioni/disp-rec-dir-2014-92/Disposizioni.pdf).

[46] Ai sensi della direttiva 2015/2366/UE, per "*multimarchio in co-badging*" si intende l'inclusione di due o più marchi di pagamento o applicazioni di pagamento dello stesso marchio in uno stesso strumento di pagamento.

segnatamente: prevedendo un regime semplificato per gli intermediari che prestano unicamente il servizio di informazione sui conti, in linea con la direttiva; disciplinando l'informativa dovuta nei casi in cui l'operazione di pagamento è disposta per il tramite di un prestatore di servizi di disposizione di ordine di pagamento.

Con riferimento alle comunicazioni alla clientela, vengono declinate le informazioni specifiche da fornire all'utente quando un'operazione di pagamento è disposta tramite un prestatore di servizi di disposizione di ordine di pagamento[47].

In tema di *gestione dei reclami*, gli Orientamenti adottati dalle ESAs in materia richiedono che gli intermediari si dotino di procedure organizzative per una gestione efficace degli stessi, allo scopo di assicurare una pronta soluzione di situazioni conflittuali insorte nei rapporti con i clienti e di promuovere in questo modo un più elevato livello di soddisfazione della clientela. Per dare attuazione agli Orientamenti sono state apportate modifiche al paragrafo 3 della Sezione XI delle Disposizioni. I principali interventi riguardano: (i) l'adozione di una politica di trattazione dei reclami, che deve essere approvata e sottoposta a esame periodico da parte dell'Organo di supervisione strategica, responsabile anche della sua corretta attuazione e di eventuali modifiche alla stessa; (ii) la fase istruttoria e decisoria dei reclami in relazione alle quali si richiede al responsabile della gestione dei reclami di acquisire ogni elemento utile per l'adeguata trattazione degli stessi; è inoltre previsto che il processo di definizione del reclamo sia documentato. Gli intermediari sono tenuti ad analizzare i dati relativi ai reclami pervenuti, per individuare eventuali criticità ricorrenti e assumere le iniziative necessarie per superarle.

Ulteriori modifiche apportate alle Disposizioni tengono conto delle buone prassi rilevate dall'autorità di vigilanza nell'esercizio dell'attività di controllo, alcune delle quali già rese note dalla Banca d'Italia. In particolare si prevede che la politica di trattazione dei reclami individui le modalità di interazione tra il responsabile della gestione dei reclami, le funzioni preposte alla commercializzazione dei prodotti e le altre funzioni aziendali coinvolte, assicurando un adeguato presidio dei possibili conflitti di interesse. Si richiede altresì che il responsabile della gestione dei reclami predisponga una relazione annuale in cui dia conto, tra l'altro, del numero dei reclami ritenuti fondati e di quelli ritenuti infondati. Si prevede ancora che la funzione di conformità riferisca annualmente agli organi aziendali con particolare riguardo alle principali criticità emerse dai reclami ricevuti e alle pronunce dell'ABF e dell'autorità giudiziaria che hanno definito in senso favorevole ai clienti controversie in precedenza oggetto di un reclamo rigettato.

Relativamente ai tempi di trattazione dei reclami, in generale il termine per riscontrare le istanze dei clienti è esteso a sessanta giorni, onde concedere agli

---

[47] Banca d'Italia, *Disposizioni di Trasparenza*, sez. VI, par. 6, p. 24.

intermediari un lasso di tempo più congruo nel quale analizzare approfonditamente i contenuti delle stesse e individuare soluzioni in grado di soddisfare al meglio le richieste della clientela.

Per i reclami in materia di servizi di pagamento vige un termine breve di quindici giorni lavorativi dalla ricezione del reclamo, secondo quanto disposto dalla PSD2. In situazioni eccezionali, ove l'intermediario sia impossibilitato a rispondere entro quindici giornate lavorative, si prevede che il medesimo invii al cliente una risposta interlocutoria, con l'indicazione chiara e concisa delle ragioni del ritardo nonché il termine entro il quale il cliente riceverà la risposta definitiva, comunque non superiore a trentacinque giornate lavorative. L'intermediario individua, nell'ambito delle procedure interne, le situazioni eccezionali, allo stesso non imputabili, al ricorrere delle quali è possibile rispondere oltre il termine delle quindici giornate lavorative. È fatto salvo quanto previsto dall'articolo 14, comma 2, del decreto legislativo 27 gennaio 2010, n. 11.

Con l'obiettivo di favorire una più adeguata trattazione dei reclami, i sistemi di remunerazione prevedono, infine, indicatori che tengano conto, *inter alia*, dei risultati conseguiti nella loro gestione e della qualità delle relazioni con la clientela.

I THIRD PARTY PROVIDER: PROFILI SOGGETTIVI E OGGETTIVI

Vincenza Profeta

1. I nuovi servizi sottoposti a riserva: disposizione di ordine di pagamento e informazione sui conti – 2. I nuovi prestatori di servizi di pagamento – 2.1 La direttiva – 2.2 la disciplina nazionale – 3. Le caratteristiche dello svolgimento dei nuovi servizi codificati nell'art. 1, nn. 7 e 8 dell'allegato I della direttiva: la relazione tra TPPs e prestatori di radicamento del conto – 3.1 L'accesso ai conti: l'art. 98 della PSD2, gli standard tecnici dell'EBA e il regolamento delegato (UE) 2018/389 – 3.2 Il consenso alla prestazione del servizio – 3.3 La responsabilità civile dei nuovi prestatori di servizi di pagamento e l'obbligo di rimborso – 4. L'applicazione della disciplina contrattuale uniforme dei servizi di pagamento

Appendice: Considerazioni in materia di contrasto del riciclaggio e del finanziamento del terrorismo in relazione a servizi con TPP, di Eugenio Maria Mastropaolo

1. I nuovi servizi sottoposti a riserva: disposizione di ordine di pagamento e informazione sui conti

La direttiva (UE) 2015/2366 del Parlamento e del Consiglio del 25 novembre 2015 (cd. PSD2 – *Payment Services Directive*) ha ampliato il novero dei servizi di pagamento soggetti a riserva, introducendo la regolamentazione di due nuove categorie di attività: i servizi di disposizione di ordine di pagamento e i servizi di informazione sui conti.

Tali attività commerciali figurano rispettivamente ai numeri 7 e 8 dell'allegato I della direttiva, dove sono separatamente enumerati e descritti tutti i servizi oggetto di regolamentazione, ai quali fa rinvio l'art. 4.3 della direttiva quando intende definire il "servizio di pagamento".

La PSD2, infatti, come già la PSD1[1], omette di indicare nel catalogo delle definizioni un'esplicazione univoca e astratta delle caratteristiche del servizio di pagamento, inteso come contratto, piuttosto, facendo rinvio a tal fine all'allegato I, offre all'interprete un'elencazione di attività commerciali tipiche ripartite in otto categorie alle quali in maniera convenzionale attribuisce la natura di servizi di pagamento. Tuttavia, per i nuovi servizi di pagamento, a differenza degli altri, è stata introdotta anche una specifica definizione nell'ambito dell'art. 4 della direttiva laddove, in particolare, si qualifica come "servizio di disposizione di ordine di pagamento" quello in forza del quale si "*dispone l'ordine di pagamento su richiesta dell'utente di servizi di pagamento relativamente a un conto di pagamento detenuto presso un altro prestatore di servizi di pagamento*" (art. 4.15 PSD2). Questo servizio, conosciuto anche con l'acronimo PIS (*payment initiation service*), consente al prestatore di servizi di pagamento che lo svolge di iniziare un'operazione di pagamento mediante un ordine che egli impartisce su richiesta del proprio cliente che lo autorizza a movimentare il proprio conto ancorché detenuto presso un diverso prestatore. Si tratta nella prassi di un servizio informatico che consente di connettere il sito web del commerciante con la piattaforma di *on line banking* della banca del pagatore per disporre pagamenti via Internet con lo strumento del bonifico,

[1] Direttiva 2007/64/CE del Parlamento e del Consiglio del 13 novembre 2007.

offrendo una soluzione di pagamento elettronico alternativa a quella delle carte e a basso costo[2].

Il servizio di informazione sui conti è, invece, quel "*servizio online che fornisce informazioni consolidate relativamente a uno o più conti di pagamento detenuti dall'utente di servizi di pagamento presso un altro prestatore di servizi di pagamento o presso più prestatori di servizi di pagamento*" (art. 4.16). Esso, noto anche come *account information service* (AIS), consente al prestatore che lo svolge di accedere ai conti di pagamento del proprio cliente, ancorché radicati presso altri prestatori, per acquisire informazioni di pagamento e mettergliele a disposizione. Scopo del servizio è fornire al richiedente una visione complessiva della propria situazione finanziaria[3], immediatamente e in qualsiasi momento, senza necessità di contattare singolarmente i vari prestatori di pagamento dove i conti sono radicati, con l'evidente utilità di consentire all'utente una migliore

---

[2] Come si legge nel considerando 27 della direttiva 2015/2366 "successivamente all'adozione della direttiva 2007/64/CE si sono diffusi nuovi tipi di servizi di pagamento, specialmente nel settore dei pagamenti tramite Internet. In particolare si sono evoluti i servizi di disposizione di ordine di pagamento nel settore del commercio elettronico. Tali servizi di pagamento svolgono un ruolo nei pagamenti in detto settore mediante un software che fa da ponte tra il sito web del commerciante e la piattaforma di online banking della banca del pagatore per disporre pagamenti via Internet sulla base di bonifici". Il servizio ha conosciuto un particolare sviluppo nell'ambito del commercio elettronico poiché consente "al prestatore di servizi di disposizione di ordine di pagamento di assicurare al beneficiario che il pagamento è stato disposto così da incentivare il beneficiario a consegnare i beni o a prestare il servizio senza indebiti ritardi" (così il considerando 29). In dottrina A. Antonucci, *Mercati dei pagamenti: le dimensioni del digitale*, in Riv. dir. banc., www.dirittobancario.it, 18, 2018, sottolinea che "le potenzialità di sviluppo del servizio sono enormi e in parte già fruibili nel contesto nazionale, dove da un canto sta divenendo operativo il servizio – sul modello Paypal – già prestato in altre realtà dalle grandi digital companies identificate con l'acronimo GAFA (Google, Amazon, Facebook, Apple), d'altro canto si affacciano offerte combinate alla prestazione di servizi di altra natura, con ricadute su mercati diversi e talora segnati da criticità concorrenziali: penso alle app di prenotazione dei taxi che, oltre ad avere in taluni casi un'ottima fruibilità per il cliente e l'offerta di servizi aggiuntivi, con un costo commissionale modesto svincolano il tassista dalla necessità di legarsi a compagnie di radiotaxi". Sulla promozione di pagamenti elettronici sicuri, efficienti e competitivi v. Libro verde della Commissione europea "*Verso un mercato europeo integrato dei pagamenti tramite carte, internet e telefono mobile*" dell'11.1.2012. La diffusione dei pagamenti elettronici si muove di pari passo con quella dei dispositivi mobili (smartphone, tablet, mobile internet device (MID)) che possono collegarsi wireless alla rete internet, permettendo di realizzare una delle moderne forme di cd. *mobile payments*. Sul tema v. S. Moneti, *Mobile payments: gli sviluppi del mercato e l'inquadramento normativo,* in *Analisi giuridica dell'economia*, 2015, 101; E. Cervone, *Strumenti di pagamento innovativi, interoperabilità e neutralità tecnologica: quali regole e quale governance per un mercato sicuro, efficiente ed innovativo,* in *Riv. trim. diritto dell'economia*, 2016, p. 41; G. Gimigliano e G. Nava, *L'inquadramento giuridico dei Mobile payment: profili ricostruttivi e distonie regolamentari,* in *Smart cities e diritto dell'innovazione* a cura di G. Olivieri e V. Falce, Milano, 2016, p.190.

[3] M. Catenacci e C. Fornasaro, *PSD2: i prestatori di servizi d'informazione sui* conti *(AISPS),* in *Dir. Banc.*, 4/2018, ritengono che possano ricondursi alla categoria degli AISPs soltanto gli operatori che forniscono i dati ad un cliente finale (per converso sarebbero esclusi dalla categoria coloro che agiscono come meri fornitori di dati senza mai relazionarsi con l'utente finale); gli operatori che forniscono informazioni aggregate o consolidate (e non quelli che forniscono una "singola" informazione); relative soltanto ai conti di pagamento (e non anche, per esempio, ai conti titoli).

consapevolezza della propria condizione finanziaria e una più efficiente pianificazione di spesa[4].

Tali servizi si caratterizzano entrambi per il fatto che il loro prestatore deve operare su un conto di pagamento *online* acceso presso un altro prestatore di servizi di pagamento al quale compete amministrare e gestire il conto per il medesimo cliente (cd. prestatore di servizi di pagamento di radicamento del conto) (art. 4.17).

La limitazione a svolgere detti servizi solo in relazione ai conti accessibili *on line* è espressamente prevista nella definizione contenuta nell'art. 4.16 con riguardo ai servizi di informazione sui conti; manca una simmetrica previsione nell'ambito della definizione del servizio di disposizione d'ordine di pagamento, tuttavia la certezza che anch'esso possa essere svolto esclusivamente sui conti *on line* si ricava agevolmente dalla disposizione contenuta nell'art. 66, comma 1, della direttiva, che esclude il diritto del pagatore di avvalersi di un prestatore di servizi di disposizione di ordine di pagamento qualora il conto di pagamento "*non sia accessibile online*".

Pertanto i servizi in discorso non possono essere svolti per eseguire operazioni o per dare informazioni con riferimento a conti di pagamento ad operatività tradizionale, non raggiungibili da remoto in maniera telematica, tenuto conto che essi vengono espletati esclusivamente in maniera telematica e si sostanziano proprio nella conoscenza o nella movimentazione digitale a distanza dei conti radicati presso un distinto intermediario.

La volontà del legislatore europeo di implementarne l'utilizzo e, per questa via, di promuovere la diffusione dei bonifici digitalizzati, si concretizza nella previsione di un diritto in capo al pagatore di avvalersi di un prestatore di servizi di disposizione di ordine di pagamento (art. 66, comma 1, PSD2) nonché nel diritto di ricorrere a servizi che consentono l'accesso alle informazioni sui conti di cui al punto 8 dell'allegato I (art. 67, comma 1 PSD2); per converso i prestatori di pagamento di radicamento di conti *online* hanno l'obbligo di consentire l'accesso al conto ai prestatori dei nuovi servizi e, a tal fine, sono stati gravati dell'onere di predisporre un'interfaccia tecnica per comunicare con gli intermediari consentendo loro lo svolgimento dei nuovi servizi.

Nella filiera delle attività che portano all'esecuzione del pagamento con l'utilizzo di moneta scritturale di conto quelle svolte nell'ambito dei nuovi servizi PIS e AIS si pongono in maniera abbastanza defilata poiché entrambi non comportano in alcun modo la custodia e la gestione dei fondi con cui il

---

[4] Cfr. il considerando 28 della Direttiva n. 2015/2366 nel quale si dà conto del fatto che gli sviluppi tecnologici degli ultimi anni successivi alla PSD1 hanno portato alla nascita di una serie di servizi accessori, quali ad esempio quelli di informazione sui conti, che forniscono "*informazioni online aggregate su uno o più conti di pagamento, detenuti presso un altro o altri prestatori di servizi di pagamento, a cui si ha accesso mediante interfacce online del prestatore di servizi di pagamento di radicamento del conto. L'utente di servizi di pagamento può così disporre immediatamente di un quadro generale della sua situazione finanziaria in un dato momento.*"

pagamento viene eseguito: la disposizione di un ordine di pagamento impartito da un PISP dà solo l'avvio ad un'operazione che verrà eseguita da e verso prestatori diversi[5]; il servizio di fornitura di informazioni relative ai dati contenuti nei conti di pagamento ha, dal canto suo, un carattere del tutto accessorio rispetto all'operazione di pagamento, alla quale non inerisce se non al fine di dare all'utente conoscenza più immediata dell'esistenza e della quantità dei fondi disponibili. Ciononostante, l'attrazione di questi servizi, già commercialmente diffusi in altri Paesi dell'Unione, nell'ambito di quelli propriamente detti "di pagamento", e la conseguente applicazione del regime soggettivo e oggettivo proprio di questi ultimi, risponde all'interesse pubblico di monitorare lo svolgimento delle attività che ne formano oggetto, poiché la tecnologia che le connota, da un lato, risulta cruciale per lo sviluppo dei pagamenti digitali, dall'altro, pone l'esigenza di implementare i presidi di sicurezza informatica sia per tutelare i fondi, che potrebbero essere aggrediti più facilmente in considerazione del fatto che i nuovi servizi consentono al prestatore che li svolge un accesso diretto e *ab externo* ai conti di pagamento, sia per assicurare la protezione dei dati relativi ai pagamenti resi conoscibili a soggetti terzi diversi sia rispetto al titolare del conto sia rispetto al prestatore presso il quale il conto è radicato[6].

La riserva di attività nasce quindi dalla consapevolezza che la tecnologia assume un valore preponderante nel mondo dei servizi di pagamento digitalizzati che si avvalgono della moneta scritturale, il cui utilizzo cresce di pari passo

---

[5] In dottrina V. Di Stasio, *Ordine di pagamento non autorizzato e restituzione della moneta*, Milano, 2016, ha evidenziato che i pagamenti fatti con moneta scritturale si caratterizzano per la loro natura procedimentale, infatti "*le operazioni di pagamento sono, in sostanza, operazioni di "trasferimento" di moneta scritturale, esito di un procedimento avviato da un ordine di pagamento, sorretto dal consenso del pagatore*" (p. 64); "*il rispetto delle procedure di per sé oblitera la dimensione negoziale dell'ordine di pagamento o dell'autorizzazione dell'operazione di pagamento e consente di dare avvio al trasferimento dei fondi senza necessità di verificare se in concreto l'intento negoziale del pagatore fosse conforme alle risultanze delle procedure dello strumento di pagamento e della sua autenticazione*" (p.110); anche A. Sciarrone Alibrandi, *Il diritto del sistema finanziario*, in AA.VV., *Diritto commerciale,* a cura di M. Cian, Torino, 2013, p. 319, evidenzia l'aspetto procedimentale del pagamento eseguito attraverso un intermediario professionale: *"il pagamento in moneta scritturale si esegue per lo più tramite il trasferimento della titolarità di fondi detenuti dal pagatore presso banche o intermediari abilitati; consiste, quindi, in un'attività di servizi a struttura quantomeno trilatera, esercitata su base imprenditoriale da intermediari specializzati, nel cui contesto il trasferimento monetario si perfeziona solo al termine di un complesso procedimento con l'annotazione nelle scritture contabili degli intermediari coinvolti*".

[6] Nel considerando 29 della direttiva n. 2015/2366 si sottolinea come l'assenza di regolamentazione dei servizi di disposizione di ordine di pagamento abbia posto "*una serie di questioni giuridiche, ad esempio sul piano della tutela dei consumatori, della sicurezza e della responsabilità nonché della concorrenza e delle questioni legate alla protezione dei dati, con particolare riguardo alla protezione dei dati degli utenti dei servizi di pagamento in conformità delle norme dell'Unione sulla protezione dei dati*" che le nuove norme intendono affrontare. A. Antonucci, *Mercati dei pagamenti: le dimensioni del digitale cit*., p. 2, ha sottolineato che "*nella costruzione di un ambiente normativo omogeneo, la PSD2 in qualche misura insegue e tende ad ingabbiare l'evoluzione di mercato nelle nuove articolazioni normative della filiera produttiva che porta al compimento dell'operazione di pagamento, disponendo due correlati livelli di estensione, funzionale all'indicata finalità normativa, nel novero dei servizi e degli intermediari che possono prestarli. Il novero dei servizi di pagamento si estende ad includere i servizi di disposizione di ordine di pagamento e di informazione sui conti, che presentano specifici problemi di tutela del fruitore del servizio, di sicurezza, di imputazione di responsabilità nella filiera del processo di pagamento*".

all'*ecommerce.* In tale contesto il procedimento di pagamento assume carattere vieppiù complesso sotto il profilo soggettivo, poiché necessita della partecipazione di più intermediari specializzati ai quali è demandato lo svolgimento di attività diverse ma strettamente connesse, tutte funzionali all'esecuzione del pagamento. Tuttavia, nonostante tale complessità soggettiva e oggettiva, i nuovi strumenti di pagamento elettronico connessi alla gestione del conto *online* e, in particolare, il bonifico ordinato per il tramite di un PISP, consentono di dare quasi istantaneità al procedimento di pagamento, permettendo di recuperare quella immediatezza propria del pagamento eseguito con la consegna fisica del numerario[7].

D'altro canto, si pone l'esigenza di monitorare il rischio che i nuovi servizi comportino un accesso indebito al conto di pagamento con pregiudizio per i fondi e per i dati ivi contenuti. Pertanto, anche se i fornitori di tali servizi non detengono mai direttamente i fondi dei clienti, ma sulla base del loro consenso si limitano o a impartire un ordine di bonifico o a fornire informazioni sui conti, i clienti potrebbero comunque subire un *vulnus* significativo dall'esercizio inappropriato di tali attività ancorché esse siano soltanto strumentali a quelle sostanzialmente qualificabili come attività di pagamento, per tali intendendo quelle che pongono in essere la movimentazione dei fondi attraverso la loro scritturazione contabile.

La nuova disciplina si preoccupa di potenziare soprattutto i presidi di sicurezza informatica dei pagamenti elettronici[8] e il monitoraggio delle frodi, attribuendo all'European Banking Authority (EBA)[9] la competenza per la definizione di standard tecnici di comunicazione sicura tra i *Third Party Providers* (TPPs) e i prestatori di radicamento del conto consentendone una revisione periodica con modalità più flessibili di implementazione e aggiornamento che consentono di tener conto della continua evoluzione tecnologica.

La regolazione delle nuove attività risponde anche all'esigenza di governare il riparto del rischio dell'inadempimento del pagamento o della sua esecuzione

---

[7] Cfr. M. Onza, *Gli strumenti di pagamento nel contesto dei pagamenti on line*, in Diritto bancario, 4/2017, p. 679, il quale rileva che "*negli strumenti di pagamento "diversi" si sopprime l'immediatezza della consegna di una res qualificata sostituita dalla movimentazione intermediata di conti. La moneta non è tanto scambiata dalle parti: è movimentata tra le parti, con queste e l'ausilio di altri, il pagamento concentrandosi sulla consistenza di conti, movimentati secondo un'unità di misura prescelta*" ed evidenzia come il pagamento eseguito con strumenti di pagamento diversi dalla moneta contante "*diventa "un procedimento", una pluralità coordinata di fatti ed atti, dunque un'attività, preordinata alla soddisfazione del creditore ed alla liberazione del debitore in cui alla consegna del numerario equivale l'accredito sul "conto" del creditore*".

[8] Cfr. F. Ciraolo, *I servizi di pagamento nell'era del FinTech*, in *Fintech. Introduzione ai profili giuridici di un mercato unico tecnologico dei servizi finanziari*, a cura di M.T. Paracampo, Milano, 2017, p. 191; l'A. evidenzia che *"È sotto il profilo della sicurezza (intesa come affidabilità, autenticità e correttezza delle transazioni) che il progresso tecnologico registrato nel settore dei servizi di pagamento ha prospettato – e continua a prospettare – alcune tra le più spinose problematiche operative"*.

[9] In generale la PSD2 e il Regolamento (UE) n. 751/2015, relativo alle commissioni interbancarie sulle operazioni di pagamento basate su carta, attribuiscono alla European Banking Authority (EBA) il ruolo di regolatore di secondo livello nonché di promotore del coordinamento tra le diverse Autorità nazionali. La cornice normativa di cui alla Direttiva e al Regolamento è quindi completata dagli standard tecnici (direttamente applicabili) e dagli orientamenti che l'EBA definisce anche al fine della loro formale approvazione (ove prevista) da parte della Commissione europea.

non autorizzata, introducendo a protezione dell'utente un diritto al rimborso, salvo l'ipotesi di frode, da far valere nei confronti del prestatore del servizio di pagamento di radicamento del conto anche quando nella filiera del pagamento sia stato coinvolto un prestatore di disposizione di ordine di pagamento; infatti, a fronte della difficoltà nell'individuazione del soggetto responsabile fra quelli a vario titolo coinvolti nell'operazione di pagamento[10], si è individuato nel gestore del conto il soggetto sul quale in prima battuta deve gravare il rischio della contestazione del pagamento, salvo il suo diritto ad ottenere a prima richiesta analogo rimborso dal PISP.

In definitiva, attraverso la nuova disciplina si vuole assicurare il buon funzionamento non solo dei nuovi servizi di pagamento, bensì dell'intera catena procedimentale del pagamento in cui essi si inseriscono, consentendo di eseguire più agevolmente i pagamenti digitali mediante bonifico. L'efficienza procedimentale complessiva risulta fondamentale per non minare la fiducia del consumatore nell'utilizzo dei nuovi strumenti di pagamento elettronico e per implementarne la diffusione.

2. I nuovi prestatori di servizi di pagamento

I soggetti che intendono fornire soltanto questi nuovi servizi, comunemente noti con l'acronimo TPPs (*Third party payment providers*)[11], debbono ora essere autorizzati in via amministrativa alla stregua di istituti di pagamento, anche se essi soggiacciono ad una disciplina parzialmente differenziata rispetto a tale generale categoria di intermediari in considerazione della specificità del loro *business*.

---

[10] Con riferimento agli AIS, v. il considerando n. 28 della Direttiva n. 2015/2366 il quale sottolinea che *"… tali servizi dovrebbero essere trattati nella presente direttiva al fine di garantire ai consumatori una protezione adeguata relativamente ai dati di pagamento e contabili nonché la certezza giuridica legata allo status di prestatore di servizi di informazione sui conti*".

[11] I TPPs si distinguono comunemente in PISPs (*payment initiation service providers*) che forniscono i servizi di ordine di pagamento e AISPs (*account information service providers*) che forniscono informazioni sui conti. Alla generale categoria dei TPPs sono riconducibili anche i prestatori di servizi di pagamento che emettono strumenti di pagamento basati su carta, cd. CBPIIs (*card based payment instrument issuers*), limitatamente allo svolgimento del servizio di conferma della disponibilità di fondi: a questi prestatori la direttiva riconosce ora il diritto di avere conferma immediata da parte del prestatore di servizi di radicamento del conto circa il fatto che sul conto del pagatore sussista la disponibilità dell'importo richiesto per l'esecuzione di un'operazione di pagamento basata su carta, a condizione che il conto sia accessibile *on line* e il pagatore, prima della richiesta di conferma, abbia fornito al prestatore di servizi di pagamento di radicamento del conto il consenso esplicito a dare risposta a tale indagine, come previsto dall'art. 65, comma 1, lett. a), b), c) PSD2. Questo servizio di conferma di disponibilità di fondi, che non ha una sua autonomia nell'elenco dei servizi contenuto nell'allegato I, non può costituire oggetto di esclusiva attività di un prestatore di servizi di pagamento, piuttosto esso è svolto soltanto dai prestatori di servizi di pagamento che emettono strumenti di pagamento basati su carta, assumendo un carattere del tutto strumentale rispetto all'utilizzo di tali strumenti solutori. Il prestatore che lo svolge, ha in comune con il PISP e l'AISP il fatto che per eseguire il proprio servizio ha accesso con il consenso esplicito del cliente al di lui conto di pagamento acceso presso un altro prestatore; il servizio di conferma di disponibilità non sarà preso in esame in questo scritto. Altri utilizzano l'acronimo con il significato di *Third parties players* così su https://www.compliancejournal.it/

2.1 La direttiva

La PSD2 (art. 37) conferma il divieto[12] di prestare servizi di pagamento da parte di persone fisiche o giuridiche che non siano prestatori di servizi di pagamento (fatti salvi i servizi espressamente esclusi dall'ambito di applicazione della medesima direttiva[13]) e, tra i prestatori[14], in linea con la precedente direttiva n. 64/2007, disciplina sotto il profilo soggettivo soltanto gli istituti di pagamento dettandone le regole per il conseguimento dell'autorizzazione amministrativa e per il loro regime di vigilanza.

La direttiva, tuttavia, introduce requisiti differenziati per ottenere l'autorizzazione o la registrazione allo svolgimento in forma isolata rispettivamente del servizio di disposizione di ordine di pagamento e di quello di informazione sui conti, in considerazione del fatto che nello svolgimento di entrambi i servizi i prestatori non detengono fondi dei clienti[15]. Infatti coloro i quali intendono svolgere soltanto servizi PIS sono tenuti ad avere un capitale iniziale di euro 50.000, più basso rispetto a quello previsto in genere per gli istituti di pagamento (IP) pari a euro 125.000, tuttavia sono obbligati a dotarsi di un'assicurazione per la responsabilità civile professionale valida in tutti i territori in cui offrono i loro servizi, o altra analoga garanzia, a copertura della responsabilità su di loro gravante per le seguenti vicende: *i)* per il compimento di operazioni non autorizzate (art. 73); *ii)* per la mancata, inesatta o tardiva esecuzione delle operazioni di pagamento (artt. 89 e 90); *iii)* per l'esercizio del regresso da parte di altri prestatori di servizi di pagamento (art. 92).

Nel caso invece di prestazione del solo servizio *on line* di informazione sui conti, la direttiva prevede che le imprese, anche individuali (art. 33 PSD2)[16] debbano presentare una domanda di registrazione, per la quale è previsto un set informativo differenziato che comprende anche il possesso di un'assicurazione per la responsabilità civile professionale valida in tutti i territori in cui esse offrono i loro servizi, o altra equivalente garanzia, per far fronte alle pretese risarcitorie derivanti da responsabilità per i danni causati al prestatore di servizi di pagamento di radicamento del conto o all'utente dei servizi di pagamento, in conseguenza dell'accesso non autorizzato o fraudolento alle informazioni del conto di pagamento o dell'uso non autorizzato o fraudolento delle stesse. Gli istituti che svolgono soltanto servizi informativi non sono tenuti al

---

[12] La Direttiva 2007/64 prevedeva analogo divieto (art. 29), tuttavia la minore ampiezza dei servizi di pagamento indicati nell'allegato I della medesima direttiva, di fatto ne riduceva la portata.

[13] Cfr. art. 37, comma 1, e art. 3, lett. k), PSD2.

[14] Elencati nell'art. 1 PSD2 (a) enti creditizi; b) istituti di moneta elettronica; c) uffici postali; d) istituti di pagamento; e) BCE e banche centrali nazionali; f) Stati membri e rispettive autorità regionali o locali ove non agiscano in quanto autorità pubbliche.

[15] Cfr. considerando n. 35 della direttiva n. 2015/2366.

[16] Cfr. anche EBA/GL/2017/09, dell'11 luglio 2017, 4.2; in particolare, la *guideline* 2 prevede quale soggetto richiedente la registrazione per lo svolgimento dei soli servizi del n. 8, alternativamente la persona fisica e quella giuridica.

possesso di un capitale iniziale (art. 7 PSD2)[17], né ad indicare i soggetti partecipanti al capitale.

I criteri per stabilire l'importo monetario minimo dell'assicurazione per la responsabilità civile professionale, o di altra comparabile garanzia, in relazione allo svolgimento dei servizi PIS e AIS sono stati definiti dall'EBA[18], così come previsto dall'art. 5.4 della PSD2, tenendo conto del profilo di rischio dell'impresa, del carattere unitario dell'attività o dello svolgimento contestuale di altri servizi di pagamento o di altre attività commerciali nonché del volume di attività che, per il servizio di disposizione di ordini di pagamento, è ragguagliato al valore delle operazioni disposte, mentre per il servizio di informazione è correlato al numero dei clienti che si avvalgono di servizi di informazione sui conti.

Il ruolo normativo dell'EBA[19], che rappresenta una sicura novità rispetto alla PSD1, risulta decisivo nello stabilire in maniera uniforme per tutti i paesi dell'Unione le caratteristiche della polizza assicurativa. Tale polizza costituisce lo strumento con il quale gli istituti che svolgono i nuovi servizi sopperiscono alla minore dotazione patrimoniale in modo da assicurare in ogni caso la copertura finanziaria per le eventuali ipotesi di responsabilità civile derivanti dai danni eventualmente arrecati, nell'esecuzione dei loro servizi, ai clienti, ai prestatori che forniscono e amministrano i conti di pagamento o ai terzi.

Sia per il rilascio dell'autorizzazione per lo svolgimento del PIS, sia per ottenere la registrazione per lo svolgimento dell'AIS particolare rilevanza assume, nell'ambito del *set* informativo che il richiedente deve fornire all'Autorità di vigilanza, il documento relativo alla politica di sicurezza, nel quale sono indicati i rischi relativi ai servizi offerti e una descrizione dei presidi organizzativi e di controllo di tali rischi, in particolare quelli di sicurezza, ivi inclusi i rischi derivanti da frode e uso illegale di dati sensibili (art. 5, comma 1, lett. *j*, PSD2). I prestatori devono individuare misure di controllo e di mitigazione dei rischi in materia di sicurezza specificando le modalità attraverso cui esse garantiscono un livello elevato di sicurezza tecnica e di protezione dei dati. Il richiedente deve descrivere la procedura esistente per monitorare e gestire gli incidenti relativi alla sicurezza e i reclami dei clienti in materia di sicurezza; aspetti, anche questi, che sono

---

[17] Coerentemente l'art. 33 PSD2 dispone che non trovino applicazione per questi soggetti l'art. 5, comma 1, lett. c), d) ed m).

[18] Il 7.7.2017 l'EBA ha pubblicato il Rapporto finale (GL/2017/08) contenente *Guidelines on the criteria on how to stipulate the minimum monetary amount of the professional indemnity insurance or other comparable guarantee under Article 5(4) of Directive (EU) 2015/2366* (PSD2).

[19] La direttiva ha conferito all'EBA il mandato ad adottare 6 *technical standards* (artt. 5.6; 28.5; 29.5; 29.6; 95.4; 98.1), 4 set di *guidelines* (artt. 5.4;5.5;95.3;96.3) e 1 registro (cfr. art 15); v. i consideranda nn. 107 e 108.

stati normati nel dettaglio dall'EBA[20]. L'attenzione prestata dalla PSD2 ai profili di sicurezza informatica a tutela della integrità e continuità operativa dell'intermediario, e nondimeno a tutela delle ragioni patrimoniali e personali degli utenti dei servizi, già a partire dalla fase di valutazione dei requisiti per la concessione dell'autorizzazione all'intermediario, e successivamente nello svolgimento dell'attività di vigilanza, costituisce un elemento di forte novità della seconda direttiva sui servizi di pagamento e testimonia, nonostante il tempo relativamente breve dall'emanazione della PSD1, la profonda evoluzione avvenuta nell'attività di questi intermediari i cui servizi sono stati segnati da una profonda rivoluzione tecnologica di cui occorre tener conto nello svolgimento dell'attività di controllo e vigilanza. Nella valutazione di tali profili non può escludersi l'esercizio di una discrezionalità tecnica da parte dell'Autorità di vigilanza designata anche con riferimento alla richiesta di registrazione presentata dagli AISPs.

Il rilascio dell'autorizzazione per l'esecuzione dei servizi di disposizione d'ordine dà luogo, come per gli altri servizi di pagamento, all'iscrizione dell'istituto richiedente e dei relativi agenti in un pubblico registro liberamente consultabile, accessibile *on line* e tempestivamente aggiornato, presso lo Stato membro di origine (art. 14, commi 1 e 2, PSD2). Medesima pubblicità viene osservata per i provvedimenti di revoca delle autorizzazioni e di revoca delle esenzioni[21]; nello stesso registro sono separatamente iscritte anche le persone fisiche o giuridiche che sono state registrate per lo svolgimento dei soli servizi di informazione sui conti e sono pubblicizzati i provvedimenti di revoca di detta registrazione[22].

---

[20] Cfr. EBA/GL/2017/09, dell'11 luglio 2017, *on the information to be provided for the authorisation of payment institutions and e-money institutions and for the registration of account information service providers*, in attuazione dell'art. 5.5 della PSD2. Ivi si indicano le informazioni che devono essere fornite per ottenere l'autorizzazione ad operare come istituto di pagamento, distinguendo a seconda che si intendano prestare solo i servizi da 1 a 7 dell'allegato I della direttiva (quindi compresi i PIS), ovvero soltanto i servizi di informazione di cui al n. 8. Tuttavia, il tema delle informazioni concernenti i presidi di sicurezza informatica e di protezione dei dati sensibili è trattato nelle *guidelines* in maniera uguale a prescindere dalla diversità dei servizi, cfr. al riguardo *guidelines* nn. 4.1. 9-13 (per i servizi da n.1 a n.7) e 4.2. 7-10 (per i servizi di cui al n. 8).

[21] Oltre alle esenzioni previste dall'art. 33, che riguardano specificamente i prestatori di servizi di informazione sui conti, ai quali in verità la stessa direttiva riserva una disciplina distinta dagli altri istituti di pagamento, si tratta delle esenzioni concesse a norma dell'art. 32 che, tuttavia, sono testualmente limitate agli IP che svolgono i servizi di pagamento indicati nei numeri da 1 a 6 dell'allegato I; pertanto, sulla base del dato letterale dell'art. 32 non sembra possa farsi luogo a forme di esenzione dell'applicazione della disciplina in capo all'istituto di pagamento che svolge l'attività di prestazione di disposizioni di ordini di pagamento, di cui al n. 7 dell'allegato I; d'altro canto, quest'ultima attività non viene indicata neanche nell'art. 33.

[22] L'art. 14, par. 3, PSD2 letteralmente indica "*la revoca... di esenzioni concesse a norma degli articoli 32 o 33*", e quest'ultimo articolo, come già rilevato, contiene l'indicazione della disciplina speciale e semplificata dei prestatori di servizi di informazioni sui conti che il legislatore dell'Unione qualifica come regime legale di esenzione. Dunque, laddove l'articolo 14 prevede la pubblicità della revoca dell'esenzione concessa a norma dell'art. 33 deve ritenersi che si voglia fare riferimento alla revoca della registrazione dell'istituto che svolge soltanto il servizio di informazione sui conti.

L'European Banking Authority detiene inoltre un proprio registro elettronico centrale, di nuova istituzione, nel quale vengono concentrate tutte le informazioni iscritte nei rispettivi registri nazionali. Il registro dell'EBA, pubblicato sul sito *web* dell'Autorità e consultabile gratuitamente, deve consentire al cittadino facile accesso e agevole ricerca delle informazioni[23].

Anche gli istituti di pagamento che svolgono il ruolo di TPPs, ivi compresi gli AISPs registrati, sono pertanto soggetti alla vigilanza informativa e ispettiva delle autorità nazionali competenti (art. 23, comma 1, par. 2, lett. *a)* e *b)* [24]), nonché alle disposizioni di *soft law* (raccomandazioni e orientamenti) e ai provvedimenti amministrativi vincolanti di queste ultime (art. 23, comma 1, par. 2 lett. *c*)). L'autorità può adottare provvedimenti di sospensione o revoca dell'autorizzazione al ricorrere delle condizioni previste dall'art. 13 della PSD2 (art. 23, comma 1, par. 2 lett. *d*)) e comminare sanzioni amministrative nei confronti di detti intermediari o di coloro che di fatto controllano l'attività degli istituti di pagamento che si sono resi colpevoli di infrazioni alle disposizioni legislative, regolamentari o amministrative in materia di vigilanza o di esercizio dell'attività di servizi di pagamento, o adottare nei loro confronti provvedimenti la cui applicazione è diretta specificamente a far cessare le infrazioni accertate o a rimuoverne le cause (art. 23, comma 2)[25].

I prestatori di servizi di informazioni sui conti sono esentati in generale dal rispetto delle disposizioni che attengono al capitale iniziale e al capitale di funzionamento, nonché alla tutela dei fondi dei clienti, poiché non ne detengono, e alle disposizioni concernenti il ricorso ad agenti o entità cui vengono esternalizzate attività[26], per il resto, come detto, anch'essi sono sottoposti alla vigilanza della competente autorità.

---

[23] Il 13 dicembre 2017 l'EBA ha pubblicato il Rapporto finale contenente il progetto di norme tecniche di regolamentazione che definiscono i requisiti tecnici relativi allo sviluppo, alla gestione e al mantenimento del registro elettronico centrale e all'accesso alle informazioni ivi contenute nonché il progetto di norme tecniche di attuazione in merito ai dettagli e alla struttura delle informazioni inserite nei registri nazionali e trasmesse dalle competenti autorità nazionali all'EBA (EBA/RTS/2017/10 e EBA/ITS/2017/07).

[24] L'art. 23, comma 3, PSD2, concernente i controlli volti a garantire un capitale sufficiente per i servizi di pagamento, specie quando, trattandosi di un istituto ibrido, lo svolgimento di altre attività commerciali ne danneggi o rischi di danneggiarne la solidità finanziaria, non si applica agli AISPs ai quali non è richiesto il rispetto di un requisito di capitale.

[25] Come si ricava dall'art. 33, comma 1, PSD2, il citato art. 23, paragrafo 1 e 2 (contenuto nella Sezione 3, Titolo II, PSD2) è certamente applicabile anche agli AISPs, che sono invece esonerati dall'applicazione delle procedure e delle condizioni di cui alle sezioni 1 e 2 del titolo II della direttiva, fatta eccezione per l'art. 5, paragrafo 1, lett. a), b), da e) a h), j), l), n), p) e q) (informazioni da fornire per l'autorizzazione); per l'art. 5, paragrafo 3 (domanda di registrazione); nonché per gli articoli 14 (iscrizione nello Stato membro) e 15 (registro europeo dell'EBA). Della sezione terza non si applica soltanto l'art. 23, paragrafo 3, concernente le misure per garantire il capitale sufficiente per i servizi di pagamento, coerentemente con il fatto che questi soggetti – come già detto – non hanno obblighi di capitale minimo.

[26] Cfr. art. 33, par. 1, PSD2.

2.2 La disciplina nazionale

La PSD2 è stata recepita nel nostro Paese con il decreto legislativo n. 218/2017[27], che ha aggiornato, da un lato, il testo unico bancario, nelle parti in cui esso disciplina gli istituti di pagamento (Titolo V-ter) e la trasparenza dei rapporti dei prestatori di servizi di pagamento con i clienti (Titolo VI), dall'altro, il decreto legislativo n. 10/2011, per i profili concernenti i rapporti contrattuali tra i prestatori di servizi di pagamento e i clienti[28]. Trattandosi di una direttiva di armonizzazione massima, volta a garantire un'applicazione uniforme del quadro legislativo in tutta l'Unione, sono stati pochi gli spazi di discrezionalità esercitati dal legislatore nazionale.

In sede di recepimento è stata quindi ampliata la definizione normativa dei servizi di pagamento, ricomprendendovi anche il servizio di disposizione di ordini di pagamento e quello di informazione sui conti (cfr. art. 1, lett. h-*septies*.1, nn.7) e 8) TUB) che, al pari degli altri servizi di pagamento, sono adesso riservati ai prestatori di servizi di pagamento (art.114-*sexies* TUB); tale riserva risulta penalmente presidiata dalla fattispecie criminale già prevista dall'art. 131-*ter* TUB. A tal proposito, deve rilevarsi che non sembra ostare all'applicazione di tale fattispecie penale anche all'esercizio abusivo della prestazione di servizi di informazione sui conti il fatto che il citato art. 131-*ter* individui l'abusivismo nell'assenza dell'autorizzazione disciplinata dall'art. 114-*novies*. Infatti, ancorché la PSD2 qualifichi il provvedimento di accesso allo svolgimento di tali servizi come una registrazione, e non come un'autorizzazione, nella disciplina di recepimento la differenziazione del regime di ingresso sul mercato degli AISPs rispetto agli altri istituti si affievolisce, essendo richiesta anche per i primi – in linea con le previsioni dell'Unione – una verifica del possesso di requisiti tecnici rimessa alla valutazione tecnico discrezionale della Banca d'Italia, quale autorità nazionale competente. Pertanto, al di là della diversa qualificazione nominalistica del provvedimento adottato dall'Autorità, esso resta contrassegnato dall'esercizio di una discrezionalità tecnica in merito all'accertamento dei requisiti di iscrizione che, nel nostro ordinamento, caratterizza i provvedimenti autorizzativi. In concreto, anche per gli AISPs l'Autorità non dovrà limitarsi ad una mera ricognizione di elementi oggettivi di cui prendere atto per far luogo alla necessaria registrazione del prestatore, piuttosto dovendo verificare il possesso in capo ai richiedenti di specifici requisiti tecnici, ancorché semplificati rispetto a quelli imposti agli altri istituti di pagamento in considerazione delle peculiari caratteristiche del servizio di informazione sui conti; essa è quindi tenuta a condurre un accertamento tecnico discrezionale utilizzando i parametri valutativi da essa individuati in linea con la disciplina primaria. A questo proposito, si può menzionare la necessità di vagliare: il programma di attività relativo allo

---

[27] I criteri di delega sono contenuti nell'articolo 12 della legge 12 agosto 2016, n. 170 (legge di delegazione europea 2015).

[28] Il medesimo decreto legislativo contiene le norme di attuazione del Regolamento (UE) n. 751/2015 del Parlamento europeo e del Consiglio, del 29 aprile 2015, relativo alle commissioni interbancarie sulle operazioni di pagamento basate su carta; a tal fine esso si è arricchito del titolo IV bis.

specifico tipo di servizi di pagamento; il piano aziendale per verificare che il richiedente sia in grado di utilizzare i sistemi, le risorse e le procedure adeguati e proporzionati ai fini di una sana gestione; la procedura di monitoraggio e gestione degli incidenti relativi alla sicurezza; la procedura di archiviazione, monitoraggio e gestione dei dati sensibili relativi ai pagamenti; la procedura che assicuri la continuità operativa; il documento relativo alla politica di sicurezza, la copertura assicurativa o la stipula di un'analoga garanzia per la responsabilità nei confronti del prestatore di servizi di pagamento di radicamento del conto o dell'utente dei servizi di pagamento derivante dall'accesso non autorizzato o fraudolento alle informazioni del conto di pagamento o dall'uso non autorizzato o fraudolento delle stesse. Si tratta di esaminare preliminarmente procedure e documenti che impongono una valutazione di merito ancorché di carattere tecnico da parte dell'Autorità, che dunque non è chiamata a registrare automaticamente il prestatore che abbia fatto richiesta di svolgere i servizi di AIS.

La Banca d'Italia, d'altro canto, coerentemente con l'attribuzione di un potere di verifica dei requisiti di accesso al mercato degli AISPs di carattere non meramente ricognitivo, nella propria disciplina attuativa (nella versione messa in consultazione nel luglio 2018[29]) qualifica il proprio provvedimento come autorizzazione (e non registrazione) anche con riferimento ai prestatori che svolgono servizi di informazioni sui conti.

I requisiti per il rilascio dell'autorizzazione allo svolgimento dei servizi di pagamento, ivi inclusi quelli di disposizione di ordini di pagamento, già indicati nell'art.114-*novies*, comma 1, TUB, non sono stati modificati in seguito al recepimento della PSD2 se non per introdurre in capo agli istituti che intendono svolgere i nuovi servizi l'obbligo di stipulare "*una polizza di assicurazione della responsabilità civile o analoga forma di garanzia per i danni arrecati nell'esercizio dell'attività derivanti da condotte proprie o di terzi*" (art. 114-*novies*, comma 1-*bis*, TUB)[30].

La disciplina primaria di recepimento non ha valorizzato le nuove indicazioni contenute nell'art. 5 della PSD2 in merito ai requisiti per l'autorizzazione,

---

[29] Cfr. Provv. BI del 23 luglio 2019 recante modifiche alle disposizioni di vigilanza per gli istituti di pagamento e gli istituti di moneta elettronica in attuazione della Direttiva 2015/2366/UE; il provvedimento modificato è stato adottato il 17 maggio 2016. Nell'ambito del capitolo II, che disciplina l'autorizzazione degli istituti di pagamento, è regolata (alla sezione VI bis) la domanda per l'esercizio del servizio di informazione sui conti, alla quale si applica la disciplina dell'autorizzazione indicandosi espressamente le norme o plessi di norme non applicabili, quali quelli in materia di capitale minimo, in materia di assetto proprietario e quelli concernenti le misure per tutelare i fondi ricevuti dalla clientela, confermandosi invece l'applicabilità della restante regolamentazione.

[30] In effetti, agli istituti che svolgono servizi di informazione sui conti si applica l'art. 114-*novies* (tranne i commi 4 e 5) relativo ai requisiti necessari per ottenere l'autorizzazione; pertanto, nonostante secondo il dato letterale dell'art. 114-*novies*, comma 1-*bis*, l'obbligo della polizza assicurativa sia espressamente riferito soltanto agli istituti che svolgono il servizio di disposizione di ordini di pagamento, esso deve ritenersi applicabile anche per gli AISPs. Cfr. anche "Modifiche alle disposizioni di vigilanza per gli istituti di pagamento e gli istituti di moneta elettronica in attuazione della Direttiva 2015/2366/UE" introdotte con il Provv. BI del 23 luglio 2019.

segnatamente quelli concernenti la politica di sicurezza, la prevenzione dei rischi relativi ai servizi offerti, compresi quelli derivanti da frode e uso illegale di dati sensibili, il monitoraggio e la gestione degli incidenti relativi alla sicurezza e i reclami dei clienti in materia di sicurezza. Tuttavia, il carattere cogente delle disposizioni di dettaglio emanate a tale proposito dall'EBA[31], alla cui applicazione fanno rinvio anche le norme secondarie messe in consultazione dalla Banca d'Italia, di fatto consente di superare tale lacuna senza pregiudizio per l'uniformità applicativa della direttiva con riguardo ai requisiti di sicurezza informatica da predisporre a tutela dell'intermediario e degli utenti dei servizi di pagamento e di cui l'intermediario stesso deve dar conto già in sede di richiesta di autorizzazione.

Il tema della sicurezza interessa le modifiche alle disposizioni secondarie di vigilanza, in linea con quanto richiesto dalla Direttiva e dagli orientamenti dell'EBA[32], con riferimento al governo societario e all'organizzazione amministrativa degli istituti di pagamento. In tale ambito, infatti, è previsto un rafforzamento delle misure organizzative di cui gli IP devono dotarsi per garantire un più efficace presidio dei rischi, in particolar modo di quelli relativi alla sicurezza dei pagamenti. A questo fine le disposizioni prevedono l'adozione di politiche di governo e procedure per la gestione della sicurezza relativa alla prestazione dei servizi di pagamento nonché sistemi di valutazione e risposta ai reclami dei clienti[33].

Con riferimento anche ai nuovi istituti di pagamento aventi sede in Italia, ove deve essere svolta almeno una parte della loro attività di erogazione di servizi di pagamento (art. 114-*novies,* comma 1*,* lett. b), competono alla Banca d'Italia il rilascio dell'autorizzazione all'esito della verifica dei requisiti previsti dalla legge e dalla disciplina secondaria (art. 114-*novies*, TUB), la verifica nel continuo del possesso di detti requisiti attraverso l'azione di vigilanza, nonché la tenuta dell'albo nazionale, consultabile liberamente *on line (art. 114-septies,*TUB). In particolare, per gli istituti di pagamento che svolgono attività di disposizione di ordini di pagamento, l'albo pubblicizza adesso anche i dati identificativi della

---

31 Cfr. EBA/GL/2017/09, dell'11 luglio 2017, in attuazione dell'art. 5.5 della PSD2, v. *supra*.

32 Le disposizioni della Vigilanza richiamano a tal proposito la diretta applicazione degli "*Orientamenti finali in materia di segnalazione dei gravi incidenti ai sensi della direttiva 2015/2366/UE (PSD2), emanati dall'EBA il 19 dicembre 2017"* e gli *"Orientamenti finali sulle misure di sicurezza per i rischi operativi e di sicurezza dei servizi di pagamento ai sensi della direttiva 2015/2366/UE (PSD2), emanati dall'EBA il 12 gennaio 2018*".

33 Cfr. Cap. VI, Sez. I, del citato provvedimento della Banca d'Italia, ove si richiede agli IP: l'adozione di procedure e sistemi idonei a: 1. tutelare la sicurezza, l'integrità e la riservatezza delle informazioni, tenendo conto della natura delle informazioni medesime; 2. archiviare e gestire i dati sensibili relativi ai pagamenti, con gli opportuni limiti di accesso; 3. acquisire dati statistici relativi ai risultati della gestione, alle operazioni di pagamento effettuate e alle frodi. Gli IP sono tenuti ad adottare politiche, sistemi, risorse e procedure per la continuità e la regolarità dei servizi, in particolare per assicurare la continuità operativa, specie per garantire la regolare esecuzione delle operazioni di pagamento, nonché la limitazione delle perdite nel caso di interruzioni di operatività. Tutti aspetti rimessi all'accertamento tecnico discrezionale dell'Autorità di vigilanza.

polizza assicurativa o dell'analoga garanzia di cui tali intermediari devono obbligatoriamente dotarsi.

I soggetti che prestano esclusivamente servizi di informazione sui conti sono iscritti in una sezione speciale dell'albo degli istituti di pagamento, che parimenti ne pubblicizza anche la polizza assicurativa obbligatoria. Coerentemente con le disposizioni della PSD2, i requisiti che consentono agli AISPs l'iscrizione nell'albo risultano semplificati rispetto a quelli imposti agli altri istituti di pagamento, non essendo richiesta l'indicazione di un capitale, né il possesso di specifiche qualità in capo ai titolari di partecipazione azionaria. Tuttavia, non sembra che tale semplificazione possa condurre a ritenere che gli AISPs siano soggetti ad una mera registrazione nell'albo in considerazione della necessaria attività valutativa tecnico discrezionale rimessa alla Banca d'Italia per accertare il possesso dei requisiti di iscrizione all'albo, la cui permanenza nel continuo è poi assicurata dal successivo esercizio dell'azione di vigilanza.

Si osserva, inoltre, che l'art. 114-*novies* TUB continua ad indicare quale forma giuridica necessaria per lo svolgimento di tale attività di impresa quella sociale (per azioni, in accomandita per azioni, a responsabilità limitata o cooperativa) ancorché il dettato della PSD2 prevedesse anche le persone fisiche tra i possibili soggetti richiedenti la registrazione per lo svolgimento del servizio di informazione sui conti; di tale allargamento soggettivo tengono conto anche gli orientamenti dell'EBA, che – come detto – contengono le regole di dettaglio per la compilazione della richiesta di registrazione e, a tal fine, contemplano anche l'ipotesi che richiedente sia una persona fisica.

Il diverso regime normativo degli istituti che svolgono soltanto servizi informativi sui conti è riassunto nel nuovo art. 114-*septiesdecies* TUB, che contiene il catalogo delle disposizioni relative agli istituti di pagamento che non trovano applicazione agli AISPs, nonché l'indicazione di alcuni articoli che, al contrario, devono ritenersi di applicazione necessaria. Con riguardo al primo tipo di disposizioni deve rilevarsi che gli istituti che svolgono soltanto le attività di informazione non possono svolgere anche attività accessorie di concessione di credito e di prestazione di garanzia o di gestione di sistemi di pagamento (art. 114-*octies* TUB), possono svolgere invece altre attività imprenditoriali ed esse non devono essere valutate dalla Banca d'Italia ai fini dell'autorizzazione (art. 114-*novies*, commi 4 e 5 TUB), tenuto conto che la loro ponderazione rileva piuttosto ai fini della copertura assicurativa obbligatoria (come si ricava dall'art. 5.4 della PSD2 e dai relativi orientamenti dell'EBA)[34]; a tali soggetti, ove costituiti in forma societaria, non si applicano le norme di tutela sulle partecipazioni azionarie, né quelle concernenti i requisiti di onorabilità e correttezza dei partecipanti al capitale (art.114-*undecies*, commi 1 e 1*ter*, TUB); inoltre non si applicano le disposizioni concernenti i conti di pagamento

[34] La disposizione nazionale è coerente con l'art. 18 PSD2, comma 1, lett. c), che dispone che gli istituti di pagamento sono autorizzati ad esercitare "*attività commerciali diverse dalla prestazione di servizi di pagamento, tenuto conto delle disposizioni dell'Unione e nazionali applicabili*".

e il patrimonio destinato (114-*duodecies* e 114-*terdecies* TUB), considerato che gli istituti che svolgono soltanto servizi di informazione sui conti, come già ricordato, non possono detenere fondi dei clienti; infine è esclusa la possibilità di ottenere dalla Banca d'Italia un regime di esenzione (totale o parziale) da alcune disposizioni dettate per gli istituti di pagamento (114-*sexiesdecies* TUB). Ad essi non si applicano le disposizioni contenute nel titolo VI del TUB concernenti la trasparenza delle condizioni contrattuali e i rapporti con i clienti (art.114-*undecies*, commi 1, TUB).

L'art. 114-*septiesdecies* TUB contiene poi un secondo gruppo di disposizioni, tutte ricomprese nell'ambito del titolo VI del TUB – che, in generale, non è applicabile agli AISPs – e ne ribadisce espressamente l'applicazione agli istituti che svolgono i servizi di informazione sui conti[35]. Tale elencazione potrebbe far dubitare del fatto che le altre disposizioni del TUB, in quanto non espressamente richiamate, debbano intendersi per ciò non applicabili. A tal proposito, sembra preferibile ritenere che esse devono piuttosto considerarsi applicabili se compatibili con la peculiarità del servizio di informazione sui conti, considerato che tale servizio, al pari di quello di disposizione di ordine di pagamento, e a differenza di tutti gli altri servizi di pagamento non comporta la tenuta di conti di pagamento né la gestione di fondi. Coerentemente deve ritenersi che gli AISPs, alla stregua di tutti gli istituti di pagamento, siano soggetti all'art. 114-*quaterdecies* TUB, che disciplina l'azione di vigilanza della Banca d'Italia, nonché anche alle disposizioni sanzionatorie contenute nel titolo VIII TUB, in particolare quelle amministrative irrogabili dalla medesima Autorità, malgrado anche tali disposizioni non siano espressamente richiamate nel citato art. 114-*sepiesdecies,* né per affermare né per escluderne l'applicazione. Ciò nella misura in cui gli obblighi violati richiamati dalla disciplina sanzionatoria siano riferibili anche agli istituti di pagamento nel cui novero sono certamente ricompresi anche gli AISPs.

In relazione al regime giuridico dei nuovi soggetti sottoposti ad autorizzazione[36], rileva certamente il richiamo alle norme concernenti il controllo pubblico sui presidi aziendali connessi con la correttezza delle relazioni con la clientela: infatti sia gli AISPs che i PISPs, per gli aspetti della "trasparenza contrattuale" regolati dal titolo VI TUB ad essi applicabili, devono considerarsi sottoposti al potere di vigilanza della Banca d'Italia (art. 128 TUB), legittimata

---

[35] Si tratta degli art. 126-*bis*, comma 4 (onere della prova dell'adempimento degli obblighi di trasparenza); 126-*quater*, comma 1, lett. a) (soggezione alla disciplina regolamentare della Banca d'Italia concernente i contenuti e le modalità delle informazioni e condizioni che il PSP fornisce o rende disponibili all'utilizzatore di servizi di pagamento, al pagatore e al beneficiario); 128 (soggezione a vigilanza informativa e ispettiva per il rispetto delle disposizioni in materia di trasparenza); 128-*bis* (adesione ai sistemi di risoluzione stragiudiziale delle controversie con la clientela); 128-*ter* (Misure inibitorie adottate dall'autorità di Vigilanza).

[36] Dell'applicazione del titolo VI anche agli istituti che eseguono disposizioni di ordini di pagamento non sembra possa dubitarsi, anche in assenza di norme espresse in tal senso, considerato che tali soggetti possono certamente ricomprendersi nella generale categoria di IP autorizzati e per essi non è dettata una distinta disciplina in ambito nazionale. Come rilevato nel testo, dovrà piuttosto escludersi l'applicazione di quelle norme che presuppongono l'esercizio di attività precluse ai PISPs, al pari di quanto rilevato per gli AISPs.

ad acquisire informazioni, atti e documenti, a eseguire ispezioni mirate anche presso tali istituti e ad adottare le misure inibitorie previste dall'art. 128-*ter* TUB, qualora nell'esercizio dell'attività di vigilanza finalizzata a verificare il rispetto della "trasparenza" essa riscontri il compimento di irregolarità da parte di tali istituti: in particolare, essa può, a tal fine, sospendere o inibire la continuazione dei servizi di pagamento da essi offerti con eventuale pubblicazione dei provvedimenti inibitori adottati[37].

I nuovi istituti di pagamento devono obbligatoriamente aderire ai sistemi di risoluzione stragiudiziale delle controversie con la clientela come previsto dall'art. 128-*bis* TUB.

3. Le caratteristiche dello svolgimento dei nuovi servizi codificati nell'art. 1, nn. 7 e 8 dell'allegato I della direttiva: la relazione tra TPPs e prestatori di radicamento del conto

Un aspetto peculiare delle nuove attività di pagamento è la fisiologica triangolazione tra i TTPs e, da un lato, i titolari dei conti di pagamento, per i quali i TTPs eseguono la disposizione di bonifico o svolgono il servizio di informazione dei conti, e, dall'altro, gli intermediari presso i quali tali conti sono accesi (o radicati, secondo l'espressione utilizzata nella traduzione della PSD2). Ulteriore elemento caratterizzante questi servizi di pagamento è l'utilizzo necessario dello strumento telematico tanto per il loro svolgimento quanto per stabilire le connessioni ad esso strumentali verso tutti i soggetti coinvolti nell'operazione. Tale triangolazione telematica è stata oggetto di attenzione proprio per gli aspetti di rischio connessi ad ipotesi di frode informatica, che possono inficiare la sicurezza della catena di pagamento nella quale sono coinvolti di necessità plurimi intermediari, nonché per gli aspetti legati alla eventuale responsabilità connessa alla mancata o inesatta esecuzione del pagamento o all'esecuzione non autorizzata dell'ordine di pagamento.

I TTPs, infatti, hanno un rapporto contrattuale con il soggetto pagatore, per conto del quale dispongono l'ordine di bonifico, o con l'utente al quale forniscono le informazioni sui conti; essi, invece, non sono obbligati ad instaurare un rapporto contrattuale con i prestatori di servizi di pagamento di radicamento del conto, con

---

[37] Cfr. Provvedimento Banca d'Italia 5 dicembre 2018, in G.U. 19 dicembre 2018, n. 294 (*Disposizioni in materia di trasparenza delle operazioni e dei servizi bancari e finanziari – correttezza delle relazioni tra intermediari e clienti*), nel quale sono disciplinate le procedure e le iniziative organizzative che gli intermediari debbono porre in essere in relazione all'attività avente a oggetto le operazioni e i servizi disciplinati ai sensi del titolo VI del TUB, nonché Provvedimento Banca d'Italia 19.3.2019 (*Disposizioni di recepimento della direttiva 2015/2366/UE (PSD2) e altri interventi)* con il quale sono state apportate "*Modifiche alle disposizioni in materia di trasparenza delle operazioni e dei servizi bancari e finanziari – Correttezza delle relazioni tra intermediari e clienti*" del 29 luglio 2009.

cui tuttavia devono necessariamente interagire (digitalmente) per l'esecuzione dei loro servizi[38].

La PSD2, nel chiaro intento di promuovere la diffusione dei bonifici digitalizzati, anche implementando i nuovi servizi tecnologici che ne facilitano l'utilizzo, ha sottratto all'autonomia privata dei prestatori di radicamento del conto la scelta di dialogare con i nuovi IP e ha previsto che gli istituti di pagamento che forniscono servizi di disposizione di ordine di pagamento (art. 66, par. 5) e di informazione sui conti (art. 67, par. 4) non necessitano di una relazione contrattuale con la banca o con il diverso prestatore che detiene il conto, i quali, dal canto loro, non possono rifiutare l'accesso ai conti né discriminare i TPPs (cfr. artt. art. 66, par. 4, lett. b) e c); art. 67, par. 3, lett. b)).

La volontà del legislatore europeo di facilitare l'utilizzo generalizzato dei nuovi strumenti si concretizza nell'attribuzione di un diritto in capo al pagatore di avvalersi di un prestatore di servizi di disposizione di ordine di pagamento (art. 66, par. 1, PSD2), nonché nel diritto di ricorrere a servizi che consentono l'accesso alle informazioni sui conti di cui al punto 8 dell'allegato I (art. 67, par.1 PSD2), con la conseguenza che i prestatori di servizi di pagamento di radicamento del conto di pagamento *on line* hanno l'obbligo di rendersi telematicamente accessibili a tali *third parties* e, a questo fine, hanno anche l'onere di dotarsi di una struttura informatica che possa consentire l'interazione sicura con gli intermediari dei nuovi servizi.

L'obbligatorietà dell'*apertura* del conto da parte del prestatore di pagamento che lo detiene costituisce la conseguenza necessaria del diritto introdotto in capo all'utente di disporre ordini di bonifico (art. 66, par. 1, PSD2) e di acquisire informazioni sui propri conti *on line* (art. 67, par. 1, PSD2), avvalendosi all'occorrenza di un prestatore di servizi diverso da quello di radicamento del conto.

I conti di pagamento nel loro insieme finiscono con il rivestire il ruolo di un'*essential facility* e la previsione di un'obbligatoria accessibilità consente di garantire la piena concorrenza tra tutti i prestatori di servizi di pagamento, anche non bancari, che operano sulla rete dei conti nell'interesse dell'utente finale dei servizi.

In definitiva, i PSPs che detengono i conti di pagamento non possono rifiutare l'accesso né discriminare i TPPs anzi, come detto, sono onerati dell'adeguamento della loro infrastruttura tecnologica per consentire l'accesso sicuro ai conti da parte dei TPPs.

---

[38] M. Catenacci e C. Fornasaro, *PSD2: i prestatori di servizi d'informazione sui* conti *(AISPS) cit.,* p. 8, con riferimento agli AISPS sottolineano come, anche in assenza di un obbligo normativo, sia opportuno che il rapporto tra il prestatore di radicamento del conto e il TPP sia regolato contrattualmente dal momento che l'art. 5-*quater* d.lgs. n. 11/2010 prevede che "*gli stessi debbano comunicare tra di loro in maniera sicura, conformemente all'art. 98(1)(d) della PSD2 e alle relative norme tecniche di regolamentazione adottate dalla Commissione europea*".

La disciplina nazionale ha puntualmente recepito la previsione secondo cui lo svolgimento del servizio di disposizioni di ordine di pagamento e quello di informazione sui conti non sono subordinati all'esistenza di un rapporto contrattuale tra il TPPs e il prestatore di servizi di pagamento di radicamento del conto (cfr. artt. 5-*ter*, comma 1, e 5-*quater*, comma 1, d.lgs. n. 11/2010).

Quest'ultimo, al fine di garantire l'esercizio del diritto del pagatore di avvalersi del servizio di disposizione di ordine di pagamento, è tenuto a comunicare in maniera sicura con i prestatori di servizi di disposizione di ordine di pagamento; a fornire a tali prestatori tutte le informazioni disponibili in merito all'ordine di pagamento e alla relativa esecuzione; ad assicurare la parità di trattamento agli ordini trasmessi mediante un prestatore di servizi di disposizione di ordine e a quelli trasmessi direttamente dal pagatore, fatte salve ragioni obiettive riferibili ai tempi, alla priorità o alle spese applicabili (art. 5-*ter*, comma 3, d.lgs. n. 11/2010).

Analogamente il prestatore di servizi di pagamento di radicamento del conto è obbligato a comunicare in maniera sicura con i prestatori di servizi di informazione sui conti e ad assicurare la parità di trattamento alle richieste di dati trasmesse dal prestatore di servizi di informazione sui conti e a quelle trasmesse direttamente dall'utente, fatte salve ragioni obiettive (art. 5-*quater*, comma 3, d.lgs. n. 11/2010).

3.1 L'accesso ai conti: l'art. 98 della PSD2, gli standard tecnici dell'EBA e il regolamento delegato (UE) 2018/389

Le modalità di accesso ai conti risultano dunque cruciali per non pregiudicare la sicurezza dei fondi e quella dei dati di pagamento e per prevenire le frodi informatiche; per tale ragione la direttiva si è preoccupata di disciplinarne le caratteristiche dettando misure alle quali devono attenersi tutti i soggetti coinvolti nell'operazione di pagamento, PISPs, AISPs, da un lato[39], e prestatori di radicamento del conto, dall'altro. Essi, infatti, devono reciprocamente comunicare "*in maniera sicura conformemente all'articolo 98, paragrafo 1, lett. d)*" della PSD2, vale a dire nel rispetto delle norme tecniche che sono state introdotte *i)* per assicurare un livello adeguato di sicurezza per gli utenti e i prestatori di servizi di pagamento mediante l'adozione di requisiti efficaci e basati sul rischio; *ii)* per assicurare la sicurezza dei fondi e dei dati personali degli utenti; *iii)* per garantire e mantenere la concorrenza equa tra i prestatori di servizi di pagamento; *iv)* per assicurare la neutralità dei modelli tecnologici e commerciali e permettere lo sviluppo di mezzi di pagamento accessibili, innovativi e di facile utilizzo.

---

[39] Queste misure si applicano anche all'operazione di conferma della disponibilità di fondi su richiesta di un prestatore di servizi di pagamento emittente strumenti di pagamento basati su carta (v. *supra* nota n. 11).

Piuttosto che disciplinare nel dettaglio le misure tecniche da adottare per assicurare la comunicazione sicura, che avrebbe comportato il rischio di adottare misure rapidamente superate dall'evoluzione tecnologica e di imporre l'utilizzo di alcune tecnologie che possono costituire un ostacolo all'ingresso sul mercato di nuovi operatori, la regolamentazione si è ispirata al criterio della neutralità tecnologica, fissando soltanto alcuni principi da rispettare e da perseguire attraverso la standardizzazione e indicando una serie di obiettivi e di finalità da assicurare nell'esecuzione dell'operazione di pagamento[40].

Nel regolamento delegato (UE) 2018/389 della Commissione del 27 novembre 2017[41] sono stati definiti i requisiti, già oggetto di un progetto di norme tecniche di regolamentazione dell'EBA[42], concernenti gli standard aperti che occorre rispettare per assicurare comunicazioni comuni e sicure ai fini dell'identificazione, dell'autenticazione, della notifica e della trasmissione di informazioni, nonché dell'attuazione delle misure di sicurezza, tra i prestatori di servizi di pagamento di radicamento del conto, i prestatori di servizi di disposizione di ordine di pagamento, i prestatori di servizi di informazione sui conti, i pagatori, i beneficiari e altri prestatori di servizi di pagamento.

La standardizzazione tecnica e l'interoperabilità sono elementi fondamentali di un ambiente di pagamento articolato in reti; in particolare l'interoperabilità tra i diversi sistemi basata su norme comuni è indispensabile per massimizzare la diffusione degli strumenti di pagamento elettronico tra pagatori, beneficiari e relativi prestatori di servizi di pagamento anche a livello transfrontaliero e gli standard tecnici permettono all'industria di innovarsi sfruttando gli avanzamenti della tecnologia e al contempo di rispondere alle future minacce alla sicurezza dei pagamenti.

Il regolamento della Commissione ribadisce l'obbligo (già previsto dall'art. 97, comma 1, PSD2) dei prestatori di servizi di pagamento di applicare

---

40 Sul tema della neutralità tecnologica come fattore fondamentale per realizzare la maggiore interoperabilità tra sistemi cfr. E. Cervone, *Strumenti di pagamento innovativi, interoperabilità e neutralità tecnologica cit.*, p. 61: "*neutralità tecnologica è sinonimo del termine "standard di prestazione", che sono gli standard che descrivono il risultato previsto, ma non impongono una data tecnologia. Neutralità tecnologica significa, dunque, che i regolatori dovrebbero astenersi dall'usare la regolazione come mezzo per strutturare il mercato in un certo modo. In un mercato altamente competitivo, i regolatori dovrebbero impegnarsi a non scegliere i "vincitori tecnologici*".

41 Il progetto di TS è stato adottato dall'EBA ai sensi dell'art. 98, par. 4, comma secondo, PSD2.

42 Come precisato nei considerando 29 e 30 del regolamento delegato della Commissione, esso si basa sul progetto di norme tecniche di regolamentazione che l'European Banking Authority (come previsto dall'art. 98, par. 4, comma primo, PSD2) ha presentato alla Commissione dopo aver svolto consultazioni pubbliche aperte e trasparenti sul progetto presentato, aver analizzato i potenziali costi e benefici della disciplina e richiesto il parere del gruppo delle parti interessate nel settore bancario, istituito dall'art. 37 del regolamento (UE) n. 1093/2010.

l'autenticazione forte[43] del cliente quando il pagatore accede al suo conto *online*, ovvero quando dispone un'operazione di pagamento elettronico o effettua qualsiasi azione tramite un canale a distanza che possa comportare il rischio di frode nei pagamenti o altri abusi.

Esso disciplina, altresì, le ipotesi di esenzione dall'autenticazione forte[44], individuando alcune fattispecie che, "*in relazione alla tipologia di operazione[45], alle modalità con le quali la stessa è compiuta[46], ai beneficiari del pagamento[47] o, semplicemente, all'importo dell'operazione[48], vengono considerate a basso rischio di frode e, come tali, non necessariamente assoggettabili a sistemi di autenticazione forte*"[49] e consentendo, comunque, al prestatore di fare una valutazione in concreto del grado di rischio dell'operazione in relazione alle circostanze del caso concreto (cd. *targeted authentication*) tenuto conto di una serie precisa di indici forniti dallo stesso regolatore comunitario[50].

Per avvalersi di tali esenzioni si presuppone, comunque, la predisposizione da parte dei prestatori di servizi di pagamento di meccanismi sofisticati di monitoraggio delle operazioni volti a rilevare le operazioni di pagamento non autorizzate o fraudolente e a consentire di calcolare il tasso di frode, disaggregando le operazioni di pagamento sulla base di numerosi indici indicati nel medesimo regolamento (tra cui: l'essere il pagamento a distanza o in presenza; con autenticazione forte o in esenzione; ovvero in base al valore medio delle operazioni) e adempiendo all'obbligo di trasmettere i dati rilevati alle autorità competenti e all'EBA.

---

[43] L'autenticazione forte è quella che consente di verificare l'identità di un utente di servizi di pagamento o la validità dell'uso di uno specifico strumento di pagamento, utilizzando due o più elementi, classificati nelle categorie della conoscenza (qualcosa che solo l'utente conosce), del possesso (qualcosa che solo l'utente possiede) e dell'inerenza (qualcosa che caratterizza l'utente) che sono indipendenti, in quanto la violazione di uno non compromette l'affidabilità degli altri, e che è concepita in modo tale da tutelare la riservatezza dei dati di autenticazione (cfr. art. 4, par. 1, n. 30, PSD2). La nuova definizione di autenticazione fa riferimento ad una procedura che consente non solo di verificare la validità d'uso di uno strumento (come già previsto prima delle modifiche apportate dal d.lgs. n. 218/2017, al riguardo v. M. Mancini, *Commento all'art. 1, comma 1, lettere q e s*, in *La nuova disciplina dei servizi di pagamento* a cura di M. Mancini, M. Rispoli Farina, V. Santoro, A. Sciarrone Alibrandi e O. Troiano, Torino, 2011, p. 26) ma di verificare l'identità di un utente di servizi di pagamento.

[44] Cfr. nel dettaglio, Reg. delegato (UE) 2018/389, capo III, artt. 10-21.

[45] Nel caso, ad esempio, di servizi aventi ad oggetto esclusivamente la consultazione del saldo e delle operazioni di pagamento eseguite negli ultimi 90 gg., ai sensi dell'art. 10 del regolamento di attuazione 2018/389/UE.

[46] Rientrano in tale ipotesi quelle disciplinate dall'art. 12 del regolamento di attuazione 2018/389/UE, che includono i pagamenti effettuati presso terminali non custoditi aventi ad oggetto il pagamento di tariffe di trasporto o di parcheggio.

[47] È il caso dei beneficiari di fiducia (art. 13 del regolamento di attuazione 2018/389/UE) o dei bonifici effettuati tra conti intestati al medesimo soggetto (art. 15 del regolamento di attuazione 2018/389/UE)

[48] Cfr. artt. 11 e 16 del regolamento di attuazione 2018/389/UE.

[49] Così G. Berti De Marinis, *La disciplina dei pagamenti non autorizzati nel nuovo sistema delineato dal recepimento della direttiva PSD2, in Diritto della borsa e del mercato finanziario*, 4/2018, p. 649.

[50] Cfr. art. 18 del regolamento di attuazione 2018/389/UE; sul punto G. Berti De Marinis, *La disciplina dei pagamenti* cit., p. 650. L'Autore ritiene che l'accesso al sistema di esenzione dall'autenticazione forte comporta, comunque, un aggravamento di responsabilità per l'intermediario (salvo il caso di frode del cliente) ai sensi dell'art. 12, comma 2-*bis*, d.lgs. 11/2010.

L'esame nel continuo dei dati di pagamento al fine di controllare le operazioni fraudolente per calcolarne anche la misura percentuale, mettendone a parte le Autorità nazionali e quella di regolazione europea, consente di valutare in concreto il rischio di sicurezza riferito al singolo istituto di pagamento per stimolare l'applicazione di proporzionate misure preventive di sicurezza; d'altro canto, il censimento dei dati da parte dell'Autorità permette di cogliere precocemente segnali di allarme di disfunzioni generalizzate che possono essere prevenute con un aggiornamento tempo per tempo della disciplina concernente le misure di sicurezza che si siano rivelate inadeguate a prevenire il compimento di illeciti.

Il regolamento della Commissione ha fissato altresì i requisiti dell'interfaccia informatica di cui i prestatori di servizi di pagamento di radicamento del conto *on line* sono obbligati a dotarsi per permettere ai nuovi IP di accedere ai conti *ab externo*. L'interfaccia deve consentire l'identificazione del TPP[51], deve permettere al prestatore di servizi di informazione sui conti e al prestatore di servizi di disposizione di ordine di pagamento di comunicare con il PSP di radicamento del conto in maniera sicura e, rispettivamente, di ricevere da esso informazioni su uno o più conti di pagamento e sulle operazioni di pagamento associate; nonché di disporre gli ordini di pagamento e ricevere tutte le informazioni sulla disposizione dell'operazione di pagamento e tutte le informazioni accessibili ai prestatori di servizi di pagamento di radicamento del conto in merito all'esecuzione dell'operazione di pagamento (cfr. art. 30, paragrafi 1-2, reg. cit.)[52].

La struttura informatica necessaria per il dialogo con i TPPs deve avere lo stesso livello di disponibilità e di prestazione delle interfacce messe a disposizione dell'utente per accedere direttamente al proprio conto *on line* e non deve creare impedimenti alla prestazione dei servizi di disposizione di ordine di pagamento e di informazione sui conti. In particolare, possono essere ravvisate condotte di ostacolo quando si impedisca l'utilizzo da parte dei TPPs delle credenziali rilasciate dai prestatori di servizi di pagamento di radicamento del conto ai loro clienti; si imponga il reindirizzamento verso l'autenticazione o altre funzioni del gestore del conto; si richiedano autorizzazioni e registrazioni aggiuntive oltre a quelle previste dalla PSD2 o ulteriori verifiche del consenso dato dagli utenti dei servizi di pagamento.

I prestatori di radicamento del conto (noti anche con l'acronimo ASPSPs: *Account servicing payment service providers*) sono tenuti a predisporre anche misure di emergenza per il caso di indisponibilità non programmata dell'interfaccia o di guasto dei sistemi (art. 33, reg. cit.), ivi inclusa la possibilità che i TPPs accedano alla stessa interfaccia messa a disposizione dei clienti in caso

---

[51] Per consentire la verifica della propria identità, il TPP si avvale dei certificati qualificati di sigillo elettronico o di autenticazione di sito *web* previsti dal regolamento (UE) n. 910/2014, alla cui applicazione fa espresso riferimento l'art. 34, comma 1, Reg. (UE) 2018/389.

[52] Sugli strumenti tramite i quali i prestatori di servizi di pagamento di radicamento del conto devono consentire ai nuovi IP di accedere ai conti *ab externo*, v. il contributo di D. Gammaldi e C. Iacomini in questo *Quaderno*.

di indisponibilità o di prestazioni inadeguate da parte di quella ad essi dedicata (cd. *fall-back option*). Le Autorità nazionali, previa consultazione con l'EBA, possono esentare gli ASPSPs dal dotarsi di queste misure di emergenza se le interfacce dedicate rispettano alcune condizioni di funzionalità indicate nel regolamento (cfr. art. 33, par. 6, reg. cit.), tra cui è prevista anche la sperimentazione sul campo per almeno tre mesi[53].

L'accesso al conto del pagatore può essere anche indiretto (considerando n. 32 della PSD2. Infatti, in alternativa alla creazione di una struttura dedicata, i prestatori che gestiscono il conto di pagamento possono consentire agli istituti che svolgono i nuovi servizi di utilizzare le stesse interfacce già disponibili per l'accesso *on line* da parte dei titolari dei conti, ai fini dell'autenticazione e della comunicazione con il prestatore di servizi di pagamento di radicamento del conto (art. 31 reg. cit.).

I prestatori che gestiscono il conto e i TPPs debbono osservare tecniche di crittografia avanzate e ampiamente riconosciute tra gli operatori al fine di assicurare la riservatezza e l'integrità dei dati durante la sessione di comunicazione e durante lo scambio dei dati via Internet. Il regolamento specifica che ciascuna sessione deve avere una durata quanto più breve possibile e deve essere conclusa in maniera deliberata dopo l'esecuzione della prestazione di pagamento.

Attraverso questa tutela tecnica delle modalità di accesso ai conti si è inteso garantire la sicurezza dei fondi e quella dei dati di pagamento potenzialmente minacciati dalla frode informatica; in questa ottica va letta anche l'esigenza di monitorare nel continuo le ipotesi di malfunzionamento dei sistemi operativi degli istituti, nonché quella di censire tempo per tempo i dati relativi alle frodi allo scopo di aggiornare e implementare nel continuo le misure di sicurezza adeguando se del caso i parametri fissati dalla disciplina europea in funzione di prevenzione del compimento dell'illecito.

Alle norme tecniche di regolamentazione adottate dalla Commissione europea fa espresso rinvio anche la disciplina nazionale di recepimento della PSD2 (cfr. artt. 5-*ter*, comma 2, lett. d), e comma 3, lett. a), nonché art. 5-*quater*, comma 2, lett. c), e comma 3, lett. a), d.lgs. n. 11/2010) per individuare le modalità di comunicazione sicura alle quali sono obbligati tanto i prestatori di servizi di pagamento di radicamento del conto quanto i prestatori di servizi di disposizione di ordine di pagamento e di informazione sui conti.

---

[53] Per chiarire le modalità applicative dei criteri fissati nell'art. 33.6 del Regolamento e garantirne un'applicazione uniforme, l'EBA ha elaborato le *Guidelines on the conditions to be met to benefit from an exemption from contingency measures under Article 33(6) of Regulation (EU) 2018/89 (RTS on SCA& CSC)* pubblicate sul sito dell'EBA il 4.12.2018 (EBA/GL/2018/07). Gli orientamenti dell'Autorità europea sono in corso di recepimento in Italia: con un documento messo in consultazione nel dicembre 2018 la Banca d'Italia ha comunicato l'intenzione di recepire integralmente tali orientamenti, i quali si applicano a tutti i prestatori di servizi di pagamento che detengono conti di pagamento, così da favorire la creazione di un quadro normativo nazionale unitario e pienamente coerente con le disposizioni europee.

La disciplina nazionale ha introdotto anche dei limiti all'accesso ai conti di pagamento da parte dei terzi prestatori di servizi di pagamento (art. 6-*bis* d.lgs. n. 11/2010). In particolare, il PSP di radicamento del conto può rifiutare l'accesso "*per giustificate e comprovate ragioni connesse all'accesso fraudolento o non autorizzato al conto di pagamento*" da parte dei prestatori di servizi di informazione sui conti o di disposizione di ordine di pagamento, "*compresi i casi di ordini di pagamento fraudolenti o non autorizzati*".

In tali casi, il prestatore di radicamento del conto è tenuto ad informare i TPPs, possibilmente anche prima di formalizzare il rifiuto, comunicandone i motivi, salvo che vi ostino ragioni di ordine pubblico o di pubblica sicurezza, individuate con proprio regolamento dal Ministro dell'economia e delle finanze[54] o altri giustificati motivi connessi con l'applicazione delle disposizioni in materia di riciclaggio e finanziamento del terrorismo.

Il rifiuto di accesso al conto e le ragioni che lo hanno determinato devono essere comunicate immediatamente anche alla Banca d'Italia, la quale "*effettua le valutazioni di competenza e, ove necessario, adotta le misure ritenute opportune*" (art. 6-*bis*, comma 2, d.lgs. n. 10/2011).

3.2 Il consenso alla prestazione del servizio

Per poter accedere ai conti i TTPs necessitano del consenso esplicito del pagatore, ovvero dell'utente nel caso del servizio di informazione sui conti, allo svolgimento dei nuovi servizi di pagamento (artt. 5-*ter*, comma 2, lett. c), e 5-*quater*, comma 2, lett. a), d.lgs. n. 11/2010), ed è ben possibile che ciò avvenga in maniera informatica considerata la natura informatica dell'attività da essi svolta e le modalità con cui essi interagiscono con gli utenti. Le modalità di prestazione del consenso per l'esecuzione della singola operazione di pagamento potranno formare oggetto del contratto quadro che regola lo svolgimento del servizio.

In particolare, il carattere esplicito del consenso a disporre l'esecuzione di un ordine di pagamento deve riguardare l'importo del pagamento, il beneficiario e ogni altro dato dell'operazione nonché la disponibilità a fornire al beneficiario qualunque informazione ottenuta nella prestazione del servizio di disposizione di ordine di pagamento; il prestatore che dispone l'ordine non può modificare tali dati.

---

[54] L'art. 6-*bis* del d.lgs. n. 10/2011 richiama a questo proposito l'applicazione dell'art. 126 TUB, che rimette ad un regolamento del MEF, adottato ai sensi dell'art. 17, comma 3, della legge 23 agosto 1988, n. 400, l'individuazione dei casi in cui gli intermediari devono astenersi dal comunicare al consumatore le ragioni della mancata erogazione del credito o della sospensione dell'erogazione individuabili nelle informazioni, ritenute riservate, contenute nelle banche dati sul credito; l'art. 126 TUB in realtà non indica ragioni di ordine pubblico o di pubblica sicurezza, ma semplicemente motivi di riservatezza delle informazioni contenute nelle banche dati sul credito il cui richiamo sembra poco pertinente rispetto all'informativa da rendere nel caso di rifiuto di accesso al conto di pagamento. Forse il rinvio all'art. 126 TUB deve considerarsi limitato allo strumento normativo costituito dal regolamento attuativo del MEF.

Il consenso ad eseguire la disposizione di ordine di pagamento sarà utilmente prestato anche per l'esecuzione dell'operazione di pagamento, nel senso che non è necessario replicarlo nei confronti del prestatore di pagamento di radicamento del conto; infatti, come disposto dall'art. 62, comma 2, PSD2, "*il consenso ad eseguire un'operazione di pagamento può anche essere prestato tramite … il prestatore di servizi di disposizione di ordine di pagamento*"[55] e, in tal caso, il prestatore di servizi di pagamento di radicamento del conto non dovrà richiedere ulteriori verifiche del consenso dato dagli utenti ai prestatori che dispongono l'ordine di pagamento così come a quelli che svolgono il servizio di informazione sui conti (cfr. art. 32, comma 3, reg. delegato (UE) n. 2018/389).

Il prestatore di radicamento del conto è esonerato dall'indagare la relazione contrattuale tra il cliente e il TTP dovendo, comunque, presumere per effetto dell'autenticazione e dell'utilizzo delle credenziali di accesso al conto che quest'ultimo agisca sulla base del consenso esplicito del cliente. Tuttavia, l'accesso al conto – e conseguentemente l'esecuzione dell'ordine di pagamento tramite un terzo prestatore – può essere rifiutato in ragione del fatto che l'ordine di pagamento non sia autorizzato dal titolare del conto e tale circostanza consti con certezza al gestore del conto (art. 6-*bis*, comma 1, d.lgs. n. 11/2010). Ciò accade sicuramente quando l'utente revoca il consenso alla prestazione dei servizi dei TPPs e ne informa il prestatore di radicamento del conto, il quale, a sua volta, è tenuto a dare informazione immediata della revoca al terzo *provider* (art. 6-*bis*, comma 3, d.lgs. n. 11/2010).

Il citato art. 6-*bis* assimila alle ipotesi di accesso non autorizzato al conto, che possono legittimamente determinare un rifiuto di colloquio da parte del prestatore di radicamento del conto, le ipotesi di ordini di pagamento fraudolenti o non autorizzati e l'individuazione di questi ultimi comporta un'attenta valutazione delle ipotesi in cui, in via generale, il consenso all'operazione di pagamento correttamente prestato sia stato successivamente legittimamente revocato dall'utente.

L'art. 5, comma 4, d.lgs. n. 11/2010 dispone che il consenso ad eseguire un'operazione di pagamento o una serie di operazioni di pagamento può essere revocato in qualsiasi momento, nella forma e secondo la procedura concordata nel contratto quadro o nel contratto relativo a singole operazioni di pagamento, purché ciò avvenga prima che l'ordine di pagamento diventi irrevocabile ai sensi dell'art. 17. Questo articolo è stato modificato con il recepimento della PSD2, prevedendosi ora che il pagatore non possa revocare l'ordine di pagamento dopo aver prestato il proprio consenso a disporre l'operazione di pagamento al prestatore di servizi di disposizione di ordine di pagamento (art. 17, comma 2) e che, decorsi i termini di legge, l'ordine di pagamento possa essere revocato solo se la revoca è stata concordata dall'utente con tutti i prestatori di servizi di pagamento coinvolti nell'operazione di pagamento. Pertanto, se l'utente si è avvalso di un prestatore di servizi di disposizione d'ordine di pagamento, non

---

[55] Nello stesso senso si esprime l'art. 5, comma 2, d.lgs. 11/2010.

sarà sufficiente negoziare la revoca con il prestatore di radicamento del conto, ma occorrerà acquisire anche il consenso del PISP e viceversa (art. 17, comma 5). Le operazioni di pagamento eseguite dopo la revoca del consenso legittimamente espresso non sono considerate autorizzate e, in tali casi, potrebbe essere inibito l'accesso al conto al TPP.

3.3 La responsabilità civile dei nuovi prestatori di servizi di pagamento e l'obbligo di rimborso

Le nuove regole sulla responsabilità dei TPPs, in particolare per i *provider*s di servizi di disposizione di ordini di pagamento, ricalcano quelle già introdotte con la PSD1 in relazione sia alla presunzione di responsabilità del prestatore del servizio di pagamento, sia all'inversione dell'onere della prova a tutela dell'utente.

Tuttavia la pluralità dei soggetti coinvolti nell'operazione di pagamento, lato debitore, per effetto del possibile intervento del prestatore del nuovo servizio di disposizione di ordine di pagamento, pone un ulteriore problema di corretta individuazione del soggetto responsabile e di eventuale riparto di responsabilità tra gli intermediari.

A tal riguardo la PSD2 semplifica la posizione dell'utente riconoscendogli il diritto a richiedere il rimborso immediato dell'operazione di pagamento non autorizzata e l'eventuale risarcimento del danno nei confronti del prestatore di pagamento di radicamento del conto, ma attribuisce a quest'ultimo un diritto di rivalsa nei confronti del PISP che abbia eventualmente preso parte all'operazione di pagamento; quest'ultimo è, a sua volta, gravato dell'onere della prova nei rapporti con il prestatore di radicamento del conto.

Pertanto, nel caso in cui alla catena dei soggetti coinvolti nell'operazione di pagamento partecipi il prestatore di disposizione di ordini di pagamento, l'utente che contesta la mancata autorizzazione di un'operazione di pagamento eseguita non sarà onerato di dimostrare quale tra i prestatori coinvolti sia stato in concreto responsabile dell'esecuzione di tale pagamento al fine di proporre correttamente nei suoi confronti domanda di rimborso o di risarcimento, potendo invece far valere sempre tale diritto nei confronti del prestatore di radicamento del conto che, a sua volta, sarà tenuto indenne dal PISP con la stessa immediatezza. Dal canto suo, il PISP, per ottenere la restituzione delle somme rimborsate (e l'eventuale risarcimento del danno), deve dimostrare di aver adempiuto correttamente agli obblighi di autenticazione, corretta registrazione e inesistenza di guasti tecnici o altri inconvenienti operativi (art. 11, comma 2-*bis*, d.lgs. n. 11/2010).

La responsabilità derivante dall'esecuzione di operazioni di pagamento non autorizzate dà luogo quindi ad un obbligo di rimborso immediato delle somme pagate e contestate dall'utente e tale obbligo grava sul prestatore di servizi di pagamento di radicamento del conto a prescindere dalla sua concreta responsabilità. Sarà onere di quest'ultimo agire in regresso nei confronti del

prestatore di servizi di disposizione di ordine di pagamento avendo titolo anche al risarcimento del danno nel caso in cui il PISP sia anche direttamente responsabile dell'esecuzione dell'operazione non autorizzata.

L'utente, infatti, può negare di aver autorizzato un'operazione di pagamento disposta per il tramite di un prestatore di ordine di pagamento o contestarne l'esecuzione inesatta, tuttavia spetta a detto prestatore l'onere di provare di aver rispettato le regole di autenticazione, di corretta registrazione e di aver dato corso all'ordine rispettando le procedure necessarie alla sua esecuzione senza che queste siano state coinvolte in malfunzionamenti o altri inconvenienti informatici. È altresì onere del PISP, al fine di escludere la propria responsabilità nei casi in cui l'operazione di pagamento sia stata eseguita sulla base di un'autorizzazione che l'utente disconosce, fornire la prova della frode e dell'inadempimento doloso o gravemente colposo dell'utente rispetto agli obblighi di corretto utilizzo dello strumento di pagamento, di tutela delle credenziali di sicurezza personalizzate e di tempestiva denuncia dell'uso non autorizzato dello strumento[56].

Analogamente, nell'ipotesi di esecuzione mancata o inesatta dell'operazione di pagamento disposta per il tramite di un PISP (art. 25-*bis*, d.lgs. n. 11/2010), il pagatore ha diritto ad ottenere il rimborso della somma, pari all'importo del pagamento erroneamente eseguito, da parte del prestatore di servizi di pagamento di radicamento del conto, che, se del caso, è tenuto a ripristinare lo stato del conto di pagamento anteriore all'esecuzione dell'operazione non correttamente eseguita. Il PISP, a sua volta, è tenuto a rimborsare al gestore del conto le somme da quest'ultimo retrocesse al pagatore, salvo l'obbligo di risarcire l'ulteriore danno, se si accerta che l'inesatta esecuzione dell'operazione di pagamento è a lui imputabile.

Per evitare gli obblighi di rimborso e di risarcimento il PISP deve dimostrare che il prestatore di pagamento di radicamento del conto ha ricevuto l'ordine tempestivamente (art. 15, d.lgs. n. 11/2010) e che, in relazione al servizio prestato di disposizione di ordine di pagamento, vale a dire per la fase di perfezionamento e di trasmissione dell'ordine di pagamento di sua competenza, l'operazione è stata autenticata, correttamente registrata e non ha subito le conseguenze di guasti tecnici o altri inconvenienti che ne hanno determinato la mancata, tardiva o inesatta esecuzione (art. 25-*bis*, comma 2, d.lgs. n. 11/2010).

---

[56] La responsabilità del (cliente) pagatore è limitata solo al caso in cui egli abbia agito fraudolentemente (con esclusione, dunque, dell'imputazione per colpa grave) quando il prestatore di servizi di pagamento non ha applicato le regole dell'autenticazione forte del cliente. Sul tema, v. G. Berti De Marinis, *La disciplina dei pagamenti non autorizzati cit.*, p. 651; P. Montella, *L'autenticazione ad accesso forte (Strong customer Authentication) e la responsabilità del Prestatore del servizio di pagamento alla luce delle modifiche al d. lgs. n. 11 del 27 dicembre 2010*, in *De Iustitia*, p. 124, il quale esamina la possibile rivalsa del prestatore di servizi di pagamento sull'azienda produttrice del software di autenticazione forte quando, nonostante l'utilizzo di tale forma di autenticazione, il sistema abbia consentito un'operazione di pagamento fraudolentemente autorizzata da terzi.

Fermo restando il diritto dell'utente ad ottenere dal gestore del proprio conto il rimborso e l'eventuale risarcimento per l'esecuzione di operazioni di pagamento non autorizzate, fraudolente e per le operazioni di pagamento non eseguite o eseguite tardivamente o erroneamente, il prestatore che ha eseguito in prima battuta il pagamento conserva il diritto di regresso verso gli altri prestatori di servizi di pagamento e verso gli altri soggetti che siano stati coinvolti nella catena dell'operazione di pagamento; l'obbligo gravante sul PISP di dotarsi di una copertura assicurativa riferita espressamente ad eventi di danno conseguenti i) al compimento di operazioni non autorizzate (art. 73 PSD2), ii) alla mancata, inesatta o tardiva esecuzione delle operazioni di pagamento (artt. 89 e 90 PSD2), iii) all'esercizio del regresso da parte di altri prestatori di servizi di pagamento (art. 92 PSD2) – come previsto dall'art. 5, comma 2, della PSD2 – dovrebbe garantire al prestatore di radicamento del conto il ristoro patrimoniale delle somme rimborsate al cliente a prima richiesta.

La semplicità dei criteri adottati nell'applicazione del rimedio restitutorio, con il ripristino dello stato del conto di pagamento ad opera del prestatore che lo gestisce in relazione ad un ordine delegatorio falso o erroneo, in contrapposizione alla complessità tecnica delle attività svolte dai plurimi soggetti coinvolti nell'operazione di pagamento, conferisce certezza al rimedio nell'interesse sia dell'utente sia degli intermediari. La PSD2, dunque, non soltanto conferma in generale la linea inaugurata dalla PSD1 di ampliare l'ambito del rischio di impresa in capo al prestatore di servizi di pagamento, gravandolo dei pericoli di danno statisticamente prevedibili in relazione allo svolgimento di tale attività, con la finalità di promuovere negli utenti la fiducia nell'utilizzo degli strumenti di pagamento elettronici[57], ma va oltre, introducendo un obbligo di rimborso in capo al prestatore di radicamento del conto a prescindere dalla sua responsabilità nella causazione dell'illecito pagamento[58] e spostando in capo al TPP che ha disposto l'ordine di pagamento la presunzione di responsabilità nella successiva regolazione dei rapporti tra gli intermediari coinvolti nell'operazione di pagamento contestata. Il terzo *provider*, che effettua il servizio di disposizione di ordine di pagamento, nel caso di esecuzione di operazioni non autorizzate o inesatte, per ottenere la restituzione delle somme rimborsate al prestatore di radicamento del conto e per evitare il risarcimento anche dei danni ulteriori, è gravato dell'onere di dimostrare che l'operazione di pagamento, per quel che riguarda la fase procedimentale di propria pertinenza, "*è stata autenticata, correttamente registrata e non*

---

[57] Sul tema cfr. I. Caggiano, *Pagamenti non autorizzati tra responsabilità e restituzioni. Una rilettura del d.lgs. n. 11/2010 e lo scenario delle nuove tecnologie*, in *Riv. dir. civ.*, 2016, p. 471.

[58] Salvo non fondare una responsabilità del prestatore di radicamento del conto sulla violazione degli obblighi derivanti dall'art. 6-*bis* del d.lgs. n. 11/2010, vale a dire sul mancato rifiuto di accesso al conto "*per giustificate e comprovate ragioni connesse all'accesso fraudolento o non autorizzato al conto di pagamento*", come se residuasse in capo a detto prestatore un controllo sugli accessi al conto da lui gestito. In tal senso, si esprime G. Berti De Marinis, *La disciplina dei pagamenti non autorizzati nel nuovo sistema delineato dal recepimento della direttiva PSD2*, in *Diritto della banca e del mercato finanziario*, 2018, p. 645.

ha subito le conseguenze di guasti tecnici o altri inconvenienti relativi al servizio di pagamento prestato" (art. 11, comma 2, d.lgs. n. 11/2010). Il TPP sarà gravato dall'onere probatorio anche nel caso in cui intenda agire per la restituzione dell'indebito nei confronti dell'utente rimborsato (art. 11, comma 3, d.lgs. n. 11/2010).

4. L'applicazione della disciplina contrattuale uniforme dei servizi di pagamento

Anche i contratti per l'erogazione del servizio di disposizione di ordine di pagamento, rientrando nella categoria dei contratti di servizi di pagamento, sono soggetti alle disposizioni dedicate a questi ultimi contenute nel titolo VI, capo II-*bis,* del TUB, concernenti la cd. trasparenza delle condizioni contrattuali e dei rapporti con i clienti, la cui applicazione anche agli istituti di pagamento è indicata in via generale nell'art. 114-*undecies*, comma 1, TUB. Tale disciplina è integrata dalle disposizioni attuative secondarie in materia di trasparenza adottate dalla Banca d'Italia, da ultimo modificate in seguito al recepimento della PSD2[59].

Dunque, per il servizio di disposizione di ordini di pagamento varranno le norme speciali, che disciplinano la forma e le modalità di redazione del contratto, sia quando si tratta di contratti quadro, che di contratti relativi ad operazioni di pagamento compiute in forma isolata; i PISPs hanno quindi l'obbligo di stipulare il contratto quadro per iscritto a pena di nullità e di fornire, al momento della sottoscrizione del contratto e successivamente con cadenza periodica, le informazioni indicate dalle disposizioni secondarie della Banca d'Italia (cfr. artt. 126-*quinquies* e 126-*quater* TUB) e di rispettare le speciali regole dettate dal testo unico bancario per i contratti di servizi di pagamento nei casi di modifica unilaterale delle condizioni contrattuali e di recesso dal contratto; essi saranno tenuti agli speciali obblighi informativi precontrattuali in relazione alla stipula di contratti quadro o di quelli per l'esecuzione di operazioni isolate[60], nonché agli

---

[59] Cfr. provvedimento della Banca d'Italia del 19 marzo 2019.

[60] Le nuove istruzioni precisano che l'IP nella redazione di un contratto quadro deve informare il cliente in merito alla "*forma e modalità per prestare e revocare il consenso alla disposizione di un ordine di pagamento*" (sez. VI, par. 1.1.1 lett. b); alla "*procedura sicura applicabile dall'intermediario per comunicare al cliente i rischi di frode nei pagamenti o di altri abus*i" (sez. VI, par. 1.1.1 lett. e); con riguardo alle singole operazioni di pagamento non rientranti in un contratto quadro, il PISP "*mette a disposizione del cliente, prima che l'ordine sia disposto, anche le seguenti informazioni in modo chiaro e completo: a) la denominazione e l'indirizzo della sede amministrativa e, ove del caso, della succursale con sede in Italia dell'intermediario che presta il servizio di disposizione di ordine di pagamento nonché, nel caso di offerta fuori sede, l'indirizzo del soggetto che entra in rapporto con il cliente; l'indirizzo, anche di posta elettronica, o altro recapito al quale il cliente può rivolgersi per chiedere ulteriori informazioni all'intermediario che effettua l'operazione di pagamento; b) le informazioni di contatto dell'autorità di vigilanza"* (sez. VI, par.4.2.1, Provvedimento Banca d'Italia del 19.3.2019).

obblighi informativi contrattuali concernenti le operazioni di pagamento per le quali hanno disposto l'ordine di pagamento[61].

Diversamente, i nuovi contratti di informazione sui conti sembrano ampiamente sottratti all'applicazione di tale disciplina[62], fatta eccezione per le norme concernenti gli obblighi informativi relativi alla stipula del contratto (art. 126-*quater* comma 1, lett. a, TUB), e l'onere probatorio dell'istituto di pagamento nel caso di contestazione mossa dall'utente per tale carente od omessa informazione (art. 126-*bis,* comma 4, TUB)[63].

In ogni caso, gli obblighi di trasparenza dei TPPs nei rapporti con la clientela soggiacciono all'attività di controllo della Banca d'Italia che a tal fine può richiedere agli istituti di pagamento informazioni, atti e documenti nonché eseguire ispezioni (art. 128, comma 1, TUB) e, nel caso di riscontrate irregolarità, può adottare misure di sospensione o di inibizione dell'attività o dell'offerta, promozione o conclusione di specifici contratti, nonché la restituzione di somme indebitamente percepite, disponendo anche forme di pubblicità di tali misure (art. 128-*ter* TUB).

Costituisce illecito amministrativo dell'istituto di pagamento la violazione di alcune specifiche disposizioni del titolo VI del TUB, quali ad esempio quelle concernenti l'obbligo di fornire le informazioni relative alle operazioni di pagamento e ai contratti di cui all'art. 126-*quater* e 126-*quinquies,* comma 2, (queste applicabili anche agli AISPs); il rispetto delle disposizioni sulla modifica unilaterale delle condizioni di contratto e sul recesso, ex artt. 126-*sexies* e 126-*septies*; l'obbligo di rispettare le misure inibitorie disposte dall'Autorità di vigilanza ex art. 128-*ter* del TUB; parimenti è sanzionabile in via amministrativa l'inosservanza delle norme contenute nel richiamato art. 128, comma 1, ovvero la condotta di ostacolo all'esercizio delle funzioni di controllo previste dal medesimo articolo, nonché quella di inottemperanza all'obbligatoria adesione ai

---

61 Nell'ambito dell'informativa dovuta nello svolgimento di servizi di disposizione di ordini di pagamento in forza di un contratto quadro è previsto che l'IP "*consegna al pagatore e, se del caso, al beneficiario una ricevuta contenente le seguenti informazioni: – la conferma del buon esito della disposizione dell'ordine di pagamento indirizzata all'intermediario di radicamento del conto del pagatore – un riferimento che consenta al pagatore e al beneficiario di individuare l'operazione di pagamento e, ove opportuno, al beneficiario di individuare il pagatore e tutte le informazioni trasmesse con l'operazione di pagamento; – l'importo dell'operazione di pagamento; – tutte le spese dovute al prestatore di servizi di disposizione di ordine di pagamento per l'operazione e, in caso di pluralità di voci di costo, la chiara distinzione delle singole voci"* (sez. VI, par. 6, Provvedimento Banca d'Italia del 19.3.2019). Se sono state eseguite operazioni isolate tali informazioni possono essere messe a disposizione del cliente (e non consegnate).

62 Tale esclusione è frutto di un doppio rinvio normativo: infatti l'art. 114-*septiesdecies* TUB esclude che agli AISPs si applichi l'art. 114-*undecies*, comma 1, il quale, a sua volta dispone l'applicazione del titolo VI del TUB agli istituti di pagamento. D'altro canto, l'art. 114-*septiesdecies* TUB, come già ricordato (v. *supra* paragrafo n. 2), prevede espressamente l'applicazione degli artt. 126-*quater,* comma 1, lett. a), e 126-*bis*, comma 4, TUB ai contratti di informazione sui conti.

63 Coerentemente, il Provvedimento della Banca d'Italia sulla trasparenza dispone che agli intermediari che prestano unicamente il servizio di informazione sui conti si applica soltanto il paragrafo 4, della Sezione VI, ove è disciplinata l'informazione precontrattuale. È richiamata anche l'applicazione delle disposizioni (disciplinate nella sez. V) concernenti la conclusione del contratto mediante una tecnica di comunicazione a distanza.

sistemi di risoluzione stragiudiziale delle controversie e al rispetto delle misure inibitorie adottate dalla Banca d'Italia in forza del richiamato art. 128-*ter* (art. 144, commi 1 e 4, TUB). La sanzionabilità delle condotte illecite presuppone che le infrazioni rivestano carattere rilevante, secondo i criteri definiti dalla Banca d'Italia con provvedimento di carattere generale, tenuto conto dell'incidenza delle condotte sulla complessiva organizzazione e sui profili di rischio aziendali (art. 144, comma 8, TUB).

La violazione degli obblighi previsti dal Titolo VI del TUB da parte di istituti comunitari la cui attività resta sottoposta alla legislazione italiana per il fatto di essere svolta sul territorio della Repubblica (art. 126-*bis*, comma 1, TUB) dà luogo ad un procedimento articolato poiché la vigilanza spettante alla Banca d'Italia, quale Autorità territorialmente competente in relazione all'attività, va combinata con quella spettante alle Autorità dello stato membro d'origine, che vigilano sui soggetti. Infatti, in tal caso la Banca d'Italia è tenuta ad inoltrare la comunicazione allo Stato membro di origine a cui compete in prima battuta il potere sanzionatorio sulle irregolarità riscontrate. Tuttavia, qualora il provvedimento sanzionatorio non venga adottato o sia inadeguato e le irregolarità commesse rischino di pregiudicare interessi generali ovvero quando sussistano ragioni di urgenza per la tutela dei diritti degli utenti dei servizi di pagamento, è attribuito alla Banca d'Italia il potere di adottare misure provvisorie ritenute necessarie, ivi comprese l'inibizione allo svolgimento di nuove operazioni e la chiusura della succursale italiana[64].

Appendice: Considerazioni in materia di contrasto del riciclaggio e del finanziamento del terrorismo in relazione a servizi con TPP

di Eugenio Maria Mastropaolo

La presenza di una pluralità di intermediari nella catena del valore relativa alla prestazione dell'attività da parte di un PISP o di un AISP rende complessa l'attribuzione a ciascun soggetto degli obblighi previsti dalla normativa in materia di contrasto del riciclaggio e del finanziamento del terrorismo di cui al d.lgs. n. 231 del 21 novembre 2007, modificato dal d.lgs. n. 90 del 25 maggio 2017.

1. Con riferimento ai soggetti obbligati, le attività di disposizione di ordini di pagamento e di informazione sui conti possono essere prestate da qualunque intermediario abilitato alla prestazione di servizi di pagamento (dunque banche, istituti di moneta elettronica ed istituti di pagamento) specificamente autorizzato all'uopo.

Rispetto tuttavia agli altri servizi di pagamento, le attività di disposizione di ordini di pagamento e di informazione sui conti non prevedono, da parte

---

[64] Cfr. art. 114-*quinquies*, commi 6-*bis* e 6-*ter*, la cui applicazione anche agli istituti di pagamento è prevista dall'art. 114-*undecies*, comma 2-*bis* TUB.

del soggetto abilitato alla prestazione di tali servizi, l'intermediazione di alcun valore monetario. Infatti per la prestazione di questi servizi non è necessario avere la disponibilità di mezzi di pagamento intestati al disponente un ordine di pagamento, oppure non è necessario adempiere ad alcuna obbligazione pecuniaria derivante dall'esecuzione dei servizi stessi.

2. In considerazione dell'assenza di mezzi finanziari oggetto di intermediazione, gli obblighi in materia di contrasto del riciclaggio e del finanziamento del terrorismo, fondamentalmente, si riducono ad un'adeguata verifica della clientela che richieda la prestazione del servizio; al monitoraggio delle operazioni di disposizione degli ordini di pagamento; alla restituzione delle informazioni aggregate, oltre ovviamente alla conservazione dei dati, delle informazioni e dei documenti derivanti dalla prestazione di tali attività.

Il ridotto numero di obblighi, in particolar modo in materia di adeguata verifica della clientela, come vedremo nel prosieguo, ovviamente è applicabile solo allorquando l'intermediario che presti le attività di PISP o di AISP, si limiti a tali servizi e dunque il rapporto con il cliente sia esclusivamente loro dedicato. Tali obblighi qualitativamente ridotti infatti sono in funzione delle peculiarità del servizio prestato.

3. Per quanto riguarda gli obblighi di identificazione formale del cliente, dell'eventuale titolare effettivo e degli eventuali soggetti deputati ad operare in nome e per conto del cliente, di acquisizione e di valutazione delle informazioni relative allo scopo e alla natura dei servizi prestati, essi vanno eseguiti alla stessa stregua e con lo stesso approccio qualitativo rispetto a quanto sarebbe eseguito da qualunque altro intermediario, in riferimento a qualunque altra attività continuativa prestata da un soggetto del settore finanziario.

Ben diversa è la situazione rispetto agli obblighi di controllo costante dell'andamento del rapporto contrattuale (monitoraggio).

In questa situazione la limitata attività prestata dai soggetti in parola rende l'esecuzione di tali obblighi, come detto, molto più complessa.

Vanno distinte intanto le due situazioni.

3.1. In riferimento al servizio di disposizione di ordini di pagamento, il suo oggetto sono appunto le disposizioni di trasferimento di mezzi di pagamento che il prestatore, dietro indicazioni del titolare del conto, fornisce all'intermediario dove è radicato il conto.

Il prestatore non ha altre informazioni se non quelle relative alle disposizioni di volta in volta impartite e quelle che gli sono state fornite nella fase genetica del rapporto con il cliente. Sulla base di queste, l'unica possibilità che il prestatore ha di adempiere correttamente agli obblighi di monitoraggio è riconducibile all'analisi di congruità e ragionevolezza delle disposizioni impartite rispetto alla posizione economico-finanziaria desumibile dalle informazioni fornite dal cliente stesso oppure ricavate attraverso fonti esterne o documenti indipendenti

e/o formali. Diversamente da altri intermediari presso i quali sono "visibili" le disponibilità finanziarie del cliente, il prestatore è assolutamente "cieco" rispetto a tale situazione. Ne deriva come al di là del richiedere alla bisogna informazioni al cliente stesso, l'analisi del PISP possa essere falsata appunto dall'assenza delle informazioni complessive. Rispetto a tale situazione il prestatore non avrebbe altra alternativa che ritenere comunque sospetta l'operatività (o la singola operazione di disposizione dell'ordine) e pertanto segnalarla alla UIF.

La stessa valutazione potrebbe invece non essere effettuata dall'intermediario presso il quale è radicato il conto. Questi giuridicamente è il soggetto deputato all'esecuzione dell'ordine di trasferimento dei mezzi di pagamento, ovviamente nei limiti delle disponibilità liquide presenti sul conto stesso. Poiché tale intermediario (contrariamente al PISP) ha maggiore visibilità sulla situazione economico-finanziaria del cliente ed in particolare sull'origine, normalmente lecita, dei fondi, ha anche la migliore posizione per effettuare una più compiuta valutazione.

Ne deriva come, mentre l'eventuale segnalazione di un'operazione sospetta effettuata dal prestatore potrebbe non essere seguita dalla segnalazione dell'intermediario presso il quale è radicato il conto, il contrario non dovrebbe accadere. Infatti a fronte della medesima operazione, le ragioni del sospetto dovrebbero essere oggettivamente tanto più fondate/infondate quante più informazioni sul soggetto siano a disposizione di un intermediario. Conseguentemente se è normale che il PISP segnali e l'intermediario presso il quale è radicato il conto di pagamento non segnali, se questi ha invece ritenuto sospetto l'ordine di pagamento come disposto dal PISP, il PISP dovrebbe aver effettuato la medesima valutazione.

Perché ciò succeda, sarebbe auspicabile una collaborazione (possibilmente attraverso protocolli di condivisione dei dati) tra i diversi intermediari, in un caso al fine di non subissare la UIF di segnalazioni basate su analisi parziali e nell'altro per rafforzare la coesione del settore finanziario rispetto allo stesso accadimento.

Lo stesso approccio andrebbe tenuto qualora l'analisi si sposti dall'ammontare dell'operazione di pagamento eseguita per mezzo dell'ordine disposto dal prestatore, all'analisi della posizione relativa al destinatario del pagamento[65].

Il PISP nell'ambito del controllo costante del rapporto e dell'operatività a valere sullo stesso, potrebbe ritenere sospetta la richiesta di impartire una disposizione di un ordine di pagamento a valere su di un determinato beneficiario. Per contro la stessa analisi potrebbe dare un risultato diverso se effettuata dall'intermediario presso il quale è radicato il conto, sulla base della complessiva operatività anche storicizzata.

Più insidiosa per l'intermediario presso il quale è radicato il conto è invece l'ultima situazione. Un cliente potrebbe infatti aprire più rapporti di

---

[65] Approccio tipicamente più da contrasto del finanziamento del terrorismo.

disposizione di ordini di pagamento con diversi PISP al fine di frazionare l'operatività (sia quantitativamente che nei confronti del medesimo beneficiario degli ordini) e confondere l'intermediario presso il quale è radicato il conto di pagamento. Questi dovrebbe dotarsi di strumenti di analisi anche delle operazioni impartite da terzi (tra cui probabilmente anche una forma di registrazione del PISP come delegato ad operare) al fine di poter aggregare le stesse per ammontare, ma soprattutto per destinatario del pagamento. Infatti potrebbe costituire un indicatore di anomalia il fatto che l'intermediario sia chiamato ad eseguire una pluralità di pagamenti a favore del medesimo beneficiario a fronte di disposizioni provenienti da diversi PISP a valere sul medesimo conto. In tal caso, si ritiene che, acclarato il motivo del sospetto dato dall'unificazione logica ed economica delle diverse operazioni, l'intermediario dovrebbe procedere con una segnalazione di operazione sospetta, eventualmente informando i diversi PISP per i provvedimenti di loro spettanza.

3.2. In riferimento al servizio di informazioni dei conti, oggetto del servizio è l'aggregazione delle informazioni provenienti da più conti e la presentazione delle stesse per categorie di spese.

Ad una prima analisi, il prestatore effettivamente non ha molto da controllare, unificando e mostrando al cliente giusto delle informazioni sull'operatività pregressa avvenuta sui conti del cliente stesso.

In realtà, anche l'attività dell'AISP presenta un profilo interessante per il contrasto del riciclaggio e del finanziamento del terrorismo. Proprio l'aggregazione delle informazioni potrebbe dare all'AISP la possibilità di rilevare incongruenze complessive dal lato delle spese e delle disposizioni varie, rispetto al profilo economico-finanziario del cliente, il quale sul punto dovrebbe essere sollecitato dall'AISP a fornire tali informazioni. Infatti l'aggregazione dei dati da parte dell'AISP risolve i limiti informativi derivanti dalla possibile esistenza di altri intermediari che prestino servizi di pagamento, che impediscono a ciascun soggetto obbligato di svolgere un'analisi complessiva, ed assolve invece alla funzione di rappresentare un quadro completo non solo al cliente ma anche alle autorità di vigilanza.

4. La presenza di più intermediari che prestino i servizi di disposizione di ordini di pagamento, esecuzione degli stessi, informazione sui conti ed apertura dei conti, fraziona l'applicazione delle disposizioni in materia di contrasto del riciclaggio e del finanziamento del terrorismo. Ciò è frutto della suddivisione di compiti e della disciplina propria di tali servizi.

La risposta dell'ordinamento, ma soprattutto degli intermediari, rispetto agli obiettivi normativi non può essere più basata su di un loro rispetto da parte del singolo soggetto, ma deve vedere l'instaurazione di forme di collaborazione che permettano, *a latere* dei rapporti contrattuali tra TPP ed intermediari dove sono radicati i conti di pagamento, la creazione di protocolli procedurali supportati da sistemi informatici di scambio delle informazioni.

Si ritiene che oltre ad un intervento delle autorità di vigilanza, sul punto sarebbe molto efficace ed efficiente un comune intervento delle associazioni delle diverse categorie di operatori, volto a definire i meccanismi di collaborazione attiva e procedure comuni da integrare in quelle proprie di ciascun intermediario e, in prospettiva, anche della conduzione dell'esercizio annuale di autovalutazione del rischio di riciclaggio e di finanziamento del terrorismo al quale ogni intermediario è esposto e rispetto al quale l'interconnessione data dalla prestazione del servizio di disposizione di ordini di pagamento costituisce un elemento di incremento del rischio, proporzionale alla perdita di controllo di alcune fasi del processo di iniziazione dell'ordine e di acquisizione della clientela.

La disciplina dei costi e delle commissioni interbancarie nella PSD2

Fabrizio Maimeri

1. Spese applicabili ai servizi di pagamento – 2. Le commissioni interbancarie – 2.1 Il Regolamento UE 2015/751 – 2.2 Il titolo IV-bis del d.lgs. 11/2010 – 2.3 Il provvedimento di attuazione della Banca d'Italia – 2.4 L'evoluzione delle commissioni interbancarie – 2.5 Il Regolamento vigente: realtà e prospettive

1. Spese applicabili ai servizi di pagamento

Il nuovo art. 3 del d.lgs. n. 11/2010 ha visto in parte ribadito e in parte integrato il suo originario contenuto, sia nel senso di mantenere la gratuità per le spese sostenute per gli obblighi informativi e per l'adozione di misure correttive e preventive sostenute – a meno che, in quest'ultimo caso, non ricorrano le ipotesi di cui agli artt. 16, comma 4[1]; 17, comma 5[2]; 24, comma 2[3] – sia nel senso che, ove una commissione è ammessa, il suo importo deve «*risultare adeguato e coerente con i costi effettivamente sostenuti*».

Si tratta di un'impostazione ormai consueta per il nostro legislatore nei riguardi delle commissioni applicate dalle banche, vale a dire l'imposizione, da un lato, della gratuità per il cliente di certi servizi e, dall'altro, l'obbligo di ancorare il prezzo, quando è consentito applicarlo, ai costi sostenuti. Ma ancorché si tratti di una impostazione ormai tanto diffusa – di cui è esempio tipico la metrica adottata dall'art. 127-*bis* t.u.b. – da considerarsi ormai una scelta legislativa, essa seguita a lasciar perplessi per una serie di motivi: riguarda solo le banche nell'ambito del mondo finanziario; imponendo un prezzo uguale a zero spinge gli operatori all'opacità nel trasferire in ogni caso (com'è inevitabile) sull'utente finale i costi che trasparentemente non possono essere a questi accollati; la coerenza prezzi-costi (peraltro declinata con espressioni che nelle varie norme non sono né equivalenti né coerenti, dando adito a interpretazioni/situazioni difformi) impedisce agli operatori di utilizzare i prezzi per uscire o entrare in un segmento di mercato, irrigidendo la competitività. Ma tutte le critiche scolorano e restano vane di fronte a un ripetuto intervento legislativo[4].

---

[1] «*Ove il rifiuto di un ordine di pagamento* [da parte dell'intermediario] *sia obiettivamente giustificato, il prestatore di servizi di pagamento può addebitare spese ragionevoli per la comunicazione all'utente, ove ciò sia stato concordato tra le parti*».

[2] In caso di revoca dell'ordine, «*il prestatore di servizi di pagamento può addebitare le spese della revoca solo qualora ciò sia previsto nel contratto quadro*».

[3] In caso di identificativo unico inesatto, il prestatore di servizi di pagamento non è responsabile della mancata o inesatta esecuzione dell'operazione di pagamento, ma deve collaborare con l'utente per il recupero dell'importo malamente accreditato: «*ove previsto nel contratto quadro, il prestatore di servizi di pagamento addebita all'utente le spese sostenute per il recupero dei fondi*». Le tre eccezioni in cui è consentito all'intermediario reclamare delle commissioni hanno tutte come presupposto che esse siano state pattiziamente concordate: «*viene con ciò individuato un principio suscettibile di essere interpretato in modo espansivo con riferimento al più complesso argomento della struttura di* pricing *dei servizi di pagamento, da analizzare anche alla luce dell'obiettivo di efficienza sancito (unitamente a quello di affidabilità) dall'art. 146 del Testo Unico Bancario*» (M. Doria, *Commento all'art. 3 del d.lgs. 11/2010*, in *La nuova disciplina dei servizi di pagamento*, a cura di M. Mancini, N. Rispoli Farina, V. Santoro, A. Sciarrone Alibrandi, O. Troiano).

[4] Per lo sviluppo di questo tema rinvio a F. Maimeri, *Controlli su spese e commissioni*, in *La trasparenza venticinque anni dopo*, a cura di A. Barenghi, Napoli, 2018, p. 280 ss.

I commentatori del previgente art. 3 del d.lgs. n. 11/2010 – di contenuto particolarmente delicato, volto com'era a fissare i criteri di definizione delle tariffe applicabili, nel cui ambito «*i profili strettamente attinenti all'efficienza dei circuiti di pagamento si integrano con obiettivi concorrenziali ed antitrust nella ricerca di un punto di equilibrio tra cooperazione e competizione, particolarmente difficile da individuare in un sistema, quale quello dei pagamenti, caratterizzato da economie di rete*» – ne individuavano i contenuti secondo una ripartizione che anche oggi può essere mantenuta: (i) disciplina dei criteri tariffari relativi al rapporto che intercorre tra prestatore dei servizi e utilizzatore; (ii) individuazione di «*vincoli tariffari univocamente orientati a favorire l'utilizzo di strumenti di pagamento elettronici in alternativa al contante e agli strumenti cartacei*»; (iii) precisazione per cui le tariffe clienti-intermediari non interferiscono sugli schemi tariffari interni ai circuiti (c.d. "tariffe interbancarie")[5].

Il comma 2 dell'art. 3 conferma l'applicazione del criterio *share*, secondo il quale le spese relative all'esecuzione delle operazioni sono sostenute dall'ordinante e dal beneficiario, ognuno nei confronti dei rispettivi clienti. Principio rigido, perentorio, che comporta l'impossibilità di scegliere le alternative del criterio *our* (secondo cui le spese dell'operazione vengono sostenute tutte dal pagatore) o del criterio *ben* (spese sostenute dal solo beneficiario del pagamento). Con norma non perentoria ma permissiva, si aggiunge che, in caso di beneficiario consumatore, è consentita una deroga al principio *share* ed esentare quest'ultimo dalle commissioni di accredito, «*ivi inclusi gli emolumenti a favore di pensionati e lavoratori dipendenti*». Il messaggio, sia pure indiretto, è abbastanza chiaro, nel senso di auspicare che per l'accreditamento di stipendi e pensioni in conto non sia richiesta alcuna commissione al beneficiario.

Nell'ambito riconducibile al profilo sub (ii) sopra menzionato rientra sia l'eliminazione del comma 3, sia la riscrittura del comma 4 e l'aggiunta dei successivi commi 4-*bis* ecc.

Il comma 3 stabiliva che «*il prestatore di servizi di pagamento consente al beneficiario di applicare al pagatore una riduzione del prezzo del bene venduto o del servizio prestato per l'utilizzo di un determinato strumento di pagamento compreso nell'ambito d'applicazione del presente decreto*». Si trattava di una disposizione che prevedeva gli "sconti" di prezzo in connessione con l'uso di mezzi di pagamento alternativi al contante[6]. Nella Relazione illustrativa del provvedimento che si è poi tradotto nel d.lgs. n. 218/2017, si è preso atto della

---

[5] Le citazioni riportate in questo capoverso sono tratte da M. Doria, *Commento all'art. 3 d.lgs. n. 11/2010*, cit., p. 62-63.

[6] «*La disposizione introduce dunque un vincolo per i prestatori di servizi di pagamento volto a creare le condizioni per la realizzazione di efficaci incentivi per gli utilizzatori a fare ricorso a strumenti di pagamento elettronici. L'obbligo in questione – che assume le caratteristiche di un divieto – si rivolge essenzialmente ai prestatori di servizi di pagamento che svolgono attività di* acquiring (…)*, che consiste nella stipula di accordi contrattuali per il convenzionamento di soggetti (usualmente, esercizi commerciali) con lo scopo di abilitare questi ultimi all'accettazione di strumenti di pagamento secondo le regole del circuito di riferimento*»: M. Doria, *Commento all'art. 3 d.lgs. n. 11/2010*, cit., p. 69.

situazione concreta che l'applicazione di questa disposizione ha creato, vale a dire che essa non ha impedito la prassi, per più versi illegittima, di operare sconti "al contrario" per privilegiare l'uso del contante, sicché «*in linea con il generale divieto di* surcharge *e a seguito di un utilizzo distorto della "scontistica", che ha reso questa pratica uno strumento per eludere il divieto di applicazione del* surcharge *(c.d.* surcharge *al contrario), si ritiene opportuno procedere all'abrogazione del comma 3*»[7].

Con il comma 4 si è mantenuto il disposto per cui «*il beneficiario non può applicare a carico del pagatore spese relative all'utilizzo di strumenti di pagamento*», favorendo – precisa ancora la Relazione – la concorrenza, promuovendo l'uso di strumenti di pagamento efficienti e garantendo all'utente una reale possibilità di scelta, stabilendo così «*un divieto generalizzato per il beneficiario di imporre spese aggiuntive, rispetto al costo del bene o del servizio, in relazione all'utilizzo di strumenti di pagamento (*surcharge*)*». Ora tale divieto non conosce eccezioni[8].

Nel rimandare alla specifica trattazione in merito al predetto divieto di *surcharge* e al relativo sistema di *enforcement*[9], si evidenzia che non è stato invece oggetto di modifica il comma 5 (e ultimo) dell'art. 3 in esame.

Tale comma stabilisce che le disposizioni del medesimo articolo non producono effetti sulle commissioni interbancarie, vale a dire sul «*pagamento di eventuali spese concordate tra prestatori di servizi di pagamento o soggetti di cui essi si avvalgono*». Siffatta norma sembra quindi dichiarare «*l'esistenza di una netta separazione fra la disciplina delle spese nel rapporto che intercorre tra prestatore e utilizzatore dei servizi di pagamento – soggetta a regole armonizzate – e le regole sulle tariffe applicate all'interno dei circuiti di pagamento prestatori, rimessa alla libera determinazione di questi ultimi*»[10]. Una simile affermazione – in ogni caso «*superata alla luce di successivi interventi comunitari*» – come dice lo stesso autore poco dopo – introduce alla seconda parte di queste note, vale a dire quella dedicata alle commissioni interbancarie.

---

[7] In questo senso cfr. altresì E: Zeppieri, *L'implementazione in Italia della nuova direttiva sui servizi di pagamento*, in www.dirittobancario.it, febbraio 2018, p. 6.

[8] Il previgente art. 4 proseguiva infatti così: «*La Banca d'Italia può stabilire con proprio regolamento deroghe tenendo conto dell'esigenza di promuovere l'utilizzo degli strumenti di pagamento più efficienti ed affidabili*», deroghe peraltro che non sono mai state precisate: M. Libertini, *Brevi note su concorrenza e servizi di pagamento*, in *Banca, borsa, tit. cred.*, 2011, p. 181 ss.; G. Coppola, *La surcharge fee sulle carte di pagamento: i biglietti aerei acquistati on line*, in *Studi e note di economia*, 2012, p. 232 ss. Così veniva spiegata questa deroga: «*per apprezzare il significato di questa scelta* [divieto con deroga] *occorre probabilmente partire dalla* ratio *di fondo ad essa sottesa che, come detto, risiede nell'obiettivo di favorire l'utilizzo degli strumenti di pagamento elettronici rispetto a quelli cartacei e al contante. In considerazione di ciò, il potere di deroga al divieto di* surcharge *conferito alla Banca d'Italia dovrebbe essere interpretato nella direzione di esplicitare una linea di demarcazione tra la prima e la seconda tipologia di strumenti: in sostanza, la deroga dovrebbe interessare gli strumenti non elettronici che potrebbero/dovrebbero essere oggetto di un sovraprezzo teso a esplicitare il maggior onere di utilizzo che li caratterizza*»: M. Doria, *Commento all'art. 3 d.lgs. n. 11/2010*, cit., p. 71.

[9] Cfr. il contributo di T. Broggiato in questo *Quaderno*.

[10] M. Doria, *Commento all'art. 3 d.lgs. n. 11/2010*, cit., p. 73.

2. Le commissioni interbancarie

Uno dei punti importanti della nuova PSD2 consiste nell'aver introdotto nel d.lgs. n. 11/2010 (con l'art. 3 del d.lgs. 15 dicembre 2017, n. 218, di recepimento della PSD2) un titolo IV-*bis* (artt. 24-*bis* – 34-*decies*) volto a coordinare con la disciplina nazionale quella del Regolamento UE 2015/751 "*relativo alle commissioni interbancarie sulle operazioni di pagamento basate su carta*".

2.1 Il Regolamento UE 2015/751

Il menzionato Regolamento prende le mosse dal rilievo che le commissioni interbancarie sono applicate tra i prestatori di servizi di pagamento convenzionatori e i prestatori di servizi di pagamento emittenti della carta appartenenti a un dato schema di carte di pagamento[11] e costituiscono una componente principale delle commissioni applicate agli esercenti da parte dei prestatori di servizi di pagamento convenzionatori per ogni operazione di pagamento basata su carta (considerando 10). Sennonché tali commissioni sono diversificate tra paese e paese e collocate talora su livelli elevati, il che «*ostacola l'affermarsi di "nuovi" operatori paneuropei sulla base di modelli commerciali che prevedono commissioni interbancarie più basse o nessuna commissione interbancaria, a scapito di potenziali economie di scala e di scopo e degli incrementi di efficienza che consentirebbero. Tale situazione ha conseguenze negative per gli esercenti e i consumatori e ostacola l'innovazione*» (considerando 11). «*Pertanto, per evitare la frammentazione del mercato interno e distorsioni significative della concorrenza dovute a leggi e decisioni amministrative divergenti, è necessario, conformemente all'art. 114 TUEF ("Trattato sul funzionamento dell'Unione Europea)*[12]*, adottare misure per risolvere il problema dovuto a commissioni interbancarie elevate e divergenti, per consentire ai prestatori di servizi di pagamento di prestare i loro servizi su base transfrontaliera e ai consumatori e agli esercenti di utilizzare i servizi transfrontalieri*» (considerando 13).

Così giustificato e delimitato l'intervento, il Regolamento ha un contenuto precettivo, i cui punti principali possono riassumersi come segue:

---

[11] Cioè «*quell'insieme unico di norme, prassi, standard e/o linee guida di attuazione per l'esecuzione di operazioni di pagamento basate su carta, separato da qualsiasi infrastruttura o sistema di pagamento che ne sostenga le operazioni, che includa specifici organi decisionali, organizzazioni o entità responsabili del funzionamento dello schema*»: così il n. 16 del comma 1 dell'art. 2 del regolamento.

[12] L'art. 114 TUEF dispone: « *1.* (…) *Il Parlamento europeo e il Consiglio, deliberando secondo la procedura legislativa ordinaria e previa consultazione del Comitato economico e sociale, adottano le misure relative al ravvicinamento delle disposizioni legislative, regolamentari ed amministrative degli Stati membri che hanno per oggetto l'instaurazione ed il funzionamento del mercato interno. – 2. Il paragrafo 1 non si applica alle disposizioni fiscali, a quelle relative alla libera circolazione delle persone e a quelle relative ai diritti ed interessi dei lavoratori dipendenti*».

1. *Ambito di applicazione (art. 1)* – Il Regolamento stabilisce requisiti tecnici e commerciali uniformi per le operazioni di pagamento basate su carta eseguite nell'Unione, quando sia il prestatore di servizi di pagamento del pagatore sia il prestatore di servizi di pagamento del beneficiario sono situati nell'Unione. Il capo II del Regolamento (artt. 3-12) non si applica:

- alle operazioni tramite carte aziendali[13];
- ai prelievi presso i distributori automatici per il prelievo di contante (ATM) o presso gli sportelli di prestatori di servizi di pagamento;
- alle operazioni tramite carte di pagamento emesse dagli schemi di carte di pagamento a tre parti[14].

2. *Limite alla misura delle commissioni interbancarie (art. 3)* – I prestatori di servizi di pagamento non offrono né chiedono per qualsiasi operazione tramite carta di debito una commissione interbancaria per ogni operazione superiore allo 0,2% del valore dell'operazione.

Per le operazioni nazionali tramite carta di debito, gli Stati membri possono:

a) definire un massimale per operazione sulle commissioni interbancarie a percentuale inferiore allo 0,2% e possono imporre un importo massimo fisso di commissione quale limite all'importo della commissione risultante dalla percentuale applicabile, ovvero:

b) consentire ai prestatori di servizi di pagamento di applicare una commissione interbancaria per operazione non superiore a 0,05 euro, eventualmente combinata con una percentuale massima non superiore allo 0,2%, a condizione che la somma delle commissioni interbancarie dello schema di carte di pagamento non superi mai lo 0,2% del valore totale annuo delle operazioni nazionali tramite carta di debito all'interno di ciascuno schema di carte di pagamento.

Questo articolo si applica dal 9 dicembre 2015.

---

[13] La carta aziendale è definita dall'art. 1, comma 1, punto 6) del Regolamento come «*qualsiasi strumento di pagamento basato su carta emesso a favore di imprese o enti del settore pubblico o professionisti per uso limitato alle spese aziendali in cui i pagamenti effettuati con le carte in questione sono imputati direttamente al conto dell'impresa o dell'ente del settore pubblico o del professionista*».

[14] L'art. 2, comma 1, punto 18 del Regolamento definisce lo schema di carte di pagamento a tre parti: «*schema di carte di pagamento in cui lo schema stesso fornisce servizi di convenzionamento e di emissione e le operazioni di pagamento basate su carta sono effettuate dal conto di pagamento del pagatore al conto di pagamento del beneficiario nell'ambito dello schema. Lo schema di carte di pagamento a tre parti che concede ad altri prestatori di servizi di pagamento la licenza di emissione di strumenti di pagamento basati su carta o di convenzionamento di operazioni di pagamento basate su carta, o entrambi, o emette strumenti di pagamento basati su carta con un partner di carta multimarchio in* co-branding *o tramite un agente, è considerato uno schema di carte di pagamento a quattro parti*». Schema di pagamento a quattro parti è invece definito (punto 17) come «*schema di carte di pagamento in cui le operazioni di pagamento basate su carta sono effettuate dal conto di pagamento del pagatore verso il conto di pagamento del beneficiario tramite l'intermediazione dello schema, dell'emittente (dal lato del pagatore) e del soggetto convenzionatore (dal lato del beneficiario)*».

Fino al 9 dicembre 2020, per quanto riguarda le operazioni nazionali con carte di debito, gli Stati membri possono consentire ai prestatori di servizi di pagamento di applicare una commissione interbancaria media ponderata non superiore all'equivalente dello 0,2% del valore medio annuo di tutte le operazioni nazionali tramite carta di debito all'interno di ciascuno schema di carte di pagamento; gli Stati membri possono stabilire un massimale medio ponderato sulle commissioni interbancarie inferiore, applicabile a tutte le operazioni nazionali tramite carta di debito.

3. *Commissioni interbancarie per le operazioni tramite carta di credito a uso dei consumatori (art. 4)* – I prestatori di servizi di pagamento non offrono né chiedono una commissione interbancaria per operazione superiore allo 0,3% del valore dell'operazione per ogni operazione tramite carta di credito. Per le operazioni nazionali tramite carta di credito gli Stati membri possono stabilire un massimale per operazione sulle commissioni interbancarie inferiore.

Anche questo articolo si applica dal 9 dicembre 2015.

4. *Separazione tra schemi di carte di pagamento e soggetti incaricati del trattamento delle operazioni (art. 7)* – Gli schemi di carte di pagamento e i soggetti incaricati del trattamento delle operazioni sono indipendenti sotto i profili contabile, organizzativo e decisionale; non operano in alcun modo discriminazioni tra le proprie controllate o i propri associati; i soggetti incaricati del trattamento delle operazioni nell'Unione assicurano l'interoperabilità tecnica del loro sistema con altri sistemi di soggetti incaricati del trattamento nell'Unione.

Questo articolo si applica dal 9 giugno 2016.

5. *Multimarchio in co-badging*[15] *e scelta del marchio di pagamento o dell'applicazione di pagamento (art. 8)* – Sono vietate le regole dello schema di carte di pagamento e le clausole dei contratti di licenza, o misure aventi effetti equivalenti, che impediscono ad un emittente di riunire in *co-badging* uno o più marchi di strumenti di pagamento o applicazioni di pagamento su di uno strumento di pagamento basato su carta o che creano ostacoli in tal senso.

Quando stipula un contratto con un prestatore di servizi di pagamento, il consumatore può chiedere di avere due o più marchi di pagamento diversi sullo strumento di pagamento basato su carta, purché il prestatore di servizi di pagamento offra un siffatto servizio. Prima della firma del contratto, il prestatore di servizi di pagamento fornisce in tempo utile al consumatore informazioni chiare e obiettive su tutti i marchi di strumenti di pagamento disponibili e sulle loro caratteristiche, compresi funzionalità, costi e sicurezza.

Anche questo articolo si applica dal 9 giugno 2016.

---

[15] Così definito dall'art. 2, par. 1, punto 31) del Regolamento: «*inclusione di due o più marchi di pagamento o di due o più applicazioni di pagamento dello stesso marchio in uno stesso strumento di pagamento basato su carta*».

6. *Autorità competenti (art. 13)* – Gli stati membri designano le autorità competenti incaricate di assicurare il rispetto delle disposizioni del Regolamento, a cui siano attribuiti poteri di indagine e di controllo. Gli Stati membri prescrivono che le autorità competenti controllino efficacemente la conformità con il Regolamento.

In verità, poiché «*il presente Regolamento è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri*» – come recita la chiusa del provvedimento - il titolo IV-*bis* inserito nel d.lgs. 11/2010 non serve a recepirlo nell'ordinamento nazionale, quanto a sciogliere alcune alternative che, come si è visto, l'atto comunitario lascia agli Stati membri.

2.2 Il titolo IV-bis del d.lgs. 11/2010

Le corrispondenti scelte compiute dal legislatore nazionale sulla base del Regolamento sono le seguenti.

a) Art. 34-*bis*. Fino al 9 dicembre 2020, per le operazioni nazionali tramite carta di debito ad uso dei consumatori, gli intermediari possono applicare una commissione interbancaria media ponderata non superiore all'equivalente dello 0,2% del valore medio annuo di tutte le operazioni nazionali effettuate all'interno dello schema di pagamento.

Per far ciò, gli schemi di carte di pagamento:

– definiscono una struttura della commissione interbancaria media ponderata improntata a criteri di trasparenza, semplicità, confrontabilità ed equità, anche tenendo conto delle specifiche caratteristiche dell'operazione di pagamento;

– trasmettono alla Banca d'Italia una relazione periodica, illustrativa delle modalità di rispetto dei criteri di cui all'alinea precedente.

Fatto salvo quanto sopra, gli intermediari, per le medesime operazioni, possono applicare altresì una commissione interbancaria non superiore a 0,05 euro per ciascuna operazione, commissione che può anche essere combinata con una percentuale massima non superiore allo 0,2% del valore di ciascuna operazione a condizione che la somma delle commissioni applicate non superi mai lo 0,2% del valore totale annuo delle operazioni nazionali effettuate all'interno dello schema di pagamento. Anche per questa ipotesi gli intermediari trasmettono alla Banca d'Italia una relazione periodica, illustrativa delle modalità di rispetto dei criteri seguiti.

In ogni caso, per le operazioni nazionali tramite carta di debito ad uso dei consumatori di importo inferiore a 5 euro, gli intermediari applicano una commissione interbancaria di importo ridotto rispetto a quelle applicate per operazioni di importo pari o superiore.

Quanto fin qui illustrato si applica anche alle carte prepagate.

La Banca d'Italia definisce modalità e termini per l'invio delle informazioni indicate, che devono essere certificate da un revisore indipendente.

b) Art. 34-*ter*. La riduzione delle operazioni di importo inferiore a 5 euro e la previsione della Banca d'Italia che determina le modalità di invio delle informazioni sono estese alle operazioni nazionali tramite carta di credito ad uso dei consumatori.

c) Art. 34-*quater*. La Banca d'Italia è designata quale autorità competente ai sensi del Regolamento e adotta le proprie decisioni previo parere dell'Autorità Garante della Concorrenza e del Mercato (AGCM).

L'AGCM è designata quale autorità competente per l'inibizione della continuazione e la rimozione degli effetti delle pratiche commerciali scorrette ai sensi del codice del consumo. Nell'esercizio di questa competenza, l'Autorità, qualora la condotta illecita sia posta in essere da un soggetto sul quale la Banca d'Italia esercita i propri poteri di vigilanza o sorveglianza, adotta le proprie decisioni previo parere della Banca d'Italia.

Le autorità collaborano nell'esercizio delle proprie competenze e non possono opporsi reciprocamente il segreto d'ufficio. Alla Banca d'Italia sono attribuiti poteri sanzionatori, di indagine e di controllo; all'AGCM competono i poteri di cui all'art. 27 cod. cons. ("Tutela amministrativa e giurisdizionale").

2.3 Il provvedimento di attuazione della Banca d'Italia

In riferimento alle previsioni stabilite negli articoli sopra riportati, la Banca d'Italia ha avviato l'8 febbraio 2018 la consultazione di uno schema di provvedimento:

a) risulta applicabile agli schemi di carte di pagamento che prestano i propri servizi nel territorio della Repubblica e la cui *governance authority* ha sede legale ubicata in uno Stato membro; definisce le informazioni e i dati che detti schemi sono tenuti a notificare alla Banca d'Italia, nonché la tempistica e le modalità di trasmissione delle segnalazioni per consentire la verifica del rispetto dei massimali alle commissioni interbancarie;

b) stabilisce una serie di obblighi di condotta, alcuni dei quali indirizzati direttamente agli schemi di carte di pagamento. Per consentire un controllo efficace del rispetto di tali previsioni, in linea con l'art. 13 del Regolamento, il provvedimento individua le informazioni che la *governance authority* dello schema di carte deve trasmettere alla Banca d'Italia. Al fine di ridurre gli oneri segnaletici in capo agli operatori, tale comunicazione va effettuata *una tantum* ed è aggiornata solo in caso di cambiamenti relativi alle informazioni comunicate;

c) dispone, per facilitare il dialogo con gli operatori, che tutte le informazioni fin qui indicate sono trasmesse alla Banca d'Italia tramite l'ufficio di rappresentanza che gli schemi operanti in Italia sono tenuti a istituire, dopo essere state certificate da un revisore indipendente. Il requisito dell'indipendenza viene valutato tenendo conto di quanto disposto dal d.lgs. 27 gennaio 2010, n. 39, come modificato dal d.lgs. 17 luglio 2016, n. 135, relativi alla disciplina della revisione legale dei conti annuali e dei conti consolidati.

Esaurita la fase della consultazione, è stato emanato il provvedimento della Banca d'Italia dell'11 ottobre 2018.

Al fine di consentire ai prestatori di servizi di pagamento di sfruttare la possibilità transitoria (fino al 9 dicembre 2020) di applicare una commissione interbancaria media ponderata non superiore all'equivalente dello 0,2% del valore medio annuo di tutte le operazioni nazionali effettuate tramite tali strumenti all'interno dello stesso schema di carte di pagamento, il provvedimento della Banca d'Italia ha prescritto che i prestatori dei servizi devono:

- definire una struttura della commissione interbancaria media ponderata improntata a criteri di trasparenza, semplicità, confrontabilità ed equità, anche tenuto conto delle specifiche caratteristiche dell'operazione di pagamento;
- trasmettere alla Banca d'Italia una relazione illustrativa delle modalità di rispetto dei criteri di cui al punto precedente.

Pertanto, la previsione del d.lgs. n. 218/2017 e il provvedimento di attuazione «*abilitano un percorso di migrazione rivolto unicamente ai prestatori di servizi di pagamento che emettono carte di debito e prepagate entro i confini nazionali che terminerà a dicembre 2020, a conclusione del quale si applicherà comunque il regime di commissione per transazione (0,05 euro di soglia massima) eventualmente combinato con una fee in percentuale dell'importo transato (in ogni caso non superiore allo 0,2%) come previsto a regime dal regolamento stesso*»[16].

2.4 L'evoluzione delle commissioni interbancarie

Il complesso normativo sopra illustrato rappresenta, ad oggi, il punto di caduta di un percorso che si è caratterizzato per diverse angolazioni e valutazioni, risultando le MIF (*multilateral interchange fee*) l'aspetto più discusso della struttura tariffaria delle operazioni di pagamento.

L'avvio di questo percorso si muove prendendo atto che i sistemi di pagamenti costituiscono "industrie di rete", nel senso che i prodotti/servizi ivi scambiati sono offerti o domandati attraverso una pluralità di nodi, collegati da più infrastrutture

---

[16] R. Garavaglia, *E che PSD" sia!...! – Settima puntata: le commissioni applicabili alle transazioni di pagamento nazionale con carte*, in www.pagamentidigitali.it, 16 novembre 2018.

condivise, che permettono ai diversi soggetti (utenti e intermediari) di scambiare informazioni e disposizioni di incasso e pagamento. Il valore attribuito al servizio è funzione del numero di utenti e del grado di diffusione del circuito: «*ogni nuovo utente aumenta l'utilità per coloro che già consumano il servizio; uno strumento di pagamento aumenta valore solo se è sempre più accettato da altre parti*»[17].

In tale contesto, le MIF rappresentano il corrispettivo che, in ciascuna transazione con carta, l'*acquirer* (la banca o il prestatore di servizi di pagamento che ha convenzionato l'esercente per il servizio di accettazione delle carte) paga all'*issuer* (all'emittente la carta o alla banca emittente) quale remunerazione per i servizi forniti all'esercente, fra i quali la garanzia di pagamento in caso di frode o d'insolvenza del titolare della carta. «*In un mercato a due versanti (*two-sided market) – *come quello dei pagamenti – i circuiti bilanciano attraverso le MIF gli interessi di entrambi i versanti (gli esercenti e i titolari di carta) in modo che ciascun versante sopporti un'equa percentuale di costi per i benefici che riceve*»[18]. In caso di commissioni interbancarie di livello troppo basso, gli esercenti si gioverebbero di benefici senza pagarli adeguatamente e l'*issuer* finirebbe per compensare tale mancata remunerazione mediante un incremento dei prezzi verso i titolari delle carte ovvero mediante una diminuzione degli investimenti.

Di qui l'esigenza di pervenire a un bilanciamento quanto più possibile adeguato della misura delle MIF per evitare gli inconvenienti menzionati e rendere più efficiente il sistema. Sotto questo aspetto sono stati nel tempo prodotti molti modelli che avevano come finalità il raggiungimento di tale scopo, ma sono chiaramente emersi «*i limiti dei numerosi modelli teorici sviluppati dalla letteratura economica*», atteso che «*la CIM* [commissione interbancaria multilaterale] *determinata privatamente può essere superiore o inferiore a quella ottimale socialmente*»[19].

Premesso come non sia logicamente da escludere in principio l'esistenza di un mercato privo di commissioni interbancarie[20], la loro giustificazione riposa su valutazioni empiriche, sui costi di transazione che l'assenza delle stesse provocherebbe, sulle complicazioni operative connesse alla conclusione di una serie di accordi bilaterali o multilaterali ma non riguardanti tutti gli operatori, e così via. Il *leading case* a questo riguardo può essere rintracciato nella decisione Visa International del 9 agosto 2001[21], in cui si sono ribaditi i benefici della commissione interbancaria, la

---

[17] G. Ardizzi e M. Condemi, *La tutela della concorrenza nei sistemi di pagamento*, in *Il diritto del sistema dei pagamenti*, a cura di G. Carriero e V. Santoro, Milano, 2005, p. 616.

[18] A. De Matteis, *Commissioni interbancarie: legittime per la Corte di giustizia quando forniscono benefici per gli esercenti*, in www.dirittobancario.it, novembre 2014.

[19] A. Minuto Rizzo, *Le carte di pagamento tra antitrust e regolamentazione*, in *Mercato, concorrenza e regole*, 2015, p. 367.

[20] E ciò è stato affermato in relazione alle MIF praticate da Mastercard nelle decisioni della Commissione del 2007: IP/071959 e MEMO/07/590, su cui cfr. E. Rossello, *Servizi bancari al dettaglio: nuova indagine antitrust sulla commissione interbancaria unilaterale*, in www.dirittobancario.it, giugno 2013, p. 3.

[21] Decisione della Commissione relativa ad un procedimento a norma dell'articolo 81 del trattato CE, dell'articolo 53 dell'accordo SEE (Caso Comp/D1/29.373 – Visa International), notificata con il numero C(2001) 2425.

cui assenza comporterebbe alti costi di transazione per le banche e quindi maggiori oneri per la clientela finale. Del resto, la necessità di riferirsi all'intero settore rende la MIF di per sé oggetto di un accordo valutabile sotto il profilo della restrizione della concorrenza, senza contare poi la tendenza degli *issuers* «*ad offrire la carta con la MIF più elevata e degli esercenti ad accettare carte di pagamento anche troppo onerose rispetto ai benefici che ne traggono*»[22], circostanza che non può non generare profili di attenzione nell'ottica del rispetto delle regole del libero mercato.

Di qui l'esigenza di un controllo che le autorità antitrust, comunitarie e nazionali, hanno avviato ribadendo che siffatti accordi di prezzo potessero ottenere l'autorizzazione in deroga (ai sensi dell'art. 101, par. 3 TFUE ovvero dell'art. 4 della legge n. 287/1990) laddove, previe verifiche caso per caso, si accertasse l'esistenza delle quattro condizioni previste: (i) miglioramenti nelle condizioni di offerta sul mercato; (ii) sostanziale beneficio per i consumatori; (iii) restrizioni alla concorrenza strettamente indispensabili per il conseguimento delle finalità di cui sopra; (iv) non eliminazione della concorrenza in una parte sostanziale del mercato.

La scelta quindi è nel senso di rispettare la natura privatistica degli accordi, riservandosene l'autorità una valutazione in termini di rispetto della competitività e, segnatamente, dei requisiti giustificativi di una autorizzazione in deroga. L'efficientamento del sistema dei pagamenti attraverso la MIF passa per la misurabile capacità della stessa di portare un vantaggio alle parti coinvolte e segnatamente ai clienti, vale a dire a una diminuzione complessiva dei costi: di qui l'affermarsi di metodologie di calcolo delle commissioni basate sull'analisi dei costi del servizio che esse intendevano remunerare. Ciò tendeva a un duplice scopo: ancorare a elementi oggettivi il criterio di calcolo delle MIF e spingere verso una costante diminuzione dei costi, in connessione con l'accrescersi di economie di scala e connesse allo sviluppo tecnologico.

Ma siffatto orientamento non è stato né costante nella direzione, né fermo nelle metodologie[23].

Sotto il primo profilo non sono mancate decisioni che hanno negato la legittimità delle commissioni interbancarie nell'ottica del rispetto della concorrenza[24], conformi a posizioni delle Autorità, come la Comunicazione Congiunta BCE/Commissione europea del marzo 2009, secondo la quale, «*sulla base delle informazioni a disposizione, non si ritiene che sussistano chiare e convincenti ragioni per consentire la sopravvivenza di un sistema di commissioni*

---

[22] A. Minuto Rizzo, *Le carte di pagamento tra antitrust e regolamentazione*, cit., p. 368.

[23] È doveroso metodologicamente affermare che quanto si esporrà vale per le commissioni interbancarie come categoria concettuale, indipendentemente dalla circostanza che se ne discuta nell'ambito delle carte o di altre operazioni di pagamento, poiché, ai fini del discorso prospettico che si è inteso affrontare, siffatta distinzione non appare particolarmente rilevante.

[24] Vedi ad esempio la decisione della Corte di Giustizia UE nella sentenza C-382/12, depositata l'11 settembre 2014 per il caso MasterCard. Cfr. al riguardo A. De Matteis, *Commissioni interbancarie: legittime per la Corte di Giustizia quando forniscono benefici per gli esercenti*, cit.

interbancarie dopo il 31 ottobre 2012»[25]; né, come si dirà fra breve, preferenze verso un indirizzo prescrittivo piuttosto che di rispetto delle decisioni del mercato.

Sotto il secondo profilo si è dubitato che la metodologia della connessione costi/commissioni sia la più corretta, come dimostra anzitutto la circostanza che si è teso ad azzerare gli uni per azzerare le seconde: nel nostro paese infatti, l'Autorità Garante «*ha promosso l'innesto di correttivi nel processo di formazione del valore della commissione di volta in volta all'esame, in vista della progressiva riduzione della sua entità e, in ultima analisi, del suo azzeramento. Più in particolare, ha confermato che in linea di principio gli accordi tesi all'uniformazione della suddetta componente di costo rischiano di rallentare la concorrenza all'interno del circuito e di interferire su quella tra sistemi, rispetto ad una variabile di primario rilievo concorrenziale. Quindi, a fronte dell'attivazione di sub-procedimenti con impegni, l'Autorità ha deliberato altrettante decisioni "patteggiate", volte a rimediare alle imperfezioni dello schema prescelto attraverso l'introduzione (concordata) di "anticorpi" concorrenziali che simulano quei meccanismi di competitività che un regolatore potrebbe, se del caso, attivare (in via forzosa) per correggere quelle stesse disfunzioni*»[26].

Ma, a conferma del disorientamento a livello comunitario, si dubita che la minor incidenza sulla concorrenza possa essere garantita da MIF parametrate ai costi e a quel criterio si sostituisce il c.d. "*tourist test*"[27]: la commissione «*viene* (…) *calcolata seguendo una metodologia in base alla quale gli esercenti non devono corrispondere commissioni superiori ai benefici che l'utilizzo delle carte genera per loro rispetto al contante. La commissione a carico degli esercenti non può eccedere tale beneficio netto, diversamente gli stessi non troverebbero conveniente accettare carte in sostituzione del contante*». Tuttavia neppure questa nuova metodologia è stata considerata appagante, dal momento che «*essa attribuisce rilevanza solamente al profilo dell'indifferenza dell'esercente e non considera invece – come dovrebbe essere in un mercato a due versanti – gli interessi del consumatore titolare di carta*»[28]. E del resto in nessuna decisione comunitaria e nazionale, salve enunciazioni di principio, vengono esplicitate «*la struttura e le modalità di funzionamento del modello.* [Va quindi confermato che] *il* tourist test *può sì tenere conto di esternalità*

---

[25] «*La posizione recentemente sostenuta dalla Banca Centrale e dalla Commissione Europea è significativa: nella Comunicazione Congiunta del marzo 2009 queste hanno di fatto negato la compatibilità con le regole antitrust degli schemi di remunerazione (delineati con riguardo al servizio di addebito diretto) basati su un meccanismo di commissioni interbancarie, sancendone l'illiceità in sé e per sé alla scadenza di un periodo di grazia della durata di tre anni*»: V. Falce, *Il funzionamento dei sistemi di pagamento al dettaglio. Ancora in materia di commissioni interbancarie*, in *Armonizzazione europea dei servizi di pagamento e attuazione della direttiva 2007/64/CE*, a cura di M. Rispoli Farina, Milano 2009, p. 531.

[26] V. Falce, *Dalla self-regulation al payment package. Storia delle commissioni interbancarie*, in www.dimt.it, 2015.

[27] Un primo accenno a questo criterio è contenuto nelle due decisioni dell'8 dicembre 2010 e del 26 febbraio 2014 rese dalla Commissione nei riguardi di VISA e meglio note come VISA I e VISA II.

[28] A. De Matteis, *Commissioni interbancarie: legittime per la Corte di Giustizia quando forniscono benefici per gli esercenti*, cit., p. 5.

ed effetti di rete, ma solo di quelli interni al sistema, così da scartarlo dalle tecniche elettive per massimizzare il benessere del consumatore»[29].

È evidente che in una simile situazione la fiducia in una soluzione di mercato per l'efficienza e la competitività delle MIF è progressivamente venuta meno: con il Regolamento (CE) n. 2560/2001 si è stabilita la parità di commissioni fra pagamenti nazionali e comunitari nell'area SEPA per gli addebiti diretti; con il Regolamento (UE) n. 260/2012 si è fissata *ex ante* e per un periodo transitorio la MIF per il SEPA addebiti diretti; infine, il Regolamento sopra esposto ha, con riferimento stavolta alle carte ma nella medesima logica, previsto una commissione interbancaria massima, articolata nel modo che si è detto.

Per completezza va altresì ricordato che il d.m. 14 febbraio 2014, n. 51, del Ministro dell'economia aveva dato attuazione a una sorta di intervento latamente "dirigistico" previsto dall'art. 12 del d.l. 201/2011, convertito nella legge n. 214/2011, il quale stabiliva che ABI, Associazione di prestatori di servizi di pagamento, Poste Italiane, Consorzio Bancomat, imprese che gestiscono circuiti di pagamento e Associazioni delle imprese maggiormente significative a livello nazionale, dovessero stabilire, entro il 1° giugno 2012, e applicare per i tre mesi successivi, le regole generali per assicurare (i) una riduzione delle commissioni a carico degli esercenti in relazione alle transazioni effettuate tramite carte, (ii) la trasparenza e chiarezza dei costi, (iii) la promozione dell'efficienza economica nel rispetto delle regole di concorrenza. Il comma 10 del medesimo articolo disponeva che, entro i sei mesi successivi all'applicazione di dette misure, il Ministero dell'economia doveva valutarle; in caso di mancata definizione e applicazione delle stesse (comma 12), doveva fissarle con decreto.

Tuttavia, a dire il vero, di dirigismo in senso proprio non può parlarsi perché il menzionato d.m. n. 51/2014 (c.d."decreto *merchant fee*") «*non definiva alcun limite alle commissioni, mentre rimarcava alcuni aspetti* (…) *molto rilevanti*»[30], a cominciare dal rafforzamento della trasparenza, limitando il c.d. *blending*, cioè l'applicazione di tariffe uniformi (o "a pacchetto"), non differenziate per tipologie di carta, al fine di migliorare il confronto fra le commissioni pagate dall'esercente. In particolare, gli *acquirers* erano tenuti «*a distinguere le commissioni da applicare per ciascuna tipologia di carte di pagamento – di debito, di credito, prepagate – anche in relazione ai diversi circuiti di riferimento nonché a ulteriori eventuali specifiche caratteristiche funzionali delle carte medesime*» (art. 3, comma 1 del d.m.); d'altro canto «*gli* acquirers *differenziano l'importo delle commissioni applicate agli esercenti e le sottopongono a revisione* [almeno annuale: art. 6], *tenendo anche conto delle economie di scala e di scopo collegate ai volumi delle transazioni eseguite con carta presso ciascun esercizio ovvero presso gruppi di esercenti unitariamente convenzionati*» (art. 3, comma 2).

---

[29] V. Falce, *Dalla self-regulation al payment package. Storia delle commissioni interbancarie*, cit.

[30] R. Garavaglia, *E che PSD" sia…! Seconda puntata: le commissioni dei pagamenti con carte*, in www.pagamentidigitali.it, 26 gennaio 2018.

Ancora: i gestori dei circuiti devono rendere noti e mantenere aggiornate le eventuali connessioni di interscambio applicate alle operazioni (art. 4) e redigere l'informativa precontrattuale in maniera tale da consentire all'esercente di comprendere i costi e le caratteristiche del servizio e di confrontare i prodotti offerti (art. 5). Insomma, disposizioni certamente prescrittive e impositive, ma nessuna che determini la misura della MIF.

2.5 Il Regolamento vigente: realtà e prospettive

Il percorso che si è ricostruito sembra quindi avviato su un versante molto diverso da quello dal quale era partito: non sembrano esserci più pregiudizi sulla legittimità della MIF, riconosciuta come un meccanismo che presenti vantaggi maggiori rispetto ai rischi di alterazione della concorrenza, rischi che in ogni caso possono essere evitati con un'autorizzazione in deroga. La questione quindi pare essersi spostata dalla liceità alla misura, rispetto alla quale tuttavia non si è stati in grado a livello europeo di fornire metodologie di calcolo affidabili.

Di qui, nella prospettiva, mai abbandonata, dell'art. 101, par. 3 TFUE, si potrebbe dire che la scelta di determinare autoritativamente questa misura, sia pure nel livello massimo, prende il posto di quella costruita, se si fosse in un ambiente di accordo multilaterale "eterodiretto", con le metodologie governate dalle autorità, presupposto necessario, insieme alla ricorrenza degli altri requisiti, per conseguire l'autorizzazione in deroga[31].

Per la verità, l'approccio regolamentare sembra ammettere implicitamente la legittimità delle MIF (o più semplicemente non chiederselo pragmaticamente più, una volta riscontrata la loro necessità/opportunità), tagliando gordianamente il nodo del loro giusto prezzo e dei criteri da utilizzare per determinarlo. Certamente si è preferito superare le incertezze del mercato e delle autorità che lo controllano – «*il Regolamento riconosce il fallimento della mano invisibile*»[32] –

---

[31] Sempre nella logica della determinazione della MIF per via convenzionale, sia pure etero diretta, mette conto riportare il considerando 20 del Regolamento 2015/751: «*i massimali di cui al presente regolamento sono basati sul cosiddetto "test di indifferenza per l'esercente" (*"Merchant Indifference Test*") sviluppato nella letteratura economica, che consente di determinare il livello delle commissioni che l'esercente sarebbe disposto a pagare se l'esercente stesso dovesse confrontare il costo che deve sostenere in caso di uso da parte dei consumatori di una carta di pagamento e il costo sostenuto in caso di pagamento (in contante) senza carta (tenendo conto della commissione per i servizi pagata alla banca convenzionatrice, vale a dire la commissione per i servizi all'esercente e la commissione interbancaria). Si stimola in tal modo l'uso di strumenti di pagamento efficienti mediante la promozione delle carte che offrono benefici commerciali più elevati, evitando allo steso tempo che agli esercenti vengano applicate commissioni sproporzionate, con la conseguente imposizione di costi nascosti ad altri consumatori. Commissioni eccessive per gli esercenti potrebbero anche essere dovute agli accordi collettivi sulle commissioni interbancarie, perché gli esercenti sono riluttanti a rifiutare strumenti di pagamenti costosi per timore di perdere un affare. L'esperienza ha dimostrato che tali livelli sono proporzionati e non rimettono in questione il funzionamento degli schemi di carte di pagamento e dei prestatori di servizi di pagamento internazionali. Essi presentano anche benefici per gli esercenti e i consumatori e creano certezza del diritto*».

[32] V. Falce, *Dalla self-regulation al payment package. Storia delle commissioni interbancarie*, cit.

e prendere atto della difficoltà di pervenire per questa via a risultati soddisfacenti e stabili e scegliere la strada della conformazione, se non del dirigismo.

Certo anche la semplice costruzione di questa alternativa non è esente da pecche, per così dire, strutturali: si determina la misura della commissione in esito a un'analisi dei costi gestita con un metodo che le stesse autorità europee non erano state capaci di definire, tanto che non era stato mai completamente e chiaramente applicato e in compenso fortemente criticato; si è posta in essere un'operazione che porterà, come sempre nei casi di determinazione di commissioni massime, a un adeguamento verso l'alto delle MIF applicate, sicché più che di un prezzo massimo, si tratta di un prezzo imposto e basta. Tanto più che il contenimento dei costi di negoziazione di commissioni non multilaterali costituisce proprio uno dei motivi della permanenza delle MIF.

È saggio affermare che «*è presto per trarre conclusioni o esprimere valutazioni sull'effettività degli strumenti introdotti nella prospettiva del benessere del consumatore*»[33]. Eppure qualche valutazione negativa già espressa induce talune perplessità sulla validità della via intrapresa dal regolatore.

A. Buona parte del già citato contributo di Minuto Rizzo è dedicata al commento del Regolamento in esame, riguardato sotto diversi profili, di tratto anzitutto economico.

La prima motivazione dell'intervento dirigistico consisterebbe nell'asserito fallimento dell'azione antitrust. Se tale azione avrebbe potuto manifestarsi con maggior chiarezza e puntualità e minori incertezze e cambiamenti di rotta, va anche precisato che tali caratteristiche apparentemente negative sono state spesso dovute alla circostanza che si sono registrate situazioni di mercato diverse, per le quali non era agevole (e forse nemmeno corretta) un'unitarietà di soluzioni. In altri termini, «*le differenze esistenti* (…) *tra mercati rilevanti in Stati membri distinti potrebbero in alcuni casi riflettere diversità strutturali di cui può essere opportuno tenere conto nella definizione del livello appropriato della CIM. L'eliminazione di tali differenze per via regolamentare, in assenza di un'accurata valutazione di tali eventuali diversità strutturali, attiene più ad obiettivi di integrazione in un mercato unico europeo che a valutazioni di efficienza più tipicamente concorrenziali*»[34].

La seconda ragione dell'intervento regolatorio parrebbe sostanziarsi negli effetti perversi della concorrenza fra circuiti, che produrrebbe prezzi più elevati per i consumatori e non già riduzione. Le esternalità presenti nei servizi di pagamento e generatrici di conseguenze concorrenziali pericolose sarebbero le seguenti: (i) da un lato, l'esercente può non accettare una carta che il titolare vorrebbe utilizzare, implicando una perdita di *surplus* per il titolare stesso; (ii) dall'altro – e per converso – il titolare potrebbe preferire un mezzo di pagamento più oneroso per l'esercente, generando così una perdita di *surplus* per l'esercente. Ma se così è, la

---

[33] V. Falce, *op. ult. cit.*

[34] A. Minuto Rizzo, *Le carte di pagamento tra antitrust e regolamentazione*, p. 378.

finalità non è quella di mettere fine al rialzo della CIM, ma di regolarne la misura a un livello tale che consenta il non prodursi di tali esternalità. Ma allora una corretta applicazione del sistema del *tourist test*, ovvero la creazione dell'indifferenza fra l'uso del contante e delle carte, può rappresentare un'alternativa migliore rispetto alla fissazione d'ufficio del massimale della commissione[35].

In terzo luogo, nel Regolamento, *tourist test* e sovraprezzi sono considerati strumenti alternativi: per i circuiti a quattro parti, la CIM è regolata sulla base del *tourist test* e l'applicazione di sovrapprezzi non è consentita, mentre con riguardo ai circuiti a tre parti, e alle carte aziendali dei circuiti a quattro parti, non è prevista alcuna regolamentazione delle rispettive CIM e l'applicazione di sovrapprezzi è consentita. Invero, il modello applicato è equivalente alla possibilità di applicare sovrapprezzi, nel senso che esso simula gli esiti di mercato che si realizzerebbero se non ci fossero i sovrapprezzi: di qui l'alternatività e l'affermazione, nel Regolamento, per cui il divieto di imporre sovrapprezzi sta nella necessità di incoraggiare la concorrenza e promuovere l'utilizzo di strumenti di pagamento efficienti. Ciò vuol dire che «*l'utilizzo di strumenti di pagamento efficienti*» non è stato raggiunto in altro modo e che l'unica via percorribile consiste nella eliminazione dei sovrapprezzi. Detto meglio: il contenimento dell'uso del contante e la promozione delle carte s'intende realizzarlo vietando la possibilità di applicare sovrapprezzi a fronte dei pagamenti con carta. «*Tale obiettivo, pur condivisibile, soprattutto in un paese come l'Italia caratterizzato da una diffusa economia sommersa, potrebbe essere raggiunto con altri strumenti di intervento pubblico, affrontando direttamente la problematica dell'evasione fiscale, senza alterare la concorrenza tra strumenti di pagamento alternativi*»[36]. Si tratta di una osservazione su cui è facile concordare ma per la quale è altrettanto facile notare come la lotta all'evasione fiscale evoca scenari e problemi che vanno ben al di là della questione affrontata.

In quarto luogo, viene sottolineata la fragilità del modello del *tourist test* non nelle sue finalità, bensì nelle corrette modalità di applicazione, difficoltà che si esaltano quando si intende dedurre dalla sua applicazione una misura unica e valida in tutti i casi. E questo comporta un rischio di fallimento della regolamentazione, rispetto al quale un'applicazione più flessibile e decentrata del *tourist test* potrebbe consentire di cogliere meglio le differenze strutturali tra singoli Stati membri in termini di eterogeneità degli esercenti e livello di

---

[35] Poiché detta misura è calcolata proprio con il modello dei *tourist test*, forse la critica consiste nella circostanza che la via scelta dalla Commissione Europea irrigidisce la commissione generalizzandola, invece di essere flessibile e applicabile caso per caso attraverso un corretto utilizzo del modello nell'ambito delle indagini antitrust.

[36] A. Minuto Rizzo, *Le carte di pagamento tra antitrust e regolamentazione*, p. 382. Anzi, sul sovrapprezzo la posizione di questo a. è di segno opposto a quello seguito dal Regolamento: «*al fine di* facilitare *la comparazione tra strumenti alternativi in base a considerazioni di efficienza, la possibilità di applicare sovrapprezzi con riguardo ai pagamenti con carta andrebbe estesa anche ai pagamenti in contante.* (…) *con la possibilità di applicare sovrapprezzi e sconti, sia con riguardo alle carte di pagamento sia al contante, accompagnata da una maggiore consapevolezza dei costi privati di accettazione del contante, possono essere forniti segnali di pezzo in grado di orientare i consumatori verso gli strumenti più efficienti per gli esercenti*» (pp. 385-386).

diffusione del contante. «*Ciò riporterebbe l'obiettivo della regolamentazione maggiormente in linea con considerazioni di efficienza del sistema e meno di integrazione in un mercato unico*»[37].

Le osservazioni riportate indicano controindicazioni all'approccio dirigistico e privilegiano piuttosto la flessibilità di soluzioni che tornino al mercato e alla competitività. Il massimale sulle MIF aiuta l'integrazione dell'area dei pagamenti europea, ma né il rispetto della concorrenza e né la diffusione di strumenti di pagamento più efficienti.

Le questioni di fondo che questo Regolamento pone (che devono essere verificate dall'esperienza, ma che già si profilano concettualmente) attengono in sostanza alla corrispondenza della scelta operata con le finalità perseguite: salvaguardia della concorrenza e orientamento verso lo strumento di pagamento più efficiente. Appare, almeno in principio, convincente ritenere inadeguata in questo ambito la via di un'unica misura di commissione valida per tutti i soggetti, tutte le operazioni e tutte le carte interessate e, per contro, tendenzialmente migliore una soluzione che tenga maggiormente conto delle segmentazioni dei mercati, anche a livello territoriale, e delle specifiche caratteristiche che essi presentano.

B. Un altro aspetto su cui i primi commentatori si sono soffermati consiste nell'interrogarsi sull'effetto che il massimale della MIF potrà avere sul cliente finale. Il Regolamento agisce su una sola delle componenti dei costi di cui l'esercente è gravato (l'*interchange fee* e non la MSC – *merchant service charge*), lasciando aperta la competizione sul fronte degli *acquirers* e liberi costoro di sviluppare offerte di convenzionamento più convenienti[38]: «*ove così fosse, l'esercente avrebbe effettivamente un beneficio che, in linea di principio, potrebbe addirittura pensare di riversare (almeno parzialmente) sul prezzo all'utente finale*»; per altro verso, sul lato dell'*issuer*, poiché la MIF costituisce per costui un ricavo, la riduzione della stessa «*potrebbe riversarsi negativamente sul consumatore-titolare della carta. Mediante l'aumento di altri costi, come la* card subscription fee *o i costi di ricarica delle carte prepagate*»[39].

«*Questi timori – già espressi dall'ABI e da diverse associazioni di consumatori –, sono fondati sulle esperienze di Paesi – quali ad esempio Spagna, Australia e USA –, in cui le commissioni interbancarie sono state oggetto*

---

37 A. Minuto Rizzo, *Le carte di pagamento tra antitrust e regolamentazione*, p. 384.

38 «*Nella prassi commerciale le commissioni interbancarie rappresentano la maggior parte delle commissioni addebitate dagli emittenti carte di pagamento agli esercenti, i quali tendono a loro volta a ricomprendere l'ammontare pagato a titolo di commissione interbancaria nel prezzo al dettaglio applicato per beni e servizi. Ne deriva quindi che tali commissioni risultano in concreto a carico dei consumatori cui in modo poco trasparente sono addebitati dei costi legati allo specifico metodo di pagamento utilizzato. Intervenendo sul punto il Regolamento MIF introduce quindi dei limiti all'applicabilità delle commissioni interbancarie*»: F. Cascinelli, V. Pistoni, G. Zanetti, *La Direttiva (UE) 2015/2366 relativa ai servizi di pagamento nel mercato interno*, in www.dirittobancario.it, luglio 2016, p. 11.

39 R. Garavaglia, *Entrano in vigore le soglie massime per le commissioni dei pagamenti con carta previste dal Regolamento (UE) 201%751: un vademecum per orientarsi meglio*, in www.pagamentidigitali.it, 9 dicembre 2015.

di regolamentazione. Esperienze che hanno dimostrato come la riduzione dei costi per gli esercenti dovuta alla riduzione delle MSC (e quindi, in primis*, anche delle MIF), non genererebbe, di per sé, una correlata riduzione dei prezzi al dettaglio*»[40].

Anzi, è qui che inizierebbero le dolenti note per il consumatore: «*quel che le banche perdono in termini di commissione pagata dal commerciante lo recuperano facilmente aumentando altri oneri per il titolare. In particolare, hanno aumentato il costo di emissione e il canone annuo delle carte che oggi facilmente si ragguaglia a 50 e più euro. Gli economisti chiamano questo modo di operare* spillover effect. *Termine appropriato perché indica la capacità di imporre i propri prezzi quando si ha una rilevante posizione di mercato, cambiando l'ambito di applicazione delle tariffe. Cioè si può passare dalla tariffazione del servizio (le singole transazioni) a quella del prodotto (le carte emesse) a quella della infrastruttura, tramite il canone dei POS*»[41].

Ovviamente occorre verificare quale sarà l'effetto del provvedimento regolamentare sul mercato; ma se fosse questo, certo occorrerebbe un'attenta verifica sulla politica della Commissione in termini di strumenti di pagamento, tutela della concorrenza e rafforzamento dell'efficienza, obiettivi che, se mancati, esporrebbero operatori e clienti a conseguenze negative non poco rilevanti e all'urgente necessità di intervenire di nuovo e secondo parametri diversi.

C. Dubbi e riserve discendono poi dal fatto che la normativa in esame, come si è detto, non si applica a tutte le tipologie di carta, ma solo a quelle che si basano sugli schemi "a quattro parti" (Mastercard e Visa), restando escluse le operazioni di pagamento basate sugli schemi "a tre parti", ossia quei circuiti che non si avvalgono di *issuer* e *acquirer* e per i quali le commissioni interbancarie sono implicite), riconducibili ad operatori quali American Express, Diners e Paypal. «*Sebbene l'obiettivo dichiarato dalla Commissione sia quello di garantire un* level playing field *tra gli operatori di mercato, vale a dirsi un seppur minimo livello di tutela della concorrenza nel settore, l'ingiustificata esclusione dei circuiti a tre parti è fonte di serie preoccupazioni circa l'efficacia stessa del regolamento, non determinando esso, di fatto, una parità di condizioni tra i concorrenti*»[42].

Ed allora – dicono i rappresentanti dei consumatori – c'è anche il rischio che «*la nuova norma, applicabile solo ad alcuni tipi di carte e non a tutti, possa contribuire alla lesione della libera concorrenza, denuncia l'Italian E-Payment Coalition (IEPC), un'iniziativa di Assoutenti, Cittadinanzattiva,*

---

[40] C. Amalfitano, *La proposta di regolamento della Commissione sulle Multilateral Interchange Fees: si tratta davvero di uno strumento a tutela della concorrenza e dei consumatori?*, in www.eurojus.it, 12 marzo 2015, § 5.

[41] G. Coppola, *Il gioco delle tre carte (di pagamento)*, in www.economiaefinanzaverde.it, 3 aprile 2019.

[42] C. Amalfitano, *La proposta di regolamento della Commissione sulle Multilateral Interchange Fees*, cit., § 5.

Confconsumatori e Mdc nata per informare sul corretto uso della moneta elettronica. Secondo la IEPC, le conseguenze negative per i consumatori saranno due: i possessori di carte soggette alla norma potrebbero ritrovarsi a pagare canoni annui più alti a causa del probabile aumento dei costi disposto dalle banche per fronteggiare i mancati ricavi delle commissioni, mentre per i titolari di carte commerciali come Diners e American Express il rischio è di subire da parte dei commercianti un sovrapprezzo sull'acquisto pari alla commissione applicata»[43].

L'esclusione dei circuiti a tre parti dall'applicazione del Regolamento «*orienterà i consumatori verso tali schemi, danneggiando così la concorrenza. I circuiti a tre parti potranno infatti continuare a garantire condizioni economiche vantaggiose per i titolari di carta, mentre gli* issuers *dei circuiti a quattro parti non potranno continuare a offrire ai propri clienti le stesse condizioni economiche e lo stesso livello di servizio. È quanto accaduto, ad esempio, in Australia, dove si è assistito a un notevole incremento delle quote di mercato dei circuiti a tre parti. Ciò non porterà benefici neanche agli esercenti, per i quali una transazione di un circuito a tre parti (per esempio American Express) è generalmente più costosa rispetto a quella di un circuito a quattro parti*»[44].

D. Il d.lgs. n. 218/2017 (di recepimento della PSD2), all'art. 6 comma 1 ha abrogato il menzionato d.m. 14 febbraio 2014, n. 51 che peraltro, conteneva, come detto, disposizioni non riprodotte dal Regolamento e che erano importanti in punto di trasparenza. Appare allora condivisibile l'auspicio «*che alcune previsioni dell'abrogato decreto "*Merchant Fee*", in particolare quelle riferite alla* ***trasparenza*** *ed alla* ***confrontabilità delle commissioni****, possano trovare effettiva applicazione in attuazione del decreto che ha recepito la PSD2 nel nostro paese*»[45].

Per la verità il combinato disposto del d.lgs. n. 218/2017, del Regolamento comunitario e del provvedimento attuativo della Banca d'Italia, sembra aver ridotto al minimo, se non annullato del tutto, siffatto rischio di aver "dimenticato" i profili di trasparenza e confrontabilità di condizioni, propri del d.m. abrogato.

E. La provvisorietà di una scelta legislativa non del tutto sicura emerge anche dall'art. 17 del Regolamento n. 751/2015 che contiene la clausola di revisione del provvedimento. Si dirà che è una clausola "d'uso" nei provvedimenti europei ed è sicuramente così, ma in questo caso non può non balzare all'occhio la numerosità degli argomenti che devono essere "rivisitati" dalla relazione della Commissione, da presentare entro il 9 giugno del 2019 e i cui lavori sono in fase ormai avanzata. Si tratta, a ben vedere,

---

[43] *Via al tetto unico alle commissioni interbancarie. I consumatori: vantaggi solo per gli esercenti*, in www.informazione.it, 9 dicembre 2015.

[44] A. De Matteis, *La proposta di regolamento sulle commissioni interbancarie: quali conseguenze per i consumatori?*, in www.dirittobancario.it, ottobre 2013, p. 10.

[45] R. Garavaglia, *E che PSD" sia…! Seconda puntata: le commissioni dei pagamenti con carte*, cit.

della rivisitazione di tutti gli argomenti che sono stati affrontati in questo paragrafo e per i quali si postula un'analisi non convenzionale, ma volta a verificare che si sia fatta la scelta giusta, pronti a cambiarla in caso contrario. Insomma, sembra divisarsi un po' più di un aggiornamento volto ad adeguare i testi alle novità eventualmente registratesi nel quadriennio trascorso, bensì l'occasione per ripensare le scelte di fondo compiute dal legislatore europeo, a cominciare dalla scelta dirigistica di inserire un massimale alle commissioni interbancarie[46].

La disamina fin qui compiuta sul Regolamento comunitario evidenzia dubbi di impostazione ma, soprattutto, insicurezza sul raggiungimento degli obiettivi che esso si era proposto. Rinviando alla saggia raccomandazione di non esporsi in giudizi avventati, si può quanto meno concludere che la vicenda delle MIF in genere, e delle MIF per operazioni di pagamento tramite carta in particolare, è lontana dall'essere conclusa, così come non si può non rilevare che l'ondivaga e irresoluta traiettoria intrapresa da qualche decennio dal legislatore comunitario permane senza dare segni di interruzione.

---

[46] La Relazione della Commissione deve valutare l'adeguatezza dei livelli delle commissioni interbancarie e i meccanismi di orientamento, quali le spese, tenendo conto dell'uso e dei costi dei vari mezzi di pagamento e del livello di ingresso sul mercato di nuovi operatori, di nuove tecnologie e di modelli commerciali innovativi. Nella valutazione si esamina in particolare:

a) gli sviluppi in ordine alle commissioni per i beneficiari;
b) il livello di concorrenza fra i prestatori e gli schemi di carte di pagamento;
c) gli effetti sui costi per il pagatore e il beneficiario;
d) la misura in cui gli esercenti hanno trasferito il beneficio della riduzione delle commissioni interbancarie;
e) i requisiti tecnici e le loro implicazioni per tutti i soggetti coinvolti;
f) gli effetti delle carte multimarchio in *co-badging* sulla facilità di utilizzo, in particolare per le persone più anziane e gli altri utenti vulnerabili;
g) gli effetti sul mercato dell'esclusione delle carte aziendali, mediante un confronto tra la situazione negli Stati membri in cui le maggiorazioni sono vietate e quelli in cui sono permesse;
h) gli effetti sul mercato delle disposizioni speciali per le commissioni interbancarie sulle operazioni nazionali tramite carta di debito;
i) gli sviluppi del convenzionamento transfrontaliero e i relativi effetti sul mercato unico, mediante un confronto tra le carte con massimali sulle commissioni e le carte senza massimali, per valutare la possibilità di chiarire quale commissione interbancaria si applica al convenzionamento transfrontaliero;
j) l'applicazione pratica delle norme relative alla separazione tra schema di carte di pagamento e trattamento e l'esigenza di rivalutare la separazione giuridica;
k) l'eventuale necessità di rivedere l'ammontare della commissione interbancaria di cui all'art. 3, par. 1 del Regolamento, stabilendo che il massimale debba essere limitato all'importo inferiore tra 0,07 euro e lo 0,2 del valore dell'operazione.

La Relazione della Commissione è accompagnata da una proposta legislativa che può contenere una proposta di modifica del massimale sulle commissioni interbancarie.

PROFILI COMPETITIVI E CONSUMERISTICI DEL DIVIETO DI SURCHARGE

Teresa Broggiato

1. Inquadramento generale – 2. Le pratiche di surcharge *prima della PSD2 – 3. Le pratiche di* surcharge *alla luce del "payment package" – 4. Le scelte del legislatore nazionale – 5. Riflessioni conclusive*

1. Inquadramento generale

Con il termine *surcharge* si fa riferimento a quelle pratiche attraverso cui gli esercenti commerciali imputano ai propri clienti maggiorazioni di prezzo collegate all'uso dei diversi strumenti di pagamento.

Si tratta di pratiche non nuove, sulle quali in passato si è concentrata l'attenzione di diverse Autorità – tanto a livello nazionale che europeo – avendo riguardo soprattutto all'impatto che esse possono avere sulla diffusione dei diversi mezzi di pagamento e sul rispetto dei principi generali di concorrenza[1].

Più di recente, le pratiche di *surcharge* sono state analizzate sotto il profilo consumeristico, essendo il loro uso spesso criticato soprattutto per le modalità in base a cui vengono imposte al cliente che finisce per subirle in modo – del tutto o quasi – inconsapevole.

In ragione di tali molteplici questioni si sono registrati nel tempo diversi interventi normativi (non sempre perfettamente coordinati tra loro) che sembrano oggi aver trovato una "ricomposizione" a seguito del recepimento della direttiva n. 2015/2366, cd. PSD2.

---

[1] Le prime applicazioni del (divieto di) *surcharge* trovano origine negli accordi contrattuali elaborati dai circuiti di carte di credito. Tali circuiti – sulla base della considerazione che il sistema si mantiene in equilibrio se il prezzo della merce che si acquista con una carta di pagamento non è diverso dal prezzo della stessa merce acquistata in contanti – introducono la *no dicrimination rule* (NDR) attraverso cui il circuito vieta agli esercenti commerciali di riservare ai clienti che utilizzano un determinato strumento di pagamento un trattamento economico peggiore rispetto a quello riconosciuto a coloro che pagano in contanti o tramite altri strumenti di pagamento.
Clausole di questo tipo hanno formato oggetto di riflessione da parte della Commissione europea sin da tempi risalenti: cfr. sul punto, L. Gyselen, *EU Antitrust Law in the Area of Financial Services, in Fordham Corporate Law Institute, 23rd Annual Conference On International Antitrust Law and Policy*, 1996.
A livello nazionale, il tema è stato analizzato dalla Banca d'Italia nell'ambito dell'istruttoria relativa all'accordo per il servizio PagoBancomat (provv. n. 23 dell'8 ottobre 1998, in Boll. AGCM, n. 42/1998). Per la disciplina di questo servizio all'epoca erano (tra l'altro) previste le Condizioni generali di contratto regolanti il rapporto tra banche acquirer ed esercizi convenzionati. Attraverso tali Condizioni veniva imposto agli esercenti di «applicare ai titolari di carta PagoBancomat prezzi non superiori e condizioni non meno favorevoli di quelli praticati alla clientela pagante in contante». Diverse sono le argomentazioni prospettate dalla Banca d'Italia e dall'AGCM (all'epoca competente per il parere ai sensi dell'art. 20, comma 3 della legge n. 287/1990) volte ad evidenziare l'effetto potenzialmente lesivo della concorrenza proprio di tale clausola. In particolare, Bankit evidenziava che tale clausola: «i) impedisce di riflettere gli effettivi costi associati all'utilizzo della carta e del contante nel prezzo finale a carico della clientela, eliminando così la possibilità di scelta tra i due strumenti di pagamento; ii) impedisce la concorrenza tra commercianti che potrebbero applicare commissioni diverse, e quindi competere, per l'utilizzo della carta da parte della clientela; iii) riduce infine la concorrenza tra le banche che commercializzano lo stesso marchio di pagamento: queste possono infatti variare la commissione interbancaria senza che commercianti e clienti si accordino per inglobare nel prezzo di acquisto di un determinato prodotto i maggiori costi del pagamento tramite PagoBancomat rispetto al contante», § 92. Entrambe le Autorità finivano peraltro per consentire il mantenimento della NDR considerato che essa aveva in pratica effetti marginali sulla situazione competitiva del mercato di riferimento a causa soprattutto della ridotta entità della commissione percentuale richiesta dalla banca all'esercente.

Per comprendere meglio la portata della nuova disciplina vigente è utile ripercorrere brevemente i diversi interventi operati dal legislatore europeo e nazionale per poi soffermarsi sulla portata delle nuove norme alla luce delle prime esperienze applicative.

2. Le pratiche di surcharge *prima della PSD2*

Nel 2007, il legislatore europeo – nel porre la base giuridica per la realizzazione dell'Area Unica dei Pagamenti in Euro (SEPA) – sceglieva di legittimare le pratiche di *surcharge* disponendo in via generale che il prestatore di servizi di pagamento non può impedire al beneficiario (ossia l'esercente commerciale) di imporre una spesa o di proporre una riduzione al pagatore per l'utilizzo di un determinato strumento di pagamento (art. 52, par. 3, PSD).

Contestualmente, la medesima disposizione riconosceva agli Stati membri la facoltà di vietare o limitare il diritto di imporre spese tenendo conto della necessità di incoraggiare la concorrenza e di promuovere l'uso di strumenti di pagamento efficaci[2].

Nel 2010, il legislatore italiano si è avvalso di questa facoltà e – ribaltando il predetto principio base della disciplina europea che sanciva la libera differenziazione delle tariffe relative all'utilizzo dei diversi strumenti di pagamento[3] – introduceva un divieto generale di *surcharge* (art. 3, comma 4, d.lgs. n. 11/2010).

A tale divieto si accompagnava tuttavia il riconoscimento alla Banca d'Italia del potere di stabilire deroghe con proprio regolamento «tenendo conto dell'esigenza di promuovere l'utilizzo degli strumenti di pagamento più efficienti ed affidabili».

---

[2] Il considerando 42 così spiega l'impostazione seguita dal legislatore europeo: «al fine di promuovere la trasparenza e la concorrenza, il prestatore di servizi di pagamento non dovrebbe impedire al beneficiario di chiedere al pagatore una spesa per l'utilizzo di uno strumento di pagamento specifico. Mentre il beneficiario dovrebbe avere la facoltà di richiedere il pagamento di spese per l'uso di un determinato strumento di pagamento, gli Stati membri potranno decidere se proibire o limitare prassi siffatte laddove, a loro giudizio, ciò possa essere giustificato in considerazione degli abusi in materia di prezzi o della fissazione di prezzi suscettibili di avere un impatto negativo sull'uso di un determinato strumento di pagamento tenendo conto della necessità di incoraggiare la concorrenza e l'uso efficiente degli strumenti di pagamento». Invero, tale scelta normativa pare il frutto del carattere "ambivalente" del *surcharge*: infatti, se, da un lato, «la possibilità di sovrapprezzo in capo all'utilizzatore del servizio, costituisce, per i fornitori del servizio stesso, un incentivo a competere», dall'altro, in passato «le clausole di *surcharge* sono state largamente vietate, su base convenzionale, perché avevano l'effetto di disincentivare l'uso della carta di credito (comportante per il *merchant* un costo maggiore rispetto ai vecchi mezzi di pagamento)» finendo dunque per ostacolare l'ingresso nel mercato dei servizi di pagamento di operatori innovativi, cfr. M. Libertini, *Regolazione e concorrenza nei servizi di pagamento*, in *Dir. banc.*, 2012, I, p. 611 ss.

[3] M. Doria, *Commento all'art. 3, d.lgs. n. 11/2010*, in *La nuova disciplina dei servizi di pagamento*, a cura di M. Mancini, M. Rispoli Farina, V. Santoro, A. Sciarrone Alibrandi e O. Troiano, Torino, 2011, p. 71.

In sostanza dunque la disciplina nazionale del 2010 riconosceva nella leva tariffaria rappresentata dal *surcharge* un mezzo per disincentivare l'utilizzo di determinati strumenti di pagamento[4], mezzo che tuttavia nella pratica non è mai stato attivato dall'Autorità di Vigilanza[5].

Va anche sottolineato che alla previsione di divieto di *surcharge* in capo ai beneficiari, il legislatore nazionale non accompagnava uno specifico sistema di verifiche (in capo a detta Autorità) rendendo pertanto meno certo il rispetto del divieto[6].

In parallelo, nel 2011 – considerato l'impatto che le pratiche di *surcharge* possono avere sul cliente che le subisce in modo inconsapevole – il legislatore europeo torna in argomento affrontando il tema del sovrapprezzo in chiave consumeristica nell'ambito di una direttiva di portata generale: la n. 2011/83 "sui diritti dei consumatori".

---

[4] Cfr. Banca D'Italia, provvedimento 5 luglio 2011 recante "*Attuazione del Titolo II del Decreto legislativo n. 11 del 27 gennaio 2010 relativo ai servizi di pagamento (Diritti ed obblighi delle parti)*"; il provvedimento è stato abrogato in virtù del provvedimento 11 ottobre 2018 emanato dalla Banca D'Italia a seguito del recepimento della PSD2.

[5] Ad avviso di M. Doria, *Commento all'art. 3*, cit., 71, «*per apprezzare il significato di questa scelta [divieto con deroga] occorre probabilmente partire dalla ratio di fondo ad essa sottesa che, come detto, risiede nell'obiettivo di favorire l'utilizzo degli strumenti di pagamento elettronici rispetto a quelli cartacei e al contante. In considerazione di ciò, il potere di deroga al divieto di surcharge conferito alla Banca d'Italia dovrebbe essere interpretato nella direzione di esplicitare una linea di demarcazione tra la prima e la seconda tipologia di strumenti: in sostanza, la deroga dovrebbe interessare gli strumenti non elettronici che potrebbero/dovrebbero essere oggetto di un sovraprezzo teso a esplicitare il maggior onere di utilizzo che li caratterizza*». Peraltro, «*l'attivabilità di siffatto meccanismo deve essere verificata alla luce del limite applicativo proprio della PSD – e quindi delle disposizioni che la recepiscono nel nostro ordinamento – relativo alla sua riferibilità ai soli strumenti di pagamento elettronici. La praticabilità di un intervento attuativo della Banca d'Italia, di fatto inclusivo degli strumenti cartacei e del contante al fine di renderli possibile oggetto di surcharge, è pertanto condizionata dalla possibilità di considerare il comma in esame applicabile anche a quest'ultima tipologia di strumenti*». In conclusione, «*la complessità e la delicatezza della materia (…) induce a considerare auspicabile un'interpretazione autentica del legislatore sul perimetro applicativo della norma in commento ovvero, ove ritenuto possibile, una modifica della stessa disposizione primaria tesa a includere esplicitamente nel perimetro della sua applicazione anche gli strumenti di pagamento diversi da quelli elettronici*».

[6] I beneficiari, infatti, non sono, di per sé, destinatari della funzione di controllo esercitata dalla Banca d'Italia ai sensi dell'art. 146, t.u.b., così come modificato dall'art. 35, comma 18, d.lgs. n. 11/2010, che, ai sensi della medesima disposizione, si rivolge invece ai prestatori di servizi di pagamento, nonché ai gestori di sistemi di pagamento e di infrastrutture strumentali al loro funzionamento. Ciò posto, il citato provvedimento della Banca D'Italia del 5 luglio 2011 – chiarito che «*il divieto di* surcharge *opera nei confronti del beneficiario di un'operazione di pagamento*» – si limitava a precisare che «*i prestatori che offrono il servizio di acquisizione di strumenti di pagamento sono tenuti a richiamare nel contratto di convenzionamento l'attenzione dei propri clienti* [ossia i *merchant*] *sul divieto in questione anche attraverso una clausola che preveda la possibilità di risoluzione del contratto medesimo in caso di violazioni*».

Al riguardo, l'art. 19 – relativo alle "Tariffe per l'utilizzo di mezzi di pagamento" – dispone che «*gli Stati membri vietano ai professionisti di imporre ai consumatori, in relazione all'uso di determinati strumenti di pagamento, tariffe che superino quelle sostenute dal professionista per l'uso di detti strumenti*».

La previsione non vieta dunque in assoluto le maggiorazioni di prezzo ma le limita consentendo al professionista[7] di recuperare – imputandolo al consumatore a titolo di "tariffa" – unicamente il costo sostenuto per l'accettazione di un determinato mezzo di pagamento[8].

Nel 2012, "anticipando" il recepimento della direttiva, una prima attuazione della norma è stata operata dal d.l. n. 179/2012 che – integrando la disciplina delle pratiche commerciali scorrette di cui al Codice del consumo – introduce, nell'ambito dell'art. 21 relativo alle azioni ingannevoli, il comma 4-*bis* che qualifica *tout court* come scorretta «la pratica commerciale che richieda un sovrapprezzo dei costi per il completamento di una transazione elettronica con un fornitore di beni o servizi».

Peraltro, nei primi interventi volti a censurare le pratiche di *surcharge*, l'Autorità Garante della Concorrenza e del Mercato (AGCM), anziché ricorrere a tale norma, ha preferito fondare il proprio giudizio sui principi generali dettati dal Codice del consumo in materia di pratiche commerciali scorrette: essa ha dunque condotto una dettagliata attività istruttoria volta a verificare se le modalità (più o meno trasparenti) secondo cui è avvenuta la richiesta di sovrapprezzo fossero

---

[7] Ossia qualsiasi persona fisica o giuridica che, nelle pratiche commerciali di cui al titolo III, Codice del consumo, «*agisce nel quadro della sua attività commerciale, industriale, artigianale o professionale e chiunque agisce in nome o per conto di un professionista*» (art. 18, comma 1, lett. b).

[8] Per agevolare l'applicazione della direttiva, la DG Giustizia, nel giugno 2014 ha pubblicato una Guida esplicativa. In merito al concetto di "tariffa", la Guida precisa che l'art. 19 si applica «*a tutti i tipi di tariffe collegate a un mezzo di pagamento, a prescindere dal modo in cui vengono proposte al consumatore*». Ad esempio, le «*tariffe, definite tariffe amministrative, di prenotazione o di gestione, comunemente usate nel settore della biglietteria* on line*, soprattutto da compagnie aeree e di traghetti, anche per la vendita* on line *di biglietti di manifestazioni varie, rientrano nell'art. 19 se possono essere evitate con l'uso di un determinato mezzo di pagamento*». Per quanto riguarda il "costo" sostenuto dal professionista, la Guida – chiarito che, per quasi tutti i professionisti la commissione per i servizi agli esercenti ("MSC") è il principale elemento di costo per l'accettazione di pagamenti tramite carta – precisa che: «la MSC generalmente comprende: 1) la commissione interbancaria pagata dalla banca del professionista (banca acquirente) all'emittente della carta; 2) le commissioni pagate dalla banca del professionista al circuito (per esempio Visa o MasterCard); 3) il margine trattenuto dalla banca del professionista per coprire i costi e ottenere un profitto». Tali indicazioni sono state ribadite nel 2016 dagli uffici della Commissione: cfr. Commissione Europea, "*Orientamenti per l'attuazione/applicazione della direttiva 2005/29/CE relativa alle pratiche commerciali sleali*" (SWD(2016)163 final).

state in grado di falsare in misura apprezzabile il comportamento economico del consumatore[9].

Nel 2014, il quadro normativo viene nuovamente modificato attraverso il d.lgs. n. 21 che – in attuazione alla citata direttiva n. 2011/83/UE sui diritti dei consumatori – novella parte del Codice del Consumo introducendo, all'art. 62, una nuova ulteriore disposizione in tema di "*tariffe per l'utilizzo di mezzi di pagamento*" che si aggiunge a quelle già vigenti.

L'articolo così dispone al comma 1: «*ai sensi dell'articolo 3, comma 4, del decreto legislativo 27 gennaio 2010, n. 11, i professionisti non possono imporre ai consumatori, in relazione all'uso di determinati strumenti di pagamento, spese*

---

[9] Per diversi anni, a partire dal 2011, l'AGCM ha assunto provvedimenti nei confronti di numerose compagnie aeree. La contestazione mossa dall'AGCM – sostanzialmente identica nelle varie istruttorie avviate – riguardava le modalità di indicazione del prezzo dei biglietti aerei offerti tramite Internet «*con specifico riferimento all'assenza di un'immediata, chiara e completa informazione in merito alla previsione, alla natura e alle modalità di calcolo di un onere aggiuntivo (di seguito anche* credit card surcharge *o supplemento carta di credito), di importo rilevante rispetto a quello del biglietto stesso, richiesto dal professionista, al termine del processo di prenotazione* on line*, in funzione della carta di credito/debito utilizzata dal consumatore per il pagamento della transazione*» (cfr., ad esempio, provvedimento n. 22343 del 28 aprile 2011, *Alitalia-commissioni pagamento con carta di credito*, in *Boll. AGCM,* n. 17/2011). Le modalità adottate per la presentazione delle tariffe sono state giudicate scorrette ai sensi degli artt. 20, comma 2, e 21, comma 1, lett. d), Codice del consumo: ciò in quanto suscettibili – attraverso lo scorporo di un onere non eventuale, falsamente rappresentato come un costo non preventivabile *ex ante* ed esterno al controllo del vettore – di indurre in errore il consumatore circa il prezzo effettivo del servizio offerto.
In particolare, la pratica è risultata scorretta rispetto: (i) ai principi di trasparenza informativa che devono essere osservati dal professionista, indipendentemente dal mezzo di comunicazione utilizzato, ai fini di una corretta rappresentazione del costo di un biglietto aereo; (ii) alla reale natura e alle modalità di calcolo del supplemento di 5 euro per biglietto, addebitato dal professionista a titolo di *credit card surcharge*.
L'AGCM – dopo aver richiamato i principi di trasparenza tariffaria propri del settore aereo e la necessità che il supplemento, non corrispondendo ad un servizio diverso e ulteriore rispetto a quello di trasporto, non venga separato dal prezzo del biglietto aereo costituendo una componente del costo del servizio – fa riferimento per sostenere la tesi della scorrettezza anche all'art. 3, comma 4, del d.lgs. n. 11/2010, di recepimento della PSD.
Attraverso tale disposizione, il legislatore italiano – osserva l'AGCM – ha chiaramente optato per l'adozione di un regime particolarmente stringente in sede di trasposizione della richiamata direttiva, che pure rimetteva agli Stati membri la libertà di applicare o meno la regola del *surcharge*.
Sotto diverso profilo, viene infine evidenziato che – alla luce dei dati forniti dal professionista – «*l'importo del supplemento in oggetto non corrisponde affatto ai costi asseritamente imposti dai circuiti delle carte di credito accettate per il pagamento on line dei biglietti, risultando rispetto ad essi, significativamente superiore; circostanza che rafforza la valutazione di scorrettezza delle informazioni fornite dal professionista sul prezzo dei biglietti. A questo deve aggiungersi che il professionista ha incluso nell'importo del* credit card surcharge *anche i propri costi interni derivanti dalla gestione del sistema per il pagamento* on line*, nonché costi presunti imputati al contrasto di eventuali frodi informatiche perpetrate attraverso carte di credito o debito clonate; costi che il vettore dovrebbe, in ogni caso, sostenere quale che fosse il sistema di pagamento adottato*» (§ 78 e 79).
In tal modo, conclude l'AGCM, il professionista non solo ha contravvenuto, nelle modalità di rappresentazione del costo dei biglietti aerei offerti, agli obblighi di trasparenza, ma ha, altresì, «*fuorviato i consumatori lasciando loro impropriamente intendere che il supplemento richiesto alla fine del processo di prenotazione* on line *corrisponda ai costi sostenuti nei confronti dei circuiti delle carte di credito accettate per il pagamento e sia, in quanto tale, totalmente estraneo al controllo e alla politica tariffaria di Alitalia*» (§ 80).

per l'uso di detti strumenti, ovvero nei casi espressamente stabiliti, tariffe che superino quelle sostenute dal professionista».

In sostanza, la disposizione – nel richiamare quanto stabilito in tema di *surcharge* in attuazione della PSD – ribadisce la scelta effettuata nel 2010 (nel mondo dei pagamenti) di vietare al professionista di imporre al consumatore spese per l'utilizzo di un determinato strumento di pagamento.

Nel contempo, la disposizione fa salvo il potere di deroga riconosciuto alla Banca d'Italia in sede di recepimento della PSD consentendo dunque al professionista, nei casi espressamente stabiliti, di richiedere maggiorazioni correlate ai costi. Peraltro, non essendo stata introdotta alcuna previsione in tal senso nell'ordinamento nazionale, il divieto vale in via generale per tutti i professionisti e per tutti gli strumenti di pagamento.

Sul rispetto dell'art. 62 vigila l'Autorità Garante che – per espresso richiamo operato dall'art. 66, Codice del consumo – si avvale dei poteri di accertamento e sanzionatori ad essa riconosciuti dall'art. 27 in tema di tutela contro le pratiche commerciali scorrette[10].

In applicazione dell'art. 62, Codice del consumo, a partire dal 2016 si sono registrati diversi interventi da parte dell'AGCM.

Sin dai primi provvedimenti – riguardanti due compagnie aeree *low cost*[11] – l'AGCM ha chiarito che il nuovo art. 62, Codice del consumo sancisce un divieto assoluto per il "venditore" di qualsiasi prodotto di imporre all'acquirente spese per l'utilizzo di un determinato mezzo di pagamento.

Il divieto, precisa l'Autorità, «*è tale da assorbire, nel caso di specie, gli altri profili inerenti le modalità di presentazione ai consumatori del sovrapprezzo de quo e/o del suo* quantum*, rilevando in via principale l'applicazione in sé di detto sovrapprezzo che, essendo indubitabilmente collegato e corrispondente*

---

[10] Accanto alla tutela amministrativa esercitata dall'AGCM ai sensi del menzionato art. 27, Codice del consumo, resta ferma per il consumatore la possibilità di richiedere il risarcimento del danno extra contrattuale riveniente dal comportamento scorretto agendo in via individuale ovvero collettiva (avvalendosi in quest'ultimo caso dell'azione di classe di cui all'art.140-bis, Codice del consumo, attualmente vigente; al riguardo, si rammenta che questa disciplina è destinata a breve ad essere sostituita dalle nuove disposizioni recate dalla legge n. 31/2019 che entreranno in vigore a partire dal 19 aprile 2020 e si applicheranno alle condotte illecite poste in essere successivamente a tale data).
Il panorama dei rimedi privatistici contro le pratiche commerciali scorrette è destinato ad ampliarsi ulteriormente all'indomani del recepimento della direttiva cd. "omnibus" approvata definitivamente dal Parlamento Europeo il 17 aprile 2019 (2018/0090(COD). Tale direttiva, la cui pubblicazione in G.U.U.E. è prevista nell'autunno 2019, contiene una specifica previsione che richiede agli Stati membri di assicurare ai consumatori lesi da pratiche commerciali scorrette anche la disponibilità di rimedi "contrattuali": per un approfondimento, cfr. T. Broggiato, *La tutela del consumatore nel rinnovato contesto,* in *Fintech: principi, regole e diritti*, a cura di G. Finocchiaro e V. Falce, in corso di pubblicazione per i tipi di Zanichelli.

[11] AGCM, provvedimento n. 26183, *Norwegian Air Shuttle-Commissioni su carta di credito* e n. 26184, *Blue Air-Credit card surcharge (CCS)* del 28 settembre 2016, in *Boll. AGCM* n. 36/2016.

all'utilizzo di uno strumento di pagamento da parte dei consumatori che vogliono acquistare un volo» [12]si pone in chiara violazione del citato art. 62, Codice del consumo [13].

Nel 2017, l'AGCM è nuovamente intervenuta ai sensi dell'art. 62, nei confronti di diverse compagnie operanti nel settore dell'energia elettrica ribadendo il carattere assoluto del divieto di *surcharge* in assenza di espresse previsioni normative che abilitino l'impresa a ribaltare sui consumatori alcun onere e/o costo per l'utilizzo di un determinato strumento di pagamento[14].

Successivamente, un altro filone di interventi ha riguardato alcune imprese che gestiscono i comparatori turistici *on line*. Alle medesime è stata, tra l'altro, contestata l'applicazione di un supplemento di prezzo in relazione alla tipologia di carte di pagamento utilizzate per l'acquisto di voli, nella misura in cui sarebbe stato inserito - di default - nei siti dei professionisti il prezzo corrispondente ad un eventuale acquisto con lo strumento di pagamento "più economico" e l'importo prospettato sarebbe poi invece stato

---

[12] AGCM, provvedimento 26183, cit., § 99.

[13] Sempre tra i primi provvedimenti assunti in applicazione del citato art. 62, si segnala la vicenda che ha condotto l'AGCM a sanzionare l'ACI per aver imposto ai consumatori spese in caso di pagamento del bollo auto *on line* sul sito ACI con utilizzo della carta di credito, nonché in caso di pagamento della stessa tassa automobilistica con carta di debito mediante il circuito PagoBancomat presso le delegazioni ACI distribuite sul territorio nazionale (provvedimento n. 26259, in *Boll. AGCM* n. 45/2016). La decisione dell'AGCM – confermata dal TAR Lazio con la sentenza 17 gennaio 2018, n. 565 – è stata annullata dal Consiglio di Stato, per carenze nell'istruttoria dell'Autorità, con sentenza del 3 gennaio 2019, n. 78.

[14] Cfr. ad esempio AGCM, provvedimento n. 26530 del 30 marzo 2017, *GDF SUEZ-Sistemi di pagamento*, in *Boll. AGCM*, n. 16/2017. L'Autorità aveva contestato alla società il fatto di aver richiesto al consumatore una commissione nel caso di pagamento *on line* delle bollette mediante carte di credito. La società respingeva le contestazioni evidenziando che le commissioni per il pagamento *on line*, non solo coincidono esattamente con il costo del servizio *on line*, ma sono anche direttamente acquisite dal gestore del servizio di pagamento (Cartasì). Infatti, le condizioni generali di adesione per l'esercente, predisposte da CartaSì prevedono che «*l'esercente riconosce che, sull'importo di ogni transazione elettronica spetterà alla Società una commissione nella misura percentuale indicata nel presente accordo* (…) *autorizzandone sin da ora l'addebito sul Conto Corrente*». Dunque, «*nel caso di specie è il fornitore del servizio di pagamento ad applicare e ricevere la commissione e non il professionista*». L'AGCM non condivide tale percorso argomentativo precisando che, ai fini della riferibilità della condotta in esame al professionista, «*non rileva* (…) *che tale commissione non entri nella disponibilità dello stesso professionista ma vada immediatamente al gestore del sistema di pagamento e che corrisponda esattamente al costo del servizio di pagamento. Engie, come tutti i professionisti che svolgono un'attività economica per i cui pagamenti si avvalgono di un sistema di pagamento con carta di credito, sia esso fisico (come nei negozi tramite pos) sia esso virtuale, si avvale della collaborazione finanziaria e tecnologica di un soggetto che gestisce la piattaforma sulla quale operano le transazioni, avvengono i pagamenti, ecc.. Questa collaborazione è meramente strumentale alla realizzazione del rapporto di consumo tra il professionista, nel caso di specie Engie, e il consumatore*» (§ 35). L'Autorità prosegue evidenziando che – nel caso di specie – il contratto concluso tra Engie (esercente) e CartaSì (società di *acquiring*) prevede che Engie paghi a CartaSì una commissione; in concreto il pagamento di questa commissione non viene, come nella prassi, scomputata dall'importo pagato dal cliente ma si aggiunge a questo ed è quindi ribaltato sul cliente, condotta questa che appunto l'articolo 62 intende vietare.

incrementato in relazione alla scelta del consumatore di pagare con una carta di credito diversa[15].

3. Le pratiche di surcharge *alla luce del "payment package"*

Nel 2015 il quadro normativo in materia di pagamenti è interessato da un profondo mutamento conseguente all'emanazione di un "pacchetto" di nuove regole che, da un lato, con la direttiva n. 2015/2366, riscrivono l'originaria disciplina dei servizi di pagamento del 2007, e, dall'altro, con il regolamento n. 2015/751 (*Interchange Fee Regulation* – IFR), introducono una disciplina armonizzata in materia di carte di pagamento, fissando in particolare un limite massimo alle commissioni interbancarie pagate dalla banca dell'esercente a quella dell'emittente della carta.

Il *payment package* è approvato a valle di un lungo processo di riflessione condotto dalle autorità europee a partire dal 2012 con la consultazione della Commissione sul Libro Verde "*Verso un mercato unico dei pagamenti tramite carte, internet e telefono mobile*"[16].

In tale ambito, era stato evidenziato come il costo reale sotteso all'uso di un determinato servizio di pagamento è spesso opaco per i consumatori che non sono consapevoli delle diverse spese sostenute dai commercianti in relazione ai vari strumenti di pagamento. Ne consegue che essi scelgono lo strumento di pagamento in base alla propria convenienza senza considerare se esso sia «*il migliore in termini di costi reali per l'economia*».

Poiché, inoltre, «*in generale, i commercianti includono nei prezzi dei beni e dei servizi offerti le spese di esecuzione dell'operazione a loro carico*» ne deriva

---

[15] Ad avviso dell'AGCM, le modalità utilizzate dai professionisti di presentare come prezzo risultante – a seguito di una ricerca di uno specifico volo senza indicare il mezzo di pagamento – quello relativo all'utilizzo della carta di credito che garantiva i maggiori sconti, costituisce una variazione di prezzo «*inequivocabilmente qualificabile come supplemento*» piuttosto che come sconto applicato per l'utilizzo di un diverso strumento di pagamento (cfr. provvedimento 20 dicembre 2017, nn.: 26913, *Lastminute. Com-commissioni utilizzo carta di credito*, 26915, *Volagratis-servizi turistici on line*, 26916, *Opodo-servizi turistici on line*, 26917, *Govolo-servizi turistici on line*, 26918, *Edreams-servizi turistici on line*, 26919, *Gotogate-servizi turistici on line*, tutti in *Boll. AGCM,* n. 2/2018). Peraltro, con le sentenze nn. 5524, 5360 e 5361 pronunciate in data 29 aprile e 2 maggio 2019, il TAR Lazio ha annullato parzialmente i citati provvedimenti nn. 26916, 26917, 26918 nella parte in cui veniva contestata una violazione dell'art. 62, Codice del consumo. Sul punto il TAR, avallando le tesi prospettate dai ricorrenti, ha ritenuto che la condotta realmente censurata dall'AGCM, al di là della formale qualificazione giuridica datane, non può essere considerata una pratica di *surcharge* ma al più una possibile omissione delle informazioni rilevanti sul prezzo offerto di default (c.d. *price display*). Al riguardo, sebbene l'AGCM formalmente contestava al professionista una CCS, in realtà essa ha offerto elementi a supporto della diversa tesi del c.d. *price display*. Secondo l'accertamento del TAR, emerge quindi una palese contraddittorietà in quanto l'AGCM avrebbe contestato una pratica (il *surcharge*) diversa da quella che emerge dalle risultanze istruttorie e dal corredo motivazionale dei provvedimenti, ossia la eventuale violazione dell'art. 22, Codice del consumo. Più di recente, nello stesso senso, cfr. TAR Lazio, sentenza n. 8747 del 4 luglio 2019 relativa al provv. AGCM n. 26919.

[16] Bruxelles, 11.1.2012, COM(2011) 941 definitivo.

che, alla fine, «*tutti i consumatori pagano di più per i loro acquisti per coprire il costo effettivo dei metodi di pagamento più cari utilizzati da alcuni*».

Dati questi presupposti, il Libro Verde aveva aperto la discussione con l'obiettivo di individuare possibili soluzioni per rendere più trasparente il costo di utilizzo di un determinato strumento di pagamento non solo sul versante commerciante-consumatore ma anche, a monte, nel rapporto commerciante-*payment service provider* (PSP) sul quale va ad influire la gestione interbancaria del pagamento regolata tramite M*ultilateral Interchange Fee* (MIF)[17].

Infatti, l'applicazione di questa tipologia di tariffe determina un onere per il beneficiario che viene da questi di regola tradotto in un sovrapprezzo sul bene o servizio acquistato. In definitiva, dunque, il tema degli incentivi all'utilizzo degli strumenti di pagamento elettronici si lega «*indissolubilmente alla considerazione sulla legittimità delle tariffe interbancarie e, ove ammesse, alla valutazione della loro adeguata misura*»[18].

Nei successivi approfondimenti sull'opportunità di rivedere la disciplina del 2007, la Commissione Europea prende atto che le originarie previsioni sul *surcharge* non hanno promosso l'auspicata *market trasparency* né politiche di prezzo che siano *cost-effective* conducendo piuttosto ad effetti opposti[19].

---

[17] Infatti, «*a causa di determinate norme che regolano i sistemi delle carte di pagamento, i commercianti hanno difficoltà ad influenzare la scelta dei consumatori quanto allo strumento di pagamento e vedono limitata la propria capacità ad accettare solo carte selezionate. Questa situazione favorisce l'applicazione di MIF elevate da parte dei prestatori di servizi di pagamento, causando un possibile aumento del costo delle carte di pagamento e frenando la concorrenza*». Tra le "norme" individuate dalla Commissione vi è anche la regola della non discriminazione, che vieta ai dettaglianti di orientare i clienti verso l'uso di uno strumento di pagamento di loro scelta, tramite maggiorazioni, sconti o qualsiasi altra forma di orientamento. Dunque – conclude la Commissione – «*modificando le norme che disciplinano i sistemi delle carte di pagamento e rivedendo le pratiche degli* acquirer*, si potrebbe conferire più potere ai commercianti nei negoziati con gli* acquirer*, in particolare per quanto riguarda le commissioni applicate al commerciante (MSC), migliorando nel contempo la capacità dei commercianti di influenzare le decisioni dei consumatori. Ciò consentirebbe di ridurre i costi delle carte di pagamento per l'economia e moltiplicare le possibilità di adozione di nuovi sistemi concorrenziali da parte dei commercianti*», Libro Verde "*Verso un mercato unico dei pagamenti tramite carte, internet e telefono mobile*", cit., par. 4.2.3.
Anche l'Autorità Garante – nel rispondere alla consultazione sul Libro Verde nell'aprile 2012 – valuta con favore le iniziative volte a migliorare le condizioni di trasparenza sia nel rapporto tra consumatori e commercianti, sia nel rapporto tra questi ultimi e i prestatori di servizi di pagamento. In questa prospettiva, essa ritiene che «*debba essere rafforzata la possibilità per i commercianti di trasferire sui lori clienti il costo effettivo per l'utilizzo dei diversi mezzi di pagamento (ad esempio mediante l'applicazione di sconti, sovrapprezzi, o anche la possibilità di accettare i pagamenti anche con carte solo per transazioni di importo superiore ad un livello minimo), di modo tale che essi [i clienti] tengano conto anche di questa variabile (oltre che dei bonus che eventualmente ricevono dalla banca* issuer*) nella scelta dello strumento di pagamento con cui regolare la transazione. In questo modo, infatti, le scelte razionali degli utilizzatori dovrebbero condurre alla prevalente affermazione degli strumenti di pagamento più convenienti in relazione all'ampiezza dei servizi che recano, ponendo un argine alla vigente concorrenza al rialzo delle MIF*».

[18] Cfr. M. Doria, *Commento all'art. 3*, cit., p. 70.

[19] Commissione Europea, Direzione Generale Mercato Interno, *Further discussion on the Review of Directive 2007/64/CE on payment services in the internal market – New issues paper*, 1° ottobre 2012.

In particolare, in alcuni casi, nei quali il *surcharging* è ammesso, esso risulta essere stato utilizzato in modo distorto – soprattutto nelle situazioni nelle quali il consumatore è "*captive*" – come una fonte addizionale di guadagno per i commercianti.

Il quadro sin qui delineato conduce all'inserimento nella PSD2 di una nuova articolata disposizione – l'art. 62 – sulle "Spese applicabili".

Tale disposizione - dopo aver stabilito che per le operazioni di pagamento eseguite nell'Unione «*il beneficiario e il pagatore sostengono ciascuno le spese applicate dal rispettivo prestatore di servizi di pagamento*» (cd. opzione "SHARE") – prevede che:

«3. Il prestatore di servizi di pagamento non impedisce al beneficiario di imporre una spesa o di proporre una riduzione al pagatore o di orientarlo in altri modi verso l'uso di un determinato strumento di pagamento. Le spese addebitate non superano i costi diretti sostenuti dal beneficiario per l'utilizzo dello specifico strumento di pagamento.

4. In ogni caso, gli Stati membri assicurano che il beneficiario non imponga spese per l'utilizzo di strumenti di pagamento le cui commissioni interbancarie sono oggetto del capo II del regolamento (UE) 2015/751 e per i servizi di pagamento cui si applica il regolamento (UE) n. 260/2012.

5. Gli Stati membri possono vietare o limitare il diritto del beneficiario di imporre spese tenendo conto della necessità di incoraggiare la concorrenza e di promuovere l'uso di strumenti di pagamento efficienti».

In sostanza, viene dunque riconosciuta, in via generale, al beneficiario la facoltà di imporre "maggiorazioni" per l'utilizzo di un determinato strumento di pagamento, a condizione che le maggiorazioni non superino i costi diretti sostenuti dal beneficiario per l'utilizzo di detto strumento pagamento: la previsione è dunque in linea con quanto stabilito dal sopra richiamato art. 19 della direttiva sui diritti dei consumatori20.

Per espresso disposto del successivo par. 4, questa regola generale non trova tuttavia applicazione in relazione agli strumenti di pagamento le cui commissioni interbancarie sono oggetto di specifica disciplina nell'ambito del regolamento n. 2015/751 (ossia carte di debito e di credito) oppure nel regolamento n. 260/2012 (addebiti diretti). Infatti, per detti strumenti di pagamento, è richiesto agli Stati membri di disporre, nei confronti del beneficiario, un divieto *tout court* di imporre maggiorazioni.

---

[20] Tale scelta di fondo è supportata dalle considerazioni espresse nella ricerca commissionata dalla DG Concorrenza e dalla DG Giustizia in merito agli effetti dell'*information disclosure* sulle scelte dei consumatori in tema di strumenti di pagamento. Ad avviso degli autori, «*the outcome of the study supports surcharging as an efficient steering mechanism for payment instruments, despite the fact that consumers are generally believed to be opposed to surcharging. According to the study, monetary incentives (rebates) and disincentives (surcharges) are considerably more effective than information-based measures in driving cost-conscious choices. While rebates are six times more effective than mere education, surcharges are twice more effective than rebates*»: *Study on the effects of information disclosure on consumer choice of payment instruments*, dicembre 2013.

Infine, il par. 5 dell'art. 62 introduce una norma di chiusura per cui – fatto salvo quanto sopra stabilito in ordine ai limiti quantitativi del *surcharge* e al suo divieto in relazione a determinati strumenti di pagamento – è riconosciuto agli Stati membri (in relazione ai restanti mezzi di pagamento) il potere di introdurre divieti/limitazioni al diritto del beneficiario di imporre spese «*tenendo conto della necessità di incoraggiare la concorrenza e di promuovere l'uso di strumenti di pagamento efficienti*».

Per comprendere le ragioni alla base di una disciplina così articolata occorre fare riferimento alle indicazioni contenute nel preambolo della direttiva laddove – nel ribadire quanto emerso nei citati approfondimenti preparatori – si evidenzia che le diverse prassi nazionali in materia di applicazione di spese per l'utilizzo di un determinato strumento di pagamento «*hanno portato a un'estrema eterogeneità del mercato dei pagamenti nell'Unione e confondono i consumatori, in particolare nel settore del commercio elettronico e in un contesto transfrontaliero. I commercianti situati negli Stati membri in cui è consentito applicare maggiorazioni offrono prodotti e servizi negli Stati membri in cui le maggiorazioni sono vietate e addebitano tali maggiorazioni ai consumatori. Vi sono, inoltre, molti esempi di commercianti che impongono ai consumatori maggiorazioni di livello molto più elevato rispetto al costo da essi stessi sostenuto per l'utilizzo di uno specifico strumento di pagamento*» (considerando 66, prima parte).

Ciò posto, la revisione delle pratiche relative alle maggiorazioni è «fortemente motivata»" dal fatto che il regolamento n. 2015/751, nello stabilire norme in materia di commissioni interbancarie per i pagamenti basati su carta, pone dei limiti stringenti a tali commissioni.

Infatti – considerato che «*le commissioni interbancarie costituiscono la componente principale delle commissioni applicate dai commercianti per pagamenti basati su carta*» e che «*le maggiorazioni rappresentano una pratica di orientamento utilizzata talvolta dai commercianti per compensare i costi aggiuntivi dei pagamenti basati su carta*» – in presenza di una norma che fissa limiti ben precisi alle MIF «*è opportuno che gli Stati membri valutino se impedire ai beneficiari di applicare commissioni per l'utilizzo di strumenti di pagamento per cui le commissioni interbancarie sono regolamentate nel capo II del regolamento (UE) 2015/751*» (considerando 66, seconda parte).

Per completezza, va infine ricordato che i principi in tema di *surcharge* dettati dalla PSD2 sono stati successivamente ribaditi dal legislatore europeo con il regolamento n. 2018/302 sul "*geoblocking*"[21].

---

[21] Regolamento (UE) 2018/302 del 28 febbraio 2018 recante misure volte a impedire i blocchi geografici ingiustificati e altre forme di discriminazione basate sulla nazionalità, sul luogo di residenza o sul luogo di stabilimento dei clienti nell'ambito del mercato interno, in GUUE L 60 del 2 marzo 2018. Per un commento, cfr. V. Falce, *Appunti sul regolamento europeo sul geo-blocking e la neutralità geografica. In cammino verso il mercato unico digitale*, in corso di pubblicazione in *Contratto e Impresa/Europa*, 2019.

Al riguardo, l'art. 5 – dopo aver vietato la discriminazione di prezzo per motivi legati alla nazionalità, al luogo di residenza o stabilimento di un cliente, all'ubicazione del conto di pagamento, al luogo di stabilimento del PSP o al luogo di emissione dello strumento di pagamento all'interno dell'Unione – chiarisce che tale divieto «*non preclude al professionista di addebitare spese per l'utilizzo di strumenti di pagamento basati su carta le cui commissioni interbancarie non sono oggetto del capo II del regolamento (UE) 2015/751 e per i servizi di pagamento ai quali non si applica il regolamento (UE) n. 260/2012, a meno che nel diritto dello Stato membro a cui è soggetta l'attività del professionista non siano stati introdotti il divieto o la limitazione del diritto di imporre spese per l'utilizzo di strumenti di pagamento a norma dell'articolo 62, paragrafo 5, della direttiva (UE) 2015/2366. Le spese addebitate non superano i costi diretti sostenuti dal professionista per l'utilizzo dello strumento di pagamento*».

4. Le scelte del legislatore nazionale

A livello nazionale, la disciplina europea è stata attuata dal d.lgs. n. 218/2017 che – nel modificare l'originario art. 3 del d.lgs. n. 11/2010 in materia di "spese applicabili" – da un lato, ha confermato il principio SHARE (pagatore e beneficiario sostengono ciascuno le spese applicate dal rispettivo PSP) e, dall'altro, ha stabilito un divieto netto di *surcharge* escludendo dunque la possibilità di introdurvi deroghe attraverso la disciplina secondaria[22]. Ciò con l'obiettivo, individuato nella Legge di delegazione europea 2015, di favorire la concorrenza, promuovere l'uso di strumenti di pagamento efficienti e, dunque, garantire all'utente una reale possibilità di scelta tra i diversi strumenti[23].

Oggi dunque, ai sensi dell'art. 3, comma 4 del d.lgs. n. 11/2010, «*il beneficiario non può applicare a carico del pagatore spese relative all'utilizzo di strumenti di pagamento*».

Sempre in conformità a quanto stabilito nella Legge delega, con il successivo comma 4-*bis*, è attribuito all'AGCM il compito di verificare l'osservanza del divieto e di applicare le relative sanzioni, avvalendosi a tal fine degli strumenti, anche sanzionatori, previsti dal Codice del consumo.

---

[22] Al divieto di *surcharge*, si accompagna l'abrogazione dell'originario comma 3 dell'art. 3, d.lgs. n. 11/2010, che consentiva al beneficiario di applicare al pagatore una riduzione del prezzo del bene venduto o del servizio prestato per l'utilizzo di un determinato strumento di pagamento: ciò in quanto l'uso distorto di tale "scontistica" ha reso questa pratica uno strumento per eludere il divieto di applicazione del *surcharge* (cd. "*surcharge* al contrario"), cfr. relazione illustrativa allo schema di decreto legislativo di recepimento della PSD2.

[23] Tale scelta è anche supportata dalla considerazione che la riduzione delle commissioni interbancarie operata dal regolamento IFR dovrebbe contribuire a ridurre i costi per i commercianti che accettano pagamenti con carte di pagamento, con conseguente riduzione dei prezzi applicati alla clientela nei confronti della quale, dunque, l'imposizione di un sovrapprezzo diverrebbe meno "giustificabile".

Grazie a queste ultime previsioni, il quadro normativo appare ricomposto, oltreché semplificato: anzitutto, attraverso il combinato disposto del Codice del consumo e della disciplina attuativa della PSD2, tutti i pagatori (siano essi consumatori o meno) beneficiano del divieto di *surcharge.*

Secondariamente, la tutela dei medesimi è affidata in modo univoco all'Autorità Garante[24], escludendo dunque in capo a Banca d'Italia una competenza "diretta" a vigilare sul rispetto della norma.

Peraltro, il successivo comma 4-*ter* – richiamando il principio sancito in via generale dalla Legge sul risparmio nel 2005 – dispone la collaborazione tra AGCM e Banca d'Italia, «*anche mediante scambio di informazioni*», per agevolare l'esercizio delle rispettive funzioni. Dette Autorità non possono reciprocamente opporsi il segreto d'ufficio.

Invero – considerate le molteplici questioni sottese al *surcharge* e la sua "ambivalenza" quanto ad effetti sul mercato – la collaborazione tra le due Autorità appare quanto mai utile ed opportuna anche al fine di monitorare, nel lungo periodo, la validità della scelta effettuata dal legislatore nazionale di vietare in modo netto e senza deroghe le predette pratiche.

Una prima applicazione del divieto – dopo il completamento del quadro normativo di riferimento operata dal d.lgs. n. 218/2017 – è rappresentata dal provvedimento con cui l'AGCM ha sanzionato una società attiva nel servizio di trasporto pubblico locale, per aver richiesto agli utenti dei propri servizi un pagamento aggiuntivo correlato all'utilizzo di un determinato mezzo di pagamento (la carta di credito)[25].

La vicenda ha tratto origine dall'invito rivolto dall'Emilia Romagna ad un'azienda di trasporto pubblico locale affinché iniziasse una collaborazione con una società intermediaria pubblica in grado di organizzare e gestire una specifica piattaforma informatica di pagamento per conto delle amministrazioni locali: ciò con l'obiettivo di creare sistemi di pagamento dei titoli di viaggio più efficienti e vantaggiosi. Grazie a tale collaborazione, il professionista aveva reso disponibile sul proprio sito web la possibilità di acquistare abbonamenti *on line*.

A fronte degli addebiti mossi dall'AGCM, il professionista si è difeso contestando il fatto di essere indicato quale "beneficiario" del sovrapprezzo in oggetto: infatti, la commissione aggiuntiva pagata dal cliente veniva trasferita direttamente all'operatore del servizio di carte di credito ossia al partner

---

[24] Con la comunicazione del 26 novembre 2018 (consultabile sul sito www.agcm.it) l'Autorità Garante ha richiamato tutti gli esercenti (ivi inclusi i dettaglianti specializzati, anche di piccola dimensione) sulla necessità di rispettare il divieto di applicare supplementi per l'uso della carta di credito/debito o altri strumenti di pagamento di cui all'art. 62 Codice del consumo e ribadito dalla PSD2.

[25] AGCM, provvedimento n. 27324, *Start-Romagna-commissioni pagamento con carta di credito*, in *Boll. AGCM*, n. 36/2018.

bancario prescelto per il tramite del quale la società intermediaria era in grado di incassare e poi trasferire gli importi dovuti dai clienti agli enti creditori aderenti alla piattaforma.

Tuttavia, l'Autorità ha ribadito il suo orientamento circa la necessità di interpretare in maniera stringente l'art. 62, Codice del consumo, nel senso di un divieto assoluto per il professionista di prevedere un sovrapprezzo legato alla scelta di un determinato strumento di pagamento. Secondo l'AGCM, il divieto in parola si riferisce a qualsiasi sovrapprezzo collegato ad uno strumento di pagamento nei confronti degli utenti, di cui risponde il professionista indipendentemente dal fatto che la commissione sia pretesa da un *partner* bancario terzo. Infatti, l'imputazione del divieto di sovrapprezzo in capo al "beneficiario" del pagamento – ossia, in concreto, al creditore delle somme trasferite mediante la transazione – comporta che il professionista resti comunque responsabile della violazione qualora il sovrapprezzo sia indicato sul sito internet del medesimo e venga quindi in ogni caso applicato al consumatore nell'acquisto che viene effettuato su detto sito.

Merita rilevare che – secondo quanto evidenziato dall'Autorità – il comportamento contestato è venuto meno dall'ottobre del 2017 quando il professionista «*è passato al noto SPC-pagoPA, sistema già implementato, in esecuzione del Codice dell'Amministrazione digitale (CAD) per i pagamenti verso le Pubbliche Amministrazioni e verso i Soggetti prestatori di servizi*».

In estrema sintesi, il sistema pagoPA consente agli utenti di eseguire il pagamento in favore della pubblica amministrazione interessata, scegliendo tra i diversi strumenti e canali di pagamento elettronico (bonifico bancario/postale, bollettino postale, carte di debito, di credito, prepagate ovvero altri strumenti elettronici che consentano anche l'addebito in conto corrente) e tra i diversi PSP che abbiano scelto di aderire all'infrastruttura tecnologica pubblica (cd. "Nodo").

Attraverso tale sistema infatti l'utente/pagatore non è più tenuto ad eseguire il pagamento attenendosi alle indicazioni stabilite dalla singola PA creditrice ma può decidere liberamente come eseguirlo scegliendo fra le diverse soluzioni offerte in via concorrenziale dai diversi prestatori di servizi di pagamento.

Nel nuovo contesto normativo, il PSP che esegue il pagamento si configura dunque come prestatore del pagatore e non come prestatore della PA/Ente Creditore beneficiario.

In assenza di uno specifico rapporto contrattuale tra il PSP e l'Ente Creditore, le commissioni per lo svolgimento del servizio sono applicate all'utente dal suo PSP (selezionato liberamente tra i PSP aderenti) per il servizio di pagamento da lui richiesto.

Cadrebbe in questo modo la stessa configurabilità di un *surcharge* a carico dell'utente il quale si trova a pagare unicamente quanto richiestogli dal PSP che ha liberamente scelto sul mercato[26].

5. Riflessioni conclusive

La scelta operata dal legislatore nazionale in tema di *surcharge* con il d.lgs. n. 218/2017 sembra rappresentare un punto di equilibrio che tiene conto delle diverse esigenze di cui sono portatori i diversi soggetti coinvolti, siano essi consumatori, esercenti commerciali ovvero prestatori di servizi di pagamento.

Sotto il profilo consumeristico, è evidente che la presenza di un divieto secco di sovrapprezzo pone il consumatore al riparo da sorprese "dell'ultima ora" consentendogli dunque di scegliere lo strumento di pagamento in base alla propria praticità/convenienza.

Per l'esercente il divieto di *surcharge* è controbilanciato dall'introduzione ex regolamento IFR di massimali alle commissioni interbancarie a carico della banca *acquirer* che rende possibile una riduzione dei costi di convenzionamento a carico del *merchant*. Si tratta di un punto importante, anche considerato l'obbligo vigente, in capo ai soggetti che effettuano l'attività di vendita di prodotti e di prestazione di servizi, «*di accettare anche i pagamenti effettuati attraverso carte di debito e di credito*»[27].

Quanto ai prestatori di servizi di pagamento, il nuovo quadro normativo conferma che il divieto di sovrapprezzo sta in capo ai beneficiari dei pagamenti ossia – secondo quanto chiarito da ultimo da AGCM in una comunicazione al mercato – «*a tutti gli esercenti commerciali, ivi inclusi i dettaglianti specializzati, anche di piccola dimensione (tabaccai, ferramenta, lavanderie, macellerie, frutterie ecc.)*»[28].

La responsabilità del beneficiario ricorre anche laddove il sovrapprezzo non sia materialmente incassato dal medesimo ma dal soggetto terzo della cui collaborazione finanziaria e tecnologica il venditore/beneficiario si avvale al

---

[26] Ad avviso dell'Agenzia per l'Italia Digitale (AgID), quanto avviene con pagoPA – ossia consentire ad un PSP aderente e selezionato liberamente dall'utente di richiedere una commissione per l'operazione di pagamento – costituisce una fattispecie in nessun modo assimilabile alla pratica vietata dalla PSD e dalla PSD2 e scorretta (art. 21, comma 4-*bis*, e art. 62, comma 1, d.lgs. n. 206/2005) del *surcharge*, in cui un beneficiario applica un sovrapprezzo per determinate tipologie di pagamento, ribaltando sull'utente, in tutto o in parte, le commissioni che lo stesso beneficiario è chiamato a riconoscere al proprio PSP; cfr. Agenzia per L'Italia Digitale, *Linee guida pagamenti elettronici a favore delle pubbliche amministrazioni e dei gestori di pubblici servizi*, 17 dicembre 2018, cap. 8.4.

[27] Art. 15, comma 4, d.l. n. 179/2012; peraltro, la norma manca a tutt'oggi di sanzione considerato che il Consiglio di Stato ha espresso parere negativo (n. 1446/18) sullo "*Schema di regolamento sulle sanzioni amministrative in caso di mancata accettazione dei pagamenti elettronici*" messo a punto dal Ministero dello Sviluppo Economico nel marzo 2018.

[28] AGCM, comunicazione del 26 novembre 2018, cit.

fine di offrire al cliente la possibilità di pagare con un determinato strumento di pagamento.

Anche in questa prospettiva di tutela ampia del consumatore, risulta logicamente fondata la scelta di attribuire l'*enforcement* dalla disciplina all'Autorità Garante della Concorrenza e del Mercato.

Peraltro, proprio in considerazione delle molteplici "sfaccettature" del *surcharge* che – come ricordato in premessa – è stato inizialmente approfondito per il suo impatto nella diffusione di strumenti di pagamento, permane l'interesse della Banca d'Italia a seguirne l'evoluzione anche in considerazione delle nuove competenze da essa acquisite in tema di commissioni interbancarie ai sensi dell'art. 34-*quater*, d.lgs. n. 11/2010[29].

Del resto, proprio su questo ultimo aspetto, ai sensi di tale disposizione è competente "per il parere" l'Autorità Garante.

L'AGCM dunque potrà valutare il *surcharge* sotto due distinte prospettive: l'una, di tipo squisitamente consumeristico, per gli effetti che tali pratiche producono in capo al pagatore, l'altra, di carattere regolatorio, a supporto dell'Autorità che esercita la sorveglianza sui sistemi di pagamento.

---

[29] In base all'art. 34-*quater*, comma 1 – introdotto dal d.lgs. n. 218/2017 – «*la Banca d'Italia è designata quale autorità competente ai sensi dell'articolo 13 del Regolamento (UE) n. 751/2015 [IFR] e adotta le proprie decisioni previo parere dell'Autorità Garante della Concorrenza e del Mercato*».

Mutamenti del mercato dopo la PSD2

Domenico Gammaldi e Costanza Iacomini

1. Premessa – 2. L'impianto regolamentare della PSD2: i servizi di disposizione di ordini di pagamento e di accesso ai conti tra gestione del consenso dell'utente e identificazione dei TPPs – 3. Open banking*: l'accesso ai conti tramite le* Application Programming Interfaces *(APIs) – 4. Conclusioni: l'*Open banking *verso un assetto del mercato che vede i dati di pagamento come* commodities *e i conti di pagamento come* essential facilities

1. Premessa

Il sistema dei pagamenti è un segmento fortemente legato al contesto tecnologico e, storicamente, è sempre stato sulla frontiera dell'innovazione; in molti casi si è potuta osservare la trasformazione 'genetica' di alcuni operatori che, da fornitori di servizi attivi in altri comparti, ad esempio nelle telecomunicazioni o nei trasporti, si sono affermati nell'offerta dei servizi di pagamenti[1]. Tale trasformazione è giustificabile, oltre che da esigenze legate a rendere più agevoli i pagamenti sottostanti necessari per la fruizione dei servizi, dall'esistenza di economie di rete e di scopo[2].

Anche le più recenti tendenze del mercato dei pagamenti vedono un forte attivismo nell'area dell'offerta di servizi finanziari[3], con un focus sui pagamenti, sia dei grandi operatori tecnologici (comunemente indicati come GAFA, ovvero Google, Apple, Facebook e Amazon[4]), sia di agili start-up innovative[5].

La direttiva 2015/2366/(UE) ('PSD2' o Direttiva) si pone l'obiettivo di favorire la concorrenza e l'innovazione nel settore dei pagamenti *retail* garantendo al contempo la sicurezza dell'utente; questi obiettivi vengono perseguiti anche attraverso l'ampliamento del novero dei servizi di pagamento sotto riserva, sottoponendo pertanto a regolamentazione alcune attività già di fatto offerte al pubblico in precedenza ma in assenza di specifiche tutele.

---

1 È il caso di American Express che originariamente era una società di trasporto; AMEX entra nel mercato dei pagamenti prima con l'introduzione dei *traveller's cheques* e poi con la emissione di carte di credito. Analoga evoluzione è quella di Western Union, società telegrafica che successivamente si è specializzata nel mercato delle rimesse di denaro.

2 G.Ardizzi, C. Impenna, P. Masi, *La teoria economica dei sistemi di pagamento*, in C. Tresoldi (a cura di), *Economia dei sistemi di pagamento*, Il Mulino, Bologna 2005, pp.81-132; il tema è ritornato di forte attualità nel dibattito sui *big data* e a tal fine si veda H. Varian, *Economie di rete e Big Data*, Aspen Institute Italia (https://www.aspeninstitute.it/system/files/private_files/2018.../Aspenia80_Varian.pdf), oltre al contributo di R. Menzella in questo *Quaderno*.

3 Al tema dell'impatto dell'innovazione sul sistema finanziario sono dedicati numerosi *papers* delle diverse autorità sovranazionali. Si segnala, senza alcuna pretesa di esaustività: Financial Stability Board (FSB), (2017b), "*Financial Stability Implications from FinTech - Supervisory and Regulatory Issues that Merit Authorities' Attention*", disponibile su: http://www.fsb.org/2017/06/fsb-issues-a-report-on-the-financial-stability-implications-from-fintech/; Financial Stability Board (FSB), (2017c), "*FinTech Credit: Market Structure, Business Models and Financial Stability Implications*", disponibile su: http://www.fsb.org/2017/05/fintech-credit-market-structure-business-models-and-financial-stability-implications/; Basel Committee on Banking Supervision (BCBS), (2017), "*Sound Practices: Implications of Fintech developments for banks and bank supervisors*", Bank for International Settlements (BIS), disponibile su: https://www.bis.org/bcbs/publ/d431.htm. Per il mercato italiano si veda F. Panetta, (2018), "*Fintech and banking: today and tomorrow". Intervento presso la "Annual Reunion of the Harvard Law School Association of Europe*", disponibile su: http://www.bancaditalia.it/pubblicazioni/interventi-direttorio/int-dir-2018/panetta-120518.pdf.

4 Cfr. Bank for International Settlements (BIS), *BigTech and the changing structure of financial Intermediation*, in *Working Papers* N. 779, april 2019.

5 Osservatorio *FinTech* Italia 2019, PWC, marzo 2019, in cui si registra che sono state 31 le uscite dal mercato nel corso del 2018 tra le aziende *Fintech* in Italia. Di queste, il 13% è stata oggetto di acquisizione da parte di altre *FinTech*; sembra esserci, anche in Italia, una tendenza al consolidamento tra le aziende *FinTech*, come strategia per competere in un mercato caratterizzato dalla presenza di grandi *players*.

In questo contesto, il *fil rouge* che ha sotteso i lavori per la messa a punto della PSD2 e le successive attività della European Banking Authority (EBA) è stato quello di favorire il diffondersi dell'innovazione tecnologica per 'lo sviluppo di nuovi tipi di servizi di pagamento, garantendo pari condizioni operative ai prestatori di servizi di pagamento esistenti e ai nuovi prestatori'[6]. *Fil rouge* che si è dipanato senza soluzione di continuità rispetto a quanto già avvenuto con la PSD1[7], che da un lato ha consentito l'ingresso ordinato sul mercato dei pagamenti di nuovi operatori – gli istituti di pagamento ("IP") – legati al contesto tecnologico dell'epoca, e dall'altro ha definito un quadro regolamentare in grado di rispondere alle esigenze poste dall'accelerazione dell'evoluzione tecnologica negli anni successivi.

Nel prosieguo del lavoro si proporrà una chiave di lettura dell'impianto regolamentare della PSD2 in relazione al – e in funzione del – contesto tecnologico e dei suoi possibili sviluppi alla luce dei profondi impatti ipotizzabili non solo nell'area dei pagamenti.

2. *L'impianto regolamentare della PSD2: i servizi di disposizione di ordini di pagamento e di accesso ai conti tra gestione del consenso dell'utente e identificazione dei TPPs*

Nell'aggiornare il quadro regolamentare per i servizi di pagamento e favorire l'ingresso sul mercato di nuovi operatori e, più in generale, la creazione di condizioni per lo sviluppo di un ecosistema più competitivo, la PSD2 ha introdotto il principio dell'accesso ai dati dei conti di pagamento da parte di operatori ("*Third-party providers*" o "TPPs") che, a tal fine, devono essere autorizzati dalle autorità nazionali competenti[8].

Si fa riferimento a quei servizi che consentono a nuovi operatori di accedere ai conti di pagamento dei propri clienti detenuti presso un diverso intermediario, tipicamente una banca (o, più raramente, un istituto di pagamento o un istituto di moneta elettronica)[9]. L'intermediario presso il quale è intrattenuto il conto

---

[6] Il considerando 33, PSD2, recita: "*La presente direttiva dovrebbe prefiggersi di garantire continuità nel mercato, consentendo ai prestatori di servizi nuovi ed esistenti di offrire i propri servizi in un quadro regolamentare chiaro e armonizzato, indipendentemente dal modello commerciale da essi applicato. Fino a che tali disposizioni non siano applicate e fatta salva l'esigenza di garantire la sicurezza delle operazioni di pagamento e la tutela del cliente dal rischio comprovabile di frode, gli Stati membri, la Commissione, la Banca centrale europea (BCE) e Autorità europea di vigilanza (Autorità bancaria europea), istituita dal regolamento (UE) n. 1093/2010 del Parlamento europeo e del Consiglio (1) (ABE) dovrebbero garantire la concorrenza leale su tale mercato evitando discriminazioni ingiustificate a danno degli operatori esistenti. Qualsiasi prestatore di servizi di pagamento, compresi i prestatori di servizi di pagamento di radicamento del conto dell'utente di servizi di pagamento, dovrebbe poter offrire servizi di disposizione di ordine di pagamento*".

[7] Direttiva 2007/64/CE.

[8] In Italia la Banca d'Italia è stata confermata autorità competente ai fini della PSD2, come già per la PSD1.

[9] Per una disamina dettagliata della disciplina applicabile a tali servizi si veda il contributo di V. Profeta in questo *Quaderno*.

è, pertanto, tenuto a consentire tale accesso, qualora i conti della clientela siano consultabili *on-line*, secondo diverse modalità che verranno esaminate in seguito.

In linea generale, l'obiettivo costantemente tenuto presente nel corso dei lavori di definizione della Direttiva, e rinvenibile nei numerosi *consideranda*, è stato quello di definire un contesto di certezza, fiducia e sicurezza in cui fosse neutrale la scelta della tecnologia sottostante i servizi offerti ai consumatori.

D'altronde, il legislatore europeo, nel suo intento di definire un contesto competitivo che consentisse il dispiegarsi dei possibili benefici legati all'innovazione tecnologica, correttamente non ha predefinito soluzioni tecniche a livello normativo, evitando così di "cristallizzarle" nella Direttiva. L'applicazione del principio di neutralità tecnologica peraltro non ha esentato il regolatore dal fissare alcuni prerequisiti di carattere tecnico per garantire, unitamente alla competitività, l'affidabilità e l'efficienza degli strumenti di pagamento elettronici e un adeguato livello di tutela del consumatore.

La tecnica legislativa adottata definisce quindi a livello di normativa primaria i principi generali nonché i diritti e gli obblighi che assistono la prestazione dei servizi; per la prima volta nel settore dei pagamenti *retail* viene rimesso all'EBA il compito di emanare standard o linee-guida sugli aspetti più tecnici, in modo da rendere concretamente applicabili le disposizioni contenute nella direttiva.

Non si può che concordare con questa soluzione, che appare strumentale a ovviare al problema legato alle lungaggini dei processi legislativi europei che, come noto, richiedono anni dalla pubblicazione della proposta da parte della Commissione europea per addivenire all'entrata in vigore del testo definitivo[10] e non appaiono quindi coerenti con la velocità che caratterizza l'innovazione tecnologica. A titolo di esempio, la proposta di revisione della PSD1 da parte della Commissione risale al 2013, l'entrata in vigore della PSD2 al gennaio 2016, il termine per il recepimento nazionale al gennaio 2018. In questi cinque anni si sono peraltro registrati, specialmente in un settore dinamico come quello dei pagamenti *retail*, cambiamenti rilevanti che hanno prodotto effetti sulla struttura del mercato tali da poter incidere sull'efficacia di alcune previsioni contenute nella PSD2.

Nell'intento del legislatore europeo, il rinvio all'EBA della predisposizione della normativa tecnica contribuisce alla definizione di un impianto regolamentare più elastico e più agevolmente modificabile, capace di meglio tenere il passo con la rapida evoluzione tecnologica che si osserva[11]. Questa scelta appare particolarmente felice in relazione ad aspetti inerenti alla sicurezza e alle modalità di accesso ai conti.

---

[10] Per le direttive, tali tempi si dilatano ulteriormente in considerazione dei due anni normalmente previsti per il recepimento negli ordinamenti nazionali dei diversi Paesi membri.

[11] Sono ben 12 i mandati assegnati all'EBA dalla PSD2: dalla sicurezza ai rapporti tra autorità *home* e *host* nel caso di prestazione di servizi su base transfrontaliera, dagli obblighi di *reporting* degli incidenti di sicurezza alla raccolta dei dati sulle frodi con mezzi di pagamento.

L'impostazione basata sul citato principio della neutralità tecnologica ovviamente implica la possibilità che sul mercato possano convivere una pluralità di soluzioni per l'offerta di uno specifico servizio o di singole componenti del servizio stesso. In una prospettiva statica, questa frammentazione del mercato può rappresentare un disvalore, anche ai fini della funzionalità dei servizi; al tempo stesso è proprio una siffatta impostazione a essere l'unica in grado di innescare un processo che, a tendere, dovrebbe accrescere l'efficienza dei servizi di pagamento, consentendo la comparazione delle diverse offerte. Questo è infatti un mercato in cui sono presenti economie di rete che devono coniugare le diverse esigenze della filiera dei soggetti che partecipano alla domanda e all'offerta dei servizi.

I nuovi servizi disciplinati dalla PSD2, ovvero i servizi di disposizione di ordini di pagamenti (*Payment initiation services* – "PIS") e di accesso informativo ai conti (*Account information services*, "AIS"), presentano delle caratteristiche che in parte li distinguono dai tradizionali servizi di pagamento in quanto non contemplano la gestione di flussi finanziari né la detenzione di fondi degli utenti. La decisione di annoverare anche tali attività tra i servizi sottoposti a riserva di legge ha comportato un ampliamento della nozione di 'servizio di pagamento' che è stata sempre associata a un trasferimento di fondi e alla gestione di un conto di pagamento. Questa scelta ha peraltro semplificato il quadro regolamentare, evitando di rinviare ad una diversa normativa la disciplina applicabile a operatori che, nel concreto, sono attivi in uno stesso ecosistema.

La natura prevalentemente informativa di questi servizi ha pertanto indotto il legislatore a riconoscerne la specificità, adattando ai relativi prestatori la disciplina generalmente applicabile agli istituti di pagamento. A titolo di esempio, non sono previsti requisiti di fondi propri né regole in tema di segregazione dei fondi dei clienti; non è richiesto di detenere un capitale iniziale per gli AISPs. Per entrambi gli AISPs e i PISPs è previsto l'obbligo di stipulare una polizza assicurativa a copertura dei rischi derivanti dalle attività prestate, ovvero di offrire un'analoga garanzia (a titolo di es., una lettera di *patronage*); aspetto quest'ultimo che può rendere più agevole il rispetto del requisito da parte di futuri TPPs emanazione di gruppi bancari e finanziari.

Come già accennato, ciò che caratterizza tali servizi è il fatto che prevedono l'accesso ai conti di pagamento *on-line* gestiti da un diverso operatore. Questo comporta profili di rischio specifici legati alla sicurezza delle credenziali di accesso degli utenti ai propri conti e al rispetto della riservatezza dei dati personali.

La direttiva quindi non fissa un generico principio di accesso non oneroso a tutti i dati dei pagamenti bancari ma solamente a quelli strumentali per consentire lo sviluppo di due servizi essenziali e imprescindibili in ogni soluzione innovativa nel campo dei pagamenti. La PSD2 può quindi a pieno titolo considerarsi un "acceleratore dell'innovazione" in quanto, obbligando le banche ad "aprirsi",

impone di effettuare investimenti in tecnologie, creando le basi per lo sviluppo di nuovi modelli di business che consentono l'offerta di servizi innovativi[12].

Questo accesso gratuito *ex lege* è circoscritto sia nel perimetro (in quanto previsto solamente per i conti di pagamento), sia nelle finalità, che sono limitate al disporre un ordine di pagamento, per il PISP, e all'offerta di servizi informativi per consentire all'utente "*di disporre immediatamente di un quadro generale della sua situazione finanziaria in un dato momento*"[13], per l'AISP; queste limitazioni appaiono funzionali a controbilanciare l'abbattimento delle barriere d'ingresso nella prestazione dei servizi di pagamento, finalizzato a stimolare la concorrenza, tutelando al contempo gli investimenti che la banca, presso cui è incardinato il conto, è tenuta a fare per preservare i valori ricevuti in deposito, le infrastrutture tecnologiche utilizzate e, più in generale, la sicurezza di tutte le informazioni raccolte.

Per poter prestare i servizi di accesso, è necessario che il TPP raccolga il preventivo consenso dell'utente titolare del conto di pagamento.

La mancanza di tale preventivo consenso dell'utente all'operatore che accede ai dati non può essere, peraltro, eccepita dalla banca presso cui è incardinato il conto; anche questa è una previsione da ascrivere a quelle volte a favorire la concorrenza, in quanto non consente alla banca di effettuare un controllo aggiuntivo sull'effettiva prestazione del consenso da parte dell'utente. Un siffatto controllo richiederebbe tempi non compatibili con l'immediatezza che caratterizza i servizi digitali, disincentivando gli utenti dall'usufruire dei servizi offerti dai TPPs. Potrebbe inoltre, nel concreto, essere utilizzato in modo improprio, con l'obiettivo di discriminare i TPPs.

Non viene tuttavia definita, a livello di normativa europea, una specifica disciplina per la revoca del consenso all'utilizzo del TPP da parte dell'utente. Se da un lato infatti sembrerebbe discendere da un principio generale dell'ordinamento che la revoca del consenso debba essere portata a conoscenza del soggetto cui il consenso era stato originariamente prestato, un'applicazione rigida di tale principio, che escludesse in via assoluta la possibilità per l'utente di revocare il consenso all'accesso ai conti anche direttamente presso la banca

---

[12] Sul punto si veda KPMG, *PSD2: a game changer*?, ottobre 2018, secondo cui la direttiva pone nuove sfide per le banche in termini di *compliance* e ha l'obiettivo di aumentare la concorrenza nel settore, con conseguente minaccia per gli operatori tradizionali, ma con nuove ed interessanti opportunità di *business*.

[13] Il considerando 28 prevede che "gli sviluppi tecnologici degli ultimi anni hanno portato anche alla nascita di una serie di servizi accessori, ad esempio servizi di informazione sui conti. Tali servizi forniscono all'utente di servizi di pagamento informazioni *online* aggregate su uno o più conti di pagamento, detenuti presso un altro o altri prestatori di servizi di pagamento, a cui si ha accesso mediante interfacce online del prestatore di servizi di pagamento di radicamento del conto. L'utente di servizi di pagamento può così disporre immediatamente di un quadro generale della sua situazione finanziaria in un dato momento. Anche tali servizi dovrebbero essere trattati nella presente direttiva al fine di garantire ai consumatori una protezione adeguata relativamente ai dati di pagamento e contabili nonché la certezza giuridica legata allo *status* di prestatore di servizi di informazione sui conti".

ove è incardinato il conto di pagamento, rischierebbe di ridurre sensibilmente il livello di tutela dell'utente.

La mancata chiarezza sulla disciplina applicabile alla revoca del consenso potrebbe creare anche una situazione di incertezza giuridica con riferimento alle fattispecie in cui la banca, a seguito dell'eventuale ricezione della revoca del consenso dell'utente all'utilizzo di un determinato TPP, dovesse procedere a bloccarne l'accesso al conto.

Inoltre, tale impostazione sembrerebbe escludere la possibilità che l'utente possa creare presso la banca delle cc.dd. '*black lists*' di TPPs, ovvero degli elenchi in cui indica gli operatori che non vuole che accedano ai suoi conti di pagamento, circostanza questa ammessa in altri casi in cui il conto dell'utente è movimentato da un soggetto diverso dall'utente stesso o dal prestatore che gestisce il conto di pagamento (a titolo di esempio, nel caso di addebiti diretti).

La revoca del consenso all'utilizzo di un TPP da parte dell'utente è un aspetto particolarmente delicato in quanto i limiti all'esercizio della stessa devono essere fissati in modo da bilanciare due esigenze diverse e potenzialmente contrapposte: da un lato la necessità di stimolare lo sviluppo di questo segmento di mercato, evitando che le banche spingano l'utente a escludere in via assoluta che il conto di pagamento sia accessibile da parte dei TPPs (ad esempio inserendo una clausola generale che neghi tale possibilità nel contratto quadro); dall'altra, quella di non abbassare il livello di tutele accordate all'utente, privandolo del diritto di comunicare direttamente alla banca che gestisce il conto la sopravvenuta volontà di negare il consenso a un determinato TPP.

Sembra pertanto auspicabile un intervento chiarificatore del legislatore europeo, o, in subordine, dell'EBA, per evitare che su un aspetto così delicato i singoli Paesi dell'Unione adottino approcci difformi. In assenza di specifiche previsioni nella PSD2 su questo aspetto, il legislatore nazionale, in un'ottica tesa ad accrescere le tutele a favore dell'utente, ha previsto che la revoca del consenso alla prestazione dei servizi da parte dei TPPs possa invero essere ricevuta *anche* dalla banca che gestisce il conto di pagamento.

Al riguardo, si segnala come la PSD2, nonostante la sua natura di direttiva di massima armonizzazione, su questo come su altri aspetti, abbia lasciato alcuni margini di incertezza che sono stati colmati, in maniera potenzialmente difforme, dalle leggi di trasposizione nazionale, rendendo quindi centrale il compito dell'EBA nell'assicurare la massima convergenza possibile delle prassi di supervisione adottate dalle diverse autorità all'interno dell'Unione.

Prima della PSD2, come già accennato, questi servizi erano già prestati di fatto da operatori che, a seguito del rilascio delle credenziali di sicurezza da parte degli utenti, le utilizzavano per accedere ai conti di pagamento tramite l'interfaccia utente messa a disposizione dalla banca; le banche che detenevano il conto, di conseguenza, non avevano sempre contezza del fatto che ad accedere non fosse effettivamente il proprio cliente ma piuttosto un soggetto terzo.

Questa modalità operativa, comunemente conosciuta come '*screen-scraping*[14]' – e ancora oggi ammissibile, con alcune limitazioni, fino all'effettiva applicazione della relativa normativa secondaria EBA[15] – poneva (e pone)alcuni problemi di natura giuridica.

Nel rapporto tra la banca e il proprio cliente si verifica infatti una violazione, da parte del cliente, dell'obbligo contrattuale di non divulgazione a terzi delle proprie credenziali di sicurezza, che può – al ricorrere di determinate condizioni – limitare l'obbligo di rimborso della banca in caso di contestazione da parte del cliente per operazioni non autorizzate. Inoltre, la difficoltà di individuare chiaramente i diversi operatori coinvolti a vario titolo nella prestazione del servizio rende di fatto impossibile allocare eventuali responsabilità, e attivare i conseguenti rimedi restitutori o risarcitori, in caso di malfunzionamento del servizio. Diventa quindi fondamentale, per assicurare il funzionamento del meccanismo di accesso delineato dalla PSD2, stabilire un corretto riparto di responsabilità tra tutti i prestatori coinvolti nell'offerta del servizio, a tutela non solo dell'utente ma anche degli stessi operatori; tale regime non sarebbe pensabile senza l'identificazione dei TPPs.

Tale obbligo di identificazione viene assolto, in base a quanto stabilito dagli standard tecnici dell'EBA, tramite l'utilizzo di certificati digitali rilasciati da parte di operatori qualificati: si tratta dei *Qualified Trust Service Providers* (QTSP), la cui disciplina è dettata da una diversa normativa (il Regolamento (UE)/910/2014 sull'identità digitale, "Regolamento e-IDAS", entrato in vigore nel mese di luglio del 2016). I certificati devono anche indicare il ruolo svolto dal TPP nella prestazione del servizio (se cioè agisca in qualità di PISP o di AISP). Pur non sussistendo un obbligo per le banche di munirsi di un certificato digitale, a parere dell'EBA sarebbe preferibile che ciò avvenisse, al fine di assicurare con certezza la mutua identificazione degli operatori coinvolti nella prestazione dei servizi di pagamento[16].

Questi certificati sono essenzialmente di due tipi: QWAC e QSeal. Il primo garantisce la confidenzialità, l'integrità e l'autenticità dei dati trasmessi tramite il canale di comunicazione certificato mentre il secondo assicura che i dati provengano effettivamente dal mittente che ha apposto il sigillo e che non siano stati alterati dal momento dell'apposizione del sigillo stesso. Sarà la banca, responsabile di mettere a disposizione l'interfaccia di comunicazione e di garantire la sicurezza del canale di accesso ai conti, a decidere di quale certificato debba dotarsi il TPP[17].

---

[14] Lo '*screen-scraping'* è il processo di raccolta dei dati di visualizzazione dello schermo da un'applicazione a un'altra, in modo che quest'ultima possa visualizzarla.

[15] Si tratta dei *regulatory technical standards* dell'EBA adottati con regolamento delegato (UE) 2018/389 della Commissione europea in tema di autenticazione forte del cliente e standard aperti di comunicazione comuni e sicuri.

[16] Cfr. *EBA*, *Opinion on the use of eIDAS certificates under the RTS on SCA and CSC.*

[17] Cfr. *supra*, *EBA*, *Opinion cit.*

Prerequisito per ottenere il rilascio di tali certificati è aver ottenuto l'autorizzazione a prestare servizi di pagamento dalla propria autorità competente. Potranno quindi prestare tali servizi in Italia le banche, in quanto – una volta autorizzate all'esercizio dell'attività creditizia – possono di default prestare tutti i servizi di pagamento (ivi compresi quindi quelli di AIS/PIS), gli istituti di moneta elettronica che - una volta autorizzati anche alla prestazione di servizi di pagamento oltre che alla emissione di moneta elettronica - sono anch'essi abilitati a offrire tutti i servizi di pagamento, e gli istituti di pagamento, se specificamente autorizzati alla prestazione dei servizi di AIS e PIS. L'autorizzazione agli IP viene infatti rilasciata per la prestazione di singoli servizi di pagamento, debitamente indicati nell'istanza.

Pertanto, le specificità normative richiamate sopra assumono particolare rilievo per l'autorizzazione di IP che prestino esclusivamente i servizi di AIS/PIS, non necessitando le banche e gli istituti di moneta elettronica di apposita autorizzazione per prestare tali servizi. Il rilascio della licenza costituisce un procedimento amministrativo e pertanto è soggetto alle regole precisate nelle Istruzioni di vigilanza della Banca d'Italia. Abbiamo già detto in precedenza delle particolarità della disciplina disegnata per tali soggetti; appare quindi necessario che l'autorità competente, sia in sede di prima autorizzazione che nella successiva fase di supervisione *on-going,* verifichi se i *benchmarks* e le metodologie di analisi utilizzati oggi a fini di supervisione per gli operatori tradizionali colgano appieno i principali profili di rischio dei nuovi intermediari[18].

L'utilizzo dei certificati qualificati è pertanto appannaggio dei prestatori di servizi di pagamento autorizzati all'offerta dei servizi di AIS/PIS. Tuttavia, un potenziale *vulnus* dell'architettura fin qui delineata risiede nella disciplina relativa agli obblighi che, in base al regolamento e-IDAS sono posti a capo del QTSP; quest'ultimo è infatti tenuto a verificare la sussistenza di tutti i requisiti prescritti dalla legge al momento del rilascio del certificato ma, una volta emesso, non appare chiaro se sia anche tenuto a effettuare una periodica analisi della permanenza del possesso di tali requisiti in capo al soggetto.

È del tutto evidente che in caso di revoca dell'autorizzazione anche i certificati dovrebbero essere revocati, al fine di evitare che operatori non più regolamentati possano accedere ai dati di pagamento degli utenti; non paiono sussistere dubbi neppure sul fatto che la responsabilità di chiedere la revoca del certificato risieda *in primis* in capo al singolo AISP/PISP non più munito di licenza.

---

[18] Inoltre, i servizi di pagamento rientrano tra le attività ammesse al mutuo riconoscimento; potranno pertanto prestare tali servizi di pagamento in Italia, in virtù del cosiddetto 'passaporto europeo', anche intermediari a ciò autorizzati in altri Stati membri dell'UE e che intendano estendere la propria operatività su base transfrontaliera in altri Paesi appartenenti all'Unione. A seconda delle modalità organizzative prescelte, si configureranno casi di esercizio del diritto di stabilimento (qualora nel Paese ospitante venga costituita una succursale o si faccia stabilmente uso di una rete di agenti) ovvero di libera prestazione, con prerogative e poteri diversi attribuiti all'autorità competente del Paese ospitante.

Per rafforzare questo meccanismo, occorre interrogarsi sull'opportunità di coinvolgere nel processo di revoca le autorità competenti a rilasciare (e revocare) la licenza. Non sembra, tuttavia, percorribile l'ipotesi che l'autorità stessa assuma al riguardo un ruolo attivo, ad es. contattando il QTSP e chiedendo di ritirare i certificati emessi a nome del soggetto cui è stata revocata la licenza. Questo alla luce della considerazione che l'autorità potrebbe non avere alcuna contezza circa quale QTSP, potenzialmente ubicato in un qualsiasi Paese dell'Unione, abbia in effetti rilasciato il singolo certificato allo specifico TPP.

Si aggiunga che l'autorità competente è tenuta a predisporre e aggiornare un registro pubblico in cui si dà evidenza di tutti gli intermediari cui è stata concessa un'autorizzazione alla prestazione di servizi di pagamento, nonché della revoca della stessa. Tali informazioni vengono inoltre inviate all'EBA, a sua volta incaricata dalla PSD2 della costituzione di un registro pubblico centralizzato in cui confluiscono tutte le informazioni contenute nei singoli registri nazionali e trasmesse dalle autorità competenti.

Per assicurare che i registri possano rappresentare fedelmente la situazione del mercato, garantendo pertanto la rispondenza tra l'effettivo status dell'intermediario e quello risultante dalle informazioni ivi contenute, appare fondamentale assicurare un aggiornamento tempestivo dei registri nazionali e una comunicazione altrettanto celere al registro dell'EBA dei cambiamenti relativi alla situazione degli operatori.

In prospettiva, le autorità saranno chiamate a ricercare soluzioni anche tecnologiche che possano ridurre al minimo la distanza temporale tra la conclusione di un procedimento amministrativo (sia esso di autorizzazione o revoca) e la pubblicazione della relativa informativa. È questo un elemento del dibattito in corso sull'impatto che le nuove tecnologie possono avere sulle stesse modalità di conduzione delle attività di vigilanza (SupTech).

3. Open banking: *l'accesso ai conti tramite le* Application Programming Interfaces *(APIs)*

Nel nuovo quadro regolamentare le banche devono consentire l'accesso ai conti di pagamento da parte dei TPPs al fine di assicurare che sia garantito il diritto dell'utente di utilizzare tali servizi. La normativa primaria, anche in ossequio al citato principio di neutralità tecnologica, non impone una specifica soluzione per assicurare tale accesso, rinviando la scelta alle banche.

Tuttavia, la normativa secondaria dell'EBA delinea due possibili modalità con cui i TPPs possono accedere, previo consenso dell'utente, ai conti di pagamento: tramite l'interfaccia-utente messa a disposizione del cliente dalla banca nell'ambiente di *home-banking*, ovvero per mezzo di un'interfaccia

dedicata a tale scopo sviluppata; si parla in quest'ultimo caso di API (*Application Programming Interface*[19]).

Quale che sia la modalità prescelta, essa dovrà ovviamente rispettare i già citati vincoli normativi posti all'accesso ai conti da parte dei TPPs: possibilità di accesso solo ai dati di pagamento contenuti in conti precedentemente individuati dall'utente, obbligo di identificazione del TPP al momento dell'accesso, impossibilità per i TPPs di conservare i dati e di utilizzarli per finalità diverse da quelle espressamente indicate dalla legge.

Ciò comporta, a titolo di esempio, che in caso di accesso tramite interfaccia utente, quest'ultima dovrà comunque essere debitamente modificata, per garantire la *compliance* con i limiti citati.

Questa impostazione declina nell'ordinamento il concetto dell''*open source*', proprio dell'evoluzione tecnologica più recente. In linea generale, sotto il profilo tecnico, le APIs consentono lo scambio di dati disponibili all'interno di reti non appartenenti allo stesso dominio. L'utilizzo di tali interfacce aperte consente di ottenere e condividere, a un costo contenuto rispetto alle tradizionali attività di *systems integration*, informazioni necessarie all'erogazione di nuovi servizi, spingendo gli operatori bancari a un vero e proprio "salto" nelle strategie commerciali e distributive adottate.

L'elemento di novità, che porta alla creazione di un ambiente favorevole alla competizione, è la pubblicità delle specifiche tecniche da utilizzare per accedere alle informazioni, che la singola azienda mette a disposizione anche in assenza di una relazione contrattuale con i soggetti che potenzialmente ne faranno uso. Sul piano tecnico, una API consente ad un'azienda di essere "scelta e inclusa" in un processo produttivo e quindi di beneficiare, in via indotta, di un prodotto di terzi.

Il concetto di API riporta immediatamente al concetto di *FinTech*, che nella definizione del Financial Stability Board vuol cogliere il fenomeno dell'innovazione finanziaria innescata da quella "tecnologica, che può concretizzarsi in nuovi modelli di business, processi o prodotti, producendo un effetto determinante sui mercati finanziari, sulle istituzioni, o sull'offerta di servizi[20]".

L'evoluzione che si osserva nel mercato europeo a seguito dell'approvazione della PSD2 è coerente con quanto auspicato dal legislatore: si sta affermando nella comunità bancaria un ecosistema aperto in cui gli aspetti cooperativi e competitivi

---

[19] Nella terminologia di sviluppo software, con il termine *Application Programming Interface* (API) si individua quell'insieme di regole di attivazione e uso di un modulo software unitamente all'ambiente operativo per la sua attivazione ed uso.

[20] Cfr. la definizione di *FinTech* data dal Financial Stability Board (FSB): "*Technology-enabled innovation in financial services that could result in new business models, applications, processes or products with an associated material effect on the provision of financial*", da *Financial Stability Implications from FinTech*, giugno 2017.

trovano un loro equilibrio per favorire l'affermarsi di servizi utili all'utente, con chiara indicazione delle responsabilità dei diversi soggetti coinvolti.

Occorre aver presente che la normativa europea, in linea con l'obiettivo di rafforzare il mercato interno dei servizi di pagamento al dettaglio, impone che qualunque soluzione adottata per assicurare l'accesso ai conti di pagamento da parte dei TPPs sia costruita in modo da rispondere alle esigenze di tutti i prestatori di pagamento europei. Talune scelte per la verifica delle previsioni della direttiva o dell'EBA ne sono la conferma; a titolo meramente esemplificativo, possiamo richiamare le norme sul *wide usage* ovvero quelle relative alla pubblicità delle soluzioni tecniche per l'interfaccia (cfr. *infra*).

Il già citato Regolamento Delegato (UE) n. 2018/389 adottato dalla Commissione europea contiene, tra le altre cose, le norme tecniche di regolamentazione per definire gli standard aperti di comunicazione comuni e sicuri tra prestatori di servizi di pagamento. L'obiettivo è quindi quello di garantire un canale sicuro di autenticazione e comunicazione tra banche e TPPs. Come anticipato in precedenza, in base a questo Regolamento, i prestatori che detengono i conti devono predisporre, entro il 14 settembre 2019, le interfacce di accesso per consentire ai TPPs di svolgere la propria attività.

Qualora venga adottata l'interfaccia dedicata è previsto che, in caso d'indisponibilità o di prestazioni inadeguate della stessa, venga assicurata ai TPPs la possibilità di accedere ai conti di pagamento attraverso l'interfaccia messa a disposizione dei clienti nell'ambiente di *home-banking* (c.d. '*fall-back option*')[21]. Il meccanismo delineato dall'EBA su impulso del legislatore europeo trovava fondamento nel timore che eventuali malfunzionamenti dell'API dedicata, in assenza di una soluzione di *back-up*, potessero costituire di fatto un ostacolo allo sviluppo dei servizi dei TPPs a detrimento, in ultima istanza, degli utenti stessi.

Un obbligo *tout court* di definire un meccanismo di *fall-back* era però apparso subito eccessivamente oneroso per le banche in quanto le costringeva, nei fatti, a investimenti ingenti per mettere a disposizione due diverse modalità di accesso ai conti (API e *fall-back*, quest'ultima da attivare in caso di inefficienze nel funzionamento dell'API).

Per bilanciare gli opposti interessi in gioco, è stata quindi prevista la possibilità, per le banche che rispettino una serie di condizioni definite nella

---

[21] L'articolo 33, comma 4, del Regolamento delegato (UE) n. 2018/389, prevede che "Nell'ambito di un meccanismo di emergenza, i prestatori di servizi di pagamento di cui all'articolo 30, paragrafo 1, [i TPPs] sono autorizzati a utilizzare le interfacce messe a disposizione degli utenti dei servizi di pagamento per l'autenticazione e la comunicazione con il prestatore di servizi di pagamento di radicamento del conto [la banca], finché per l'interfaccia dedicata non viene ripristinato il livello di disponibilità e di prestazioni previsto dall'articolo 32 [ovvero lo stesso livello di disponibilità e di prestazione, anche in relazione all'assistenza, delle interfacce rese disponibili all'utente dei servizi di pagamento per accedere direttamente al suo conto di pagamento *online*".

normativa predisposta dall'EBA[22], di ottenere dalla propria autorità nazionale competente – per l'Italia, la Banca d'Italia – un'esenzione dall'obbligo di predisporre la *fall-back option*[23].

Le citate condizioni possono così riassumersi:

- definire e pubblicare i contenuti tecnici dell'interfaccia che il TPP può richiamare per sviluppare le proprie procedure;
- attivare l'interfaccia operativa per l'accesso alle funzioni necessarie allo sviluppo dei servizi;
- mettere a punto le procedure di autenticazione dei TPPs basate su certificati digitali conformi al regolamento e-IDAS, di cui si è detto sopra;
- implementare misure di sicurezza a protezione dei dati e delle credenziali;
- rendere possibile ai TPPs l'utilizzo delle procedure di autenticazione messe a disposizione del cliente;
- attivare processi di *change management* dell'interfaccia che consenta ai TPPs di adeguarsi con immediatezza alle modifiche delle procedure di colloquio della banca con i propri clienti;
- mettere a disposizione gli ambienti *test* e di supporto alle attività dei TPPs;
- disporre di procedure di *contingency* in caso di malfunzionamento o degrado della interfaccia.

Queste previsioni, funzionali ad assicurare il diritto dei TPPs a prestare i propri servizi, si sono poste all'attenzione degli operatori come un investimento ineludibile, con diverse possibili soluzioni attivabili nel concreto. Una riflessione che ha accomunato tutti gli operatori europei è stata volta all'individuazione dei possibili spazi di cooperazione, per ridurre i costi di investimento ed attivare le esternalità positive proprie di una economia di rete.

In una prima fase, anche sotto la spinta di lavori avviati in ambito European Retail Payments Board (ERPB)[24], vi è stata la ricerca di una convergenza su

---

[22] Le condizioni per l'esenzione specificate all'articolo 33, par. 6 del Regolamento delegato (UE) n. 2018/389, sono dettagliate negli Orientamenti dell'EBA, "*Guidelines on the exemption from the contingency mechanism under the RTS on SCA and CSC*", pubblicate il 4 dicembre 2018.

[23] Cfr. Banca d'Italia, *Comunicazione al sistema*, 24 dicembre 2018, "*PSD2 – accesso ai conti: istruzioni per il procedimento amministrativo di esenzione dall'obbligo di realizzare procedure di* contingency ('fall-back solutions')".

[24] L'ERPB è un organismo operativo dal 2014, presieduto dalla BCE e composto da esponenti sia del lato dell'offerta che del lato della domanda dei pagamenti *retail* in Europa che, attraverso il dialogo tra i diversi *stakeholders* e le istituzioni, si propone di promuovere lo sviluppo di un mercato integrato, innovativo e competitivo dei pagamenti in euro nell'UE.

standard tecnici in grado di soddisfare i requisiti fissati dal quadro regolamentare. Nel mercato europeo si sono quindi delineate quattro soluzioni riconducibili principalmente alle iniziative portate avanti da organismi attivi nella definizione di standard nel settore dei pagamenti. Si tratta in particolare, degli standard definiti dal Berlin Group, da Open Banking UK, dal francese STET e dall'*integration hub* polacco Banqware platform.

I singoli operatori di mercato sono liberi di decidere se implementare o meno gli standard, tranne nel caso di Open Banking UK; con un provvedimento del 2018 infatti la Competition and Markets Authority (CMA) inglese ha imposto l'utilizzo delle specifiche tecniche per le APIs dedicate alla prestazione dei servizi di AIS e PIS definite da Open Banking UK alle nove principali banche inglesi, al fine di assicurare piena interoperabilità all'interno del Paese. Questa scelta, che di fatto supera i problemi legati alla necessità di assicurare l'interoperabilità tra diverse iniziative di mercato, non appare del tutto in linea con l'impostazione della Direttiva e dei lavori dell'EBA, che volutamente hanno evitato di imporre soluzioni che potessero condizionare le scelte degli operatori.

Nella seconda fase sono state messe a punto alcune soluzioni applicative, sempre ricercando soluzioni condivise; questo processo è tipico del mondo dei pagamenti, in cui la definizione di soluzioni cooperative o infrastrutturali costituisce il prerequisito per assicurare l'efficienza del sistema e lo sviluppo delle dinamiche competitive sui servizi.

La necessità di consentire un rapido adeguamento alle previsioni regolamentari, visti anche i tempi stringenti imposti dalle autorità europee, ha favorito la ricerca di opzioni tecnologiche in grado di soddisfare una molteplicità di utenti e, sul mercato italiano, sono state presentate quattro soluzioni, ovviamente e necessariamente aperte anche a soggetti non italiani: i) *CBI Globe*, messa a punto dal Corporate Banking Interbancario e riconducibile all'esperienza associativa propria del Consorzio[25]; ii) la soluzione offerta da Cedacri[26]; iii) *Fabrick*, promossa dal Gruppo Sella e iv) *Open Banking*, offerta da SIA[27]. Tali soluzioni consentiranno a larga parte del sistema di rispettare le previsioni regolamentari nei tempi prescritti; ad oggi, infatti, sono poco numerosi gli operatori che hanno optato per soluzioni proprietarie.

---

[25] Il Consorzio CBI definisce in ambito condiviso le regole e gli standard tecnici e normativi di diversi servizi ("Servizio CBI", "Servizio CBILL", servizi di Nodo), nonché gestisce l'infrastruttura tecnica di connessione tra i consorziati, per consentire agli stessi di realizzare, in via telematica, il collegamento ed il colloquio con la clientela, in un'ottica di interoperabilità a livello nazionale ed internazionale, per l'erogazione degli stessi servizi.

[26] Cedacri S.p.A. è un'azienda italiana specializzata in servizi di *outsourcing* informatico per il settore bancario a capo di un gruppo di società che presidiano completamente le molteplici attività correlate ai servizi di *outsourcing*: *outsourcing* completo, *facility management, system integration, business process outsourcing.*

[27] SIA è leader europeo nella progettazione, realizzazione e gestione di infrastrutture e servizi tecnologici dedicati alle istituzioni finanziarie, alle banche centrali, alle imprese e alle pubbliche amministrazioni, nelle aree dei pagamenti, della monetica, dei servizi di rete e dei mercati dei capitali.

Il rispetto dei tempi regolamentari da parte dei singoli operatori e le esigenze di pianificazione delle attività di sviluppo di applicazioni che comunque rappresentano una novità per la maggior parte degli intermediari, hanno stimolato il regolatore italiano a ricercare soluzioni organizzative atte a coniugare le diverse esigenze grazie alla presenza, all'interno della Banca d'Italia, sia della funzione di vigilanza sui singoli operatori che di quella di sorveglianza sulle infrastrutture rilevanti per il sistema dei pagamenti[28].

In questo quadro quindi le citate iniziative di sistema, in quanto infrastrutture di rilevanza per il corretto funzionamento del sistema dei pagamenti, sono oggetto di specifica valutazione di funzionalità, antecedente rispetto alla messa in produzione, che viene effettuata da parte della Banca d'Italia nell'esercizio della sua funzione di sorveglianza sul sistema dei pagamenti. L'adesione a un'iniziativa di sistema, come quelle sopra descritte, consente quindi alle banche una meno onerosa dimostrazione, in un'ottica di vigilanza, della *compliance* con alcuni dei requisiti tecnici indicati ai fini del riconoscimento dell'esenzione dalla *fall-back option*; ciò grazie ai controlli già effettuati dalla Banca d'Italia in relazione ai servizi offerti dall'iniziativa di sistema, ferma restando la responsabilità della singola banca sulla soluzione prescelta, in linea con la disciplina applicabile alle esternalizzazioni.

*4. Conclusioni: l'***Open banking** *verso un assetto del mercato che vede i dati di pagamento come* **commodities** *e i conti di pagamento come* **essential facilities**

L'impostazione fin qui delineata sta imponendo il superamento di alcuni paradigmi consolidatisi negli anni e mai messi in discussione prima dell'entrata in vigore della PSD2.

Oltre al già citato ampliamento della nozione di 'servizio di pagamento', che non presuppone più né un trasferimento di fondi né la gestione di un conto di pagamento, viene scardinato il concetto per cui i dati relativi alle attività dei clienti rientrano nella disponibilità delle sole banche che gestiscono i conti di pagamento presso i quali sono incardinati. La Direttiva introduce invero il concetto secondo il quale i dati sono nella disponibilità del cliente che li ha "generati", che può quindi consentirne l'uso a terzi per le finalità individuate nella Direttiva: avviare pagamenti

---

[28] Giova qui ricordare i poteri di cui all'art 146 TUB, il quale prevede che la Banca d'Italia esercita la sorveglianza sul sistema dei pagamenti avendo riguardo al suo regolare funzionamento, alla sua affidabilità ed efficienza nonché alla tutela degli utenti di servizi di pagamento. Per tali finalità, nei confronti dei soggetti che emettono o gestiscono strumenti di pagamento, prestano servizi di pagamento, gestiscono sistemi di scambio, di compensazione e di regolamento o gestiscono infrastrutture strumentali tecnologiche o di rete, può, tra le altre cose, richiedere la comunicazione, anche periodica, di dati, notizie, atti e documenti concernenti l'attività esercitata; emanare disposizioni di carattere generale aventi a oggetto il contenimento dei rischi, l'accesso dei prestatori di servizi di pagamento ai sistemi di scambio, di compensazione e di regolamento nonché alle infrastrutture strumentali tecnologiche o di rete; il funzionamento, le caratteristiche e le modalità di prestazione dei servizi offerti; gli assetti organizzativi e di controllo relativi alle attività svolte nel sistema dei pagamenti; disporre ispezioni, chiedere l'esibizione di documenti al fine di verificare il rispetto delle norme disciplinanti la corretta esecuzione dei servizi di pagamento, adottare provvedimenti specifici volti a far cessare le infrazioni accertate o a rimuoverne le cause.

ovvero ricevere informazioni per disporre immediatamente di un quadro generale della propria situazione finanziaria. Le previsioni della PSD2 sono in linea con l'evoluzione tecnologica che fa assumere al dato una valenza "commerciale", una sorta di '*commodity*': il confine di questa disponibilità è oggetto di ampio dibattito.

In base a quanto previsto dalla PSD2, se da un lato è chiara la previsione che il cliente può accedere ai propri dati senza costi per il TPP "delegato", dall'altro emerge un contesto operativo che spinge le banche ad adattare i propri modelli di business al fine di valorizzare le informazioni di cui dispongono, al di là delle previsioni della Direttiva.

Inoltre, i nuovi servizi di pagamento disciplinati dalla direttiva non possono che appoggiarsi sui conti di pagamento gestiti dalle banche; l'accesso al conto diventa quindi necessario per assicurare l'offerta e lo sviluppo dei servizi di PI e AI nonché di altri servizi a valore aggiunto. I conti di pagamento diventano una sorta di *essential facility*, un'infrastruttura funzionale allo sviluppo di un ecosistema aperto per i pagamenti *retail*.

Le banche tuttavia sostengono costi per lo sviluppo e la manutenzione delle reti e dei sistemi informativi e sono chiamate ad aprire a titolo gratuito i conti detenuti a potenziali concorrenti sul mercato.

Per bilanciare queste due esigenze la Direttiva, come già menzionato, limita il diritto di accesso *ex lege*. Ne discende che l'utilizzo dei dati di pagamento per finalità diverse o a conti di natura diversa dovrà essere disciplinato da accordi contrattuali tra la banca e il TPP, sempre previo consenso dell'utente.

La portata innovativa della norma è costituita dalla conseguenza che le banche devono farsi carico di un investimento per soddisfare un obbligo normativo[29]; quest'ultimo determina nel contempo la creazione di un ecosistema aperto di cui è difficile valutare tutte le possibili evoluzioni, in grado di incidere profondamente sulla struttura non solo del mercato dei pagamenti, atteso il valore di previsione dei dati sui pagamenti, che emerge chiaramente in recenti lavori[30].

---

[29] Secondo l'indagine di ABI Lab, *Scenario e* trend *del mercato ICT per il settore bancario del 2019*, ai primi posti delle priorità d'investimento ICT troviamo, sulla scia della PSD2, le iniziative che riguardano *l'Open Banking*. Seguono il potenziamento dei canali digitali, con attenzione ai servizi di *mobile banking* e all'identificazione da remoto del cliente, e il rafforzamento delle componenti di sicurezza.

[30] Recenti studi mostrano l'esistenza di una forte correlazione tra l'attività economica nel breve periodo e i dati di pagamento; tramite questi ultimi è possibile infatti anticipare le previsioni degli aggregati economici (es. reddito, consumi, investimenti) e misurare tempestivamente l'impatto sui comportamenti di consumatori e imprese di *shock* nelle aspettative, nell'incertezza economica, nella fiducia nella moneta. Cfr. V. Aprigliano, G. Ardizzi, L. Monteforte**,** *Using the payment system data to forecast the Italian GDP*, Banca d'Italia – *Working Papers* (Temi di discussione) 2017, n. 1098; V. Aprigliano, G. Ardizzi, L. Monteforte, *Using payment system data to forecast the economic activity*, in *International Journal of Central Banking* (forthcoming) 2019; G. Ardizzi, S. Emiliozzi, J. Marcucci, L. Monteforte *News and consumer card payments*, presentato al Workshop della Banca d'Italia *Harnessing Big Data & Machine Learning Technology for Central Banks*, 26-27.3.2018, e in pubblicazione in Banca D'Italia – *Working Papers* (Temi di discussione).

Certamente le banche potranno ampliare l'offerta di servizi alla propria clientela, che siano quelli obbligatori per legge o piuttosto servizi a valore aggiunto; già si assiste a banche/IP che, oltre a offrire i servizi previsti dalla direttiva, si stanno attrezzando, tramite forme di collaborazione con la galassia delle imprese *Fintech*[31], alla prestazione di servizi il cui elemento necessario è poter disporre dei dati dei clienti. Il rapporto tra banche e aziende *Fintech* non deve quindi essere visto solo in una logica concorrenziale in quanto entrambi hanno spazi da condividere per offrire servizi a valore aggiunto. Focalizzandoci solo sulla relazione con la clientela, le *Fintech* hanno dalla loro una maggiore conoscenza delle tecnologie e della relativa *user experience* mentre le banche godono della storica fiducia relazionale, che può favorire una più rapida accettazione di nuovi servizi.

Dopo una prima fase di attesa, in alcuni casi quasi "conflittuale", nei confronti delle *start-up* considerate come potenziali *competitors*, il sistema bancario ha assunto consapevolezza delle possibili evoluzioni del modello di business per adeguarsi al nuovo ecosistema. Sul piano strategico da un lato vi è un forte interesse delle banche ad offrire "in proprio" i nuovi servizi di PI e AI, che, pur non prevedendo alcun processo autorizzativo, richiedono adeguamenti delle infrastrutture tecnologiche. Nel contempo, il rapporto con le *Fintech* evolve verso soluzioni collaborative che in taluni casi sfociano in rapporti partecipativi, anche di maggioranza[32].

Il fenomeno più interessante, che andrà ad incidere profondamente sulla struttura del mercato, è quindi rappresentato dall'evoluzione dei servizi legata alla disponibilità di un'ampia gamma di informazioni: dall'analisi del merito di credito "*real time*" a proposte commerciali customizzate. Si sta affermando un modello già ampiamente diffuso nell'industria manifatturiera, ossia lo 'spacchettamento' dei prodotti bancari in diverse componenti (*unbundling*[33]) che ha due effetti: un ampliamento dei processi di esternalizzazione e una maggiore flessibilità nei possibili prodotti da offrire.

Non è un fenomeno del tutto nuovo; nel dibattito sugli effetti del processo di innovazione tecnologica e di consolidamento degli operatori bancari, già sul finire del secolo scorso alcuni autori individuarono una possibile risposta nel '*contract banking*'. Si ipotizzava un profondo ripensamento del modello organizzativo delle banche, che avrebbero mantenuto la relazione con il cliente

---

[31] Si veda al riguardo il *Rapporto Fintech Community 2019*, The European House – Ambrosetti, secondo il quale le aziende *Fintech* hanno il potenziale per incidere in modo sostanziale sulla struttura e sulle dinamiche dei mercati finanziari, rappresentando inoltre un'opportunità di collaborazione che le banche possono cogliere per avviare la trasformazione digitale.

[32] Nel rapporto dell'European Financial Management& Marketing Association (EFMA) di Maggio 2019, '*Building the bank of the future'*, si parla di '*Bank as a Platform*': *the bank maintains the privileged relationship it has with its customers and enriches its value proposition by using services from other players* e di '*Bank as a Service'*: *the bank offers its value-added services to other players with the aim of increasing the flows and amortizing its IT investments at the risk of losing the relationship with its customers*.

[33] Si veda sul punto S. Walchek, *The unbundling of finance*, TechCrunch, 2015.

ed erogato prodotti e servizi messi a punto in tutto o in parte da terzi sulla base di rapporti di *outsourcing*. In questo scenario emergeva la figura della '*virtual bank*', in cui tutti i processi potevano essere esternalizzati e la banca 'proprietaria' del rapporto con il cliente diveniva un "*broker between the customer and the ultimate supplier of services which go to make up the final products and services demanded by the customer*"[34].

Al di là degli aspetti regolamentari, le nuove tecnologie possono quindi riportare all'attenzione questa impostazione in cui tuttavia la relazione con il cliente potrebbe essere appannaggio di un *brand* non bancario che completerebbe la propria proposta commerciale con servizi finanziari, ancillari alla propria offerta, ricorrendo a operatori finanziari.

Si aprirebbe uno scenario del tutto nuovo anche per le autorità, chiamate a riflettere sul modello di regolamentazione e di controllo da applicare.

In questa prospettiva, gli effetti della PSD2 sul mercato potranno valutarsi solo nel medio periodo ma è indubbio che le scelte del legislatore europeo hanno innescato un percorso di innalzamento del livello di concorrenza nel rispetto di elevati standard di sicurezza nei pagamenti elettronici necessario e ineludibile in un contesto in cui è sempre più ampia la platea dei fruitori di questi servizi.

Inoltre, ciò che risulta evidente è che la tenuta di questa architettura non può prescindere da una stretta collaborazione, sia a livello nazionale che a livello europeo, tra le varie autorità, con competenze nei diversi settori interessati.

In base a quanto sopra, oltre alla Banca d'Italia, nella sua duplice veste di autorità di vigilanza sugli intermediari che prestano i servizi di pagamento e di *overseer* sul sistema dei pagamenti, viene in rilievo il ruolo dell'Agenzia per l'Italia digitale (AgID), incaricata di riconoscere i QTSP, operatori necessari per assicurare l'avvio dello sviluppo dei servizi di accesso ai conti.

Vista la natura prevalentemente informativa dei servizi di AI/PI, appaiono particolarmente rilevanti i profili legati alla protezione dei dati personali, tra cui rientrano i dati relativi ai pagamenti. La PSD2, che precede, sotto il profilo temporale, la *General Data Protection Regulation*[35], tenta di risolvere il problema legato all'interazione tra le due normative richiamando, in più punti, la necessità di rispettare la normativa sulla *privacy* nel trattamento delle informazioni relative ai pagamenti. Infine, possibili comportamenti lesivi della parità concorrenziale, oltre a violare la normativa pagamenti, potrebbero rilevare sotto profili antitrust; da ultimo, non occorre tralasciare i rapporti con le autorità preposte al controllo delle infrastrutture di telecomunicazioni, tenuto conto che le Telco sono soggetti rilevanti per l'offerta dei servizi di mobilità.

---

[34] D. T. Llewellyn, (2001), "*The new economics of banking*", *SUERF Study 5, Amsterdam,* ripreso in "*Group of Ten Report on consolidation in financial sector*", gennaio 2010.

[35] Regolamento (UE)/2016/679.

Pur non essendo questa la sede per esaminare più nel dettaglio le interazioni e le possibili sovrapposizioni tra le diverse normative richiamate, appare comunque opportuno che le autorità siano consapevoli del fatto che uno stesso comportamento potrebbe rilevare sotto diversi profili, rendendo astrattamente configurabile la comminazione concorrente di diverse sanzioni, anche di importo molto rilevante, stabilite a tutela dei diversi interessi presidiati dalle richiamate normative di settore.

In conclusione, il nuovo contesto pone all'attenzione dei regolatori problematiche in cui i profili regolamentari e tecnici interagiscono: la vera novità della PSD2, dal punto di osservazione delle autorità di supervisione, è rappresentata dal fatto che, rispetto al passato, la disciplina dei pagamenti al dettaglio presuppone – ed esige – un presidio stretto anche dei profili più operativi e tecnici che caratterizzano il funzionamento del mercato. Anche la Commissione europea, nel suo *Fintech Action Plan*[36], sottolinea come le Autorità devono impegnarsi per comprendere a fondo le tendenze nel settore delle tecnologie finanziarie e rafforzare i contatti con il mercato per accrescere le proprie conoscenze e competenze sulle innovazioni digitali.

---

[36] COMMISSIONE EUROPEA, *Piano d'azione per le tecnologie finanziarie: per un settore finanziario europeo più competitivo e innovativo*, marzo 2018.

Il ruolo dei big data e il mobile payment

Raffaella Menzella

1. "Knowledge is power" *– 2. I* Big Data *in "3V" – 3. Progresso tecnologico,* FinTech *e* Big data *nel settore bancario – 4. L'evoluzione del quadro normativo europeo in materia di pagamenti digitali – 5. Il* mobile payment *e i suoi paradigmi – 6.* Big data *e modalità innovative di analisi dei dati nel* mobile payment *– 7.* Big data *e* mobile payment*: questioni di merito creditizio e prezzi*

L'avvento del *FinTech* e, con esso, di nuovi operatori che sulla innovazione tecnologica fanno leva per scardinare barriere all'ingresso e acquisire sempre maggiori quote di mercato impone un ripensamento delle tradizionali strategie di analisi bancaria e, più in generale, un cambiamento di prospettiva da parte di vigilati e vigilanti. La varietà dei dati a disposizione dell'industria bancaria e le nuove tecniche di analisi degli stessi rappresentano un fondamentale strumento di sostegno alla crescita economica e al progresso, purché correttamente guidate e irreggimentate nell'ambito di un quadro normativo e regolamentare che al vertice della gerarchia ponga la piena tutela degli utenti e la minimizzazione dei rischi derivanti dalla immediatezza e pervasività dei flussi informativi che attraversano la rete Internet.

1. "Knowledge is power"

"*Knowledge is power*" ("*Scientia potestas est*"): il ruolo centrale della conoscenza, intesa in senso lato come "informazione", nella società è racchiuso in questo aforisma – comunemente attribuito a Sir Francis Bacon[1] – che, dal 1597, ha attraversato indenne i secoli sino ad approdare all'epoca in cui viviamo, attagliandosi perfettamente a essa.

È invero innegabile che l'informazione, oggi più che mai, sia assurta al ruolo di risorsa strategica, tanto da condizionare l'efficienza dei sistemi e così divenire fattore di sviluppo sociale ed economico.

L'importanza dell'uso dei dati nei processi decisionali di imprese, istituzioni e singoli cittadini trova la sua epifania nella diffusione dei processi di "datizzazione".

Il termine "datizzazione" è un neologismo che identifica le tecniche che consentono la conversione in formato digitale – cioè in dati – di qualsiasi informazione. La raccolta delle informazioni e la loro gestione in forma strutturata sono dunque strumenti indispensabili per qualsiasi operatore di mercato, destinati ad assumere un'importanza crescente, anche e soprattutto nel settore bancario e finanziario.

Come rilevato dalla Commissione Europea nella Comunicazione del 25 maggio 2016[2], le piattaforme digitali «hanno cambiato considerevolmente l'economia digitale degli ultimi due decenni, e offrono oggi molti vantaggi alla società digitale contemporanea, svolgendo un ruolo di spicco nella creazione di "valore digitale" a sostegno della crescita economica futura nell'UE». La Commissione ha peraltro evidenziato che, anche in tale ambito, «l'applicazione

---

[1] Nelle *Meditationes sacrae* del 1597 F. Bacon aveva così scritto: «*Nam et ipsa scientia potestas est*». La versione corrente della frase («*Scientia potentia est*») è secondo taluni attribuibile a T. Hobbes, in gioventù segretario di Bacone, che la utilizzò nel suo *De Homine* (1658).

[2] COM(2016) 288 *final*: "*Le piattaforme online e il mercato unico digitale – Opportunità e sfide per l'Europa*".

effettiva delle norme è fondamentale e […] richiede una buona cooperazione tra le autorità competenti»; cruciale, nell'opinione della Commissione, è dunque «la capacità delle autorità pubbliche di rispondere efficacemente ai nuovi *modelli aziendali e ad eventuali sviluppi tecnologici e di mercato destabilizzanti*», anche mediante «*l'analisi dei big data*».

In questa prospettiva, una compiuta disamina del fenomeno dei *Big data* e del ruolo da essi svolto sulle dinamiche competitive, sull'innovazione e sulla posizione degli utenti finali, tanto sotto il profilo dell'accesso a beni e servizi di consumo, a informazioni e notizie rilevanti, quanto con riferimento alla rilevanza della selettività degli algoritmi nella determinazione delle scelte, appare fondamentale, anche al fine di individuare i più efficaci strumenti di tutela nei mercati e nei settori di competenza, *in primis* quello bancario/finanziario.

Il fenomeno dei *Big data* sta assumendo, anche dal punto di vista prettamente giuridico, un rilievo sempre più marcato, sotto molteplici aspetti: dalla disciplina antitrust alla tutela dei consumatori, dal diritto d'autore alla tutela della riservatezza dei dati, con riguardo alla quale sta peraltro sorgendo un profilo collettivo mai emerso in precedenza.

Invero, il valore delle informazioni raccolte *online* non risiede più solo nel suo scopo primario, ossia nell'uso per finalità commerciali dei dati personali, ma altresì nell'utilizzo secondario, per la cui realizzazione la prestazione del consenso esplicito (liberamente espresso dagli utenti) potrebbe non essere più sufficiente a garantire il rispetto della *privacy*.

Alla luce di tali preliminari considerazioni, la necessità di conciliare il *trade-off* tra il valore commerciale dell'informazione e il rispetto di diritti individuali e collettivi fondamentali, quali la *privacy*, la tutela della concorrenza e le garanzie del pluralismo informativo, rende indispensabile un'analisi trasversale e multidisciplinare del fenomeno dei *Big data*, che tenga conto dell'impatto dello stesso sulla concorrenza (con particolare riguardo al vantaggio competitivo generato dalla disponibilità di dati in via esclusiva), sulla tutela dei consumatori e sulla protezione dei dati personali[3].

2. I Big data *in "3V"*

Letteralmente, *Big data* è una espressione inglese composta dall'aggettivo *big* ('grande') e dal sostantivo *data* ('dati'), che in senso più ampio sottende la

---

[3] Cfr. Autorità per le Garanzie nelle Comunicazioni (Agcom) - *Big data Interim report nell'ambito dell'indagine conoscitiva di cui alla delibera n. 217/17/CONS*, giugno 2018. A tale *Interim report*, redatto nell'ambito dell'indagine conoscitiva avviata il 30 maggio 2017 tra l'Autorità Garante della Concorrenza e del Mercato, l'Agcom e il Garante per la protezione dei dati personali, ha fatto seguito un documento recante le "Linee Guida e raccomandazioni di policy" condivise dalle tre Autorità (luglio 2019).

capacità di estrapolare, analizzare e mettere in relazione una notevole quantità di dati eterogenei, strutturati e non[4].

In letteratura non è tuttavia stata ancora individuata una definizione comunemente accettata di *Big data*[5].

Ai fini del presente contributo appare ad ogni modo condivisibile la definizione offerta dal Vocabolario Treccani, secondo cui per *Big data* si intende un «Ingente insieme di dati digitali che possono essere rapidamente processati da banche dati centralizzate».

Il flusso di dati in cui si muovono i *Big data* attinge la sua portata dalla rapida diffusione di forme nuove di "sorgenti dati": l'utilizzo crescente di Internet, in particolare tramite i dispositivi mobili, è, tra tutte, una sorgente inesauribile. La c.d. *online footprint* viene infatti lasciata in rete in ogni momento: l'uso massivo dei telefoni cellulari per l'effettuazione di operazioni bancarie, la diffusione dell'Internet delle cose (*IoT – Internet of Things*) e di sensori di ogni specie, la navigazione in rete, i dati geografici e di localizzazione prodotti dai *Geographic Information System* (GIS) rappresentano fonti di dati diffuse e tra loro integrate, idonee a tracciare con precisione scientifica una vera e propria "radiografia" dei soggetti da cui detti dati provengono.

Dave Menninger, *Head of Business Development & Strategy* di Greenplum (Divisione DELL-EMC), nell'osservare che «*Il pianeta è diventato un organismo vivente, che comunica continuamente, e Internet ne rappresenta il sistema nervoso*», ha così offerto una suggestiva immagine del fenomeno dei *Big data*.

Oltre che suggestiva, questa immagine appare particolarmente incisiva, se solo si considera che nella rete Internet circolano ogni giorno 2,5 quintilioni di *bytes* di dati, prodotti da fonti diverse: in questo flusso, i *Big data* individuano non solo il volume di dati prodotti, ma anche la velocità di produzione e propagazione e la varietà tipologica degli stessi.

In tale prospettiva è stata proposta una diversa definizione dei *Big data*, che li identifica come «*High volume, high velocity, and/or high variety information assets that require new forms of processing to enable enhanced decision making, insight discovery and process optimization*»[6], così enfatizzando le "3V" che tradizionalmente li connotano, ossia: volume, velocità, varietà.

---

[4] I *Big data* sono dati eterogenei, ossia, alternativamente, dati strutturati, semistrutturati o non strutturati – cioè dati che hanno un formato tale da potere impedire (totalmente o parzialmente) ai database tradizionali di archiviarli ed elaborarli in maniera ordinaria – i quali provengono da fonti molto differenti tra di loro. I *Big data* sono, inoltre, dati prodotti in tempo reale: ciò ne rende ancora più complicata l'archiviazione e la loro elaborazione da parte dei database relazionali tradizionali.

[5] Le diverse definizioni di *Big data* e la loro ambivalenza sono state oggetto dell'interessante contributo di J.S. Ward e A. Barker: *Undefined By Data: A Survey of Big Data Definitions*, School of Computer Science, University of St Andrews, UK, settembre 2012.

[6] *Gartner report*, 2012 - https://www.gartner.com/it-glossary/big-data/.

La teoria delle "3V" dei *Big data* fu originariamente formulata da Douglas Laney[7]: in particolare, il volume fa riferimento alla ingente quantità di dati provenienti da sorgenti differenti; la velocità fa riferimento alla rapidità con cui i dati affluiscono in tempo reale ed alla conseguente necessità di utilizzarli in modo tempestivo; la varietà fa riferimento alla eterogeneità nelle fonti sorgenti dei dati, nei formati con cui vengono acquisite le informazioni (tradizionali/strutturati da un lato, non strutturati dall'altro) e nella rappresentazione e analisi (anche semantica) dei dati immagazzinati.

I *Big data* rappresentano quindi un insieme di dati che per la loro estensione in volume, velocità e varietà consentono di estrarre informazioni aggiuntive sui soggetti da cui provengono, rendendo obsolete le tradizionali tecnologie di conservazione ed elaborazione dei dati medesimi.

Alle tradizionali "3V" dei *Big data* se ne sono aggiunte progressivamente altre: tra queste, la V di "variabilità", che denota il livello di incostanza della produzione dei dati (es: il flusso delle informazioni sui *social network*)[8].

Soprattutto, i *Big data* consentono di estrarre "valore" da enormi quantità di dati, così rivelando informazioni nascoste custodite dai flussi telematici e disvelando elementi utili a partire dall'analisi dei *bytes*. I dati in sé non hanno valore; l'elaborazione di *set* massivi di dati in forma di *Big data* conferisce loro un valore. Da qui, la più importante caratteristica dei *Big data*, ossia la V di "valore".

I *Big data* rappresentano, dunque, un fenomeno dirompente, la cui portata, in termini di cambiamenti economici e sociali, non è ancora ben definita; alle prospettive di crescita si affiancano invero rilevanti perplessità, correlate sia alla tutela della riservatezza e della concorrenza e all'accesso al mercato in genere, sia al rischio di distruzione di mercati, imprese, mestieri e posti di lavoro, rischio che inevitabilmente si accompagna – precedendole – alle esternalità positive connesse al progresso tecnologico e allo sviluppo sociale e culturale[9].

3. Progresso tecnologico, FinTech *e* Big data *nel settore bancario*

La rivoluzione digitale rappresenta un elemento di forte discontinuità per i mercati di beni e servizi, per le transazioni e per i rapporti tra imprese e consumatori/utenti[10].

---

7 D. Laney, *3-D Data Management: Controlling Data Volume, Velocity, and Variety,* gennaio 2001.

8 R. Patgiri e A. Ahmed, *Big Data: The V's of the Game Changer Paradigm*, 2016 IEEE 18th International Conference on High Performance Computing and Communications.

9 Agcom, *Big data Interim report nell'ambito dell'indagine conoscitiva di cui alla delibera n. 217/17/CONS,* cit.

10 Si veda l'intervento di C. Barbagallo, Capo del Dipartimento Vigilanza Bancaria e Finanziaria della Banca d'Italia, presso il Convegno Invernale 2019 – Associazione dei docenti di economia degli intermediari e dei mercati finanziari e finanza d'impresa: *Fintech: Ruolo dell'Autorità di Vigilanza in un mercato che cambia*, Napoli, 8 febbraio 2019.

Attraverso le nuove tecnologie dell'informazione e delle telecomunicazioni, da un lato, gli operatori "tradizionali" del settore creditizio, ricompresi nel perimetro della vigilanza, hanno incrementato la qualità e la quantità dei servizi offerti sviluppando, al contempo, nuove tecniche di gestione dei rischi e una più efficace e sicura gestione dei pagamenti, e, dall'altro, operatori estranei al perimetro della vigilanza, quali le imprese operanti nel settore *FinTech*, hanno potuto offrire servizi (servizi di pagamento, di investimento, di consulenza e di finanziamento) in precedenza esclusivo appannaggio del sistema bancario[11].

Il *FinTech* sta investendo ogni segmento dei mercati dei servizi bancari e finanziari, modificandone finanche la struttura attraverso l'eliminazione delle tradizionali barriere all'ingresso e la conseguente agevolazione dell'accesso al mercato da parte di *start-up* tecnologiche, grazie anche all'abbattimento dei costi fissi d'impresa.

L'innovazione tecnologica è dunque il grimaldello attraverso cui imprese che in passato, in un mercato governato da logiche e regole "tradizionali", non avrebbero avuto possibilità alcuna di affermarsi, assurgono al ruolo di nuovi e aggressivi *players*, scardinando le posizioni dominanti e costringendo gli *incumbents* a investire, a loro volta, nell'innovazione e nel progresso tecnologico e a rinunciare a diritti quesiti, a quote di mercato in precedenza considerate immutabili. Le imprese *FinTech*, in particolare quelle coinvolte nel *BankTech* (che offrono applicazioni e servizi bancari) e nel *RegTech* (che offrono strumenti di regolazione e *compliance*), si basano sulla condivisione e sull'elaborazione di dati personali, utilizzando i dati immessi nel flusso telematico per acquisire una conoscenza approfondita dei clienti attraverso la cronologia delle ricerche, le informazioni e le preferenze condivise sui social media, le abitudini di consumo e di spesa[12].

Le criticità connesse al settore *FinTech* sottendono peraltro questioni connesse non solo alla vigilanza prudenziale, ma anche alla *cybersecurity*, alla tutela dei consumatori/utenti e della riservatezza dei dati.

Ne discende la necessità di riconsiderare il ruolo dei dati e delle relative forme di trattamento e di tutela, esigenza rilevantissima in relazione alla diffusione di nuovi sistemi di raccolta/conservazione/elaborazione di dati personali (cc.dd. *Big data analytics*) e alla rivoluzione digitale che sta investendo il settore bancario e finanziario[13]. Occorre, pertanto, indagare approfonditamente in ordine alle possibili implicazioni negative derivanti da un uso non corretto o non "governato" dei *Big data*.

In questa rinnovata realtà economica, il tradizionale principio della capacità del soggetto di autodeterminarsi mediante il rilascio o il diniego del consenso

---

[11] G. Biferali, *Big data e valutazione del merito creditizio per l'accesso al peer to peer lending*, in *Diritto inf. e inform.*, fasc. 3, giugno 2018, p. 487.

[12] G. Biferali, *op.cit.*, *ibidem*.

[13] A. Ross, *Il nostro futuro*, Milano, 2016.

rispetto alle scelte che riguardano il trattamento dei dati appare ormai obsoleto, e impone di individuare nuove forme di tutela, per la cui identificazione appare imprescindibile prendere le mosse, facendo uso del metodo "induttivo", proprio dalla concreta determinazione dei singoli usi cui i dati si prestano nei rispettivi settori di riferimento[14].

Spesso i nuovi operatori riescono a sfruttare informazioni che i clienti forniscono loro gratuitamente, ottenendo un valore di gran lunga superiore a quello del servizio reso.

Il tema della "profilazione" della clientela, strettamente interconnesso alla tutela dei dati personali, è recentemente giunto all'attenzione del legislatore europeo, che è intervenuto sulla materia con il Regolamento UE 2016/679 (*General Data Protection Regulation* – GDPR)[15], attuato in Italia con il d.lgs. n. 101/2018[16].

Ad esempio, l'art. 22, comma 1, del GDPR stabilisce che «L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona».

Tale disposizione, che pure evidenzia la volontà del legislatore europeo di limitare i rischi derivanti dall'utilizzo incontrollato dei *Big data analytics*, appare, pur nella sua innovatività formale, non del tutto adeguata a raggiungere lo scopo di tutela sostanziale degli interessati, in particolare, come si vedrà, se letta in connessione con le implicazioni derivanti dall'uso dei dispositivi mobili nell'esecuzione di operazioni bancarie[17].

---

[14] La questione era già stata esaminata, con mirabile lungimiranza, da A. Gambaro, *Falsa luce agli occhi del pubblico (False light in the public eye),* in *Rivista di diritto civile*, 1981, I, 84. Nell'affrontare il tema dei danni derivanti dalla divulgazione di informazioni false o "distorte", o comunque impropriamente utilizzate, Gambaro ha evidenziato, in particolare, come la "sinteticità e standardizzazione" tipiche del linguaggio informatico, inidonee a rappresentare adeguatamente la "complessità dei casi della vita", ben si prestino alla diffusione di informazioni poco accurate, in grado di gettare "falsa luce" sugli affari dell'interessato. L'osservazione si attaglia perfettamente ai *Big Data* e ai rischi connessi a un eccessivo affidamento riposto sul contenuto degli stessi, precipuamente nella valutazione del merito creditizio.

[15] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

[16] D. lgs. 10 agosto 2018, n. 101: "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)", in vigore dal 19.9.2018.

[17] Sul punto si rinvia a A. Montelero, *Responsabilità e rischio nel Reg. UE 2016/679*, in *Nuove leggi civ. comm.*, 2017, p. 144 ss.; G. Stanzione, *Il Regolamento europeo sulla privacy: origini e ambito di applicazione*, in *Eur. dir. priv.*, 2016, p. 1252; F. Pizzetti, *La protezione dei dati personali e la sfida dell'intelligenza artificiale*, in Id., *Intelligenza artificiale, protezione dei dati personali e regolazion*e, Torino, 2018, p. 37 ss.

Il fenomeno dei *Big data* ha reso difatti obsoleta la tradizionale distinzione tra "dati personali" e "non", dal momento che risulta estremamente difficile stabilire *ex ante* tra tutte le informazioni raccolte su un individuo cosa rappresenta un dato personale, cosa no. Il riutilizzo dei dati, anche personali, per fini differenti rispetto a quelli per cui sono stati raccolti, l'integrazione delle banche dati e l'elaborazione dei dati contenuti al loro interno, che, di fatto, contribuiscono a rivelare informazioni personali, la tendenza alle profilazioni e categorizzazioni, hanno fatto sostenere che il fenomeno dei big data stia mettendo totalmente in crisi i principi su cui si basa la disciplina europea e statunitense della tutela della riservatezza: nel contesto dei *Big data analytics*, in cui l'originaria definizione della privacy come "*right to be let alone*"[18] è mutata in quella di privacy come diritto di controllare l'uso che altri fanno delle informazioni che ci riguardano o come "*diritto di mantenere il controllo sulle proprie informazioni e di determinare le modalità di costruzione della propria sfera privata*"[19].

Le scelte di un individuo in ordine alla cessione di propri dati al fine di ottenere un servizio si indirizzano a seconda del bilanciamento operato tra benefici, spesso immediati (es. l'accesso a un servizio) e costi (spesso incerti e non conosciuti). In questo contesto, l'asimmetria informativa tra utenti e operatori è pervasiva e strutturale: non solo il consumatore non ha a disposizione tutte le informazioni di cui avrebbe bisogno per prendere una scelta informata, ma molti dei comportamenti, per essere efficienti, presupporrebbero un grado di conoscenza tecnica che va molto al di là delle competenze diffuse tra la popolazione[20].

4. L'evoluzione del quadro normativo europeo in materia di pagamenti digitali

Il *mobile payment* sta attraversando, grazie a una combinazione di fattori quali l'innovazione tecnologica in ambito bancario/finanziario e l'evoluzione del quadro normativo europeo, un periodo di capillare diffusione.

L'ampia rete di accettazione *contactless* italiana (una delle più importanti a livello europeo) e l'uso pervasivo dello *smartphone* rendono l'Italia uno degli Stati con il potenziale più alto in termini di pagamenti da mobile[21].

In questo contesto, l'evoluzione del quadro normativo ha assunto un ruolo determinante nella progressiva affermazione ed espansione dei pagamenti digitali. Negli ultimi anni il sistema europeo dei pagamenti è stato infatti interessato da un'evoluzione senza precedenti, che ne ha plasmato in modo incisivo la fisionomia. Il progresso della tecnologia ha, in particolare, determinato

---

[18] S. Warren e L.D. Brandeis, *The Right to Privacy*, in *Harvard Law Review*, v. 5, n. 5, 1980, p. 193.

[19] S. Rodotà, *Tecnologia e diritti*, Bologna, 1995, p. 122.

[20] Sul tema della obsolescenza delle leggi e delle gravi distorsioni dalla stessa provocate si v. A. Gambaro, *Ancora in tema di falsa luce agli occhi del pubblico*, in *Quadrimestre*, 1988, 301 ss.

[21] Così C. Barbagallo, *Fintech: Ruolo dell'Autorità di Vigilanza in un mercato che cambia*, cit.

l'esigenza di provvedere all'adeguamento del contesto normativo di riferimento anche sulla base dell'accelerazione delle transazioni commerciali e all'aumento della smaterializzazione dei trasferimenti in denaro.

La prima direttiva europea sui servizi di pagamento (Direttiva 2007/64/CE), nota anche come "PSD1" - *Payment services directive*[22], aveva definito un quadro giuridico comunitario rinnovato per i servizi di pagamento elettronici, ponendosi i seguenti obiettivi:

- regolamentare l'accesso al mercato per favorire la concorrenza nella prestazione dei servizi;
- garantire maggiore tutela degli utenti e maggiore trasparenza;
- standardizzare i diritti e gli obblighi nella prestazione e nell'utilizzo dei servizi di pagamento per porre le basi giuridiche per la realizzazione dell'Area unica dei pagamenti in euro (SEPA);
- stimolare l'utilizzo di strumenti elettronici e innovativi di pagamento per ridurre il costo di inefficienti strumenti quali quelli cartacei e il contante[23].

La PSD1 rispondeva all'esigenza di definire e normare un quadro giuridico europeo tale da favorire la creazione di un mercato interno dei servizi di pagamento nell'Unione Europea.

Il 25 novembre 2015 il Consiglio dell'Unione europea ha approvato la direttiva c.d. "PSD2", con lo scopo di consentire pagamenti più sicuri e innovativi[24].

Nel mutato contesto economico e tecnologico, la PSD2 risponde all'esigenza di fornire una risposta concreta non solo all'evoluzione del mercato dei pagamenti, ma anche alle criticità riscontrate nella vigenza del precedente regime delineato dalla PSD1. In particolare, la PSD2 ha dato piena cittadinanza giuridica in Europa a modelli di "*open banking*", basati sulla condivisione di dati bancari tra i diversi operatori dell'ecosistema finanziario.

Con l'obiettivo di evitare rischi di frammentazione della componente più innovativa dei servizi e migliorare la competizione tra soggetti finanziari nuovi e tradizionali, la PSD2 ha per la prima volta aperto i conti bancari all'accesso di non banche. L'idea di base è che l'elemento di maggior valore della filiera produttiva sia costituto dai "dati": la capacità di leggerli in modo orizzontale diventa il vero valore aggiunto dell'economia digitale; il "sistema dei conti

---

[22] La PSD1 è stata recepita nell'ordinamento nazionale con il d. lgs n.11 del 27 gennaio 2010, entrato in vigore il 1° marzo 2010.

[23] Sul passaggio dalla PSD alla PSD2 cfr. anche il contributo di F. Porta in questo *Quaderno*.

[24] Direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio del 25 novembre 2015 relativa ai servizi di pagamento nel mercato interno, che modifica le direttive 2002/65/CE, 2009/110/CE e 2013/36/UE e il regolamento (UE) n. 1093/2010, e abroga la direttiva 2007/64/CE. La "PSD2" è stata recepita in Italia con il d.lgs. n. 218/2017.

di pagamento" assurge al ruolo di "infrastruttura essenziale" *sui generis*, con rilevanti impatti sul sistema di relazioni tra gli operatori.

La PSD2 accelera, quindi, il passaggio al modello "*open banking*" introducendo e disciplinando due nuove tipologie di attori:

1. i *Payment Initiation Service Providers* (PISP), che si frappongono tra il pagatore ed il suo conto di pagamento *on line*, avviando il pagamento a favore di un terzo beneficiario. Il pagatore potrà quindi disporre un pagamento *on line* mediante addebito diretto sul proprio conto corrente;

2. gli *Account Information Service Providers* (AISP), che consentono a chi paga di ottenere, grazie ad una piattaforma unica, un'informativa completa su tutti i propri conti di pagamento, anche se tenuti in diverse banche. Gli AISP tuttavia non potranno utilizzare i dati del cliente o effettuare l'accesso ai relativi conti di pagamento per scopi diversi da quelli previsti dal servizio[25].

Dal punto di vista della tutela dei dati immessi nel sistema, la PSD2 stabilisce che le banche restituiscano la proprietà dei dati ai clienti e garantiscano loro la libera scelta del fornitore di servizi di pagamento, aprendo il mercato a nuovi concorrenti anche non finanziari.

5. Il mobile payment *e i suoi paradigmi*

Per la trasformazione dei pagamenti digitali in mobilità è stata determinante, oltre alla introduzione di un rinnovato quadro normativo a livello europeo, anche l'evoluzione delle tecnologie.

Da questo punto di vista, può ritenersi che il *mobile payment* sia un modello composito che racchiude in sé molteplici paradigmi[26]:

---

[25] Il Regolamento delegato 2018/389 della Commissione Europea del 27 novembre 2017, che integra la direttiva (UE) 2015/2366 (PSD2) per quanto riguarda le norme tecniche per l'autenticazione forte del cliente e gli standard aperti di comunicazione (nel seguito RTS), prevede che tutti i prestatori di servizi di pagamento che detengono conti accessibili *on line* (*Account Servicing Payment Service Providers* o ASPSP) predispongano, entro il 14 settembre 2019, un'interfaccia di accesso per consentire a terze parti (*Third Party Providers* o TPP) di svolgere la propria attività. Tale obbligo è volto a garantire un canale sicuro di autenticazione e comunicazione tra l'ASPSP e il TPP e può essere alternativamente soddisfatto attraverso:
a) la realizzazione *ex novo* di un'interfaccia *on line* dedicata all'accesso dei TPP;
b) l'adattamento di interfacce già disponibili ai clienti per accedere direttamente ai propri conti di pagamento *on line*.
Su questi nuovi servizi cfr. il contributo di V. Profeta in questo *Quaderno*.

[26] Secondo una ricerca dell'Osservatorio *Mobile Payment & Commerce* del Politecnico di Milano, il *Mobile Payment* in Italia vale 6,7 miliardi di euro con tassi di crescita del 60% rispetto all'anno precedente. A trainare la crescita dei pagamenti da mobile è soprattutto la componente *mobile remote commerce* che nel 2017 ha toccato quota 5,8 miliardi di euro. La componente dei pagamenti *mobile* in prossimità ha mosso invece i primi passi concreti negli ultimi anni grazie al lancio in Italia di *Apple Pay* e *Samsung Pay*, servizi di *proximity payment* che sfruttano la tecnologia NFC. Assieme ai pagamenti NFC si stanno sviluppando soluzioni alternative che sfruttano la geolicalizzazione e il *qr code*.

– *Mobile Remote Payment*: servizi che consentono, anche in remoto, di effettuare il pagamento di un bene o servizio attraverso il telefono cellulare. Questi servizi utilizzano la rete wireless, sia essa rete Gsm, Umts o altro e sono fruiti tramite varie piattaforme di interazione: l'invio di un sms, la navigazione su siti *mobile* ottimizzati per il cellulare o applicazioni installate su telefono cellulare o sulla Sim (*Sim Toolkit Application*), la Chiamata a Ivr (risponditore automatico che guida l'utente nell'attivazione del servizio) e l'invio di USSD (*Unstructured Supplementary Service Data*);

– *Mobile Commerce*: servizi che offrono la possibilità di effettuare attraverso il telefono cellulare molteplici attività connesse al processo di acquisto (selezione, acquisto, confronto di prezzi e prodotti, configurazione del prodotto ecc.), oltre al pagamento del prodotto/servizio, con un modello simile a quello dell'*e-commerce* da pc.

– *Mobile Money Transfer*: servizi che consentono il trasferimento di denaro da persona a persona senza che vi sia uno scambio di beni o servizi. Sono spesso legati a trasferimenti tra familiari (ad esempio genitori e figli) o rimesse di denaro da parte di immigrati ai propri congiunti nei paesi d'origine (in questo caso si parla di *Mobile Remittance*). Questi servizi possono utilizzare sia la rete cellulare per trasferimenti a distanza (ad esempio tramite sms o applicazioni) sia tecnologie di prossimità a corto raggio (ad esempio il *Bluetooth*);

– *Mobile Proximity Payment*: pagamenti elettronici "di prossimità", ossia pagamenti per cui è necessaria una vicinanza fisica tra l'acquirente ed il venditore del prodotto/servizio acquistato. Nel *Mobile Proximity Payment* il cellulare emula un pagamento tramite carta. In questo caso non ci si appoggia necessariamente alla rete cellulare (che può però aumentarne l'interattività), ma si fa uso di tecnologie *wireless* di comunicazione.

6. Big data *e modalità innovative di analisi dei dati nel* mobile payment

Dal quadro sino ad ora tracciato risulta con evidenza la stretta interconnessione tra la diffusione dei pagamenti in formato digitale, in particolare mediante la rete mobile, e i molteplici usi cui si prestano in tale ambito i *Big data* raccolti mediante i flussi telematici collegati ai pagamenti.

Con i *Big Data* le banche possono fare offerte personalizzate ai propri clienti grazie ad una migliore profilazione e conoscenza delle loro esigenze, preferenze e abitudini di consumo, individuare frodi tramite *alert* sui sistemi di pagamento come le carte di credito e debito e sulle apparecchiature Atm, creare un miglior profilo di rischio di credito del proprio cliente, effettuare previsioni sui trend dei consumi, ridurre le inefficienze e favorire l'interazione banca-cliente nella creazione di nuovi prodotti/servizi, quali il *crowdfunding* e il *peer to peer lending*.

Il controllo sistematico dei dati relativi alle transazioni, unito all'azione di algoritmi atti a individuare comportamenti sospetti nelle operazioni di pagamento,

nel prelevamento di contanti o nella negoziazione di titoli, potrebbero inoltre integrare i processi di *compliance* degli istituti di credito riducendo, altresì, il rischio di riciclaggio e di altri atti illeciti.

L'analisi dei *Big Data* parte dall'incrocio e valorizzazione sia di dati interni strutturati provenienti dalle transazioni delle carte di pagamento, dagli investimenti finanziari e immobiliari, dall'anagrafica generale interna della banca, dall' elenco fidi e affidamenti attuali e storici, da dati esterni tradizionalmente utilizzati dalle banche come Crif ed Experian, sia di dati non strutturati.

Oltre alla possibilità di personalizzare le campagne marketing, con i *Big Data* è altresì possibile realizzare modelli di rischio e investimento bancario.

Sono stati individuati, in particolare, cinque principali casi di analisi dei Big data utilizzati in ambito bancario in generale e, in particolare, in relazione ai *mobile payments*:

1. ***Sentiment Analytics***

   Il *Sentiment Analytics* si pone come obiettivo la comprensione del *sentiment* degli utenti verso prodotti e servizi tramite l'analisi dei commenti *on line* effettuata tramite algoritmi di *text analytics*. Trattasi di dati non strutturati e dinamici, oggetto di un flusso che si genera costantemente, utili anche per un controllo a lungo termine.

2. ***Customer insight***

   Questo metodo si pone l'obiettivo di definire il profilo del cliente per elaborare campagne di marketing più incisive, vendite targettizzate e miglior *customer service* tramite reti neurali o *decision trees*. In tal modo è possibile acquisire una visione a 360° del cliente tipo e arrivare a prevederne le scelte mediante lo studio delle abitudini e dei comportamenti. Il principale uso di questi dati è per il marketing: questo tipo di risorsa offre le informazioni demografiche essenziali e altri dati utili a creare messaggi efficaci.

3. ***Customer Segmentation***

   Il primo obiettivo che si pone la segmentazione del consumatore è quello di costituire cluster coerenti con la costruzione di programmi di marketing mirati. Inoltre, permette di ottimizzare la strategia di prezzo e di costruire relazioni consolidate con i clienti.

4. ***Next Best Offer***

   La *Next Best Offer* permette di aumentare le opportunità di vendita facendo previsioni sui prossimi acquisti di un cliente, aumentando la fedeltà della clientela e il *cross selling*. I dati dell'utente consentono di capire in che momento della sua vita il cliente si trova e ottimizzare le tempistiche per eventuali campagne marketing da comunicargli.

5. *Channel Journey*

Tracciare la *Customer Journey* in un momento in cui esistono numerosi canali con cui un cliente può interagire può essere facilitato dall'utilizzo dei *Big Data*, che permettono una visione olistica dell'intero processo e delle esperienze associate ai singoli canali. Si delinea in tal modo una visione generale delle esperienze dell'utente bancario.

7. Big data *e* mobile payment: *questioni di merito creditizio e prezzi*

Le strategie di regolazione a tutela della clientela bancaria e finanziaria a livello europeo stanno attraversando una fase di significativi mutamenti: invero – accanto al paradigma della mera trasparenza e correttezza sostanziale – si pone ora l'obiettivo di stabilire una stretta interconnessione tra normativa a tutela della clientela e sana e prudente gestione.

Le questioni relative al comportamento tenuto dagli intermediari finanziari verso i propri clienti non sono più circoscritte al limitato ambito settoriale riguardante la protezione della clientela, ma vengono collocate in una prospettiva più ampia, afferendo precipuamente, in un'ottica prudenziale, alla stabilità finanziaria e all'integrità complessiva del sistema. La globalizzazione finanziaria e l'integrazione dei mercati hanno infatti evidenziato che le condotte scorrette degli intermediari nei confronti dei propri clienti si riverberano non solo sul piano del rapporto negoziale tra cliente e intermediario (*retail conduct failure*), ma possono altresì minare la fiducia nel mercato e, conseguentemente, mettere a repentaglio la stabilità e l'integrità del sistema nel suo complesso (*market conduct failure*).

Il contemperamento tra obiettivi di integrità ed efficienza del sistema bancario e finanziario, da un lato, e istanze dirette a incrementare i livelli di protezione del pubblico dei risparmiatori e degli investitori, dall'altro lato, va peraltro inserito nel complesso mosaico normativo e regolatorio che attualmente disciplina i mercati finanziari.

Muovendo dal paradigma della centralità della tutela della clientela nel sistema di regolazione e di vigilanza bancaria e finanziaria, il legislatore e i *regulators* stanno pertanto adottando, in tale mutato contesto, una prospettiva più ampia e "sistemica" nella individuazione delle misure più adeguate ad assicurare una efficace protezione del consumatore. Il fondamentale postulato della trasparenza e correttezza contrattuale diviene così punto di partenza, e non punto d'arrivo, apparendo ormai imprescindibile l'interdipendenza tra le questioni afferenti al comportamento tenuto dagli intermediari bancari e finanziari nei confronti dei propri clienti e gli obiettivi di stabilità finanziaria e di integrità complessiva del sistema, e, dunque la necessità di introdurre regole ispirate alla interconnessione tra tutela della clientela e sana e prudente gestione.

Esattamente in questa linea si spiega il crescente interesse anche per il processo di "produzione" e di "distribuzione" dei contratti bancari-finanziari-assicurativi allo scopo di pervenire ad una limitazione del c.d. *conduct risk*[27].

I *rating* di credito e le offerte personalizzate sono due esempi del modo in cui la tecnologia dei *Big Data* potrebbe incrementare la competitività nel settore bancario.

La valutazione del merito creditizio è uno dei servizi offerti dai gestori delle piattaforme digitali sulla base dei *Big Data* e viene effettuata prendendo in considerazione un'ampia gamma di informazioni considerate idonee alla determinazione del *credit scoring*[28].

In proposito una parte della dottrina[29] ritiene che il dovere di valutazione del merito creditizio sia un corollario dell'obbligo di astenersi dall'assunzione di decisioni arbitrarie e immotivate, finalizzato ad inibire al finanziatore di concedere credito ogni qualvolta emerga una scarsa capacità del consumatore di adempiere all'obbligo di restituzione della somma mutuata.

Secondo tale interpretazione, l'obbligo di verifica della solvibilità del debitore sarebbe espressione del più generale principio del dovere di sana e prudente gestione sancito dall'art. 5 t.u.b.

La valutazione del merito creditizio effettuata sulla base dei *Big data* sarebbe dunque, in questa prospettiva, non solo legittima ma anzi auspicabile, ferma restando la necessità di effettuare un contemperamento tra l'interesse degli utenti ad evitare pregiudizi o valutazioni negative sulla propria solvibilità che possono

---

[27] Allo scopo di rafforzare la tutela dei clienti e ridurre il c.d. *conduct risk*, il legislatore e i regolatori europei hanno integrato la tradizionale produzione normativa incentrata sulla trasparenza e correttezza contrattuale con regole e misure volte a disciplinare il processo di strutturazione del prodotto/servizio (*product design*) e la successiva definizione delle modalità distributive e di vendita (*product governance*). La *Product Oversight and Governance* mira ad assicurare l'adeguatezza del prodotto bancario-finanziario-assicurativo rispetto alle caratteristiche e alle esigenze del target di clientela cui lo stesso è rivolto, mediante l'adozione, l'implementazione e la revisione da parte delle imprese di procedimenti diretti ad assicurare che gli interessi, gli obiettivi e le caratteristiche dei destinatari dei prodotti siano sempre tenuti in considerazione, così evitando, altresì, potenziali pregiudizi e minimizzando il rischio di conflitti d'interesse.

[28] BCE, *Guide to assessments of fintech credit instistution license applications*, settembre 2017, 4.1, p. 9.

[29] A. Mirone, *L'evoluzione della disciplina sulla trasparenza bancaria in tempo di crisi: istruzioni di vigilanza, credito al consumo, commissioni di massimo scoperto*, in *Banca borsa tit. cred.*, 2010, 1, p. 592-593; M. Gorgoni, *Spigolature su luci (poche) e ombre (molte) della nuova disciplina dei contratti di credito ai consumatori*, in *Resp. civ. prev.*, 2011, p. 765; M. De Poli, *Gli obblighi gravanti sui «creditori» nella fase anteriore e posteriore alla stipulazione del contratto e le conseguenze della loro violazione*, in *La nuova disciplina europea del credito al consumo*, a cura di G. De Cristofaro, Torino, 2009, p. 70; S. Pellegrino, *Le disposizioni attuative in materia di credito al consumo*, in *Obbl. contr.*, 2011, p. 298; G. Biferali, *Il credito ai consumatori*, in *Concorrenza, mercato e diritto dei consumatori*, diretto da G. Cassano, A. Catricalà, R. Clarizia, Milano, 2018, p. 1857. Sul punto cfr. anche F. Sartori, *Disciplina dell'impresa e statuto contrattuale: il criterio della «sana e prudente gestione»*, in *Banca borsa tit. cred.*, 2017, I, 152; A. Dolmetta, *Trasparenza dei prodotti bancari, Regole*, Bologna, 2013.

eventualmente derivare dall'utilizzo dei *Big data* e l'interesse dei prestatori ad una valutazione prudenziale del merito creditizio.

L'uso dei *Big data* nella valutazione del merito creditizio impone peraltro di distinguere, anche riguardo ad eventuali responsabilità, due diverse questioni: quella della legittimità delle modalità di utilizzo delle informazioni reperite e quella della legittimità delle indagini e delle ricerche svolte per reperirle.

La prima questione si incentra sull'esigenza di un utilizzo corretto, non pregiudizievole e non discriminatorio e sull'esigenza di trasparenza riguardo alle modalità di tale utilizzazione. Il gestore della piattaforma dovrebbe dunque attenersi a obblighi informativi volti a garantire la conoscenza delle tecniche adottate per il reperimento dei dati e dei criteri secondo cui tali dati vengono considerati rilevanti per la valutazione del merito di credito[30]. Il "costo" derivante dal rispetto di tali obblighi potrebbe comunque essere compensato e sopravanzato dai "benefici" che la trasparenza è in grado di determinare in termini di fiducia degli utenti e affidabilità dei servizi, anche sul piano concorrenziale.

La seconda questione prende le mosse dalla consapevolezza che l'eventuale violazione di norme a tutela della privacy è compiuta, oltre che dal soggetto (il gestore della piattaforma) che usa le informazioni disponibili grazie ad internet, anche dal soggetto che permette che queste ultime siano reperibili da chiunque ne abbia interesse e che le utilizza come fonte ulteriore di ricavi tramite la rivendita.

Tra le criticità connesse all'uso dei *Big data* nel settore creditizio vi è anche la discriminazione dei prezzi derivante da offerte personalizzate formulate all'esito del processo di profilazione degli utenti in base ai loro gusti, bisogni e propensioni di spesa[31].

La discriminazione di prezzo consente all'impresa di offrire lo stesso bene o servizio a prezzi differenti (discriminazione nel prezzo) a seconda della disponibilità a pagare dei singoli consumatori (o prezzo di riserva), così come individuata dagli operatori tramite tecniche di *Big data analytics*.

L'enorme disponibilità di dati individuali connessa all'avvento dei *Big data* sta rendendo sempre più evidente la possibilità per gli operatori *on line* di attuare

---

[30] E. Prosperetti, *Algoritmi dei Big Data: temi regolamentari, responsabilità, concorrenza, in Informazione e big data tra innovazione e concorrenza*, a cura di V. Falce, G. Ghidini, G. Olivieri, Milano, 2018.

[31] Si veda M. Maggiolino, *Big data e prezzi personalizzati*, in *Concorrenza e mercato*, fasc.1, gennaio 2016, p. 95; F. Vessia, *Big data: dai vantaggi competitivi alle pratiche abusive*, in *Giur. comm.*, 2018, I, p. 1064.

strategie di perfetta discriminazione di prezzo. Sia la dottrina[32] sia le Autorità[33] hanno peraltro evidenziato una certa ambivalenza degli effetti, al contempo positivi e negativi, prodotti dalle offerte personalizzate. In linea generale, le strategie di discriminazione del prezzo sono considerate come un fenomeno in grado di accrescere, o comunque non diminuire, il benessere sociale. Sul versante della domanda, in senso pro-concorrenziale viene riscontrata la tendenza all'aumento ed alla massimizzazione del benessere generale dei consumatori (*consumer welfare*), intesi nella loro totalità (*social welfare*), nonché una maggiore rivalità tra le imprese; in senso anti-concorrenziale si registra una perdita di benessere individuale per alcuni consumatori (quelli disposti a pagare prezzi più alti per avere determinati beni) a fronte del risparmio di spesa riservato soltanto ad alcuni consumatori (quelli disposti a pagare prezzi più bassi per fruire di determinati beni).

Appare evidente che anche la discriminazione dei prezzi operata «all'insaputa» del consumatore è giudicabile come una pratica carente di trasparenza e contraria alla correttezza professionale, poiché attiene ad un elemento essenziale (il prezzo del prodotto) capace di ledere la libertà di scelta del consumatore, ossia di incidere sulle sue scelte di consumo[34].

Infine, è utile evidenziare anche l'esistenza di alcune criticità legate ai costi sostenuti dalle imprese per porre in essere la discriminazione di prezzo, dal momento che simili strategie necessitano di allocare risorse che altrimenti sarebbero destinate ad altre attività.

In conclusione, può ritenersi che la "rivoluzione digitale" in atto imponga di mettere in discussione i paradigmi giuridici che finora hanno guidato la disciplina dei diversi fenomeni connessi all'uso dei *Big data* nel settore bancario e, in specie, in relazione al *mobile payment* per stabilire nuovi riferimenti e nuovi paradigmi.

In questo contesto, le autorità pubbliche sono chiamate a svolgere un'attenta analisi dei fenomeni in atto per identificare iniziative e interventi che

---

[32] Cfr. M. Armstrong, *Price Discrimination*, in www.else.econ.ucl.ac.uk, 6 ss.; M. Libertini, *Concorrenza*, in *Enc. dir., Annali III*, Milano, Giuffrè, 2010, 191 ss.; G. Colangelo, *Big data, piattaforme digitali e antitrust*, in *Merc. conc. reg.*, 3/2016, pp. 429-430.

[33] Si vedano i seguenti Report: *Big data and differential pricing*, by *The Executive Office of the President of the US*, February 2015, disponibile su http://obamawhitehouse.archive.gov; *UK Competition & Markets Authority Report (CMA38, June 2015)*, *The commercial use of consumer data*, in www.gov.uk; *Big Risks, Big Opportunities: the Intersection of Big Data and Civil Rights, Latest White House Report on Big Data*, 4th May 2016; *US Federal Trade Commission Report* (January 2016), *Big Data. A tool for Inclusion or Exclusion?*, in www.ftc.gov; Report congiunto *Autorité de la Concurrence* francese e *Bundeskartellamt* tedesco, C*ompetition Law and Data*, May 10, 2016, in www.autoritedelaconcurrence.fr/doc/reportcompetitionlawdatafinal.pdf.

[34] Essenziale è dunque la predisposizione di strumenti di protezione avanzati, idonei a operare sia sotto il versante informativo, sia sotto il versante delle regole di condotta. Sul punto si rinvia a R. Natoli, *Il contratto "adeguato". La protezione del cliente nei servizi di credito, di investimento e di assicurazione*, Milano, 2012.

salvaguardino l'interesse pubblico garantendo in tal modo un adeguato equilibrio tra opportunità e rischi del processo innovativo[35].

È, peraltro, evidente che gli interventi delle autorità di vigilanza, in Italia e all'estero, non possono travalicare l'attuale cornice regolamentare e normativa, che ad oggi, pur in continua evoluzione, si mostra ancora non del tutto adatta a cogliere le problematiche poste in luce dal progressivo sviluppo di questo fenomeno.

Un approccio innovativo alla regolazione non sembra peraltro poter prescindere dal fondamentale principio di cooperazione: cruciale appare, in questo senso, un'interazione sinergica tra le istituzioni coinvolte, che consenta di elaborare una visione comune.

I dati, perciò, devono essere considerati non più come semplici numeri ma come un *asset* fondamentale sia dal punto di vista degli operatori, sia dal punto di vista degli utenti, sia da quello, soprattutto, del legislatore e delle autorità di settore.

---

[35] Notevoli sono i rischi connessi, tra l'altro, all'abusiva concessione del credito derivante da errore nell'algoritmo: sarebbe pertanto auspicabile la predisposizione di forme di controllo dei modelli di analisi utilizzati, nell'ambito del mandato delle autorità di vigilanza.

Finalità, funzionamento e tipologia di utilizzi delle Blockchain

Roberto Garavaglia

1. Introduzione

Il compito che mi è stato affidato consiste nello spiegare cosa sia la *Blockchain*, consentendo al lettore di capire perché essa rappresenti una delle più straordinarie tecnologie innovative degli ultimi anni.

Occorre prendere le mosse da ciò che Satoshi Nakamoto[1] – per primo – ha ipotizzato, ossia come possa un pensiero economico tradizionale declinarsi tramite l'impiego di tecniche digitali (crittografia, protocolli di trasmissione, marcatura temporale), dando origine a un nuovo concetto di "cripto-economia".

Nel mondo tradizionale esistono gli scambi di informazioni e il trasferimento di beni fisici o competenze, ossia valori che assumono tale significato in quanto scarsi. L'avvento di Internet ha consentito a una pluralità più ampia di accedere e distribuire le informazioni. Grazie alla tecnologia ognuno può intervenire sul dato stesso replicandolo (anche all'infinito) modificandolo e rimettendolo in circolo. Se chiamiamo "*asset*" tale dato digitale (*rectius* l'informazione digitalizzata) ci appare evidente come, in assenza di alcuni accorgimenti, non possa essere considerato unico. Qualora tale *asset* fosse invece crittografato e, come vedremo in seguito, "depositato" su un registro distribuito, potrebbe diventare un ***asset* unico**.

Nel mondo fisico, se passiamo un documento cartaceo a un amico o collega ne perdiamo il possesso. Quel documento è come se uscisse dal "nostro controllo" per entrare "nel controllo di chi lo riceve".

La *Blockchain* consente di "riconquistare" al mondo digitale il concetto di scarsità dei beni del mondo reale e nel momento in cui tramite di essa ci si scambia un *asset* digitale, quel bene non sarà più in alcun modo nella disponibilità di chi lo cede all'altro. Parimenti, se la controparte cui si è trasferito l'*asset* vorrà (o dovrà) a propria volta condividerlo, ne perderà la disponibilità a favore di un altro soggetto. Il dato resterà unico e non sarà possibile duplicarlo.

Per poter eseguire un trasferimento di "valore" (o "valori") via Internet, dunque, era necessario trovare un metodo che rendesse molto difficile vanificare l'immutabilità delle transazioni, che fosse il più possibile immune da un attacco esterno, volto ad alterarne le proprietà, e che potesse garantire tutto ciò anche in assenza di fiducia.

La *Blockchain* è questo: un sistema matematico che ripropone nel digitale il concetto di scarsità, consentendo lo scambio di *asset* immune al rischio di replica, trasparente e tracciabile. In tal senso, si può dire che il trasferimento di questi valori avviene nel rispetto di regole "cripto-economiche".

---

[1] Colui cui si attribuisce la paternità putativa dei *Bitcoin*, uno pseudonimo dietro al quale, ancora oggi, non si è scoperto chi vi sia. A Nakamoto va riconosciuto il pregio di aver progettato la *Blockchain*, quale tecnologia che sottende alla più famosa criptovaluta del mondo; in questo contributo, tale invenzione sarà analizzata sotto il profilo delle opportunità che la stessa permette, di là del suo impiego "a supporto" della criptovaluta medesima.

Attese queste premesse, molti considerano la *Blockchain* come la nuova generazione di Internet, o meglio ancora la "Nuova Internet". Io (ma non solo) ritengo che possa rappresentare la Internet del Valore e, su tale assunto, condurrò il lettore nel merito di un'esplorazione che possa permettere a tutti di comprendere i reali benefici di questa tecnologia.

2. DLT, **blockchain…** *o* **Internet of value***?*

In ossequio all'incipit, occorre definire una prima tassonomia tale da consentire la migliore comprensione delle diverse definizioni che, quotidianamente, affollano i media (specialistici e non). L'obiettivo è definire, con ragionevole chiarezza, cosa significhino i termini – e quali siano le differenze tra i medesimi – ***Distributed Ledger Technology*** (o DLT), ***Blockchain*** e **Internet del Valore** (o IoV).

Con DLT s'intendono tutti quei sistemi digitali, tecnologici, infrastrutturali che consentono di raggiungere un consenso sulle modifiche di un registro distribuito in assenza di un ente centrale datore di fiducia.

Con *Blockchain*[2] ci si riferisce ai protocolli (o tecniche) che caratterizzano alcuni DLT dove il registro è strutturato in blocchi di transazioni validate concatenati gli uni agli altri mediante l'impiego di tecniche crittografiche.

Con IoV, infine, si vuole assumere un concetto più ampio (che ricomprende i primi due) di rete digitale di nodi che si trasferiscono valore (o, meglio, "valori"), **anche** in assenza di fiducia, attraverso un sistema di algoritmi e regole crittografiche che permette di raggiungere il consenso sulle modifiche di un registro distribuito, tenendo traccia dei trasferimenti di valore tramite *asset* digitali univoci.

3. La **Blockchain** *in quattro parole*

Chiarite le prime definizioni, procediamo con una semplice disamina della tecnologia *Blockchain*, precisando subito che, quanto descritto, è essenzialmente riferito a una particolare tipologia di DLT, ossia quella che prevede l'accesso al registro in modalità "***permissionless***". Successivamente, si entrerà in un maggiore dettaglio al fine di evincere talune caratteristiche distintive delle DLT che permetteranno di declinare l'ulteriore macrocategoria "***permissioned***" e le modalità (**private**, **ibride** e **pubbliche**) con cui è possibile prevederne l'utilizzo.

---

[2] Con il termine "*Blockchain*" (quando l'iniziale è maiuscola) ci si riferisce alla tecnologia che supporta i *Bitcoin*, mentre con il termine "*blockchain*" (con l'iniziale in minuscolo) si intende l'architettura tecnologica posta alla base di altri sistemi dove il *criptoasset* non è necessariamente il *Bitcoin*. Convenzionalmente il termine "*Bitcoin*" è utilizzato con l'iniziale maiuscola quando ci si vuole riferire alla tecnologia e al protocollo di rete (ossia alla *Blockchain*), mentre l'iniziale minuscola ("*bitcoin*") è impiegata se ci vuole riferire alla criptovaluta in sé.

Blockchain è una tecnologia che consente a persone (o entità) diverse, che potrebbero fra di loro – anche – non conoscersi, di verificare e validare il succedersi di transazioni memorizzate su un registro condiviso di eventi, chiamato altresì "Libro Mastro Digitale Distribuito" o, più semplicemente, "***Distributed Ledger***".

Il registro condiviso è distribuito fra tutti i partecipanti che operano sulla rete tramite dei "**nodi**" mettendo a disposizione risorse di calcolo. Tali risorse permettono di verificare e validare le transazioni, evitando il ricorso ad un intermediario terzo e consentendo di pervenire a un "consenso distribuito".

I partecipanti che concorrono a validare le transazioni sul *Distributed Ledger* sono chiamati "***Miners***" (o semplicemente "**validatori**") ed il loro lavoro viene **remunerato** tramite l'emissione di nuova moneta (nuova criptovaluta). Tale aspetto, tuttavia, è tipico (come vedremo) solo delle DLT "*permissionless*" dove esiste un *asset* nativo (p.es. il *Bitcoin*).

4. La verifica e la validazione delle transazioni sulla Blockchain

Quando un'entità che ha accesso al *Distributed Ledger* richiede di effettuare una transazione, la scrittura viene propagata sulla rete che ne **verifica la legittimità**, inserendola in un "**blocco di transazioni**" in attesa di validazione.

Tale processo, cui si attribuisce il nome di "**processo di verifica indipendente**", precede quello di validazione effettiva che si avrà con il *mining* del blocco ed è eseguito da ciascun singolo nodo, senza ancora preoccuparsi di cosa stiano facendo nello stesso istante (o staranno per fare nell'immediato) e magari sulle medesime transazioni, gli altri nodi. In questa fase ciascun nodo non si preoccupa di raggiungere quel consenso distribuito che avverrà successivamente con la validazione del blocco nel quale risulteranno inserite le transazioni verificate.

Ogni transazione sulla *Blockchain* viene rappresentata dalla propria storia (ossia la storia dei saldi associati a ciascuna entità) e in tal modo qualsiasi nodo che accede al *Distributed Ledger* è in grado di verificare se l'entità mittente che ha avviato la transazione è realmente nella disponibilità degli *asset* unici che sta trasferendo al destinatario. Inoltre, come si avrà modo di spiegare più avanti quando si parlerà di chiavi crittografiche e firme digitali, il processo di verifica indipendente avviene tramite la verifica dell'autenticità di ciascuna transazione[3].

I nodi aggiorneranno la propria copia di registro solo con il nuovo blocco validato da un *Miner*, a seguito di un processo che conduce all'ottenimento di una fiducia complessiva. La ratifica di tale fiducia viene espressa tramite l'accordo su un **Consenso Distribuito** cui si perviene mediante **l'adozione di regole comuni** e grazie a un **sistema di incentivi** o di **regole di *governance*** accettate da ciascuna entità.

---

[3] È importante osservare che il processo di verifica indipendente, per come si è sin qui descritto, può essere adottato anche su DLT *permissioned*.

5. La costruzione dei blocchi

Quando un nodo riceve una transazione verificata, inizia a "costruire" un blocco, al cui interno includerà tutte le successive transazioni che, con il tempo, si propagheranno sulla *Blockchain*.

In un singolo blocco possono esservi transazioni verificate ma in attesa di conferma, ossia che si trovano all'interno di un blocco che non è ancora stato validato.

In un determinato istante si avrà quindi che sulle "n" copie del registro distribuito, insistono serie di transazioni verificate per le quali tuttavia si attende di convenire su un unico ordine temporale (*rectius* su un'unica "storia" delle transazioni).

6. Il problema del "Double Spending"

Poiché ogni nodo contiene le stesse informazioni degli altri e, in questo modo, conosce tutta la storia delle transazioni avvenute così come tutti gli altri nodi, come si può essere certi che non siano validati blocchi che contengono transazioni mendaci?

Se ci fosse un nodo che, surrettiziamente, provasse (riuscendovi) ad alterare la storia delle transazioni, inserendo una transazione falsa tale da ingenerare un problema circa la "proprietà" (o lo "scambio di proprietà") dell'*asset* scambiato, si correrebbe il rischio del c.d. "***Double Spending***".

Si potrebbe dare che l'*asset* trasferito da un generico mittente a un certo destinatario, di cui quest'ultimo crede di vantare la disponibilità, sia, un istante dopo il trasferimento dal generico mittente, riattribuito ed esso stesso, grazie all'intervento di un nodo che, volontariamente, altera (in questo caso a discapito del destinatario) la storia delle transazioni.

Solo nel momento in cui il destinatario tentasse, a propria volta, di trasferire ad altri l'*asset* che crede nella sua piena disponibilità, si accorgerebbe che è come se non ne fosse mai entrato in possesso (… quindi potrebbe accorgersene anche dopo molto tempo).

7. Il Consenso Distribuito sulla Blockchain

Il processo di validazione sulla *Blockchain* significa "mettere in ordine" le transazioni verificate, ossia convenire su un unico ordine con cui le transazioni sono occorse.

Per evitare l'azione fraudolenta di un nodo in malafede è necessario complicare il processo di validazione. Ogni nodo intenzionato a validare deve

dimostrare di avere risolto anche un **puzzle crittografico associato al blocco di transazioni**. Il cripto-enigma pone in competizione tutti i nodi, per la soluzione del quale ognuno mette a disposizione la propria potenza/capacità di calcolo. Solo il primo nodo che risolve il puzzle avrà diritto di validare l'insieme di transazioni racchiuse in un blocco, presentando la c.d. "***Proof-of-Work***" (ossia la soluzione del puzzle) e ricevendo in cambio una ricompensa in criptovaluta.

Una volta che il nodo validatore ha risolto il puzzle criptografico vincendo contro gli altri, segnala alla rete il proprio blocco validato acciocché gli altri nodi possano verificarne l'effettiva correttezza. La *Proof-of-Work* è tale da poter essere riconosciuta come corretta da tutti in modo molto facile e senza alcun ulteriore dispendio di energia[4].

Una volta che la *Proof-of-Work* presentata dal nodo vincitore viene ricevuta dagli altri nodi, questi possono rapidamente appurarne l'esattezza ed esprimere il loro consenso aggiungendo il blocco validato alla catena ed iniziando a creare il blocco successivo.

La **concatenazione dei blocchi** avviene impiegando l'*Hash* del blocco accettato quale riferimento al blocco precedente

Su una rete *peer-to-peer* di entità che non si conoscono fra di loro e che accedono al *Distributed Ledger* in modalità *permissionless*, questa attività che consente di pervenire ad un **consenso distribuito** sull'ordine con cui sono eseguite le transazioni viene chiamata "***Mining***" e rappresenta un possibile modo per raggiungere quella fiducia che, in assenza di un'autorità centrale, deve essere comunque conseguita, al fine di poter considerare valida la storia delle transazioni sulla *Blockchain*.

8. Definizione di **"asset"***,* **"criptoasset"** *e di* **"token"**

Chiarito cosa sia una *Blockchain*, prima di procedere con un'analisi di dettaglio delle transazioni che avvengono su DLT (con ciò volendo prescindere dal protocollo di *blockchain* testé descritto), vengo ora a proporre alcune definizioni di "*asset*", "*criptoasset*" e "*token*" utili al fine di agevolare il lettore nel prosieguo di questa lettura.

Con "***asset***" (termine già impiegato nei precedenti paragrafi) si può intendere ogni entità materiale o immateriale suscettibile di **valutazione economica soggettiva**; i diritti connessi all'utilizzo e allo sfruttamento delle attività, materiali o immateriali che siano, si possono concentrare **in titoli**

---

[4] Un'analogia che ben s'attaglia a spiegare la *Proof-of-Work* rimanda al famoso cubo di Rubik, un rompicapo piuttosto famoso negli anni '80. Il giocatore, in competizione con altri, impiega tempo e risorse per allineare i colori delle sei facce del cubo; tuttavia, allorché risolto il gioco, la dimostrazione della corretta soluzione è rapidamente accettata da tutti, in quanto ognuno è in grado di accorgersi che le facce sono colorate uniformemente senza particolari sforzi.

finanziari rappresentativi dei diritti stessi. Gli *asset* sono scambiabili su piattaforme di scambio tradizionali.

Con "***criptoasset***" si assume una rappresentazione digitale di valore resa univoca grazie all'impiego di **meccanismi crittografici**; i *criptoasset* possono essere "depositati" su piattaforme DLT rispettando le regole di un **protocollo di *blockchain*** (si parla in questo caso di "*asset* nativi"). I *criptoasset* possono essere **scambiati** su piattaforme DLT rispettando le regole di un protocollo di *blockchain* (anche in questo caso si tratta di "*asset* nativi").

Con "*token*", infine, si può rappresentare una sorta di "**legatura digitale**" della legittimazione di un diritto al titolo rappresento dal *criptoasset*. Il *token* è scambiabile su piattaforme DLT e in una transazione in *token* su DLT la **validità dei negozi giuridici sottostanti** è garantita da un protocollo di *blockchain* (quale quello precedentemente descritto), anche tramite l'impiego di opportuni "***Smart Contract***", per una spiegazione in dettaglio dei quali si rimanda il lettore al successivo § 17.

9. Le chiavi crittografiche

La gestione di una transazione su *blockchain* implica che un'entità possieda due chiavi crittografiche che manterrà al sicuro all'interno di "*wallet*":

- una **chiave pubblica**, con cui riceve *criptoasset* (o *token*);
- una **chiave privata** con cui dispone/spende – o trasferisce verso altri a propria volta – i *criptoasset* (o i *token*) ricevuti.

La chiave pubblica "rappresenta" il recapito verso il quale è possibile trasferire la disponibilità di *criptoasset*. Dalla chiave pubblica di un *wallet* si ricava l'indirizzo. Chiave pubblica e indirizzo del *wallet* non sono la stessa cosa.

La chiave privata **permette** a colui che sottende al recapito suddetto (e solo a lui) di disporre effettivamente della quantità ricevuta. La chiave privata **deve essere custodita in massima sicurezza** per evitare che chi ne entri in possesso possa disporre di quantità non sue. Dalla chiave pubblica non è mai possibile (almeno al livello di avanguardia tecnologica attuale) ricavare la chiave privata.

10. I wallet

La custodia della coppia di chiavi crittografiche avviene con strumenti chiamati comunemente "***wallet***".

In funzione della diversa tecnologia che implementa il *wallet* e dei servizi resi disponibili, si possono avere due macrocategorie alle quali ascrivere differenti servizi di custodia delle chiavi:

- *hot wallet*;
- *cold wallet*.

Un *hot wallet* può essere un software che, messo a disposizione dell'utente, gli consente di riceve e inviare *criptoasset* usando un'applicazione connessa a Internet.

Un *cold wallet* dà solo la possibilità di custodire le chiavi in un luogo sicuro non connesso alla rete (può ad esempio essere un semplice pezzo di carta su cui sono trascritte – spesso sotto forma di *QR code* – le chiavi).

Un *cold wallet* che contiene (anche solo) la chiave privata, potendo non essere connesso telematicamente ad altri sistemi, può essere impiegato solo per ricevere la disponibilità di *criptoasset*, senza tuttavia dare la possibilità di disporne in seguito a proprio piacimento, operazione per la quale è necessario accedere alla rete.

Il generico fornitore di un **servizio *wallet* (ovvero un servizio di custodia delle chiavi crittografiche)** è un **soggetto terzo** che mantiene in luogo sicuro le chiavi di coloro che, **riponendo fiducia in lui**, gli affidano lo strumento mediante cui potrebbe disporre operazioni di trasferimento dei *criptoasset* in custodia.

Tale "custode" assume la denominazione di "***Custodial Wallet provider***" ed è in grado di offrire una notevole semplificazione nella disposizione delle transazioni, oltre a garantire l'impossibilità di perdita delle chiavi stesse,

Per contro, il *Custodial Wallet provider* rappresenta un **punto di debolezza**, laddove, avendo potenzialmente l'abilità di disporre transazioni in *criptoasset* di terzi, può essere esposto ad attacchi informatici, corruttivi, censori e, nel caso di *Hard Fork*[5] potrebbe non essere in grado di restituire la piena disponibilità dei criptoasset di coloro che gli avevano affidato le chiavi.

Esiste anche un'altra tipologia di fornitore di custodia delle chiavi chiamato "***Non-custodial Wallet provider***" che permette, a coloro che ne fruiscono, di avere il **pieno** e **totale controllo** della disponibilità dei propri *criptoasset*. Diverse tipologie di *Non-custodial Wallet provider* possono essere sinteticamente evinte, in funzione della diversa tecnologia impiegata:

- quelle che fanno uso del **web** (le chiavi sono memorizzate nel *browser*);
- quelle che fanno uso di un **dispositivo mobile** come lo *smartphone* o il *tablet*;
- quelle che fanno uso del **PC** (altresì noti come "*Desktop Wallet provider*");
- quelle che fanno uso di un **dispositivo hardware** particolarmente sicuro (un *vault* fisico, ad esempio);

---

[5] Si veda più avanti la definizione di *Hard Fork*.

- quelle che fanno uso di un **semplice foglio di carta** su cui sono impresse entrambe le chiavi pubbliche e private, che sarà cura di chi le avrà stampate riporre in cassaforte.

11. Gli exchange provider

Sono soggetti che **oltre a svolgere l'attività di *Custodial Wallet***, permettono di **ricevere** fondi in **valuta *fiat* o criptovaluta** al fine di attuare una **conversione**, alla pari di ciò che normalmente accade nel mondo fisico e materiale dei cambia-valute.

I cambia-valute "fisici" si limitano a convertire valute a corso legale presentate dal portatore al banco e **non hanno la possibilità di disporre dei portamonete** dei loro clienti, così come i "*Custodial Exchange provider*" potrebbero invece fare.

Anche in questo caso è utile classificare differenti categorie di *exchange provider*: ***Centralized Exchange provider*** e ***Decentralized Exchange provider***.

I *Centralized Exchange provider* sono soggetti che per eseguire una qualsiasi conversione (*fiat*->cripto, cripto->cripto, cripto->*fiat*), trattengono fondi (rappresentati sia da *criptoasset* sia da valuta *fiat*) non "propri", ossia di terzi, di cui possono disporre in qualsiasi istante, ovvero sino a quando l'operazione di conversione viene eseguita; i fondi sono trattenuti su un conto c.d. "***escrow***". Se operano **anche come *Custodial Exchange provider***, **custodiscono** le **chiavi private del *wallet*** di chi chiede la conversione (non possono però disporre in piena autonomia di alcuna operazione per conto di essi). Per quanto attiene le **garanzie** dei fondi sul conto *escrow*, oggigiorno i principali *Centralized Exchange provider* prevedono dei collaterali costituiti da ***asset-backed token* "ancorati" a valute *fiat*** (altresì noti come "*fiat pegged token*") caratterizzate da un tasso di volatilità molto basso o *asset class conservative* (p.es. i *Tether*).

I *Decentralized Exchange provider* sono soggetti che **non trattengono fondi di terzi** e si limitano a (lasciar) gestire in modo totalmente automatizzato – grazie all'impiego di *Smart Contract* – il ***trading*** fra utenti. Possono essere considerati dei ***market place* decentralizzati** che permettono di gestire **l'incontro fra domanda e offerta**, **automaticamente**, mettendo a **garanzia** delle transazioni:

- collaterali costituiti da ***fiat pegged token*** caratterizzati da un tasso di volatilità molto basso;
- particolari **conti *escrow*** basati su sistemi decentralizzati multi-firma.

12. Transazioni su DLT

Siamo giunti al termine di questa prima disamina di dettaglio delle DLT e delle *blockchain* e, acquisiti i primi rudimenti, possiamo finalmente trattare di come avvengono le transazioni mediante l'adozione delle suddette tecnologie.

Effettuare una transazione in *criptoasset*, significa **scambiare** (tra due o più parti) **unità di valore**. Un soggetto "cedente" (o mittente) che vuole trasferire *criptoasset* ad un soggetto "cessionario" (o destinatario), deve creare una transazione firmandola con la propria chiave privata.

Chiunque (nella rete *peer-to-peer*) è in condizione di **verificare l'autenticità della transazione** originata dal pagatore, **usando la chiave pubblica** del medesimo.

Quando un nodo crea una transazione, prima di inviarla agli altri esegue queste procedure:

- crea il *Digest* (la c.d. "impronta digitale) della transazione applicando la funzione di *Hash*[6];
- firma il Digest usando la chiave privata del mittente ottenendo così la firma digitale della transazione;
- aggiunge la chiave pubblica del destinatario.

Quando il destinatario riceverà la transazione, essendo a conoscenza della chiave pubblica del mittente può:

- decifrarne la firma digitale apposta ottenendo il Digest;
- applicare la Funzione di Hash alla transazione e confrontare il risultato con il Digest creato dal mittente;

Se i due valori combaciano significa che quella transazione è integra e autentica.

13. Transazioni in criptoasset

Con transazione in o di (a seconda che si consideri l'accezione rappresentativa in digitale del valore referenziato, piuttosto che il valore stesso) criptoasset s'intende un'azione che comporta (o comporterà) il trasferimento delle disponibilità che ogni entità vanta nel rispetto di una più ampia comunità di soggetti paritari.

Tali soggetti entrano tra loro in **rapporto negoziale** secondo forme di accordo **bilaterale**, ma anche **multilaterale**.

Si osservi come, sulle DLT, **non ci si preoccupa** di mantenere l'oggetto rappresentato dal *criptoasset* – nel proprio valore – al riparo o custodito in cassaforte. L'appartenenza dell'oggetto all'effettivo titolare, così come la sua

---

[6] La funzione di *Hash* è un sistema matematico che consente di convertire un messaggio di lunghezza arbitraria in un messaggio in codice alfanumerico di lunghezza fissa (o prefissata) chiamata *Digest* o Impronta Digitale.

custodia, **sono a carico di chi dimostra di possederlo sulla base di quantità di sicurezza impiegate negli scambi**.

14. La "spendibilità" dei criptoasset *ricevuti con una transazione*

La chiave privata del destinatario che sottende alla chiave pubblica presente nella transazione servirà al medesimo quando vorrà "spendere" la disponibilità di *criptoasset* che gli è stata trasferita dal mittente. Per spendere (ovvero trasferire ad altri destinatari) i *criptoasset* dovrà ripetere lo stesso procedimento.

Se il destinatario non fosse quello che dice di essere, ossia volesse usare la disponibilità trasferita dal mittente non essendo il beneficiario legittimo della transazione, non potrebbe usare la propria chiave privata per firmare la transazione a beneficio di altri destinatari. La disponibilità di *criptoasset* trasferita dal mittente al destinatario è "bloccata" sul vero indirizzo del destinatario consentendo solo all'autentico destinatario di poterla "sbloccare" con la propria chiave privata.

15. Tipologie di DLT

Chiarito cosa siano le DLT, cosa significhi il termine *blockchain*, come avvenga la scrittura delle transazioni sul registro distribuito e in che modo sia possibile pervenire alla sua validazione, si vuole ora scendere in un ulteriore dettaglio classificando le DLT in base alla modalità con cui si accede, si modifica e si valida il registro stesso. Avremo in tal senso due macrocategorie in cui ascrivere le DLT: ***permissionless ledger***, e ***permissioned ledger***.

Vediamo innanzitutto le caratteristiche comuni a entrambe le tipologie, per poi significare le differenze nelle proprie specificità.

Per ambedue le tecnologie esiste un registro distribuito governato da una logica decentralizzata, che tiene traccia di tutte le transazioni. I nodi sono connessi tra di loro in modalità *peer-to-peer* senza un server centrale e le transazioni sono irreversibili (o immutabili).

Nel caso "*permissionless*", non vi è mai una terza parte "*trusted*" e l'accesso al *Distributed Ledger* **non è in alcun modo condizionato**. La validazione delle transazioni viene svolta dai *Miners* che ottengono come ricompensa l'emissione di nuove unità di *criptoasset*. Gli attori che operano su DLT *permissionless* sono pseudonimizzati, rendendo così le transazioni non direttamente riconducibili a persone fisiche. Infatti, mentre si è assolutamente "certi" dell'indirizzo che ha originato la transazione, non è identificabile in modo diretto e altrettanto "certo" la persona fisica che possiede la chiave privata associata a quell'indirizzo.

Nel caso "*permissioned*", vi è una terza parte "*trusted*" incaricata di **governare l'accesso al *Distributed Ledger***. La validazione delle transazioni viene svolta da entità preselezionate e appositamente incaricate che possono venire

ricompensate grazie alla condivisione delle *revenues* originate per l'esercizio in operativo di alcuni servizi "*deployed*" sulla piattaforma *permissioned*[7]. Gli attori che operano su DLT *permissioned* sono, necessariamente, noti, in quanto identificati *ex ante* dalla terza parte "*trusted*".

Alla luce di quanto sin qui espresso, si vuole ora segmentare ulteriormente le DLT, raggruppandole in tre macrocategorie: **pubbliche**, **private**, **ibride** (o **consortili**).

Nelle DLT pubbliche, chiunque può leggere e presentare transazioni sul *Distributed Ledger*, partecipando alla loro verifica e convalida mediante strumenti quali la *Proof-of-Work* descritta in precedenza.

Nelle DLT private, vi è un ente centrale che assegna compiti e ruoli a soggetti noti (ossia identificati a priori) che possono accedere al *Distributed Ledger* scrivendo, leggendo e validando le transazioni. In tale configurazione, i soggetti validatori non devono presentare alcuna *Proof-of-Work*, non avendo bisogno di competere con altri al fine di pervenire a un consenso distribuito, poiché la fiducia di cui essi godono è riconosciuta – da tutti – per "investitura".

Nelle DLT ibride, il solo processo di validazione è attuato da individui o organizzazioni, come ad esempio un consorzio di istituti finanziari, o clienti di un'azienda, preselezionati. La federazione può quindi distribuire il potere e le responsabilità tra i suoi membri secondo **modelli di *governance*** che possono variare in base agli scopi della DLT, in tal modo mitigando la pressoché totale centralizzazione tipica delle DLT private.

Nelle DLT private o ibride vengono adottati sistemi per raggiungere il consenso distribuito diversi da quelli della *Proof-of-Work* della *Blockchain* (con la "B" iniziale maiuscola), generalmente basati su **BFT (*Byzantine Fault Tolerance*)** ispirato alla metafora dei generali bizantini[8].

La metafora è utilizzata nei sistemi informatici distribuiti ogni volta che si ha la necessità di determinare una votazione il cui risultato può essere o vero o falso e quando si rende necessario efficientare il più possibile il lavoro di determinazione del voto stesso. Questo scenario può rappresentare il problema tipico del consenso distribuito su una *Blockchain*, dove si cerca di individuare un protocollo alternativo alla *Proof-of-Work* al fine di risparmiare energia, avendo comunque la certezza di raggiungere un'unica versione di verità verso la quale converge una maggioranza di consensi.

---

[7] Spesso ciò avviene mediante l'attribuzione di *token*.

[8] La metafora dei generali bizantini: ci sono alcuni generali (in numero dispari) dell'Impero Bizantino che stanno accerchiando la città di Roma, ognuno con il proprio esercito. Per espugnare la città i generali devono decidere se attaccare o ritirarsi. La situazione a contorno impone che i generali possano comunicare solo tramite messaggeri e che sia impedito loro di riunirsi; inoltre si è a conoscenza dell'esistenza di alcuni traditori infiltratisi nel gruppo, ma non se ne conosce l'identità e neppure il numero. L'assedio avrà successo se i generali leali riescono a trovare un accordo sulla loro strategia.

Fuor di metafora, il consenso sulla *blockchain* (questa volta con la "b" iniziale in minuscolo) viene raggiunto quando vi è un rapporto tra nodi validatori "in buonafede" e nodi validatori "in malafede" predeterminato, la cui validazione è risolta dall'algoritmo di derivazione BFT.

16. Le caratteristiche chiave delle DLT e delle blockchain

Volendo sintetizzare le caratteristiche chiave delle DLT e delle *blockchain*, sulla base di quanto sin qui esposto, è possibile evincere la seguente elencazione:

- **Decentralizzazione**,
  ossia garanzia di sicurezza e resilienza tramite distribuzione dei dati e dei ruoli fra una pluralità di nodi;

- **Disintermediazione**,
  ossia semplificazione (efficientamento) dei processi eliminando la necessità di alcuni attori;

- **Programmabilità**,
  ossia la possibilità di programmare determinate azioni che vengono eseguite al verificarsi di certe condizioni;

- **Immutabilità**,
  una volta scritti sul *Distributed Ledger*, i dati diventano pressoché impossibili da modificare;

- **Verificabilità**,
  ossia facilità di consultazione e verifica di ciò che è scritto nel *Distributed Ledger*;

- **Accountability**,
  ossia la possibilità di accertarsi di chi (o di cosa) abbia scritto il *Distributed Ledger* e quando ciò sia avvenuto (marcatura temporale);

- **Tracciabilità**,
  ciascun elemento sul *Distributed Ledger* è tracciabile in ogni sua parte e se ne può risalire all'esatta provenienza;

- **Trasparenza**,
  il contenuto del *Distributed Ledger* è trasparente e visibile a tutti i nodi.

17. Gli Smart Contract

Veniamo in questo paragrafo a trattare nello specifico degli "***Smart Contract***" (di cui già si è accennato precedentemente), volendo offrire al lettore un contributo che gli consenta di comprendere quali possano essere i possibili

casi d'impiego delle *blockchain* e (più in generale) delle DLT, di là dell'impiego meramente declinato a supporto delle criptovalute, nonché offrendo alcuni spunti di discussione su talune criticità che, in particolare sotto il profilo giuridico, animano non pochi dibattiti tuttora in corso.

Uno *Smart Contract*[9] è la "traduzione" o "trasposizione" in codice informatico di un contratto, che permette di verificare in automatico l'avverarsi di determinate condizioni e di eseguire, altrettanto automaticamente, azioni (o dare disposizione affinché si possano eseguire determinate azioni) nel momento in cui le condizioni determinate tra le parti siano raggiunte e appurate. Lo *Smart Contract* è basato su una serie di *script* che "leggono" sia le clausole che sono state concordate sia la condizioni operative nelle quali devono verificarsi le condizioni stesse e si auto-esegue nel momento in cui i dati riferiti alle situazioni reali[10] corrispondono ai dati riferiti alle condizioni e alle clausole concordate.

Evoluzione (se così si può dire) dei cc.dd. *Ricardian Contracts*, programmi leggibili sia dalla macchina (in linguaggio informatico) sia dall'uomo (linguaggio naturale), si inseriscono nel solco iniziato a tracciarsi nei primi anni '90 che vuole la realizzazione di software che generino gli effetti di "clausole contrattuali" in modo immutabile dalle "parti", potendosi con ciò definire "vincolanti".

L'esecuzione su *blockchain* degli *Smart Contract* è "garantita" grazie a quelle caratteristiche tipiche riassunte nel precedente paragrafo, consentendo di pervenire a una maggiore (o migliore) certezza delle operazioni (*rectius* degli esiti delle operazioni), in tutti quei contesti dove – essenzialmente – si vuole: prevenire l'azione della corruzione, mitigare il rischio di un *cyber* attacco, amplificare la trasparenza, coinvolgere una pluralità più ampia di soggetti nel rispetto di regole (nuove) di *governance*.

Primo fra i paesi europei, l'Italia, grazie all'intervento del legislatore, con l'art. 8-*ter* del d.l. n. 135/2018[11], come convertito in legge n. 12/2019, ha previsto una definizione di *Smart Contract* riveniente al comma 2:

«*Si definisce "smart contract" un programma per elaboratore che opera su tecnologie basate su registri distribuiti e la cui esecuzione vincola automaticamente due o piu' parti sulla base di effetti predefiniti dalle stesse. Gli smart contract soddisfano il requisito della forma scritta previa identificazione informatica delle parti interessate, attraverso un processo avente i requisiti fissati dall'Agenzia per l'Italia digitale con linee guida da adottare entro*

---

[9] La prima definizione di Smart Contract viene proposta da Nick Szabo nel 1996 come «*Un insieme di promesse, espresse in forma digitale, incluse le regole che le parti vogliono applicarvi*».

[10] Sul significato esteso del termine "reali" si veda anche la spiegazione degli oracoli offerta nel successivo paragrafo.

[11] Il c.d. "Decreto Semplificazioni".

novanta giorni dalla data di entrata in vigore della legge di conversione del presente decreto».

Molti sono i dubbi che, tuttora, insistono nel merito di tale definizione e delle sue conseguenze giuridicamente rilevanti, fra i quali vale rimarcare: possibilità di accertare un vizio di consenso, verifica dell'identità e dell'idoneità delle "parti contraenti", necessità di adeguamento al nuovo modello contrattuale dei principi e delle clausole generali (ad esempio buona fede, diligenza, forza maggiore, caso fortuito), garanzia di una giustiziabilità dello *Smart Contract*, problematiche connesse alle misure a tutela dei consumatori[12].

La natura (eccessivamente) generale ed astratta, nonché la mancata formale riconducibilità delle formulazioni adottate all'interno del Codice dell'amministrazione digitale[13], inducono a interrogarsi circa questo intervento che, di là dal voler essere considerato potenzialmente incauto, necessita di ulteriore chiarimento. La regolamentazione secondaria[14], affidata all'AGID[15], potrà (si auspica) chiarire meglio in termini attuativi. Nell'attesa, è lecito postulare una domanda che, in sé, contiene già taluni indizi risolutivi, chiedendosi se il legislatore abbia realmente voluto creare una nuova figura di contratto o se, attesa l'esistenza (e la validità?) di alcuni strumenti funzionalmente "utili" a concludere ed eseguire automaticamente (ossia senza intervento umano altro o alcuno) un accordo negoziale fra più parti, quali si candiderebbero essere quelli basati su DLT, possa essersi limitato a riconoscerne, *ipso iure*, altrettanta validità.

Appare, infine, utile riflettere sul binomio innovazione tecnologica e mutamento giuridico e, laddove si volesse riconoscere la non necessaria coincidenza, potrebbe rendersi *«(…) preferibile – per chi di regolamentazione delle nuove frontiere high tech voglia occuparsi – concentrarsi sulle ricadute del singolo fenomeno in ordine a specifici aspetti giuridici (ad esempio, i problemi di tutela del consumatore che la diffusione di queste tecnologie – in primis le criptovalute – pongono), evitando le tentazioni di un approccio che, nell'anelito d'intercettare tematiche "disruptive", mette a repentaglio il rigore critico e metodologico della ricerca, esponendola al pericolo concreto di svaporare nel genericismo di una futurologia manierata*»[16].

---

[12] Si veda anche intervista a G. Nava, "*La via italiana alla blockchain sicura (e utile)*", in *Nova24 – Il Sole 24 Ore*, 11 marzo 2019 (https://nova.ilsole24ore.com/nova24-tech/la-via-italiana-alla-blockchain-sicura-e-utile).

[13] Di cui al D.Lgs. n. 82/2005.

[14] La regolamentazione secondaria, al momento in cui si redige questo contributo, non è ancora stata emanata.

[15] Agenzia per l'Italia Digitale.

[16] Come concludono R. Pardolesi e A. Davola, *«Smart contract»: lusinghe ed equivoci dell'innovazione purchessia*, in *Foro Italiano*, 4, V, 2019.

18. Oracoli e digital twins

Gli "**oracoli**" rappresentano un sistema mediante cui una (o più) parti possono contribuire all'interazione fra *Smart Contract* e mondo esterno alla *blockchain*. Le informazioni (ovvero i dati) possono essere avvalorate tramite l'impiego di prove crittografiche o tecniche di *prediction market*.

In altri termini, gli oracoli fanno da ponte tra il **mondo reale** e la ***blockchain*** (possono usare IoT, droni, nanotecnologie), permettendo agli *Smart Contract* di elaborare informazioni "reali" la cui provenienza (o la cui esistenza conseguente a un'occorrenza) nasce in un contesto di realtà fisica.

Precisato il significato del termine oracolo, si vuole ora contribuire ad una migliore contezza cui il lettore potrà pervenire sul significato del termine "***digital twin***", sovente confuso con il primo. A tal proposito, è utile riprendere (estendendola) la definizione di *token* precedentemente data, intendendo ora per *token* una "legatura digitale" della legittimazione di un diritto al titolo rappresentato dal *criptoasset* che consente di **creare un legame tra un bene fisico** (oppure un bene "*off chain*", ossia che sta al di fuori della *blockchain*) **e un *asset* nativo delle *blockchain***; il *token* è scambiabile su piattaforme *Distributed Ledger* e in una transazione in *token* su *Distributed Ledger*, **la validità dei negozi giuridici sottostanti è garantita da un protocollo di *blockchain***, anche tramite l'impiego di opportuni "*Smart Contract*".

Nei processi di "*tokenizzazione*" dei beni fisici, può essere di grande aiuto la tecnica dei cc.dd. "*digital twins*", ovvero delle copie digitali ottenute, ad esempio, tramite l'uso congiunto di *smart objects* in un contesto IoT (*Internet-of-Things*) e certificati digitali.

19. I vantaggi di usare gli Smart Contract

Chiarito cosa siano gli *Smart Contract* e cosa significhino i termini "oracolo" e "*digital twins*", si vuole ora sintetizzare i principali benefici derivanti dall'impiego dei medesimi provvedendo alla seguente breve elencazione:

- **registrazione del contratto su *Digital Ledger*** che rende, nei fatti, immodificabile il contratto stesso;
- **garanzia (tramite crittografia e firma digitale) della effettiva provenienza e destinazione** dei messaggi che costituiscono input e output degli *Smart Contract*;
- possibilità che su un'infrastruttura DLT, soggetti aderenti che non si conoscono tra di loro **possano interagire senza la necessità di un intermediario terzo** datore (e garante) di fiducia;

- aumento del **livello di automazione nei processi industriali**, laddove si riesce a limitare al massimo il coinvolgimento umano esterno (in tutti quei casi in cui fosse necessario), avendo garanzia di una maggiore certezza dell'esecuzione degli automatismi.

20. I principali rischi delle **blockchain**

Il discorso intrapreso non può concludersi senza offrire una rapida disamina dei principali rischi.

In generale è opportuno considerare con attenzione i **partecipanti** alla *blockchain* (utenti, applicazioni esterne, *device* IoT, etc.) e le ***business application*** (sicurezza infrastrutturale, sicurezza applicativa), oltre, ovviamente, a ponderare la scelta della tipologia di DLT (pubblica, privata, ibrida) in funzione delle esigenze e degli obiettivi che si vuole perseguire.

Sul fronte degli *Smart Contract*, attesa l'immutabilità tipica della DLT su cui vengono eseguiti[17], è parimenti necessaria un'efficace attività di *auditing*, tale da poter garantire la correttezza del contratto (competenza legale) e la sua trasposizione in codice interpretabile da una macchina (competenza informatica).

Sulle *blockchain* di tipo *permissionless* nelle quali la *governance* è decentralizzata[18], non essendovi un unico decisore centralizzato in grado di determinare risoluzioni, quando si vogliono cambiare le regole è necessario che la rete stessa sia d'accordo. A tale situazione, talora di compromesso, si perviene mediante la sottomissione di proposte di modifica che saranno votate. Nel corso di tali votazioni è possibile incorrere in particolari situazioni, spesso problematiche, chiamate "***fork***". Il termine anglosassone evoca una biforcazione e, in concreto, ciò che avviene è un autentico "sdoppiamento" della catena di blocchi che, in alcune circostanze, può dar luogo alla creazione di nuove criptovalute[19]. Nei casi in cui si consumano le *Hard fork* emergono alcuni rischi che pongono in pericolo l'affidabilità e l'immutabilità delle transazioni avvenute. Possono infatti manifestarsi i cosiddetti "***replay attack***", azioni perpetrate da soggetti malintenzionati che replicano le transazioni (appena effettuate sulla catena di origine) nella nuova catena.

Un ultimo (non per importanza) aspetto che deve essere preso in considerazione è quello cui gli informatici riferiscono (da sempre) con l'acronimo "**Gi-Go**" (*Garbage In – Garbage Out*). Non si può pensare che

---

[17] Una volta scritto lo *Smart Contract* e lanciato in esecuzione su una DLT non è più possibile rimuoverlo o modificarlo.

[18] Si veda al riguardo anche quanto descritto al § 15.

[19] Le *fork* si suddividono essenzialmente in "*Soft fork*" e "*Hard fork*". Le prime si realizzano dando vita a una versione aggiornata del protocollo compatibile con le versioni precedenti. Le seconde prevedono invece un cambiamento irreversibile obbligando i nodi ad effettuare l'aggiornamento. Uno degli effetti delle *Hard fork* è la creazione di nuove criptovalute.

un *asset* fisico *tokenizzato*, depositato e scambiato su qualsiasi DLT, laddove corrotto (o "sporco") all'origine possa magicamente "pulirsi" (o ripulirsi) grazie alla tecnologia che sottende la DLT stessa.

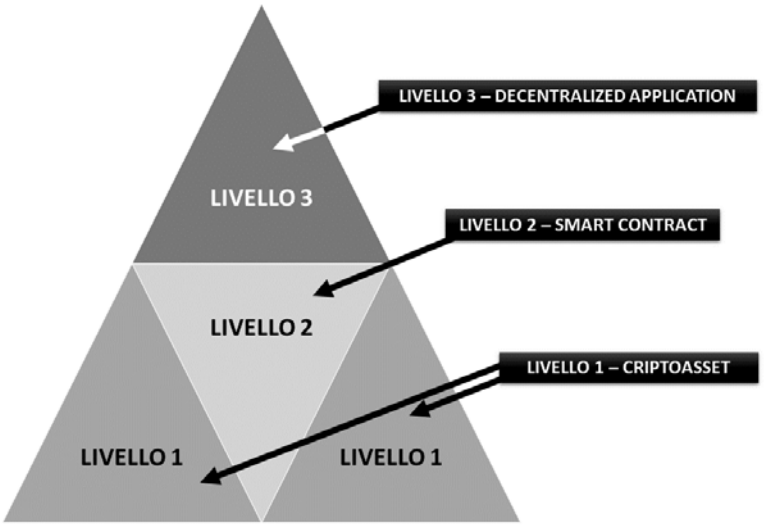
Se si mette su una piattaforma DLT il frutto dell'elaborazione digitale di un'informazione non autentica o impura (quale può essere il dato "*off-chain*"), si corre il rischio di rendere immutabile l'impronta digitale di tale informazione e, cosa assai più grave, di rendere opponibile di fronte a un giudice, qualsiasi transazione commerciale che con tale dato si sia compiuta sulla DLT stessa, adducendo una possibile valenza probatoria che, nei fatti, nulla dice (né potrebbe dire) in merito alla correttezza e completezza dei dati imputati.

Quando si parla di "*legal enforcement*" degli *smart contract*, sarebbe sempre opportuno – prima – chiedersi chi può (deve) garantire la "bontà" di un'occorrenza esterna (un'informazione, un evento che appartengono al mondo fisico) che viene mediata tramite un oracolo mediante l'applicazione di un processo di *digital twin*.

21. L'evoluzione degli utilizzi della **blockchain**

Concludo questo mio contributo condividendo alcuni spunti di riflessione[20] su come l'impiego della *blockchain* (e, in generale, delle DLT) possa rappresentare un'opportunità sotto il profilo di un possibile efficientamento dei processi e di una maggiore relazione con la realtà delle cose e degli umani, non senza prima proporre una semplice raffigurazione architetturale con cui voglio rappresentare l'evoluzione della *blockchain* (Figura 1).

Figura 1: L'evoluzione della *blockchain* (fonte "*Tutto su* Blockchain", R. Garavaglia, Hoepli editore, aprile 2018)



[20] I contenuti esposti in questo paragrafo sono liberamente tratti dal mio libro *Tutto su* Blockchain, Hoepli, 2018.

Sulla base delle peculiarità analizzate in questo contributo possiamo riassumere i benefici nell'adozione di una DLT, in particolare quelli che emergono dal solo livello 1, come al seguito puntualizzati:

1. **sicurezza ottenuta tramite l'impiego di tecniche criptografiche avanzate:** la crittografia che sta alla base delle *blockchain* è un metodo molto efficace per verificare l'identità digitale e permette di aumentare la sicurezza e la protezione dei dati in qualsiasi sistema che ne richieda un impiego affidabile;

2. **immutabilità e irreversibilità**[21] permettono di sviluppare piattaforme di rete sicure dove la trasparenza si rende apprezzabile e nelle quali è possibile consentire un accesso, parimenti trasparente e tracciabile, da parte delle autorità che regolano le norme di settore;

3. **assenza di una terza parte "*trusted*"**; grazie all'implementazione di diversi protocolli di consenso distribuito è possibile avviare transazioni tra soggetti che non devono necessariamente conoscersi e tra i quali non è richiesto un rapporto di fiducia *ex ante*, anche in assenza di intermediari terzi.

A livello 2 della piramide, la capacità offerta dagli *Smart Contract* di eseguire in automatico azioni controllate e validate grazie al supporto del livello 1, di reagire a input anche esterni alla rete e di produrre output che possono avviare azioni altrettanto esterne alla *blockchain*, consente di evincere i seguenti principali benefici nell'adozione di una DLT:

1. **programmabilità della moneta** grazie alla presenza di regole scritte nelle transazioni che vengono eseguite in modo sincrono con la transazione stessa, tramite *Smart Contract*;

2. **impiego di *Smart Contract*** tale da consentire un efficientamento per tutti quei processi che per loro natura richiedono momenti approvativi intermedi consecutivi, nella esecuzione dei quali è fondamentale avere livelli di garanzia elevati e dove la possibilità di integrazione con il mondo esterno delle cose e degli oggetti (IoT *in primis*) si rende necessaria senza il bisogno di un intervento umano;

3. **interazione con il mondo esterno (*off-chain*)** grazie alla gestione di *digital twins* e l'integrazione con gli oracoli.

---

[21] A questo livello 1 è possibile ascrivere le applicazioni più diffuse di "notarizzazione", che, in parole brevi ma efficaci per l'obiettivo che ci si prefigge in questa sede, avvengono tramite la scrittura su *Distributed Ledger* dell'*hash* di un documento informatico "ancorato" a una transazione in *criptoasset* che sarà validata dalla *blockchain*.

Salendo ulteriormente di livello nella piramide di Figura 1, l'opportunità offerte dalle Dapp[22] di eseguire applicazioni anche complesse e la possibilità di organizzarne la gestione in una DAO[23], propone i seguenti benefici:

1. **esecuzione di interi processi** in modo automatico e autonomo con l'affidabilità garantita dalle implementazioni di livello 1 e 2;

2. ***governance* decentralizzata** la cui affidabilità è garantita da un insieme correlato di macchine e di umani che interagiscono autonomamente fra loro nel rispetto di regole comuni, secondo un algoritmo *open source*, in trasparenza e nella consapevolezza di essere parte attiva e integrante del sistema;

3. **efficientamento delle procedure burocratiche** tramite il riuso di *framework* programmati e riduzione del *time-to-market* per nuove iniziative ad alto contenuto tecnologico.

---

[22] *Dapp* è l'acronimo di *Decentralized Application*, ossia un'applicazione decentralizzata sviluppata per creare ed erogare un servizio operato da *Smart Contract* su una *blockchain*. Le *Dapp* possono avere un'interfaccia utente mediante cui è possibile fruire dei servizi.

[23] Le Organizzazioni Autonome Decentralizzate (DAO) sono organizzazioni imprenditoriali che operano come aziende digitali senza personalità giuridica (o – potenzialmente – rappresentabili da "entità logaritmiche"), che agiscono attraverso regole codificate come programmi per computer (*Smart Contract*) eseguiti su una *blockchain*.

Criptovaluta, valuta digitale, moneta elettronica e modelli di circolazione

Francesco Moliterni

1. Una introduzione all'idea di moneta e all'idea di valuta avente corso legale: un confronto con il modello delle "valute virtuali" – 2. Valuta virtuale privata e/o criptovaluta, e moneta elettronica. – 2.1 Moneta reale tradizionale, moneta elettronica e/o valuta virtuale emessa da una banca centrale – 3. Blockchain*: ecosistema e sistema di pagamento fra modello peer to peer e (tentazione del) modello "centralizzato" – 4. Alcune considerazioni conclusive*

1. Una introduzione all'idea di moneta e all'idea di valuta avente corso legale: un confronto con il modello delle "valute virtuali"

Il potere normativo della sostanza delle cose[1] ha avuto[2] ed ha un ruolo strategico nello sviluppo delle regole della "circolazione della moneta" e nella elaborazione della stessa idea di "moneta".

L'ordine seguito nella indicazione della circolazione della moneta, prima, e della moneta stessa, poi, non è il risultato di un casuale errore logico.

Se si tratta di un "ordine inverso"[3] è un ordine inverso consapevolmente così articolato, che vuole evidenziare immediatamente, come nella dimensione della sostanza delle cose o, se si preferisce, della "realtà giuridica effettuale" (ovviamente Tullio Ascarelli[4])[5], la destinazione funzionale alla circolazione è elemento essenziale dell'idea di moneta[6].

A tal fine mi piace muovere ancora[7] dalle parole di Carnelutti rintracciabili nella sua "teoria giuridica della circolazione": «delle merci come del denaro

---

1 Circa la «*natura delle cose come fonte di produzione normativa che si impone, sia, all'organizzazione, sia (…) all'attività*», si veda F. Merusi, *Democrazia e autorità indipendenti*, Bologna, il Mulino, 2000, p. 25 testo e nota n. 25. Sul punto si vedano pure le considerazioni di R. Sacco, *Il diritto muto*, Bologna, il Mulino, 2015, p. 46.

2 Cfr. B. Geva, *The Payment Order of Antiquity and the Middle Ages: a Legal History*, Oxford e Portland, Hart, 2011, p. 17, testo e nota n. 7, che rinvia fra l'altro ad Aristotele, di cui riferisce il pensiero: «*money both facilitates the exchange and acts as measure (…) making things commensurable*»; T. Ascarelli, *La moneta. Considerazioni di diritto privato*, Padova, 1928, p. 5 ss., testo e nota n. 2, si veda in particolare la parte dove si rinvia ad Aristotele; F. A. Mann, *The Legal Aspect of Money*, Oxford, Clarendon Press, 1982, IV ed., p. 3, testo e nota n. 1, e spec. p. 14; come pure nell'ultima edizione curata da C. Proctor (ed.), *Mann on the Legal Aspect of Money*, Oxford, 2012, VII ed., p. 5. Sul rapporto fra "moneta" e "bisogni", si veda Aristotele, *Etica Nicomachea*, Libro V, 8, 1133b, a cura di Marcello Zanatta, Milano, Rizzoli, 2012, XI ed., p. 349. Si vedano pure *ex multis* S. Rossi, *Oro*, Bologna, 2018, p. 77 ss.; P. De Vecchis, voce *Moneta e Carte valori I) Profili generali e diritto privato*, in *Enciclopedia giuridica Treccani*, XXIII, Roma, 2007, p. 6, par. 3.1, e p. 7, par. 4.1; F. Capriglione, voce *Moneta*, in *Enc. dir.*, *Aggiornamento*, III, Milano, 1999, p. 747 e p. 748, testo e nota n. 3; T. Padoa Schioppa, *La moneta e il sistema dei pagamenti*, Bologna, 1992, p. 45. L. Cerenza, *Profilo giuridico del sistema dei pagamenti in Italia*, in *Quaderni di ricerca giuridica della Banca d'Italia,* Roma, 1995. Nella prospettiva del passaggio dalla moneta tradizionale (banconote e monete metalliche) alla moneta digitale, nonché del confronto fra tali due dimensioni della moneta, si veda ancora B. Geva, *Banking in the Digital Age – Who is Afraid of Payment Disintermediation*?, 2018, *All Papers.* 322, p. 3 ss., consultabile al sito www.digitalcommons.osgoode.yorku.ca/cgi/viewcontent.cgi?; in una prospettiva diversa, si veda pure A. Rahmatian, *Electronic Money and Cryptocurrencies (Bitcoin): Suggestions for Definitions*, in *Journal of International Banking Law, and Regulation*, 2019, 3, p. 119.

3 Prendo in prestito l'immagine dell'«ordine inverso» dal premio Nobel R. P. Feynman, *Sei pezzi facili*, Milano, Adelphi, 2000, p. 15.

4 P. Ferro-Luzzi, *Riflessioni sulla riforma: la società per azioni come organizzazione del finanziamento di impresa*, in *Riv. dir. comm.*, 2005, I, p. 680.

5 T. Ascarelli, *Norma e realtà sociale*, in Id., *Problemi giuridici*, I, Milano, 1955, p. 70 ss.; e prima ancora vedi C. Vivante, *Il contratto di assicurazione. Le assicurazioni terrestri*, I, Milano, 1885, p. 1 ss.

6 Cfr. G. Olivieri, *Compensazione e circolazione della moneta nei sistemi di pagamento*, Milano 2002, p. 4 ss.

7 Sul punto sia consentito rinviare pure a F. Moliterni, *I sistemi di pagamento informali fra rimesse di denaro e contratto di rete*, Milano, 2019, p. 173.

il commercio sente il bisogno di evitare il trasporto materiale», che, è (quanto meno) «incomodo»[8], «difficile e costoso»[9].

Ma «*per le merci, a differenza del denaro, in ragione della diversa funzione economica tale possibilità è senza confronto più ristretta: il denaro, infatti, non è destinato ad altro che a circolare* (…); (…) *mentre le merci ad un certo punto devono uscire dal magazzino per entrare, come si dice, nel consumo*»[10].

La moneta, intesa come "bene"[11] destinato alla circolazione, è nozione basata a sua volta sul classico "*functional approach*"[12], ed è in qualche modo sintesi (o risultato) delle funzioni tradizionalmente riconosciute come caratterizzanti la moneta: in particolare (e prima di tutto), quella di unità di misura e/o misura di valore (degli altri beni)[13], "*universal medium of exchange*"[14] o strumento di pagamento ad accettazione generalizzata (sia pure) in *una determinata comunità*, cui consegue la funzione di strumento di conservazione di valore (*store of value*)[15]. Destinata ad assolvere efficacemente a tale(i) funzione(i), è, come noto, l'invenzione della moneta-segno[16], già grazie al conio della moneta metallica[17],

---

8 F. Carnelutti, *Teoria giuridica della circolazione*, Padova,1933, p. 239.

9 T. Ascarelli, *Compensazione privata e cambio traiettizio*, in Id., *Studi giuridici sulla moneta*, Milano, 1952, p. 233. Sul punto si veda pure B. Geva, *The Payment Order of Antiquity*, cit., p. 3.

10 F. Carnelutti, *Teoria giuridica della circolazione*, cit., p. 239; si veda pure A. Arena, *La polizza di carico*, I, Milano, 1951, p. 7, nota n. 9. T. Ascarelli, *Legislazione sulle divise e principi generali delle obbligazioni*, in Id., *Studi giuridici sulla moneta*, cit., p. 233. Cfr. P. De Vecchis, voce *Moneta e carte valori*, cit., p. 3, par. 1.3, in fine. Si tratta a mio parere di considerazioni riconducibili, piuttosto che a categorie storiche, a categorie logiche circolanti nel tempo, come pare ricavarsi fra l'altro dalle riflessioni in materia di moneta, rinvenibili nell'*Etica Nicomachea* di Aristotele, libro V, 8, 1133a 30, cit., p. 349 ss.

11 Con riferimento alle criptovalute, si veda G. Rinaldi, *Approcci normativi e qualificazione giuridica delle criptomonete*, in *Contr. impr.*, 2019, 1, p. 290 ss.

12 Cfr. C. Proctor (ed.), *Mann on the Legal Aspect of Money*, cit., p. 12 ss., spec. par. 1.10; F. A. Mann, *The Legal Aspect of Money*, cit., p. 3 ss.

13 S. Rossi, *Oro*, cit., p. 77 ss.; F. Capriglione, voce *Moneta*, *cit.*, p. 747 e p. 748, testo e nota n. 3; P. De Vecchis, voce *Moneta e Carte valori I) Profili generali e diritto privato*, in *Enciclopedia giuridica Treccani*, XXIII, Roma, 2007, p. 6, par. 3.1, e p. 7, par. 4.1., dove fra l'altro si precisa: «*la moneta normalmente non è oggetto di scambio (salvo per le operazioni di cambio…) ma strumento perché gli scambi avvengano*». Sul punto si veda pure C. Proctor (ed.), *Mann on the Legal Aspect of Money*, cit., p. 34, par. 1.53. Nella prospettiva del contratto di compravendita, con specifico riferimento al "prezzo" come "secondo termine dello scambio", si osserva fra l'altro che «*la prestazione corrispettiva del trasferimento del diritto deve cioè essere rappresentata da un bene assunto in funzione di intermediario degli scambi e soprattutto di misura del valore, qual è tipicamente la funzione della moneta (denaro)*»; si veda P. Greco – G. Cottino, *Della vendita. Art. 1470-1547*, in *Comm. Scialoja-Branca* a cura di Francesco Galgano, Bologna – Roma, 1981, II ed., p. 1.

14 B. Geva, *The Payment Order of Antiquity*, cit., p. 78, 1° cpv.

15 S. Rossi, *Oro*, cit., p. 77 ss. A. Rahmatian, *Electronic Money and Cryptocurrencies (Bitcoin): Suggestions for Definitions*, cit., p. 115.

16 In sostanza circola l'informazione (con specifico riferimento alla "moneta-segno", T. Ascarelli, *Obbligazioni pecuniarie*, in *Comm. Scialoja-Branca*, Bologna – Roma, 1959, p. 12; si vedano pure le considerazioni di B. Geva, *The Payment Order of Antiquity*, cit., p. 38 e spec. p. 39, 2° cpv., e p. 98, 2° cpv.).

17 Tecnica di monetazione adottata fra l'altro già dalle città-stato greche e magno-greche, in particolare da Atene (B. Geva, *The Payment Order of Antiquity*, cit., p. 82, 3° cpv., e p. 83, 2° cpv.) come pure dall'antica Taranto, *Taras*, da Siracusa e da Agrigento (cfr. P. De Vecchis, voce *Moneta e carte valori*, cit., p. 2, par. 1.3).

e la conseguente estrema standardizzazione dei pezzi monetari dello stesso tipo[18], cui conseguono due effetti "miracolosi" strettamente collegati fra loro, l'uno conseguenza dell'altro: la fungibilità di ciascun pezzo monetario rispetto ad un altro dello stesso tipo, e l'estrema standardizzazione dell'"informazione"[19] rappresentata e veicolata dalla moneta medesima[20].

Il rapporto "fattuale"[21] fra moneta e comunità[22] è suggestivamente segnalato da Tullio Ascarelli[23], che avvisa come non sia possibile intendere la moneta slegata dalla comunità dei soggetti che la usano come tale: ossia dall'insieme di persone che la accettano come strumento di pagamento o, per utilizzare le parole della direttiva 2018/843/UE riferite alle "valute virtuali", come "mezzo di scambio" (art. 1, lett. *d* della direttiva 2018/843/UE)[24].

Sul solco del ricordato insegnamento di Tullio Ascarelli, sottolineo ancora come il legame fra moneta e comunità[25] – dove la moneta medesima è accettata come mezzo di pagamento, e prima ancora come misura di valore, e (conseguentemente) strumento di conservazione di valore – sia strategico ai fini della distinta considerazione, e dell'idea di moneta in generale, e della fattispecie di valuta o moneta avente corso legale (art. 1277 c.c.): e quindi, in particolare, ai fini del ragionamento che si vuole svolgere in tema di valuta digitale privata[26].

---

[18] «*The evolution of coined money out of primitive (…) introduction of coins*» (B. Geva, *The Payment Order of Antiquity*, cit, p. 78, 2° e 3° cpv., testo e note nn. 82 e 83).

[19] Per le qualità di "uniformazione e informazione" nella dimensione di "pesi e misure" in generale, A. Gambaro, voce *Pesi e misure*, in *Digesto Disc. Priv. sez. Civ.*, XIII, Torino 1995, si veda p. 540 s. par. 4.

[20] T. Ascarelli, *Obbligazioni pecuniarie*, cit., p. 17. Cfr. C. Proctor (ed.), *Mann on the Legal Aspect of Money*, Oxford, 2012, VII ed., 2012, p. 12 ss., spec. par. 1.10; F. Capriglione, voce *Moneta*, cit., p. 761 ss.

[21] Per il rapporto fra "fattualità economica", (ritorno alla) fattualità del diritto e *lex mercatoria*, si veda P. Grossi, *Ritorno al diritto*, Roma – Bari 2015, p. 26 ss.

[22] La categoria di comunità va ricondotta al concetto di 'insieme' e/o 'complesso umano' inteso come "aggregato" e cioè come «*molteplicità di elementi tra loro collegati in modo da costituire un 'complesso', capace di funzionamento unitario.* [In particolare] *i complessi umani costituiscono degli insiemi in quanto i componenti condividono gli aspetti fondamentali della realtà umana: l'esistenza materiale nella forma della coesistenza; la vita materiale nella modalità della convivenza; la coscienza istintiva nell'atteggiarsi del comune sentire; la coscienza spirituale nella forma creativa della comune cultura*» (A. Falzea, voce *Complessità giuridica*, in *Enc. dir.*, *Annali*, I, 2007, p. 204).

[23] T. Ascarelli, *Obbligazioni pecuniarie*, cit., p. 11.

[24] Cfr. V. De Stasio, *Verso un concetto europeo di moneta legale: valute virtuali, monete complementari e regole di adempimento*, in *Banca, borsa e titoli di credito*, 2018, I, p. 747.

[25] Cfr. F. A. Mann, *The Legal Aspect of Money*, cit., p. 8, 1° cpv.; S. Rossi, *Oro*, cit., p. 90, 1° cpv.

[26] È nella dimensione del rapporto fra "valuta virtuale" o *digital-virtual currency* e comunità dei suoi utenti, e non fra tutti i componenti del genere umano, che va verificato se bitcoin o altra simile valuta virtuale privata "*is not a generally accepted means of payment*" (cfr. A. Rahmatian, *Electronic Money and Cryptocurrencies (Bitcoin)*, cit., p. 119, c. 2, 2° cpv.). e con specific riferimento a bitcoin, va considerate che "*the system of bitcoin is based on scarsity, that is, the 'mining of 'coins' is limited by the algorithm to just 21 million bitcoins. In this regard, it is not dissimilar to commodity money or commodity-backed money based on precious metal*" (cfr. A. Rahmatian, *Electronic Money and Cryptocurrencies (Bitcoin)*, cit., p. 119, c. 1, ult. cpv.; sul punto cfr. M. Mancini, *Valute virtuali e Bitcoin*, in *Analisi Giuridica dell'Economia*, 2015, 1, p. 124). Riguardo a quest'ultimo punto si veda pure S. Rossi, *Oro*, cit., p. 88.

In tale prospettiva, è ancora suggestivo osservare come il rapporto funzionale biunivoco fra moneta e comunità dei suoi utenti sia già rintracciabile nell'idea di moneta di Aristotele che ne accentua la valenza simbiotica, assumendo che non vi è comunità senza scambi, e non vi è scambio (o sistema di scambi) senza moneta[27].

La moneta svolge in sintesi la funzione di "medio"[28] fra tutte le cose, e a tal fine deve appunto essere "*métron*"[29], misura (del valore) di tutte le cose, per *essere* generale mezzo di scambio, capace di soddisfare i "bisogni attuali", come pure quelli futuri[30].

Si tratta di idea, che è davvero "impronta delle cose" (Eco), le cui regole funzionali hanno una continuità nel tempo ed una diffusione nello spazio geografico, che induce a riflettere sulla loro natura di categoria logica piuttosto che categoria storica, e – volendo utilizzare categorie tornate ad essere oggetto di recente riflessione in dottrina – sulla loro appartenenza alle "leggi degli dèi", piuttosto che (solo) alle leggi degli uomini: «*una legge non scritta e immutabile, lo* ius*, di cui è ignota la rivelazione*»[31].

Un diritto da "inventare"[32], come suggerisce Paolo Grossi, da scoprire o riscoprire nella (o dalla) natura profonda (dell'ordine) delle cose e nella loro realtà giuridica effettuale (Tullio Ascarelli).

La dimensione del ragionamento è quella della pluralità degli ordinamenti giuridici "inventata" da Santi Romano[33]con il suo fondamentale libro "l'ordinamento giuridico"[34]: e sia consentito sommessamente osservare come l'uso del singolare nel titolo del libro ne tradisca la affascinante «complessità

---

[27] "(…) *bisogna che tutti i beni siano stimati. In questo modo infatti sarà sempre possibile uno scambio, e se sarà possibile questo, sarà possibile una comunità. Ebbene, la moneta riporta ad un livello di eguaglianza, come misura che rende i beni commensurabili.*" (enfasi mia) (Aristotele, *Etica Nicomachea*, V, 8, 1133b 15, cit., p. 351). Cfr. E. Barcellona, *Ius monetarium. Diritto e moneta alle origini della modernità*, Bologna, il Mulino, 2012, p. 24 ss.

[28] Circa il "*medium* del denaro" ed il suo potere di "domini(o)" verso l'intera società, si vedano le interessanti considerazioni di G. Teubner, *Ibridi e attanti. Attori collettivi ed enti non umani nella società e nel diritto*, trad. a cura di Ludovica Zampino, Milano – Udine, Mimesis, 2015, p. 153 ss.

[29] Aristotele, *Etica Nicomachea*, V, 8, 1133b 15-20, cit., p. 351.

[30] Per il riferito rapporto fra bisogni e moneta, per cui la moneta nasce dal bisogno di soddisfare i bisogni, si veda ancora Aristotele, *Etica Nicomachea*, V, 8, 1133a 25-30, cit., p. 349; S. Rossi, *Oro*, cit., p. 87 ss.

[31] M. Cartabia – L. Violante, *Edipo, Antigone, Creonte: il governo e la giustizia*, in M. Cartabia – L. Violante, "*Giustizia e Mito*", Bologna, 2018, p. 19 ss. T. Ascarelli, *Antigone e Porzia*, in Id., *Problemi giuridici*, I, Milano, Giuffrè, 1959, p. 150 ss.

[32] P. Grossi, *L'invenzione del diritto*, Roma – Bari, Laterza, 2017, p. XV. Cfr. P. Zanelli, *Detipizzazione legale e (ri)costruzione contrattuale*, in *Contratto e impresa*, 2019, 1, p. 19 e p. 22.

[33] Cfr. P. Grossi, *L'invenzione del diritto*, cit., p. 31.

[34] Santi Romano, *L'ordinamento giuridico*, Macerata, Quodlibet, 2018, copia anastatica della 2^ edizione, pubblicata da Sansoni, Firenze, nel 1946.

giuridica»[35] del contenuto, celebrato peraltro da convegni e contributi nel 2018, in occasione del centenario della pubblicazione della prima edizione[36].

L'ordinamento giuridico originato dalla "potestà dello Stato", la "sovranità"[37], non è *solo*.

Insopprimibile è la forza normativa (informale) del «*comportamento collettivo* delle parti di un sistema»[38] sociale complesso (o comunità), quello che Guido Alpa chiama il «potere normativo della collettività»[39] e il conseguente «diritto dei privati»[40]: un ordinamento giuridico (altro da quello statuale)[41], la cui autonomia[42], non inibisce relazioni sinergiche con l'ordinamento giuridico statuale.

Ciò vale anche e forse soprattutto per la moneta (*fatto* sociale e *fatto* giuridico) ed il sistema dei pagamenti.

La moneta privata o la moneta dei privati è tale in quanto una comunità le riconosce le funzioni tradizionali della moneta e, come anticipato, prima di tutto quella di misura di valore di tutti i beni e di "medio" (moneta di conto), e quindi di strumento di pagamento ad accettazione generalizzata nella comunità considerata[43] (moneta di pagamento), nonché quella di riserva di valore.

È evidente, quasi tautologico, che una moneta privata, sia essa reale[44] o digitale[45], non è una moneta avente corso legale in forza della sovranità di uno Stato[46]: quindi, per forza di cose, Bitcoin, che, come noto, è invenzione dei privati, «*legally, (…) does not have the status of legal tender*»[47].

---

35 Cfr. A. Falzea, voce *Complessità giuridica*, in *Enc. Dir.*, *Annali*, I, 2007, *ad vocem.*

36 Cfr. N. Irti, *Per una lettura critica di Santi Romano. Note introduttive*, in "*Diritto pubblico*", 2018, 1, p. 16 ss.

37 Per tutti, si vedano le considerazioni fondamentali di C. Mortati, *Istituzioni di diritto pubblico*, I, 10^ edizione rielaborata ed aggiornata a cura di Franco Modugno, Antonio Baldassarre e Carlo Mezzanotte, Padova, 1991, p. 96 ss., testo e nota n. 1, per un riferimento alla dottrina di Santi Romano sulla pluralità degli ordinamenti giuridici, si veda p. 9, nota n. 1.

38 G. Caldarelli e M. Catanzaro, *Scienza delle reti*, Milano, Egea, 2016, p. 16.

39 G. Alpa, *Potere normativo della collettività*, in *IlSole-24Ore*, inserto *Domenicale*, 25 novembre 2018, p. 25.

40 W. Cesarini Sforza, *Il diritto dei privati*, Macerata, Quodlibet, 2018, copia anastatica dell'edizione de "Il diritto dei privati" ripubblicata nel 1963 da Giuffrè nella collana "Civiltà del diritto".

41 W. Cesarini Sforza, *Il diritto dei privati*, cit., p. 27 ss.

42 In tale prospettiva, si veda pure G. Teubner, *Ibridi ed attanti*, cit., p. 153 ss.

43 Cfr. N. Nardi, *"Criptovalute" e dintorni: alcune considerazioni sulla natura giuridica dei bitcoin*, in *Diritto dell'informazione e dell'informatica*, 2015, 3, p. 446, par. 1.2.

44 S. Rossi, *Oro*, cit., p. 88 ss., e spec. p. 88 ult. cpv.

45 A. Rahmatian, *Electronic Money and Cryptocurrencies (Bitcoin)*, cit., p. 120, c. 1.

46 Cfr. T. PadoaSchioppa, *La moneta e il sistema dei pagamenti*, cit., p. 17 ss.; F. A. Mann, *The Legal Aspect of Money*, cit., p. 14. Con specifico riferimento alle criptovalute private come *bitcoin*, si veda N. Nardi, *"Criptovalute" e dintorni*, cit., p. p. 445.

47 European Central Bank, *Virtual Currency Schemes – A Further Analysis*, February 2015, p. 30, consultabile al sito www.ecb.europa.eu/pub.../virtualcurrencyschemesen.pdf.; G. Rinaldi, *Approcci normativi e qualificazione giuridica delle criptomonete*, cit., p. 269.

Tuttavia, atteso che «*the existence of formal, legal tender status is like wise not a essential part of definition of money*»[48], *bitcoin* è una moneta[49], se *di fatto* svolge in una determinata comunità le funzioni che la caratterizzano come tale: e si torna alla fattualità del diritto. A tal fine non rileva che si tratti di una "*buona* moneta" (moneta stabile) o che sia una "*affidabile* riserva di valore"[50]: gli aggettivi in tal caso sono ultronei e diventano leva per argomenti che proverebbero troppo se si guarda alla storia delle monete aventi corso legale ed alle crisi[51] finanziarie palesate o nascoste dei relativi Stati emittenti.

Come pure, per altro verso, non importa che sia *solo* una moneta in "purezza"[52] e nient'altro, o sia piuttosto suscettibile di essere usata "anche per

---

[48] C. Proctor (ed.), *Mann on the Legal Aspect of Money*, cit., p. 51, par. 1.81.

[49] Cfr. M. F. Campagna, *Criptomonete e obbligazioni pecuniarie*, in *Rivista di diritto civile*, 2019, 1, p. 202 ss.

[50] Cfr. A. Caloni, *Bitcoin: profili civilistici e tutela dell'investitore*, in *Rivista di diritto civile*, 2019, p. 166. Né mi pare utile assumere che *bitcoin* "*is not a normal money*". Sul punto si vedano le considerazioni di M. F. Campagna, *Criptomonete e obbligazioni monetarie*, cit., p. 219, dove fra l'altro si osserva: "*le criptomonete segnano un passaggio* (…)*: cambia la moneta nella sua più intima essenza. A voler cercare una formula di sintesi, si potrebbe dire che la moneta è, in un certo senso almeno, tutt'uno col procedimento telematico*". Allo stato delle mie riflessioni, non sono sicuro del fatto che le criptomonete cambino l'essenza della moneta, se per tale si intende l'"idea" di moneta in senso aristotelico, incentrata sulla definizione delle *funzioni* della moneta rispetto alla comunità dei suoi utenti. Invece, mi pare vero, che la forma monetaria (della valuta) virtuale ed il suo rapporto simbiotico "col procedimento telematico", o meglio con il suo sistema di pagamento, ossia *blockchain*, enfatizzi la destinazione funzionale della moneta alla circolazione – come anticipato, già segnalata fra gli altri da Carnelutti – al fine ultimo di agevolare gli scambi attuali e futuri, anche e soprattutto quelli che intercorrono fra soggetti non compresenti.Mi pare piuttosto utile spostare la riflessione, su come il bisogno di "monete" internazionalmente accettate, soprattutto a fronte della evoluzione ed implementazione del commercio internazionale, abbia evidenziato come la funzione di misura di valore (o unità di conto) abbia una sua fondamentale importanza, autonoma rispetto alla pur speculare funzione di strumento di pagamento o di mezzo di scambio per l'acquisto di beni e servizi, con la conseguente divaricazione dell'idea di moneta di conto e dell'idea di moneta di pagamento di cui è "epitome" il "Diritto Speciale di Prelievo" (*Special Drawning Right*) del Fondo Monetario Internazionale, che come noto è moneta di conto, ma non è moneta di pagamento (con specifico riferimento al "Diritto Speciale di Prelievo come definito dal Fondo Monetario Internazionale" come "unità di conto" e l'art. 4 della Convenzione di Bruxelles sulla polizza di carico, si veda, F. Berlingieri, *Le convenzioni internazionali di diritto marittimo e il codice della navigazione*, Milano, Giuffrè, 2009, p. 136 ss., spec. p. 139 e p. 140). E sul tema sia consentito limitarsi a segnalare altresì, come tale evoluzione del "*concept of money*" si può osservare confrontando ad esempio la quarta edizione di F. A. Mann, *The Legal Aspect of Money*, cit., p. 3 ss., con l'ultima edizione curata da C. Proctor (ed.), *Mann on the Legal Aspect of Money,* cit., p. 26 ss.

[51] Cfr. M. F. Campagna, *Criptomonete e obbligazioni pecuniarie*, cit., p. 213.

[52] Circa la "fattualità del diritto" e "la sua ineliminabile impurità", si veda P. Grossi, *Ritorno al diritto*, cit., p. 10.

altri scopi", oltre a quello di "mezzo di pagamento" o "mezzo di scambio"[53] e "prodotto di riserva di valore" (cfr. considerando n. 10 della direttiva 2018/843/UE)[54]: funzioni classiche della moneta da Aristotele sino a Mann.

Importa piuttosto che si tratti di una "moneta": e, sia consentito ribadirlo, è tale quello strumento, cui, in una determinata comunità, vengono riconosciute le qualità o funzioni (mezzo di scambio e prodotto di riserva di valore), che, come risulta dalle riferite parole del considerando 10 della direttiva 2018/843/UE, V direttiva antiriciclaggio, sono riconosciute dal legislatore europeo alle c.d. "valute virtuali" (art. 1, lett. d della medesima direttiva 2018/843/UE).

Ciò considerato, la "valuta" in senso stretto, ossia la moneta emessa da uno Stato sovrano o comunque avente corso legale nel territorio di uno Stato sovrano, è, per un verso, legata alla potestà statuale, per altro verso, beneficia dell'accettazione obbligatoria nel *territorio* dello Stato[55].

Invece, le valute digitali (o criptovalute) *private* sono aterritoriali[56]: in tale dimensione la "realtà del diritto" assume una valenza "subbiettivistica": così, per usare un'immagine di Cesarini Sforza, «*alla concezione obbiettivistica* [del diritto] *si oppone quella subbiettivistica, ma non negandola, bensì dialettizzandola*»[57], con una possibile conseguente circolazione dei modelli giuridici ed una loro

---

[53] Sotto un profilo funzionale, intendere la moneta come "mezzo di pagamento" o intenderla come "mezzo di scambio" o "*medium of exchange*", come fa ad esempio Mann (F. A. Mann, *The Legal Aspect of Money*, cit., p. 3) non mi pare muti la sostanza delle cose o dei fatti. Almeno se l'approccio è quello funzionale e il ragionamento si concentra sull'idea di moneta in generale e non sulla categoria di valuta in senso stretto, ossia di moneta emessa da una banca centrale ed avente corso legale nel territorio del relativo Stato: qualità indubbiamente esclusiva della moneta che sia creazione dello Stato sovrano. Ma forse sto sottovalutando il fascino o la "fascinazione" della "magia delle parole" prestate (o prestata) dai giuristi al mondo delle cose (cfr. P. Spada, in M. Cossu – P. Spada, *Dalla ricchezza assente alla ricchezza inesistente*, cit., p. 403). L'importante è, per utilizzare le parole di Berardino Libonati, (B. Libonati, *Titoli di credito e strumenti finanziari*, Milano, Giuffrè, 2002, p. 106) non accorgersi "*che forse si era troppo presi dalla magia delle parole - e lo osservava Ascarelli* – (…)". Il pensiero va a T. Ascarelli, *Cooperativa e società. Concettualismo giuridico e la magia delle parole*, in *Rivista delle società*, 1957, p. 397 ss.

[54] Sul punto si veda però Banca Centrale europea, *Parere della Banca Centrale Europea del 12 ottobre 2016 su una proposta di direttiva del Parlamento europeo e del Consiglio che modifica la Direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario ai fini di riciclaggio o finanziamento del terrorismo e che modifica la Direttiva 2009/10/CE.* Al riguardo, si veda l'analisi di G. Rinaldi, *Approcci normativi e qualificazione giuridica delle criptomonete*, cit., p. 277 e spec. p. 278, 2° cpv. Per una disamina della direttiva e della disciplina italiana di recepimento, si veda, altresì, in questo Quaderno, N. De giorgi, *Criptovalute: l'approccio dei* Policy Makers.

[55] Cfr. B. Geva, *Disintermediating Electronic Payments: Digital Cash and Virtual Currencies* in *Journal of International Banking Law and Regulation,* 2016, 12, p. 2 del dattiloscritto. M. Mancini, *Le valute virtuali e Bitcoin*, cit., p. 123, ult. cpv.

[56] Cfr. M. F. Campagna, *Criptomonete e obbligazioni pecuniarie*, cit., p. 213. G. Rinaldi, *Approcci normativi e qualificazione giuridica delle criptomonete*, cit., p. 260, testo e nota n. 8.

[57] W. Cesarini Sforza, *Il diritto dei privati*, cit., p. 27. Per il rapporto fra dimensione soggettiva dell'ordinamento giuridico, *lex mercatoria* e circolazione dei modelli giuridici si veda U. Mattei, voce *Circolazione dei modelli giuridici*, in *Enciclopedia del diritto*, *Annali,* I, Milano, 2007, p. 177.

possibile osmosi di cui mi paiono esemplificativi i contenuti dell'art. 8-*ter* della l. 11 febbraio 2019, n. 12[58].

È, più in generale, l'affascinante dialettica fra sistema o ordinamento giuridico informale e sistema o ordinamento giuridico formale (o statuale)[59] (*infra* § 3).

2. Valuta virtuale privata e/o criptovaluta, e moneta elettronica

Mi preme precisare, con specifico riferimento alle "valute virtuali", che appunto la dialettica fra realtà giuridica effettuale (o sistema giuridico informale) e sistema giuridico formale spiega i contenuti della seconda parte del generoso considerando n.10 della direttiva 2018/843/UE (V direttiva antiriciclaggio), dove, come già ricordato, si riconosce che «le valute virtuali possano essere spesso utilizzate», per un verso, «come mezzo di pagamento», per altro verso, «come prodotti di riserva di valore»[60].

Si tratta, come anticipato, di due funzioni che tradizionalmente appartengono alla moneta, e volendo utilizzare le parole di Giorgio de Nova[61], ne costituiscono i "tratti" distintivi e caratterizzanti. A ciò si aggiunga, che è difficile immaginare un mezzo di pagamento, che non sia anche e prima di tutto misura di valore.

Ecco perché «*bitcoin and other digital tokens have raised questions about the nature of money*»[62]. Si tratta ovviamente di "*intangible tokens*"[63].

---

[58] Cfr., con specifico riferimento ai recenti progetti di legge di Malta e del Lichtenstein, P. L. Athanassiou, *Tokens and the Regulation of Distributed Ledger Technologies: Where Europe Stood in the Last Quarter of 2018*, in *Journal of International banking Law and Regulation*, 2019, 3, p. 108 ss.

[59] Cfr. D. C. North, *Istituzioni, cambiamento istituzionale, evoluzione dell'economia*, Bologna, il Mulino, 1994, p. 27, per una distinzione fra sistema formale e sistema informale vedi p. 65 ss., edizione originale, *Institutions, Institutional Change and Economic Performance*, Cambridge University Press, 1990.

[60] Cfr. B. Geva, *Banking in the Digital Age*, cit., p. 29, nota n. 148, dove sisegnala come, in sede di *Regulation of Virtual Currency Act*, sidefinisca come "virtual currency" "*a digital representation of value that used as a medium of exchange, a unit of account, or a store of value; and is it not a legal tender*". Sul punto si veda G. Rinaldi, *Approcci normativi e qualificazione giuridica delle criptomonete*, cit., p. 272 e p. 281 nota n. 110.

[61] G. De Nova, *Il tipo contrattuale*, Padova, Cedam, 1974, p. 60 ss. e spec. p. 70 ss.

[62] N. Popper, *Bitcoin Comes to Campus*, in *New York Times. International Edition*, 8 febbraio 2018; si veda pure N. Popper, *Cryptocurrrency Comes to Campus*, consultabile al sito www.nytimes.com.

[63] Per una definizione di "digital tokens" sia consentito rinviare in questo Quaderno a R. Garavaglia, *Finalità, funzionamento e tipologia di utilizzi delle* Blockchain. Con specifico riferimento alla nozione di "cryptotoken in general" si veda D. Kunschke e R. Pfefferl, *CurrentIssuesRelating Financial Institutions and Markets from a RegulatoryPerspective*, in *Journal of International Banking Law, and Regulation*, 2019, 1, p. 25, testo e nota n. 13, dove fra l'altro si riferisce che "*BaFin generally understands cryptotokens to be 'the digital representation of an intrinsic value or value promised on the market using distributed ledger technology (DLT)'*". Pur in una dimensione di "tangible tokens", mi pare comunque utile ricordare la definizione adottata dall'*official commentary* dello *Uniform Electronic Transactions Act* (1999), così come riferita dall'*Yearbook* 2001 dell'UNCITRAL: "*Paper negotiable instruments and documents are unique in the fact that tangible token – a piece of paper – actually embodies intangible rights and obligations* (…)" (*Yearbook 2001*, par. 88, p. 290).

Ciò considerato, seguendo ancora la traccia del ricordato considerando n. 10 della direttiva 2018/843/UE, secondo cui è importante non confondere la valuta virtuale con la moneta elettronica di cui all'art. 2, n. 2 della direttiva 2009/110/CE, è necessario marcare l'"autonomia concettuale" dell'una rispetto all'altra[64].

A tal fine, sia consentito muovere da (e confrontarsi ancora con) l'ampia nozione di valuta virtuale (o "valute virtuali") disegnata dalla ricordata direttiva 2018/843/UE, all'art. 1, lett. d), secondo cui è tale «*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 o giuridiche come mezzo di scambio e può essere trasferita, memorizzata e scambiata elettronicamente*» (cfr. art. 1, comma 2, lett. qq del d.lgs. n. 90/2017[65]).

Si tratta di una definizione, improntata "*to 'technology agnosticism'*"[66], o neutralità tecnologica, capace di comprendere prima di tutto le valute virtuali private, aventi *bitcoin* come epitome[67], destinate ad essere veicolate mediante il sistema *blockchain* o comunque mediante un sistema riconducibile al modello *blockchain* e basato sulla relativa tecnologia[68]. Infatti, "*bitcoin operates on the basis of blockchain technology. Blockchain ensures the digital transfer of information with a mathematical algorithms, a hash function, that takes an input and transforms it into an output (hash). The alghorithm use is cryptographic*"[69] (enfasi mia). Ecco perché, sostanzialmente, le "*cryptocurrencies*" e le "*private digital currencies*" finiscono per coincidere[70]. E l'intrinseca destinazione funzionale delle "valute virtuali" alla circolazione, contribuisce a spiegare l'essenzialità della crittografia fra le caratteristiche "ontologiche" delle valute virtuali ed in particolare di *bitcoin*[71]: è, fra l'altro, il rapporto funzionale fra la

---

64 N. Nardi, *"Criptovalute" e dintorni*, p. 447, par. 1.3.

65 Con specifico riferimento alla definizione di valuta virtuale di cui all'art. 1, lett. qq del d.lgs. n. 90/2017, sostanzialmente coincidente con quella successivamente adottata dalla direttiva 2018/843/UE, per una prima lettura, sia consentito rinviare pure a F. Moliterni, *Commento all'art. 131-ter*, in *Commentario al testo unico delle leggi in materia bancaria e creditizia*, diretto da Francesco Capriglione, III, Padova, 2018,IV ed., p. 2565 ss.

66 P. L. Athanassiou, *Tokens and the Regulation of Distributed Ledger Technologies: Where Europe Stood in the Last Quarter of 2018*, cit., p. 109.

67 B. Geva, *The Law of Electronic Funds transfers*, cit., §1.04[7] [e].

68 G. Rinaldi, *Approcci normativi e qualificazione giuridica delle criptomonete*, cit., p. 259 ss. Con riferimento alla tecnologia sottostante al sistema *blockchain* mi piace segnalare come già nel 1985 Mario Losano facesse riferimento alla «tecnica della diagrammazione a blocchi» ed al singolo «blocco dell'informatizzazione», così M. Losano, *Diritto e informatica*, in Aa. Vv., *Tecnologia domani*, a cura di A., Roma – Bari, p. 272.

69 A.Rahmatian, *Electronic Money and Cryptocurrencies (Bitcoin)*, cit., p. 118.

70 M. F. Campagna, *Criptomonete e obbligazioni pecuniarie*, cit., p. 183 ss., dove fra l'altro si assume: «*il* Bitcoin *è un protocollo di comunicazione telematica che serve ad effettuare pagamenti.* (…)». In particolare, «bitcoin *è* (…) *basato su un sistema algoritmico di chiavi pubbliche e private*».

71 Bank of International Settlement (BIS), *Distributed Ledger Technology in payment, clearing and settlement. An Analytical Framework*, 2017, p. 2, punto 2.1, e spec. p. 4, punto 2.2.2.a, consultabile al sito www.bis.org/cpmi/pub/d.153.pdf

"valuta virtuale" *bitcoin* ed il suo sistema di circolazione (sistema di pagamento), *blockchain*, che richiede una protezione crittografica[72].

Il testo della nozione di valuta virtuale appena riferito evidenzia immediatamente i tratti caratterizzanti della fattispecie (di valuta virtuale): sia quelli positivi (in particolare, rappresentazione di valore digitale accettata come mezzo di scambio), che quelli negativi[73]: non essere emessa o garantita da una banca centrale o da un ente pubblico, non essere necessariamente legata ad una valuta avente corso legale.

Quest'ultimo "tratto", non essere necessariamente legata ad una valuta avente corso legale, è, in via di principio, caratterizzante la fattispecie di valuta virtuale rispetto alla "moneta elettronica" così come definita all'art. 2, punto 2 della direttiva 2009/110/CE, dove, fra l'altro, si considera tale un «*valore monetario memorizzato elettronicamente*» che rappresenta un credito nei confronti dell'emittente[74].

La differenza fra la moneta elettronica e la valuta virtuale, non legata ad una valuta legalmente costituita, sarebbe netta: la moneta elettronica rappresenta un valore monetario ed è tale in ragione del fatto che, per un verso, "documenta"[75] un credito del detentore della moneta elettronica nei confronti dell'emittente, conseguente alla consegna di fondi in favore di quest'ultimo, per altro verso, l'ammontare del credito è pari "al valore nominale" della somma di valuta o moneta reale ricevuta dall'emittente.

E in coerenza con l'esistenza di un credito del detentore della moneta elettronica verso l'emittente, la direttiva 2009/110/CE, prevede che, «*su richiesta del detentore di moneta elettronica*», gli emittenti ne «*rimborsino, in qualunque momento e al loro valore nominale, il valore monetario*» (art. 11, par. 2, della direttiva 2009/110/CE).

Non si tratta solo di una regola volta a "salvaguardare" la fiducia degli utenti nella moneta elettronica, che intuitivamente viene rafforzata dall'obbligo degli emittenti di moneta elettronica di rimborsarne il valore nominale su richiesta dei detentori (cfr. considerando 18 della direttiva 2009/110/CE). Si tratta piuttosto di un effetto giuridico derivante appunto dal riconoscimento in capo al

---

[72] «*Cryptography is thus used in cryptocurrencies to express and protect the value of the coins (the sequence of the bits), to prevent counterfeiting and fraudulent transactions, as well as to perform the validation and execution of transactions records via a distributed ledger, such as the blockchain*» (B. Geva, *Banking in the Digital Age*, cit., p. 32, 3° cpv.). Sul punto si veda pure Y. Braouézec – B. Beaupain – T. Renault, *Monnaie Fiduciaire, Electronique et Cripto-monnaies*, in *Revue Banque*, 2019, 3, p. 65.

[73] Cfr. P. L. Athanassiou, *Tokens and the Regulation of Distributed Ledger Technologies: Where Europe Stood in the Last Quarter of 2018*, cit., p. 110.

[74] Da ultimo, cfr. A. Rahmatian, *Electronic Money and Cryptocurrencies (Bitcoin)*, cit.; sul punto, *ex multis*, si veda pure C. Proctor (ed.), *Mann on the Legal Aspect of Money*, cit., p. 50, par. 1.80, testo e nota n. 229.

[75] Cfr. C. Angelici, voce *Documentazione e documento*, in *Enc. giur. Treccani*, XIII, Roma, 1989, p. 2, par. 1.2, p. 4 s. par. 3.1.

detentore di moneta elettronica di un "credito" nei confronti dell'emittente, cui non può che corrispondere un'obbligazione pecuniaria dell'emittente medesimo, per un ammontare equivalente alla somma di denaro (moneta reale) ricevuta. E l'equivalenza – fra la somma di denaro ricevuta dall'emittente e la somma di denaro restituita dall'emittente medesimo al detentore di moneta elettronica – va garantita se davvero si vuole che la moneta elettronica sia un «*sostituto elettronico delle monete e delle banconote*» (considerando 12 della direttiva 2009/110/CE).

Il modello logico della moneta elettronica sembrerebbe distinto da quello della valuta virtuale nettamente e con una «consequenzialità ineludibile»[76], tuttavia la realtà effettuale presenta casi di contaminazioni fra il modello della valuta virtuale e quello della moneta elettronica: e preciso subito che, a mio parere, talune contaminazioni non sono giustificate dal fatto che la valuta virtuale «*non è necessariamente legata a una valuta legalmente istituita*», e quindi, per converso, potrebbe essere legata ad una valuta legalmente istituita. La questione sorge se tale legame avvicina la valuta cosiddetta virtuale alla fattispecie di moneta elettronica.

Infatti, meno distante dal modello della moneta elettronica è quella valuta digitale o "*virtual cryptocurrency*"[77] come *Tether*, «*i cui creatori hanno sempre assicurato ai clienti di accumulare riserve di un dollaro per ogni Tether creato*»[78].

Tale "riserva" è essenziale, atteso che, come segnala Benjamin Geva, «*in Tether, the cryptocurrency is a claim-check to a fiat currency*»[79]. Infatti, «*Tether converts cash as well as bank money into digital currency, and anchors or tethers the value of the currency it issues to the price of national currencies like the US dollar, the Euro, and the Yen. As such, it is a stable currency*»[80].

In tale dimensione, il "legame" fra la "virtual currency" e la "valuta avente corso legale" è tale da indurre, se non giustificare, nei clienti dell'emittente di *Tether*, e di valute virtuali simili, un affidamento nel loro valore (monetario) comparabile o simile a quello delle monete elettroniche di cui all'art. 1, punto 2, della direttiva 2009/110/CE. L' "osservazione"[81] del dato sperimentale, specie in tal caso, mi sembra decisiva [82].

---

[76] Cfr. F. Merusi, *Democrazia e autorità indipendenti*, cit., p. 21, 1° cpv.

[77] B. Geva, *The Law of Electronic Funds transfers*, cit., §1.04[7][e] testo e nota n. 155.

[78] M. Longo, *Bitfinex, scandalo sulla borsa dei Bitcoin*, in *IlSole-24ore*, 30 aprile 2019, p. 12.

[79] B. Geva, *The Law of Electronic Funds transfers*, cit., §1.04[7][e] testo e nota n. 155, dove si precisa altresì che «*each claim-check is in the form of a digital bearer instrument that has an address assigned to it with a denomination that is immutable. It is recommended that these attributes, along with others determined by the issuer, be cryptographically signed by the issuer when the bearer instrument created*». Si veda pure Id., *Banking in the Digital Age*, cit., p. 29.

[80] B. Geva, *The Law of Electronic Funds transfers*, cit., §1.04[7][e] testo e nota n. 155.

[81] «*La scienza come metodo di indagine* (…) *si basa sul principio che l'osservazione è il giudice ultimo di come stanno le cose*» (R. P. Feynman, *Il senso delle cose*, Milano, Adelphi, 1999, p. 25).

[82] Cfr. M. Longo, *Bitfinex, scandalo sulla borsa dei Bitcoin*, cit., p. 12.

Tornando ai tratti distintivi della fattispecie: se le valute virtuali come *Tether* sono (dal loro emittente) emesse «*al valore nominale dietro ricevimento di fondi*» (art. 11, par. 1, della direttiva 2009/110/CE), destinati ad essere vincolati totalmente a "riserva", e, quindi, «*in a claim-check format*», rappresentano «*a claim against (…) a fiat currency*»[83]. Esse sono pertanto simili alle monete elettroniche in senso stretto: se non di fatto loro omologhe come sostituto elettronico della moneta legale (specie se quanto versato a fronte dell'emissione del valore nominale di *Tether*, viene o, meglio, venisse vincolato interamente a riserva). E a fattispecie omologhe o simili dovrebbe corrispondere conseguente analoga disciplina[84], specie in materia di tutela dei fondi ricevuti da parte dell'emittente in cambio della "valuta virtuale" (cfr. art. 7, par. 1 e art. 11 della direttiva 2009/110/CE). E gli eventi recentemente segnalati dalla stampa specializzata sembrerebbero confermare tale esigenza[85].

2.1 Moneta reale tradizionale, moneta elettronica e/o valuta virtuale emessa da una banca centrale

Il crescente fenomeno della moneta digitale, che come già segnalato, è attualmente in una fase iniziale[86], rappresenta una rivoluzione[87] nell'economia monetaria, e non solo, difficilmente arginabile[88] (e a mio parere non arginabile)[89].

La conseguente attenzione verso tale "forma" monetaria non poteva e non può non tradursi in un corrispondente interesse delle banche centrali[90], tradizionali emittenti di moneta "reale" (avente corso legale), ad emettere loro monete elettroniche[91], significativamente indicate come "*public and regulated*

---

83 B. Geva, *Banking in the Digital Age*, cit., p. 30.

84 E. Betti, *Interpretazione della legge e degli atti giuridici (teoria generale e dogmatica)*, Milano, Giuffrè, 1971, II edizione a cura di Giuliano Grifò, p. 163 ss.; F. Modugno, *L'interpretazione giuridica*, Padova, 2012, II ed., p. 415 ss.

85 Cfr. M. Longo, *Bitfinex, scandalo sulla borsa dei Bitcoin*, cit., p. 12.

86 B. Geva, *The Law of Electronic Funds Transfers*, cit., § 1.04[7] [a].

87 Cfr., in una dimensione diversa, C. Barbagallo, *Fintech: ruolo dell'Autorità di Vigilanza in un mercato che cambia*, in *Bancaria*, 2019, 1, p. 10 ss. e p. 13, c. 2.

88 In una prospettiva diversa, si veda A. Ruberti, *Introduzione*, in Aa. Vv., *Tecnologia domani*, a cura di A. Ruberti, Roma-Bari, 1985, p. XII, dove fra l'altro si osserva come «*la transizione sia oggi il tema di maggiore rilevanza; perché se obiettivamente non è possibile bloccare la trasformazione, è almeno auspicabile riuscire ad addomesticarla, e a questo scopo occorre conoscere quali variabili, parametri e vincoli ne governano l'evoluzione*».

89 Già nel marzo 1986 Carlo Azeglio Ciampi osservava come l'impatto delle «*nuove tecnologie* (…) *sta*[nno] *rapidamente modificando in molti paesi il sistema dei pagamenti, la cui efficienza e sicurezza sono componenti essenziali della moneta*»: parole riferite da T. Padoa Schioppa, *La moneta e il sistema dei pagamenti*, cit., p. 15.

90 Cfr. B. Coeurè, *Foreword*, in BIS, *Distributed Ledger Technology in payment, clearing and settlement. An Analytical Framework*, cit., p. iii.

91 B. Geva, *The Law of Electronic Funds transfers*, cit., §1.04[7][e] testo e note n. 166 e 167.

digital currencies"[92], e «*generally known as Central Bank Digital Currencies (CBDCs)*»[93].

Al riguardo, viene quasi naturale osservare come «*can become complicated distinguish the pedigree of different versions of electronic money if a central bank decide to issue digital currency: what is traditional cash and what is electronic cash*»[94]?

Tradotta la domanda (apparentemente pleonastica) nella dimensione della nozione di "fondi" di cui alla direttiva 2015/2366/UE all'art. 4, n. 25 (art. 1, lett *m,* del d. lgs. 27 gennaio 2010, n. 11), come distinguere le tradizionali "banconote o monete" dalla moneta elettronica (art. 2, punto 2, della direttiva 2009/110/CE) e/o dalla valuta virtuale emesse da una banca centrale[95]?

Mi pare che la questione sia tutt'altro che peregrina: la distinzione è difficile e, sotto un profilo funzionale, forse non utile, se si assume che «*nonetheless, a digital currency issued by a central bank may not be self-anchored; rather, it must be a claim-check in the sense that it entitles its holder to redeem or convert it either to bank money or physical currency in the same amount*»[96].

3. **Blockchain***: ecosistema e sistema di pagamento fra modello peer to peer e (tentazione del) modello "centralizzato"*

Una riflessione sulle valute virtuali non può essere slegata dal sistema che ne consente la circolazione: *blockchain*.

Ed è appena il caso di sottolineare come la valuta virtuale *bitcoin* e le altre valute virtuali simili vanno tenute distinte dal sistema *blockchain*: *bitcoin* è il veicolo, *blockchain* è il suo sistema di circolazione[97].

Blockchain viene considerato come un "ecosistema"[98] per la poliedricità e la capacità espansiva delle sue applicazioni.

---

92 A. Rahmatian, *Electronic Money and Cryptocurrencies (Bitcoin)*, cit., p. 116.

93 B. Geva, *Banking in the Digital Age*, cit., p. 29 ss.

94 A. Rahmatian, *Electronic Money and Cryptocurrencies (Bitcoin)*, cit., p. 117.

95 Cfr. V. De Stasio, *Verso un concetto europeo di valuta legale: valute virtuali, monete complementari e regole di adempimento*, cit., p. 755.

96 B. Geva, *Banking in the Digital Age*, cit., p. 29 e spec. p. 30.

97 Per un confronto fra sistema di pagamento e sistema di trasporto delle merci, si veda quanto osservato da Carlo Azeglio Ciampi in sede di *Presentazione* a Banca d'Italia, *Libro bianco sul sistema dei pagamenti in Italia*, Roma, 1987.

98 Cfr. M. Mancini, *Valute virtuali e Bitcoin*, cit., p. 121 ss.; cfr. P. Soldavini, *Blockchain, è l'ecosistema a costituire il valore vero*, in *IlSole-24Ore*, inserto Nòva, 29 febbraio 2019, p. 40. Per l'idea di "ecosistema", si veda G. Caldarelli e M. Catanzaro, *Scienza delle reti*, cit. p. 15 ss., dove fra l'altro si assume che «*gli ecosistemi sono reti complesse formate da specie differenti: è quindi fondamentale tenere in considerazione questa struttura, se vogliamo comprenderli e gestirli*» (p. 16, par. 1.1, 2° cpv.).

Ciò vale anche nella specifica dimensione di *blockchain* come sistema di pagamento e/o di regolamento titoli.

In tale prospettiva, va sì riconosciuto che «*for the transfer of information, for example, payment, blockchain technology ensures the elimination of double-payment*»[99] o "*double spending*"[100], o meglio, che «*are designed to prevent the ' double spending'*»[101].

Ma la sicurezza del sistema di pagamento basato sul modello *blockchain* è effettivamente tale, ossia (quasi) assolutamente certa, nella sua dimensione di catena o serie continua di accordi bilaterali, in un modello decentralizzato e/o *peer to peer*, che ricorda il modello di circolazione dell'ordine di pagamento (o di consegna) nei titoli di credito all'ordine[102]: è la serie continua delle girate, in un modello "*peer to peer*" o da "*payer to payee*", che appunto «*ensures the elimination of double-payment*».

È il modello dell'operazione, che garantisce, o contribuisce a garantire in modo decisivo la sicurezza del sistema complesso *blockchain*.

La stessa sicurezza non mi pare possa essere assicurata dal modello centralizzato o "*centralisedsystem*", basato su di un partecipante al sistema che assume la posizione di *hub*-centro aggregatore[103], finendo per svolgere la funzione di gestore del sistema e/o di agente di regolamento o controparte centrale: e che soprattutto potrebbe finire per svolgere la funzione di "custode" del "registro condiviso" (*distribuited ledger*[104]) o "Libro Mastro Digitale Distribuito"[105], riconducibile all'ampio genere dei "Private registries" così come definito e/o descritto fra l'altro dall'UNCITRAL, *Yearbook* 2001[106].

---

[99] A. Rahmatian, *Electronic Money and Cryptocurrencies (Bitcoin)*, cit, p. 118, 2° cpv. Sul punto si veda pure quanto già osservato da M. Mancini, *Valute virtuali e bitcoin*, cit., p. 119 ss.

[100] Sul rischio di "*double spending*" si veda in questo *Quaderno* R. Garavaglia, *Finalità, funzionamento e tipologia di utilizzi delle* Blockchain, cit.

[101] B. Geva, *Banking in the Digital Age*, cit., p. 37.

[102] Sul punto sia consentito rinviare a F. Moliterni, *Commercio internazionale,* letters of indemnity, bills of lading *(o polizze di carico), e sistema di circolazione e regolamento delle* electronic bills of lading*: suggestioni dal modello dei sistemi di pagamenti elettronici «istantanei»* peer to peer *e dal modello del sistema blockchain*, in *Diritto del commercio internazionale*, 2018, 1, p. 112 ss. e spec. p. 114 ss.

[103] F. Sylos Labini, *Rischio e previsione. Cosa può dirci la scienza sulla crisi*, Roma – Bari, 2016, p. 51 ss.

[104] Cfr. S. Rossi, *Oro*, cit., p. 92, 1^ cpv., dove, pur in altra prospettiva, si segnala l'importanza del "gestore del registro".

[105] Cfr. in questo *Quaderno* R. Garavaglia, *Finalità, funzionamento e tipologia di utilizzi delle* Blockchain cit.; G. Rinaldi, *Approcci normativi e qualificazione giuridica delle criptomonete*, cit., p. 262; M. Mancini, *Le valute virtuali e Bitcoin*, cit., p. 119.

[106] «*Private registries. These registries are conducted over open or semi-open networks, where the issuer of the document, its agent (as in the systems of electronic warehouse receipts in the United States (…) administers the transfer or negotiation process*» (UNCITRAL, *Yearbook 2001 of the United Nations Commission on International Trade Law*, XXXII, New York, 2001, p. 292, par. 97, lett. c), consultabile al sito www.unicitral.org. Per un'osservazione sul piano funzionale, fra la idoneità di *blockchain* a certificare, proteggere e conservare la "*authenticity*" dei "*documents of title*", e quella di un "*public registry*" si veda S. Morrison, *Smart Contracts Enforcement of Islamic Finance Deals*, in *Journal of International Banking Law and Regulation*, 2019, 4, p. 146, dove si osserva come le «*crucial features of blockchain are also exibited by a public registry, for example, that of the Land Registry in England and Wales*».

Un tale modello di "*centralised system*" mi pare comunque basato su di un "*registry approach*"[107] tradizionale, che, per utilizzare un'immagine suggerita da Paolo Spada, rischia di replicare la figura del «grande fratello orwelliano»[108].

In altre parole, mi pare che la *peculiare* filosofia di *bitcoin* e di *blockchain*[109] leghi in modo biunivoco la valuta virtuale privata (moneta privata) al modello di circolazione disintermediata della moneta (e più in generale dell'informazione)[110]. Se così è, le c.d. "piattaforme"[111] di scambio[112], qualora siano mercati[113] a gestione centralizzata o "a schema accentrato"[114] dove "creare" (o meglio, emettere) e trasferire valuta virtuale, sembrano estranee alla filosofia, alla "*original idea*" ed al modello di *bitcoin*, atteso che, come già osservato, «*the distributed, as opposed to a centralised, method makes the apparent appeal of Bitcoin*»[115].

Ma soprattutto, dette "piattaforme" basate su di un "*centralised system*" (ri)presentano la stessa tipologia di rischi dei modelli tradizionali di sistema di pagamento e regolamento titoli, basati su di un partecipante-hub (cfr. art. 2, lett. a, primo alinea della direttiva 98/26/CE; art. 2, n. 1, del regolamento BCE n. 795/2014): solo che probabilmente la misura dei medesimi rischi, anche sotto

---

[107] Cfr. UNCITRAL, *Yearbook 2012 of the United Nations Commission on International Trade Law*, New York, 2012, p. 287, par. 38, p. 309, par. 52. Si veda pure UNCITRAL, *Yearbook 2001 of the United Nations Commission on International Trade Law*, cit., p. 292, par. 98, lett. C, e per "*functions registry*" in genere p. 282 par. 31-32.

[108] P. Spada, in P. Spada – Cossu, *Dalla ricchezza assente alla ricchezza inesistente – Divagazioni del giurista sul mercato finanziario*, in *Banca, borsa, tit. cred.*, 2010, I, p. 407; A. Rahmatian, *Electronic Money and Cryptocurrencies (Bitcoin)*, cit., p. 118, c. 2, ult. cpv.

[109] B. Geva, *Banking in the Digital Age*, cit., p. 32, ult. cpv., testo e nota n. 165, dove riferendo le parole di Satoshi Nakamoto, autore di quello che è diventato una sorta di manifesto di *Bitcoin*, oltreché «mythological founder» di *bitcoin*, definisce «*Bitcoin as an 'electronic coin' consisting of a 'chain of digital signatures' transferable from the payer to payee 'by digitally signing a hash of the previous transaction and the public keys of the next owner and adding them to the end of the coin*». Sul punto si veda pure G. Rinaldi, *Approcci normativi e qualificazione giuridica delle criptomonete*, cit., p. 262.

[110] A. Rahmatian, *Electronic Money and Cryptocurrencies (Bitcoin)*, cit., p. 120, c. 1, 2° cpv.

[111] Sulla definizione di "piattaforma o "*platform*", si veda Bank of International Settlement (BIS), *Distributed Ledger Technology in payment, clearing and settlement. An Analytical Framework*, cit., p. 1.

[112] M. Mancini, *Valute virtuali e Bitcoin*, cit., p. 121. Cfr. M. F. Campagna, *Criptomonete e obbligazioni pecuniarie*, cit., p. 208 ss.

[113] «*Moreover, merely using or mining cryptocurrencies is not by itself subject to a licence requirement. Payment tokens are, however, classified by Bafin as units of account (…) and, accordly, a financial instrument within the ambit of the KWG. They are thus subject to a licence requirement is, in addition to mere use or mining, other circumstances apply, in particular the creation of a market on which they can be traded*» (enfasi mia), così D. Kunschke e R. Pfefferl, *Current Issues Relating Financial Institutions and Markets from a Regulatory Perspective*, cit., p. 25.

[114] M. Mancini, *Valute virtuali e Bitcoin*, cit., p. 118.

[115] A. Rahmatian, *Electronic Money and Cryptocurrencies (Bitcoin)*, cit., p. 118, c. 2, ult. cpv., in fine.

il profilo sistemico[116], è accentuata. In particolare, mi preoccupa la dimensione che assume o può assumere il "rischio operativo"[117], specie se combinato con il "rischio di custodia"[118], in un sistema basato su " '*permissioned*' *DLT [Distributed Ledger Technolgy] arrangements (whichthereis an owner for the ledger)*"[119]. E sia consentito segnalare, pur per inciso, che la traduzione letterale di *owner* è quella di "proprietario" ed in tal caso, oltre ad essere la "più ovvia"[120] è anche quella più vicina al pensiero dell'autore, che assume come la "governance" dei riferiti "*ledger(s)*" sia "*simpler because by definition there is a proprietor*"[121]. In tal caso, per converso, non mi pare possibile riconoscere la medesima «*resilience and reliability*» verso gli «*operational and security risk[s]*»[122], che la Bank for International Settlements individua nei sistemi di pagamento basati su "*permissionless DLT [Distributed Ledger Technology] arrangements*", ossia sul modello originario di *blockchain* disintermediato, dove ciascun nodo ha il medesimo numero di *links* (e quindi nessun nodo o partecipante al sistema è un *hub* con un numero più o meno importante di collegamenti con altri nodi-partecipanti)[123].

In ogni caso, l'esistenza di rischi operativi e di custodia, cui possono seguire rischi di credito e di liquidità (cfr. art. 2, nn. 8 e 9 del regolamento BCE

---

[116] Per la nozione di rischio sistemico si veda l'art. 2, n. 3 del Regolamento BCE n. 795/2014. Cfr. D. Kunschke e R.Pfefferl, *Current Issues Relating Financial Institutions and Markets from a Regulatory Perspective*, cit., cit., p. 23 ss. Circa «*l'utilizzo di valute virtuali* [e i conseguenti] *rischi per gli utenti* (…) *e soprattutto, per gli interessi pubblici all'integrità e stabilità del sistema finanziario, regolare funzionamento del sistema dei pagamenti, e alla sana e prudente gestione degli intermediari bancari e finanziari vigilati*», si veda M. Mancini, *Valute virtuali e Bitcoin*, cit., p. 132. Con riferimento al sistema dei pagamenti in genere, si veda G. Carriero, *Verso un nuovo diritto privato dei pagamenti*, in G. Carriero – V. Santoro, *Il diritto del sistema dei pagamenti*, Milano, 2005, p. 3 ss., testo e nota n. 1.

[117] Si fa riferimento al "rischio operativo" inteso come «*rischio che carenze nei sistemi informativi o procedure interne, errori umani, carenze gestionali* (…) *provochino la riduzione o la sospensione dei servizi forniti*» dal sistema, e che comunque determinino perdite (cfr. art. 2, n. 10 del regolamento BCE n. 795/2014). In una prospettiva diversa, si veda C. Barbagallo, *Fintech: ruolo dell'Autorità di Vigilanza in un mercato che cambia*, cit., p. 14 e p. 15, spec. c. 2.

[118] «*Per rischio di custodia si intende il rischio di perdite sulle attività detenute in custodia in caso di insolvenza di un custode o sub-custode, negligenza, frode, cattiva gestione o errori contabili*» (art. 2, n. 11 del Regolamento BCE n. 795/2014). Cfr. M. Mancini, *Valute virtuali e Bitcoin*, cit., p. 121.

[119] B. Geva, *Banking in the Digital Age* , cit., p. 35. Per una definizione di DLT si veda fra l'altro veda D. Kunschke e R. Pfefferl, *Current Issues Relating Financial Institutions and Markets from a Regulatory Perspective*, cit., p. 25, nota n. 13.

[120] F. De Franchis, voce *Owner*, in Id., *Dizionario giuridico Inglese – Italiano, English – Italian – Lawdictionary*, Milano, Giuffrè, 1984, p. 1088.

[121] B. Geva,*Banking in the Digital Age* , cit., p. 35.

[122] Bank of International Settlement (BIS), *Distributed Ledger Technology in payment, clearing and settlement. An Analytical Framework*, 2017, p. 14, punto 3.3.1, consultabile al sito www.bis.org/cpmi/pub/d.153.pdf; sulla «*straordinaria resilienza di Internet di fronte a errori, attacchi* (…)» come «*prestazione della rete nel suo complesso*», si veda G. Caldarelli e M. Catanzaro, *Scienza delle reti*, cit., p. 18. Con specifico riferimento alle «*technologies underlying cripto-assets, particularly distributed ledger*» si veda il contributo del Governatore della Bank of England M. Carney, *The Future of Money*, 2 marzo 2018, p. 12, consultabile al sito www.bankofengland.co.uk/speeches

[123] Cfr. G. Rinaldi, *Approcci normativi e qualificazione giuridica delle criptomonete*, cit., p. 263, par. 2.1, in fine.

n. 795/2014), comporta l'esigenza di inibire o contenere i rischi, e quindi di adeguati sistemi di controllo e di gestione dei rischi medesimi[124].

Si pone quindi la necessità di regolamentare tali fenomeni, atteso che «*it is a misconception to think of such arrangement as existing indipendent of human rule-making*»[125].

Si è altresì affrontato il problema di regolare i sistemi basati su "*permissionless DLT [Distributed Ledger Technology] arrangements*", i sistemi disintermediati "in senso proprio", privi di un *owner*-proprietario o un gestore, e si è osservato come «*compared with both permissioned DLT arrangements as well as traditional payments systems, governance costs in permissionless DLT arrangements are bound to be higher because of the greater complexity of the technical arrangements, the sheer greater number of partecipants directly involved and the difficulty of getting a timely agreement*»[126].

Si aggiunge ancora che «*this can be seen from the drawn-out process and uncertainty in term of responsability and 'chain of command'*»[127].

In realtà, mi pare si riproponga nella dimensione delle valute virtuali come *bitcoin* e dei relativi sistemi di circolazione e/o sistemi di pagamento (*blockchain*) l'enigma giuridico di "formalizzare l'informale"[128]. E l'enigma di formalizzare la moneta ed il sistema di pagamento informali imponendo autoritativamente regole eteronome potrebbe rivelarsi appunto un "enigma" – a chi applicare le regole e come assicurarne l'effettività, atteso l'anonimato, sia pure "parzialmente protetto"[129], dei titolari di *bitcoins* e/o dei *miners* o nodi partecipanti al sistema –, la cui soluzione potrebbe essere trovata, almeno in parte, nella fuga verso una autoregolamentazione "incentivata"[130] e, quindi, riconosciuta dall'ordinamento giuridico formale.

---

[124] Ed è particolarmente importante nei modelli di produzione di valuta virtuale e sistemi di circolazione, che comportano una concentrazione del rischio, legata alla emissione di "valuta virtuale" prodotta in quantità indefinita da un (unico)emittente privato, che vincola il valore della valuta virtuale al valore nominale di una valuta emessa da una banca centrale (ad esempio con un rapporto uno ad uno: un "pezzo monetario" di valuta virtuale equivale ad un euro, o a un dollaro, o a un yen), assumendo l'obbligo di destinare a riserva l'intero ammontare di euro (o dollari o yen, ecc.) raccolti a fronte dell'emissione della ricordata valuta virtuale.

[125] B. Geva, *Banking in the Digital Age*, cit., p. 35.

[126] B. Geva, *Banking in the Digital Age* , cit., p. 35. Sul punto si veda pure in questo *Quaderno* R. Garavaglia, *Finalità, funzionamento e tipologia di utilizzi delle* Blockchain cit..

[127] B. Geva, *Banking in the Digital Age* , cit., p. 35.

[128] N. Passas, *Formalizing the Informal? Problems in the National and International Regulation of Hawala*, in Aa. Vv., *Regulatory Frameworks for Hawala and Other Remittance Systems*, Monetary and Financial Systems Department – International Monetary Fund, Washington, 2005, p.8. Con specifico riferimento all'ecosistema delle valute virtuali e del sitema *blockchain*, si vedano le considerazioni conclusive di M. Mancini, *Le valute virtuali e Bitcoin*, cit., p. 138, spec. ult. cpv.

[129] G. Rinaldi, *Approcci normativi e qualificazione giuridica delle criptomonete*, cit., p. 265, par. 2.3.

[130] Pur in una prospettiva diversa cfr. in questo *Quaderno* R.Garavaglia, *Finalità, funzionamento e tipologia di utilizzi delle* Blockchain cit.. Cfr. M. Mancini, *Valute virtuali e Bitcoin*, cit., p. 136, 3° cpv. In una dimensione differente, si vedano le considerazioni in tema di "*jus* digitale", *soft law* e "nuova età del diritto", in P. Zanelli, *Detipizzazione legale e (ri)costruzione contrattuale*, cit., p. 23, p. 24, p. 29.

Mi pare vada in tale direzione la valorizzazione dell'efficienza e della sicurezza del modello *blockchain* come sistema di documentazione delle informazioni, destinate a circolare: in tal caso il modello logico conserva la sua ineludibile consequenzialità, se si riconosce come indispensabile la continuità della serie o della catena delle transazioni o accordi bilaterali, che elimina la possibilità di un percorso diverso e la duplicazione, fraudolenta o meno, dei pagamenti (o, per le *bills of lading*, della consegna della merce). Per altro verso, la "scoperta" (Grossi) che la documentazione informatica[131] della serie continua delle transazioni (*blocks*) aventi ad oggetto *bitcoin* (dall'originario creatore o "mittente" della "*sequence of bits*", costitutiva del *bitcoin*, sino all'ultimo acquirente, che ne ha il "controllo") rappresenta, nel suo insieme, un registro condiviso appartiene, a sua volta, alla forza della sostanza delle cose.

Riconoscere a tale registro l'efficacia della forma scritta (cfr. il citato art. 8-*ter* della l. n. 12/2019), è parte di uno "specchio"[132] giuridico della sostanza delle cose, ed in particolare della forza della catena (*chain*) continua delle operazioni di pagamento[133], che ha in sé la forza di quella particolare rete, – appartenente alla categoria delle reti definite dai matematici come "alberi" – dove «*esiste uno ed un solo percorso possibile tra ogni coppia di nodi*»[134].

4. Alcune considerazioni conclusive

L'ecosistema o il mondo delle valute virtuali e dei loro modelli e/o sistemi a "utilizzazione (…) distribuita"[135] è probabilmente protagonista e vittima di una straordinaria e singolare accelerazione della sua evoluzione[136].

La qualità dei soggetti partecipanti, e soprattutto intenzionati a partecipare, all'ecosistema delle valute virtuali (ed ai loro sistemi) è, o può essere, intuitivamente determinante.

---

131 Cfr. M. Mancini, *Valute virtuali e Bitcoin*, cit.; G. Rinaldi, *Approcci normativi e qualificazione giuridica delle criptomonete*, cit., p. 263.

132 L'immagine dello "specchio giuridico" è suggerita da G. Zagrebelsky, *Diritto allo specchio*, Torino, Einaudi, 2018, p. XIX.

133 Per la nozione di "operazioni di pagamento", si veda A. Sciarrone Alibrandi, *L'adempimento dell'obbligazione pecuniaria tra diritto vivente e portata regolatoria indiretta della Payment Services Directive 2007/64/CE*, in M. Mancini – M. Perassi (a cura di), *Il nuovo quadro normativo dei servizi di pagamento. Prime riflessioni*, in *Quaderni di ricerca giuridica della Banca d'Italia,* n. 63, Roma, 2008, p. 62.

134 P. Higgins, *La matematica dei social network. Una introduzione alla teoria dei grafi*, Bari, 2012, p. 12.

135 L'espressione, ricavata da una densa riflessione in tema di "innovazione tecnologica" e "sistemi complessi", si rintraccia in un risalente contributo di A.Ruberti, *Introduzione*, in Aa. Vv., *Tecnologia domani*, a cura di A. Ruberti, cit., p. VII ss. e spec. p. X.

136 Con riferimento al peculiare "dinamismo" del settore dei sistemi di pagamento, si veda M. Mancini – M. Perassi, *Prefazione*, in M. Mancini – M. Perassi (a cura di), *Il nuovo quadro normativo dei servizi di pagamento*, cit., p. 15. Con specifico riferimento alla rilevanza dei "*digital payments*", "*money transfers*" e "*fintech firms*" nei trasferimenti di fondi che coinvolgono i migranti, si veda *Cross-border payments. The Migrants Migraine*, in *The Economist*, 13 aprile 2019, p. 14

In tale prospettiva, non è rilevante solo la natura giuridica dei partecipanti all'ecosistema delle valute virtuali e dei loro modelli: in particolare banche[137] o intermediari finanziari e relativi sistemi di pagamento[138] vigilati. È importante anche la dimensione delle imprese e soprattutto la diffusione e capillarità della loro rete, prima di tutto sotto il profilo del rischio sistemico[139].

Si fa ormai ripetutamente riferimento a Google o Facebook con la sua "*digital currency*"[140], e più in generale alle "*IT firms*"[141].

È suggestivo, oltreché verosimile, che «*for sure, there is nothing to preclude IT firms from becoming banks and competing with existing banks on equal footing. Indeed, in Antiquity and the Middle Ages it was the money changer who became a deposit banker. In the Middle Ages it was the large merchant who made and deceived intercity commercial payments. Subsequently, it was the goldsmith who became a banker in post-Medieval England. According to this logic, there is nothing new in the transformation of the IT firm into a bank*»[142].

Tuttavia, se ciò è vero o, meglio, verosimile, è probabilmente vero pure che «*IT firms must develop a model different than that of 'banking'; the ensuing discussion is designed to disprove the adequacy if not the existence of such model*»[143].

Stando così le cose, la dote di rischi che tradizionalmente segue un'impresa bancaria non verrà meno, in particolare nei modelli basati su di un "*centralised system*" (simile ad un modello di banca e di sistema bancario tradizionale[144]):

---

137 Si segnala il caso di Jp Morgan e della piattaforma *Interbank Information Network* (Inn), riferito da P. Soldavini, *Jp Morgan e Facebook puntano sulle criptovalute (ma stabili)*, in *IlSole-24Ore*, 30 aprile 2019, p. 12.

138 Con specifico riferimento a SWIFT, si veda B. Geva, *Banking in the Digital Age*, cit., p. 46 ss.

139 Cfr. P. Ciocca, *La banca che ci manca*, cit., p. 66.

140 A. Rahmatian. *Electronic Money and Cryprocurrencies*, cit., 120, c. 2. Sul punto si veda quanto segnalato fra l'altro da P. Soldavini, *Jp Morgan e Facebook puntano sulle criptovalute (ma stabili)*, cit., p. 12. Con specifico riferimento a Facebook ed alla sua *digital currency*, Libra, si veda quanto segnalato da R. Barlaam, *Facebook, via al bitcoin con Visa e Mastercard*, in *Il Sole 24 Ore*, 15 giugno 2019, p. 6. Si vedano, in particolare, le interessanti considerazioni di M. Carney, *The Growing Challenges for Monetary Policy in the Current International Monetary and Financial System*, Jackson Hole Symposium, 23 agosto 2019, p. 15 del dattiloscritto, consultabile al sito www.bankofengland.co.uk/news/speeches, dove fra l'altro, si definisce "Libra" come "*a new payments infrastructure based on international stablecoin fully backed by reserve assets in a basket of currencies including the US dollar, the euro, and sterling*". Si tratta di uno scenario suggestivo, ed è agevole assumere che proprio tale "fenomeno" monetario privato ha indotto Mr. Carney a suggerire lo sviluppo di "*a new Sybthetic Hegemonic Currency (SHC) … perhaps through of network of central bank digital currencies*". Sul punto si veda pure quanto anticipato da R. Sorrentino, *Carney: super valuta digitale contro l'egemonia del dollaro*, in *Il Sole 24 Ore*, 25 agosto 2019, p. 5.

141 B. Geva, *Banking in the Digital Age*, cit., p. 23.

142 B. Geva, *Banking in the Digital Age*, cit., p. 23. Ma si veda pure quanto osservato da G. M. Gros-Pietro, *Il denaro è cosa buona se è collegato all'economia reale*, in *Bancaria*, 2019, 1, p. 7 ss.

143 B. Geva, *Banking in the Digital Age*, cit., p. 23.

144 Bank of International Settlement (BIS), *Distributed Ledger Technology in payment, clearing and settlement. An Analytical Framework*, cit., p. 1.

piuttosto, potrebbe mutare la velocità di propagazione del rischio (con conseguente crescita di quello sistemico), in considerazione della velocità e dell' "efficienza delle reti", soprattutto se complesse[145], su cui è basata la banca e un sistema bancario digitale. E se i rischi ci sono, devono, o dovrebbero esserci, anche sistemi di controllo dei rischi (in senso lato): «*il fatto è*» parafrasando le parole di Feynman, «*che come far funzionare il potere di* [*blockchain* e delle valute virtuali] *è chiaro, come controllarlo non è affatto ovvio*»[146].

Pur senza cedere a tentazioni di "*over-regulation*", ciò potrebbe comportare, la implementazione di un corrispondente modello di vigilanza, anche regolamentare, adeguato al differente modello di "banca-*IT firm*" vigilata.

A tal fine, è quanto mai essenziale, imparare dalle "crisi" o meglio dai *failures*[147], specie se riguardanti le c.d. valute virtuali stabili (ad es. *Tether*), che pare rappresentino la attrazione, non tanto nascosta, delle banche come pure delle *IT firms*.

---

[145] Cfr. F. Sylos Labini, *Rischio e previsione*, cit., p. 51 ss.

[146] R. P. Feynman, *Il senso delle cose*, cit., p. 17.

[147] Per il significato di "*failure*" e di "*market failure*" si veda T. Padoa Schioppa, *Il governo dell'economia*, Bologna, 1997.

Criptovalute: l'approccio dei policy makers

Nicola De Giorgi

1. Premessa – 2. Virtual currency*: un primo timido approccio del legislatore europeo – 3. La normativa nazionale di recepimento – 4. La prospettiva delle istituzioni internazionali – 5. Osservazioni conclusive*

1. Premessa

Il termine "*Fintech*" (*Financial Technology*), di recente utilizzato anche dal legislatore nazionale in una norma primaria[1], indica l'innovazione finanziaria resa possibile dall'innovazione tecnologica.

Quest'ultima, in effetti, accompagna i recenti sviluppi nel mercato dell'intermediazione bancaria e finanziaria: dal credito (*crowd-funding* e *peer to peer lending*) ai servizi di pagamento (*instant payment*) e di consulenza (*robo-advisor*), oltre alle tecnologie di validazione decentrata delle transazioni (*block-chain* o DLT – *distributed ledger technology*), di identificazione biometrica (impronta digitale, retina o riconoscimento facciale), di supporto all'erogazione di servizi (*cloud computing* e *big data*).

Quasi tutte le banche di maggiori dimensioni stanno avviando progetti *Fintech*, in tal modo sollecitando specifiche attenzioni da parte delle Autorità che vigilano sui settori bancario, finanziario e dei pagamenti[2].

Riguardo alle cc.dd. criptovalute o valute virtuali, componenti importanti del mondo *Fintech*, si assiste da anni, unitamente alla loro proliferazione e diffusione, ad un ampio e crescente dibattito concernente tutti i principali aspetti, da quello tecnico a quello giuridico, per arrivare alle questioni regolatorie, fino ai possibili impatti sociali.

Per il giurista il tema delle criptovalute è reso complesso, tra l'altro, dall'alto grado di tecnicismo e dalla multiformità dell'oggetto: pare che al momento esistano più di 2.000 tipologie, con caratteristiche tecniche e di funzionamento anche molto differenti; non esiste una definizione scientifica condivisa del concetto di "criptovaluta" o "valuta virtuale"; la "materia" da esaminare, inoltre, evolve continuamente sotto gli occhi dell'interprete.

Nel presente contributo saranno svolte talune considerazioni prendendo spunto dalla normativa che, di recente, ha fornito una definizione di "valuta virtuale" e ha posto, nell'Unione europea e a livello nazionale, una prima

---

[1] Difatti, il d.l. 30.4.2019, n. 34, convertito in legge, con modificazioni, dall'art. 1, c. 1, l. 28.6.2019, n. 58, prevede una serie di iniziative volte alla sperimentazione delle "*attività di tecno-finanza (FinTech)*", istituendo al riguardo, presso il Ministero dell'economia e delle finanze, l'omonimo "Comitato FinTech", con il compito di "*individuare gli obiettivi, definire i programmi e porre in essere le azioni per favorire lo sviluppo della tecno-finanza, anche in cooperazione con soggetti esteri, nonché di formulare proposte di carattere normativo e agevolare il contatto degli operatori del settore con le istituzioni e con le autorità*" (cfr. art. 36, in particolare, commi 2-bis e 2-octies, d.l. n. 34/2019).

[2] La Banca d'Italia ha attivato il "canale *Fintech*", accessibile dal sito Internet dell'Istituto, con l'obiettivo di accompagnare i processi di innovazione nel campo dei servizi finanziari. Attraverso il nuovo punto di contatto – canale-fintech@bancaditalia.it – gli operatori (*start-up*, banche, intermediari finanziari) possono prospettare progetti connotati da caratteristiche di innovazione riferite sia alla tipologia dei servizi offerti sia alla tecnologia utilizzata per la loro fornitura. Inoltre, è prevista la pubblicazione nel sito di informazioni e documenti utili a seguire lo sviluppo del quadro di riferimento regolamentare, a livello nazionale e internazionale.

regolamentazione nel settore specifico dell'antiriciclaggio e dell'antiterrorismo (rispettivamente, Direttiva UE 2018/843 del Parlamento Europeo e del Consiglio del 30.5.2018 e d.lgs. 21.11.2017, n. 90).

Si può subito premettere che le poche regole introdotte non sembrano avere alle spalle una piena padronanza delle complesse *technicalities* sottese al fenomeno. Tuttavia, ciò non deve stupire, considerato che, al di là dell'euforia suscitata nell'ultimo decennio fin dal parto prodigioso del *Bitcoin* ad opera di Satoshi Nakamoto, le criptovalute hanno finora mostrato alcuni lati oscuri, che le rendono appetibili in contesti criminali e nel c.d. *deep web*. Non a caso, quindi, la prima preoccupazione del legislatore dell'Unione è stata quella di contenere il rischio che le valute virtuali possano aumentare i fenomeni di riciclaggio e finanziamento del terrorismo[3].

Peraltro, la prudenza non conduce alla demonizzazione del fenomeno, rispetto al quale è diffusa la convinzione che lo stesso possa portare, se opportunamente gestito, benefici notevoli in molti settori[4].

2. **Virtual currency***: un primo timido approccio del legislatore europeo*

In base alla definizione recentemente fornita dalla c.d. V Direttiva Antiriciclaggio, per *virtual currency* ("valuta virtuale" nella traduzione italiana) si intende una "*digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically*" (art. 1, Dir. UE 2018/843).

---

[3] Nelle premesse della Direttiva si fa riferimento alla possibilità che gruppi terroristici trasferiscano denaro verso il sistema finanziario dell'Unione o all'interno delle reti delle valute virtuali dissimulando i trasferimenti o beneficiando di un certo livello di anonimato (cfr. il considerando 8 nonché, ancora sul tema dell'anonimato, il considerando 9).

[4] La Banca Centrale Europea (BCE), ad esempio, pur nella consapevolezza dei possibili rischi connessi all'utilizzo e alla diffusione delle valute virtuali, riconosce che "*besides their drawbacks and disadvantages, VCS could also have some advantages over traditional payment solutions and specifically for payments within virtual communities/closed-loop environments and for cross-border payments. As such, it is not excluded that a new or improved VCS may be more successful in future. Therefore, the Eurosystem will continue monitoring developments, notably for payments-related aspects of VCS*" (Banca Centrale Europea, *Virtual Currency Schemes, a further analysis*, febbraio 2015, p. 33). Anche la Banca d'Italia ha recentemente sottolineato che la *distributed ledger technology* potrebbe portare benefici all'economia, ad es. se applicata alle attività di compensazione e regolamento degli acquisti di titoli finanziari (Banca D'Italia, *Rapporto sulla stabilità finanziaria*, 2018/1, aprile 2018).

Riguardo a tale definizione possono essere formulate talune considerazioni critiche, anche con il supporto dell'*Opinion* adottata il 12.10.2016 dalla Banca Centrale Europea (di seguito, BCE) sulla proposta di Direttiva[5].

Innanzitutto, deve essere posta particolare attenzione alla scelta della locuzione "*virtual currency*" per identificare le criptovalute.

Nella citata *Opinion* si nota che la definizione sembra derivare da quella – in effetti molto simile – utilizzata dall'European Banking Autority (EBA) nel documento pubblicato il 4.7.2014 con il titolo "*Opinion on Virtual Currencies*". Al riguardo, è da soggiungere che nel documento EBA si chiarisce opportunamente che "*virtual currencies*" (di seguito, anche, VCs o, al singolare, VC) è locuzione di uso comune e si ha cura di sottolineare, al tempo stesso, che l'uso del termine "*currency*" è *misleading* per varie ragioni, inclusa quella di suggerire l'idea, che non sempre trova poi effettivo riscontro, che sia comunque possibile cambiare le "*virtual currencies*" con altre *currencies*.

Il rilievo critico è sostanzialmente ripreso, sebbene sotto differenti profili, nell'*Opinion* della BCE, laddove si sottolinea che le VCs non costituiscono "*currencies from a Union perspective*", poiché in base ai Trattati istitutivi dell'Unione Europea e al Regolamento del Consiglio (EC) n. 974/98 l'unica *currency* degli Stati Membri dell'area euro è, appunto, l'euro. La BCE, pertanto, suggerisce la ricerca di una definizione più specifica, che chiarisca esplicitamente che le VCs "*are not legally established currencies or money*"[6].

Più in generale, nell'*Opinion* si consiglia, anche in considerazione di talune specifiche raccomandazioni adottate in precedenza dalla *Financial Action Task Force* (FATF), di evitare di dare l'impressione che il legislatore europeo promuova l'uso delle "*privately established digital currencies*".

Il testo finale della definizione in esame non appare del tutto coerente a quanto osservato dalla BCE.

In particolare, sebbene l'*Opinion* proponesse al riguardo uno specifico emendamento, non risulta espressamente chiarito che le VCs non sono

---

[5] L'*Opinion* della BCE è stata adottata in base agli artt. 127(4) e 282(5) del Trattato sul Funzionamento dell'Unione Europea (TFUE), sul presupposto che la materia della Direttiva ricada nell'ambito delle competenze della BCE. Nel preambolo dell'*Opinion* si afferma che il tema delle valute virtuali potrebbe avere implicazioni connesse ai compiti di sorveglianza sul sistema dei pagamenti, nonché alle competenze della BCE concernenti la stabilità del sistema finanziario e l'autorizzazione all'emissione di euro nell'Unione.

[6] In effetti, sia pure ad un'analisi superficiale, risultano al momento poco riconoscibili nelle VCs – se non in modo parziale o sporadico – le funzioni tipiche normalmente attribuite alla "*currency*" (mezzo di pagamento, unità di conto e riserva di valore). Create da soggetti privati che operano sul web, le VCs non sono emesse o garantite da una banca centrale o da un'autorità pubblica e generalmente non sono regolamentate. Inoltre, non hanno corso legale e, pertanto, non devono per legge essere obbligatoriamente accettate per l'estinzione delle obbligazioni pecuniarie, ma possono essere utilizzate per acquistare beni o servizi solo se il venditore è disponibile ad accettarle.

"*legally established currencies or money*" e la Direttiva si limita a fornire, nel considerando n. 8, una spiegazione del concetto di "*fiat currency*" (declinato in "*coins and banknotes that are designated as legal tender and electronic money, of a country, accepted as a medium of exchange in the issuing country*"), senza soffermarsi sulle differenze tra le due tipologie di *currencies* (risalto viene dato, invece, nel considerando n. 10, alla distinzione tra VC e moneta elettronica).

Più radicalmente, si potrebbe osservare che – rispetto a un fenomeno complesso, nuovo e foriero di rischi, evidenziati da tempo in pubblicazioni ufficiali – la mera scelta della locuzione "*virtual currency*", tra le altre utilizzabili come alternativa alla prima (ad esempio "*cryptoasset*" o "*virtual asset*"[7]), possa avere l'effetto di promuovere l'uso delle stesse, già solo per la forza suggestiva del termine "*currency*".

Tale sensazione potrebbe essere addirittura rafforzata dal fatto che, in base alla direttiva in esame, la VC è innanzitutto una "*digital representation of value*". In effetti, il termine "*value*", a prescindere dai suoi numerosi significati, ha una connotazione semantica indubbiamente positiva, che evoca quindi l'idea di un bene utile, apprezzabile (e quindi *di valore*). In tal modo, sembra darsi *a priori* una valutazione, che potrebbe contribuire a suggestionare il potenziale utente. In buona sostanza, si potrebbe essere indotti a ritenere che se qualcosa ha, per definizione normativa, un valore, è del tutto normale che abbia un mercato e, soprattutto, un costo.

Dall'analisi complessiva del testo in esame, in verità, sembra potersi ritenere che il valore della VC, nell'ottica del legislatore europeo, deriverebbe unicamente dal fatto di essere "*accepted ... as a means of exchange*". L'utilizzo di tale formula (suggerita nella *Opinion* della BCE, a fronte del *wording* "*means of payments*" presente nella bozza iniziale della Direttiva) ha, a ben guardare, rilevanti conseguenze, poiché impone di individuare le VCs alla luce di considerazioni di fatto, relative non al prodotto in sé (e alle sue caratteristiche) ma al suo effettivo utilizzo negli scambi.

La scelta di tecnica normativa, dunque, non è stata quella di enucleare – dal variegato, complesso, in parte oscuro mondo delle VCs – un minimo

---

[7] Quest'ultima è la formulazione adottata dal Gruppo di Azione Finanziaria Internazionale (GAFI) nell'aggiornamento di ottobre 2018 alle Raccomandazioni per combattere il riciclaggio e il terrorismo (http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf).

denominatore comune a tutte le criptovalute relativo, appunto, alle loro caratteristiche intrinseche[8].

Sembrerebbe, quindi, che un *cryptoasset* non possa rientrare nell'alveo delle VCs se non dopo la prova del mercato: solo quelli effettivamente accettati come mezzi di scambio sono valute virtuali (sempre che, beninteso, soddisfino gli ulteriori requisiti previsti dalla definizione).

Evidentemente, tale criterio ermeneutico rischia di presentare difficoltà in sede applicativa, se non altro perché non sono chiare le condizioni al ricorrere delle quali possa ritenersi che una determinata VC sia accettata come mezzo di scambio.

Si tratta di difficoltà che, se non affrontate in sede di recepimento, potrebbero compromettere il raggiungimento dell'obbiettivo perseguito con l'intervento normativo. Difatti, considerato che la Direttiva è tesa, tra l'altro, a monitorare la diffusione e l'utilizzo delle VCs e che a tale fine viene estesa la platea dei soggetti tenuti agli obblighi *Anti Money Laundering/Combating the Financing*

---

[8] Sebbene ciascuna valuta virtuale presenti propri meccanismi di funzionamento, sono state enucleate talune caratteristiche comuni alla maggior parte di esse: sono create da un emittente privato (nel caso delle cc.dd. valute centralizzate) o, in via diffusa, da utenti che utilizzano *software* altamente sofisticati (nel caso delle cc.dd. valute decentralizzate); non sono fisicamente detenute dall'utente, ma sono movimentate attraverso un conto personalizzato noto come "portafoglio elettronico" (cd. *e-wallet*), che si può salvare sul proprio computer o su uno *smartphone*, o che può essere consultato via internet, al quale si accede grazie ad una password; possono essere acquistate con moneta tradizionale su una piattaforma di scambio ovvero ricevute *on line* direttamente da qualcuno che le possiede, per poi essere detenute sul "portafoglio elettronico"; utilizzando questo portafoglio i titolari possono effettuare acquisti presso esercizi commerciali o persone fisiche che accettano in "pagamento" le valute virtuali, effettuare rimesse in favore di altri soggetti titolari di portafogli di valute virtuali, nonché (nel caso di valute virtuali pienamente convertibili) riconvertirle in moneta legale; i titolari dei portafogli elettronici e i soggetti coinvolti nelle transazioni rimangono anonimi; le transazioni tramite le quali avvengono i trasferimenti di valuta virtuale sono tecnicamente irreversibili (Banca D'Italia, *Avvertenze sull'utilizzo delle cosiddette "valute virtuali"*, 2015).

of Terrorism (AML/CFT)[9], è necessario che i nuovi soggetti obbligati, ossia i "*providers engaged in exchange services between virtual currencies and fiat currencies*" e i "*custodian wallet providers*"[10], possano essere individuati senza incertezze.

Tuttavia, entrambe le categorie di operatori (sia quelli che "scambiano" che quelli che forniscono i *wallet*s) vengono individuati attraverso la verifica del fatto che i servizi da essi offerti abbiano ad oggetto *virtual currencies*. Sarebbe opportuno, quindi, pervenire a un'interpretazione univoca e condivisa del concetto di VCs, per evitare che, in difetto, possa risultare incerta anche l'individuazione dei soggetti obbligati.

3. La normativa nazionale di recepimento

Il legislatore nazionale, con il d.lgs. 25.5.2017, n. 90, ha introdotto una prima forma di regolamentazione delle valute virtuali, anticipando la successiva adozione della V Direttiva AML/CFT ma, evidentemente, tenendo conto di quella che era all'epoca la proposta di direttiva. La trasposizione è stata successivamente completata con il d.lgs. 4.10.2019, n. 125.

---

[9] Nelle premesse della Direttiva si chiarisce che, al fine di prevenire e ridurre l'utilizzo di VCs per attività illecite, è necessario includere nell'ambito di applicazione della disciplina antiriciclaggio e antiterrorismo i soggetti che forniscono servizi di scambio tra *virtual currency* e *fiat currency* e i fornitori dei cc.dd. *e.wallet*. Al riguardo, il legislatore europeo mette in evidenza, tra l'altro, che "*i prestatori di servizi la cui attività consiste nella fornitura di servizi di cambio tra valute virtuali e valute aventi corso legale (vale a dire le monete e le banconote considerate a corso legale e la moneta elettronica di un paese, accettate quale mezzo di scambio nel paese emittente) e i prestatori di servizi di portafoglio digitale non sono soggetti all'obbligo dell'Unione di individuare le attività sospette*"; che "*pertanto, i gruppi terroristici possono essere in grado di trasferire denaro verso il sistema finanziario dell'Unione o all'interno delle reti delle valute virtuali dissimulando i trasferimenti o beneficiando di un certo livello di anonimato su queste piattaforme*"; che, di conseguenza, la diffusione della valuta virtuale deve essere oggetto di monitoraggio "*equilibrato e proporzionale*", come tale idoneo a salvaguardare "*i progressi tecnici e l'elevato livello di trasparenza raggiunto in materia di finanziamenti alternativi e imprenditorialità sociale*" (cfr. considerando n. 8). Degno di nota è anche il successivo considerando n. 9, nel quale si sottolinea che "*l'anonimato delle valute virtuali ne consente il potenziale uso improprio per scopi criminali. L'inclusione dei prestatori di servizi la cui attività consiste nella fornitura di servizi di cambio tra valute virtuali e valute reali e dei prestatori di servizi di portafoglio digitale non risolve completamente il problema dell'anonimato delle operazioni in valuta virtuale: infatti, poiché gli utenti possono effettuare operazioni anche senza ricorrere a tali prestatori, gran parte dell'ambiente delle valute virtuali rimarrà caratterizzato dall'anonimato. Per contrastare i rischi legati all'anonimato, le unità nazionali di informazione finanziaria (FIU) dovrebbero poter ottenere informazioni che consentano loro di associare gli indirizzi della valuta virtuale all'identità del proprietario di tale valuta. Occorre inoltre esaminare ulteriormente la possibilità di consentire agli utenti di presentare, su base volontaria, un'autodichiarazione alle autorità designate*".

[10] In base all'art. 1 della Direttiva, "*custodian wallet provider means an entity that provides services to safeguard private cryptographic keys on behalf of its customers, to hold, store and transfer virtual currencies*".

Innanzitutto, con alcune modifiche al d.lgs. 21.11.2007, n. 231, sono state fornite le definizioni di "valuta virtuale"[11], di "prestatori di servizi relativi all'utilizzo di valuta virtuale"[12] e di "prestatori di servizi di portafoglio digitale"[13]. I due gruppi di *prestatori* sopra menzionati sono stati inclusi tra i "soggetti obbligati" agli adempimenti antiriciclaggio di adeguata verifica della clientela e segnalazione di operazioni sospette[14].

Inoltre, intervenendo sul d.lgs. 13.8.2010, n. 141, è stata introdotta una prima disciplina della valuta virtuale, prevedendo un meccanismo di segnalazione/monitoraggio/iscrizione che ruota intorno all'esistenza di un preciso obbligo di comunicazione a carico dei suddetti *prestatori*, i quali sono tenuti a comunicare al Ministero dell'economia e delle finanze la propria operatività sul territorio nazionale.

Un regolamento del Ministero dell'economia e delle finanze fornirà la disciplina attuativa[15]. La bozza di regolamento, resa disponibile in consultazione pubblica nel febbraio 2018, appare ispirata all'obiettivo di realizzare una prima rilevazione sistematica del fenomeno, a partire dalla consistenza numerica degli operatori del settore che, a regime, dovrebbero poi iscriversi in una sezione speciale del registro tenuto dall'Organismo degli Agenti e dei Mediatori (OAM) previsto dall'art. 128-*undecies*, TUB.

Se, dunque, il legislatore nazionale, al pari di quello europeo, non ha sciolto i dubbi concernenti la natura giuridica della valuta virtuale, non si è limitato, tuttavia, a dettare regole confinate ai settori specifici dell'antiriciclaggio e dell'antiterrorismo, avendo invece fornito indicazioni che sembrano avere un valore più generale, come si nota già dal fatto che è stato modificato non solo il d.lgs. n. 231/2007 ma anche l'art. 17-*bis* del d.lgs. n. 141/2010, relativo all'attività di cambiavalute.

In buona sostanza, il legislatore fornisce una prima disciplina attinente non tanto all'oggetto – ossia alla valuta virtuale – quanto ai soggetti che prestano specifici servizi in valuta virtuale, i quali, analogamente a quelli

---

[11] Per "valuta virtuale" si intende la "*rappresentazione digitale di valore, non emessa né garantita 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 o per finalità di investimento e trasferita, archiviata e negoziata elettronicamente*" (art. 1, c. 2, lett. qq), d.lgs. 21.11.2007, n. 231, come modificato dall'art. 1, c. 1, del d.lgs. 25.5.2017, n. 90, e successivamente dall'art. 1, c. 1, d.lgs. 4.10.2019, n. 125).

[12] Come definito dall'art. 1, c. 2, lett. ff), d.lgs. 21.11.2007, n. 231, ossia "*ogni persona fisica o giuridica che fornisce a terzi, a titolo professionale, servizi funzionali all'utilizzo, allo scambio, alla conservazione di valuta virtuale e alla loro conversione da ovvero in valute aventi corso legale*". Non è del tutto chiaro se la definizione in esame, che pur menziona la fornitura di servizi di "conservazione", sia idonea ad includere nella categoria anche i "*digital wallet providers*" ai quali fa riferimento la direttiva.

[13] Ossia "*ogni persona fisica o giuridica che fornisce, a terzi, a titolo professionale, anche on line, servizi di salvaguardia di chiavi crittografiche private per conto dei propri clienti, al fine di detenere, memorizzare e trasferire valute virtuali*" (art. 1, c. 2, lett. ff-*bis*), d.lgs. n. 231/2007).

[14] Art. 3, c. 5, lett. i) e i-*bis*), d.lgs. 21.11.2007, n. 231. In particolare i prestatori di servizi in esame rientrano nella sotto-categoria degli "*operatori non finanziari*", ai sensi del predetto art. 3, c. 5.

[15] Al momento della stesura del presente scritto il regolamento del MEF non risulta ancora adottato.

che svolgono attività di cambiavalute, devono avere determinati requisiti in tema di cittadinanza o sede, sono tenuti a effettuare una specifica comunicazione (che, ai sensi del nuovo art. 17-*bis*, c. 8-*ter*, d.lgs. n. 141/2010, è "*condizione essenziale per l'esercizio legale dell'attività*"), vengono iscritti in una speciale sezione del registro tenuto dall'OAM e, oltre a tutto ciò, devono assolvere a taluni obblighi ex d.lgs. n. 231/2007.

Non è molto, in verità (sebbene l'approccio appaia comunque più articolato di quello adottato dal legislatore europeo)[16]. Restano dubbi importanti: solo per citarne alcuni, non è chiaro se tra i *prestatori* in esame possano ritenersi incluse alcune rilevanti tipologie di soggetti che operano in VCs (tra cui, ad esempio, i cc.dd. "*miners*", intesi come coloro che producono valuta virtuale) né se l'attività dei *prestatori* possa considerarsi lecita nelle ipotesi in cui risulti impossibile identificare il titolare effettivo delle VCs; sono indeterminate le conseguenze in caso di attività esercitata in difetto di comunicazione obbligatoria[17].

Si vedrà se alcune risposte a tali interrogativi arriveranno con la normativa di attuazione, il cui ritardo potrebbe giustificarsi con la necessità di elaborare soluzioni organiche e, auspicabilmente, coordinate (quanto meno) con gli altri Paesi dell'Unione.

4. La prospettiva delle istituzioni internazionali

Come accennato, la *ratio* ispiratrice delle novità introdotte dalla Direttiva UE 2018/843 è strettamente connessa al rischio che le VCs vengano utilizzate per commettere reati di riciclaggio o di finanziamento del terrorismo.

È opportuno rilevare che il pericolo anzidetto è solo uno dei vari rischi da tempo messi in evidenza da vari organismi e istituzioni nazionali e internazionali che, nell'attesa di poter verificare compiutamente le potenzialità delle tecnologie digitali sottostanti al funzionamento delle VCs, hanno manifestato atteggiamenti prudenti (e talvolta affatto critici) a fronte della rapida espansione delle stesse.

La Banca d'Italia, ad esempio, già in data 30.1.2015 ha pubblicato nel proprio sito Internet taluni documenti informativi – indirizzati agli utilizzatori o potenziali utilizzatori di valute virtuali nonché agli intermediari bancari e finanziari – nei quali si sottolinea tra l'altro che l'acquisto, il possesso o lo scambio di VCs può comportare rischi significativi, soprattutto per coloro che ne fanno

---

[16] Per una disamina delle ragioni che renderebbero opportuna l'introduzione di una più articolata disciplina europea delle valute virtuali, si veda il contributo di N. Ruccia in questo *Quaderno*.

[17] Approfondimenti in merito a talune delle questioni segnalate sono presenti in A. Caponera e C. Gola, "*Aspetti economici e regolamentari delle ‹‹cripto-attività››*", in *Questioni di economia e finanza*, Banca d'Italia, 2019.

uso senza disporre di un'adeguata conoscenza del fenomeno[18]. L'avvertenza è stata aggiornata nel marzo 2018, quando la Banca d'Italia ha diffuso un avviso prodotto dalle tre Autorità Europee di Vigilanza sul medesimo tema[19]. Anche l'Unità di informazione finanziaria per l'Italia (UIF, istituita presso la Banca d'Italia dal d.lgs. n. 231/2007) ha emesso un analogo documento informativo[20] e, recentemente, una nota di ausilio per l'individuazione di operazioni sospette connesse con valute virtuali.

Altre Autorità sovra nazionali, come detto, hanno preso posizione sul tema, a dimostrazione del fermento da esso sviluppato a livello globale[21].

Nel complesso, con specifico riferimento ai rischi, appare evidente che gli stessi non attengono unicamente alla possibilità di utilizzo delle VCs in operazioni di riciclaggio o finanziamento del terrorismo (o, comunque, per finalità criminali e illecite). Al riguardo, sono state rilevate, tra l'altro, le seguenti criticità[22]:

- carenza di informazioni (in assenza di obblighi informativi e di presidi di trasparenza può risultare difficile reperire indicazioni affidabili per comprendere il funzionamento, i costi, il valore e i rischi di ciascun tipo di valuta virtuale);
- assenza di adeguata tutela legale (l'acquisto, lo scambio e l'utilizzo di valute virtuali non sono assistiti da tutele legali analoghe a quelle che accompagnano le operazioni in valuta legale; le transazioni in valuta virtuale sono di solito tecnicamente irreversibili, spesso non sono supportate da un contratto né da procedure di reclamo e le controparti sono anonime);
- assenza di forme di garanzia delle somme depositate (in caso di condotta fraudolenta, di fallimento o cessazione di attività delle piattaforme di scambio non esistono tutele normative specifiche atte a coprire le perdite subite; analogamente, per le somme in valuta virtuale depositate presso

---

[18] Banca D'Italia, *Avvertenze sull'utilizzo delle cosiddette "valute virtuali"*, 2015. Nel documento (reperibile all'indirizzo https://www.bancaditalia.it/compiti/vigilanza/avvisi-pub/avvertenza-valute-virtuali/AVVERTENZA_VALUTE_VIRTUALI.pdf) vengono evidenziate numerose tipologie di rischio nell'utilizzo delle valute virtuali, peraltro con l'avvertenza che la velocità dell'evoluzione tecnologica comporta la possibile insorgenza di nuovi ulteriori pericoli.

[19] L'ESMA, l'EBA e l'EIOPA, ossia rispettivamente l'Autorità europea degli strumenti finanziari e dei mercati, l'Autorità bancaria europea e l'Autorità europea delle assicurazioni e delle pensioni aziendali e professionali.

[20] Unità Di Informazione Finanziaria per l'Italia, *Utilizzo anomalo di valute virtuali*, 30.1.2015.

[21] Di seguito sono citate alcune importanti pubblicazioni relative al tema delle valute virtuali: Banca Centrale Europea, *Virtual Currency Schemes*, ottobre 2012; Banca Centrale Europea, *Virtual Currency Schemes, a further analysis*, febbraio 2015; Financial Action Task Force, *Virtual Currencies, Guidance for a risk-based approach*, giugno 2015; Financial Action Task Force , *Virtual Currencies, Key Definitions and Potential AML/CFT Risks*, giugno 2014; European Banking Authority, *EBA Opinion on 'virtual currencies'*, luglio 2014; Bank for International Settlement, *Digital currencies*, novembre 2015.

[22] Banca D'Italia, *Avvertenze sull'utilizzo delle cosiddette "valute virtuali"*, 2015.

terzi non operano i tradizionali strumenti di tutela, quali i sistemi di garanzia dei depositi);

- possibili malfunzionamenti, attacchi informatici, smarrimento (la valuta virtuale archiviata nel "portafoglio elettronico" potrebbe andare persa a seguito di malfunzionamenti o attacchi informatici; anche in caso di smarrimento della password del portafoglio elettronico la perdita potrebbe essere permanente, in quanto non esistono autorità centrali che registrano le password o ne emettono altre sostitutive);

- elevata volatilità del valore (il valore delle valute virtuali è caratterizzato da una grande volatilità, anche a causa dei meccanismi di formazione dei prezzi – talora opachi – e dall'assenza di un'autorità centrale in grado di intervenire per stabilizzarne il valore; tale circostanza può comportare perdite anche di rilevante entità in caso di detenzione di valuta virtuale).

L'esperienza empirica ha dimostrato che si tratta di rischi concreti, materializzatisi talvolta con clamorosi attacchi informatici che hanno determinato perdite straordinarie[23].

Al riguardo, è anche da sottolineare il recente aggiornamento compiuto dalla Financial Action Task Force (FATF) alle proprie Raccomandazioni, teso a tenere conto dei nuovi rischi che la presenza delle valute virtuali porta nei settori del riciclaggio e del terrorismo[24].

5. Osservazioni conclusive

Le valute virtuali possono essere esaminate da molte angolazioni. Alcune di queste, come quelle tecnico-informatiche, risultano particolarmente impervie per

---

[23] In particolare, con riguardo ai rischi operativi *sub specie* di *cyber attacks*, A. Caponera e C. Gola, in "*Aspetti economici e regolamentari delle 'cripto-attività'*", cit., p. 17, riportano alcuni casi esemplificativi: nel 2012 sono stati rubati 24 mila *bitcoins* (per un valore all'epoca di 250 mila dollari) dalla piattaforma Bitfloor; nel 2013 la piattaforma giapponese Mt. Gox (uno dei primi operatori in "valute virtuali" inizialmente specializzato in giochi *on line*) ha subìto un attacco informatico con una perdita di 850 mila *bitcoins* (con un valore all'epoca di 450 milioni di dollari). Nel 2015 Bitstamp ha dichiarato un furto di 19 mila *bitcoins* (pari a 5 milioni di dollari). Nel 2016 un *exchange* (Bitfinex) basato a Hong Kong, che svolge anche attività di custodia, ha subito un attacco informatico con una perdita di 72 milioni di dollari. Nel gennaio 2018, Coincheck, una piattaforma giapponese, ha annunciato di aver subìto il furto di 260 mila *hot wallets* custoditi presso la piattaforma per un controvalore di circa 530 milioni di dollari. Altri eventi sono stati a danno di LoppX (febbraio 2018, 4,5 milioni di dollari), Titanium (aprile 2018, 21 milioni di dollari). La piattaforma italiana BitGrail ha subito un furto di 11 milioni di *Nano* (una "valuta virtuale" creata negli Stati Uniti), per un valore pari a 170 milioni di dollari. Il 5 gennaio 2019, la criptovaluta *Ethereum Classic* ha subito un attacco informatico (51% attack) che ha comportato la perdita di 53 mila ETC.

[24] Per approfondimenti sul tema, cfr. http://www.fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-assets.html

il giurista. Ma anche quelle di taglio legale sono complesse, come è dimostrato dall'incertezza che regna in merito alla stessa natura giuridica delle VCs[25].

In questo breve contributo sono state esposte riflessioni concernenti il dato positivo, partendo da elementi di base (come la definizione di "*virtual currency*") e associando ai rischi insiti nella diffusione delle VCs la scelta politico-legislativa di intervenire senza indugi nel settore AML/CFT.

A margine dei temi qui affrontati, o anche solo accennati, ve ne sono altri che meriterebbero di essere approfonditi, come quello relativo alle cc.dd. *Central Bank Digital Currencies* (moneta di banca centrale emessa al pubblico in forma digitale per pagamenti *retail*) o quello della possibile incidenza delle VCs sull'esercizio delle funzioni tipiche delle banche centrali (politica monetaria, sorveglianza sul sistema dei pagamenti, tutela della stabilità del sistema finanziario, vigilanza bancaria e finanziaria).

A tale ultimo riguardo, è stato espresso l'avviso che le valute virtuali potrebbero avere degli impatti anche sullo svolgimento dei predetti compiti, qualora aumentasse il volume emesso, l'accettazione di esse da parte degli utenti e la connessione con l'economia reale[26].

Anche alla luce di ciò, sarà necessario continuare ad esaminare con attenzione lo sviluppo delle criptovalute. Il mercato delle VCs ha ancora dimensioni contenute (la loro capitalizzazione globale è stimata ai primi di marzo 2019 in misura pari a 130 miliardi di dollari)[27], tuttavia l'eventuale ingresso dei giganti del web nel settore potrebbe portare cambiamenti di straordinario rilievo.

---

[25] Al riguardo, possono segnalarsi due recenti *papers*, particolarmente accurati. Il primo, pubblicato dall'Autorità Europea degli strumenti finanziari e dei mercati, esamina la possibilità che talune specifiche VCs siano considerate, dal punto di vista giuridico, strumenti finanziari (European securities and markets authority, *Initial Coin Offerings and Crypto-Assets*, 9 January 2019). Il secondo, a cura dell'Autorità Bancaria Europea, valuta la possibilità di far rientrare alcune VCs nella nozione di moneta elettronica (European banking authority, *Report with advice for the European Commission on Crypto-assets*, 9 January 2019).

[26] Cfr. Banca Centrale Europea, *Virtual Currency schemes, a further analysis*, 2015. Nel documento si afferma, in particolare, che "*in theory, VCS could have an impact on monetary policy and price stability. However, it was concluded that VCS did not pose a risk for price stability in practice, provided that the issuance volume of virtual currency continued to be stable and their usage low*" e inoltre che "*conceptually, VCS could jeopardise financial stability. However, it was considered that they were inherently unstable, but did not jeopardise financial stability given their limited connection to the real economy (i.e. the exchange rates and the exchange markets), the low volumes traded and the lack of wide user acceptance*" (p. 26). Con specifico riguardo alla politica monetaria, è stato osservato che "*if the adoption and use of digital currencies were to increase significantly, the demand for existing monetary aggregates and the conduct of monetary policy could be affected ... The effect of digital currencies on the implementation of monetary policy will depend on the change in demand for bank reserves and the degree of economic and financial interconnection between the users of sovereign currency and the users of digital currencies*" (Bank for International Settlements, *Digital currencies*, 2015, p. 16).

[27] Il dato è tratto da A. Caponera e C. Gola, "*Aspetti economici e regolamentari delle 'cripto-attività'*", cit., p. 14.

Si potrebbe arrivare in breve ad avere circuiti di regolamento delle transazioni economiche diversi e coesistenti rispetto agli attuali sistemi di pagamento. Se così fosse, sarebbe verosimile aspettarsi interventi normativi ben più incisivi di quelli attuati fino ad ora.

In questo contesto, caratterizzato da complessità e mutevolezza, il giurista è chiamato ad un esercizio non solo di aggiornamento e, al tempo stesso, visione complessiva, ma anche di estrema elasticità, poiché non si può escludere che il futuro imporrà di guardare al *Fintech* e alle valute virtuali con una sensibilità nuova, che possa confrontarsi, se del caso, con nuovi istituti e categorie del diritto.

Criptovalute e modelli di sorveglianza

Nicola Ruccia

1. La necessità di disciplinare la materia – 2. La mancanza di una posizione di vertice in seno all'UEM – 3. Le criptovalute negli Stati membri dell'UEM – 4. La possibile interazione tra le Autorità nazionali – 5. Osservazioni conclusive

1. La necessità di disciplinare la materia

Le valute virtuali, nel diritto dell'Unione europea, non sono oggetto di una specifica disciplina. Ciò non ha compromesso, in ogni caso, la loro crescente diffusione che appare giustificata, quantomeno in parte, dall'insofferenza dei loro utilizzatori verso la regolazione del sistema economico ed il controllo sullo stesso operati dalle autorità pubbliche, sia interne che sovranazionali. Siffatta insofferenza trae origine dal c.d. movimento della *Cryptoanarchy*. Quest'ultimo – nato negli Stati Uniti quasi trent'anni fa e successivamente sviluppatosi anche in Europa – si poneva quale obiettivo quello di giungere, mediante la crittografia e l'anonimato, a un sistema di navigazione nella rete avulso da qualsiasi forma di controllo pubblico e, più in generale, da qualsiasi forma di ingerenza statale. I suoi sostenitori ritenevano, infatti, che le procedure c.d. *peer to peer* permettessero di raggiungere dei livelli di democraticizzazione dei mercati suscettibili finanche di destabilizzare il monopolio pubblico sul controllo di questi ultimi. In altri termini, attraverso il sistema delle criptovalute, per un verso, si sarebbe annullata la necessità dell'intermediazione di soggetti terzi nelle transazioni tra privati e, per altro verso, si sarebbe ridotta l'ingerenza pubblica sul mercato della moneta e nella gestione dei sistemi digitali di pagamento[1].

La disintermediazione nella raccolta dei capitali di rischio – propria delle operazioni effettuate con ricorso alle valute virtuali – contribuisce a quel processo di democraticizzazione finanziaria fondato sul potere della rete e caratterizzato da una considerevole riduzione dei costi di transazione, dall'implementazione della rapidità degli scambi e dall'eliminazione della possibilità di sequestro e confisca da parte di autorità pubbliche. Queste ultime, infatti, siccome non emettono, né garantiscono le valute virtuali, finiscono sostanzialmente per non governarle[2].

Occorre, inoltre, sottolineare quanto complesso sia l'inquadramento delle criptovalute all'interno del sistema monetario poiché esse, sebbene si connotino per un'origine telematica, possono essere considerate, all'occorrenza: contante virtuale, moneta complementare, titolo finanziario, bene immateriale oppure documento informatico. Diverse sono anche le funzioni ad esse assimilabili: mezzo di pagamento, di scambio, unità di conto oppure riserva di valore. Risulta, pertanto, alquanto difficoltoso procedere all'individuazione della disciplina da applicarsi – fondamentalmente sotto il profilo dell'antiriciclaggio, tributario e di monitoraggio fiscale, di contrasto dell'abusivismo nell'intermediazione creditizia e finanziaria, della tutela del contraente e del consumatore – all'attività degli operatori nel mercato

---

[1] L. D'Agostino, *Operazioni di emissione, cambio e trasferimento di criptovaluta: considerazioni sui profili di esercizio (abusivo) di attività finanziaria a seguito dell'emanazione del D. Lgs. 90/2017*, www.dirittobancario.it, 1/2018, p. 6.

[2] F. Di Vizio, *Lo statuto giuridico delle valute virtuali: le discipline e i controlli. Tra oro digitale ed ircocervo indomito*, Atti del Convegno annuale «Bitgeneration. *Criptovalute tra tecnologia, legalità e libertà*», Fondazione Cav. Lav. Carlo Pesenti e Fondazione Corriere della Sera, Milano, 15 marzo 2018, reperibile *on line*, p. 2.

delle valute virtuali, oltre che alle loro relazioni, anche con riferimento alle possibili interferenze con le monete correnti e con l'economia reale.

Appare possibile rinvenire, nella suddetta difficoltà – e non nella volontà di trascurare l'importanza di un fenomeno via via crescente – la carenza del legislatore dell'Unione nel disciplinare la materia in esame in maniera puntuale e articolata. L'unico riferimento normativo in vigore, infatti, è la c.d. V Direttiva antiriciclaggio[3]. Anche la Corte di giustizia, considerata il motore dell'integrazione europea, sinora si è espressa esclusivamente sui profili tributari delle criptovalute[4]. Esse, peraltro – data la loro configurazione – possono funzionare senza sostegno istituzionale ed assumere una dimensione mondiale poiché sono intrinsecamente senza frontiere. Pertanto, occorre domandarsi se, e in quale misura, la loro regolamentazione possa essere efficace.

Innanzitutto, occorre osservare se gli interventi regolamentari possano incidere sui mercati delle criptovalute. Le analisi condotte a tal proposito hanno evidenziato quattro risultati[5]. *In primis*, le notizie di maggiore impatto sono quelle concernenti il loro status giuridico. In generale, le informazioni in base alle quali esse non sono considerate come valute, al pari di quelle sul loro possibile inserimento in leggi sui mercati mobiliari, hanno implicazioni negative. Diversamente, le notizie concernenti nuovi possibili quadri normativi incentrati su di esse oltre che sulle c.d. *initial coin offering* (ICO) determinano rialzi significativi sui mercati. Inoltre, le notizie concernenti l'adozione di misure contro il riciclaggio di denaro e il finanziamento del terrorismo – c.d. *anti-money laundering and countering the financing of terrorism* (AML/CFT) – e quelle sulla limitazione della loro interoperabilità con il sistema finanziario regolamentato hanno un impatto negativo sui rispettivi mercati. Invece, gli avvertimenti generali delle autorità non determinano conseguenze sui mercati, al pari delle notizie sulla possibilità dell'emissione delle c.d. *central bank digital currency* (CBDC), ossia le valute digitali delle banche centrali. Infine, si riscontrano delle differenze di prezzo tra le giurisdizioni, il che manifesta una certa segmentazione del mercato. In definitiva, non sembra che lo sviluppo di un quadro normativo implichi,

---

[3] 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 e che modifica le direttive 2009/138/CE e 2013/36/UE. Per una disamina della direttiva e della disciplina italiana di recepimento, si veda in questo *Quaderno* il contributo di N. De giorgi. Sulla direttiva (UE) 2018/843, cfr. anche, *ex multis*, R. Razzante, Bitcoin *e criptovalute. Profili fiscali, giuridici e finanziari*, Rimini, 2018; P.M. Sabella, *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*, in www.dpce.it, 2018, p. 549.

[4] Sentenza della Corte del 22 ottobre 2015, in causa C-264/14, *Skatteverket* c. *Hedquist*, ECLI:EU:C:2015:718. Sul punto cfr. G. Capaccioli, *Nota a sentenza della Corte di Giustizia UE C-264/14,* in *Il Fisco*, 2015 p. 4270 ss.; G. Costa, *Profili fiscali delle operazioni di acquisto e vendita di Bitcoin*, in *Riv. dott. comm.*, 2017, p. 467 ss.; M. L. Perugini, Distributed Ledger Technologies *e sistemi di* Blockchain*:* Digital Currency, Smart Contract *e altre applicazioni*, Frosinone, 2018, p. 116 ss.
Sui profili fiscali delle criptovalute cfr., in questo *Quaderno* il contributo di D. Conte.

[5] L'analisi più puntuale è stata compiuta da R. Auer e S. Claessens, *Regolamentazione delle criptovalute: valutazione delle reazioni dei mercati*, in *Rassegna trimestrale BRI*, settembre 2018, reperibile *on line*.

inevitabilmente, degli effetti negativi per il mercato. In particolare, le reazioni dei prezzi mostrano una netta preferenza per uno status giuridico preciso, sebbene all'interno di uno schema regolamentare non troppo rigido.

Attraverso l'attività di regolamentazione delle criptovalute si perseguirebbero obiettivi analoghi a quelli di altre attività o servizi finanziari. *Viceversa*, la determinazione, a livello dell'Unione, dell'applicabilità della vigente normativa sui servizi finanziari alla materia in esame permetterebbe di comprendere, effettivamente, la misura in cui la legislazione attuale affronta i rischi e sostiene le opportunità relative ai *cripto-assets* e ai *distributed ledger technology* (DLT)[6].

Siffatti obiettivi possono essere sintetizzati in tre macro-aree principali:

i) contrasto nell'impiego di risorse finanziarie per attività illecite;

ii) tutela dei consumatori e degli investitori;

iii) garanzia della stabilità finanziaria generale.

I suddetti obiettivi possono essere raggiunti attraverso diversi strumenti che possono essere classificati in tre categorie fondamentali:

i) Sorveglianza sulle imprese che forniscono accesso alle criptovalute. I consumatori e gli investitori, infatti, generalmente non le posseggono né le scambiano direttamente. Essi, piuttosto, si avvalgono dei c.d. *crypto-wallet* o di altri intermediari che le detengono. Pertanto, la regolamentazione potrebbe concernere i fornitori di cripto-infrastrutture. In altri termini, oltre alla V direttiva antiriciclaggio, potrebbe essere emanato un atto di diritto derivato dell'Unione concernente la tutela dei consumatori e degli investitori.

ii) Interazione delle criptovalute con gli operatori del mercato finanziario soggetti ai relativi regolamenti quali: banche commerciali, società di gestione di carte di credito e piattaforme di scambio. Tali operatori, infatti, permettono a singoli individui di convertire valute sovrane in quelle in esame e viceversa. Appare, pertanto, opportuna l'emanazione di norme sull'ammissibilità di queste ultime e dei prodotti correlati – quali derivati o *exchange traded fund* – sulle borse regolamentate. Le disposizioni da emanarsi, inoltre, dovrebbero definire le modalità attraverso cui i suddetti operatori sono autorizzati a operare sulle criptovalute per i propri clienti o per proprio conto, anche con riferimento al profilo fiscale.

iii) Definizione più chiara dello *status* giuridico delle criptovalute, con particolare riferimento ai profili della tutela dei consumatori, dei diritti di proprietà, oltre che al furto e alla vendita fraudolenta nonché all'uso

---

[6] European Banking Authority (EBA), *Report with advice for the European Commission on Crypto-Assets*, 9 gennaio 2019, reperibile *on line*, p. 9.

al dettaglio, specificando, ad esempio, i soggetti legittimati al loro scambio e le condizioni alle quali il medesimo scambio abbia luogo. Occorrerebbe, inoltre, definire se esse debbano essere considerate alla stessa stregua dei titoli – e quindi come strumenti negoziabili impiegati per la raccolta di fondi tramite una promessa di pagamento posticipata – con le conseguenti implicazioni in merito ai profili della loro regolamentazione e della sorveglianza. Esse potrebbero, comunque, essere considerate come attività generiche, con la conseguenza di poter essere detenute e scambiate, anche su mercati organizzati, senza dover essere sottoposte alle più rigide norme concernenti i mercati mobiliari e alla relativa sorveglianza.

2. La mancanza di una posizione di vertice in seno all'UEM

La mancanza, nel diritto dell'Unione, di una disciplina precipua concernente la materia in esame implica l'impossibilità di individuare, nel quadro istituzionale esistente, una posizione di vertice. Siffatta impossibilità, a sua volta, genera una serie di problemi che riguardano sia i singoli operatori nel relativo mercato, sia quest'ultimo considerato nel suo insieme[7]. Innanzitutto, si osserva come l'assenza di una pubblica autorità di regolamentazione e controllo della materia abbia quale conseguenza principale l'elevata volatilità delle criptovalute. In altri termini, il loro valore – a causa di un mercato sostanzialmente incontrollato, oppure in conseguenza dei rischi di *hackering* propri dei portafogli elettronici nonché di uno *status* giuridico non definito e obbligatorio delle strutture che dovrebbero garantire la loro riconversione in valuta corrente – potrebbe oscillare in misura considerevole[8]. In un sistema di scambi caratterizzato dall'anonimato degli operatori e privo di un'autorità preposta al controllo, inoltre, risulta alquanto difficile l'applicazione della normativa antiriciclaggio[9]. Infine, non appaiono condivisibili le opinioni di coloro che, subendo – *de facto* – l'incalzare

---

[7] A. Carstens, *Money in the Digital Age: What Role for Central Banks?* 2018, reperibile *on line*.
Cfr. anche D. Niepelt, *Central banking and Bitcoin: Not yet a threat*, in *CEPR policy portal*, 2016, reperibile *on line*; PE, *Criptocurrencies and monetary policies*, 2018, reperibile *on line*; M. Bech e R. Garrat, *Criptovalute delle banche centrali*, in *Rassegna trimestrale BRI*, settembre 2017, reperibile *on line*.

[8] EBA, *Warning to consumers on virtual currencies*, 12 dicembre 2013, reperibile *on line*; Id., *EBA Opinion on 'virtual currencies',* 4 luglio 2014, reperibile *on line*; PE, *European Parliamentary Research Service, Bitcoin – Market, Economics and Regulation*, 11 aprile 2014, reperibile *on line*; ESMA, *ESMA alerts firms involved in Initial Coin Offerings (ICOs) to the need to meet relevant regulatory requirements*, 13 novembre 2017, reperibile *on line*; ESMA, EBA and EIOPA *Warn consumers on the risks of Virtual Currencies*, 2018, reperibile *on line*; BCE, *Virtual Currencies Schemes*, 2012, reperibile *on line*; Banca d'Italia, *Rapporto sulla stabilità finanziaria*, 2018, reperibile *on line*.

[9] E. Simoncini, *Il* cyberlaundering*: la "nuova frontiera" del riciclaggio*, in *Riv. trim. dir. pen. econ.*, 2015, 4, p. 904.
Sui profili antiriciclaggio delle criptovalute, cfr., in questo *Quaderno*, il contributo di E. M. Mastropaolo.

della diffusione delle criptovalute, finiscono per considerare la loro liceità come presupposta e inevitabile[10].

Occorre domandarsi se l'emissione delle criptovalute sia un'operazione legittima o meno. Apparentemente, la risposta al quesito – sulla base del combinato disposto degli artt. 128 TFUE[11] e 16 Statuto SEBC[12], in base ai quali la BCE ha competenza esclusiva nell'emissione di banconote in euro nell'Unione – sarebbe negativa. Siffatta esclusività, tuttavia, concerne soltanto la moneta avente corso legale e non implica alcun divieto di conio di una moneta che, diversamente, non lo abbia. Lo spirito della norma sembra orientato alla protezione della fede pubblica piuttosto che al divieto di emissione di una moneta sprovvista del medesimo corso legale. Essa, più semplicemente, costituisce uno strumento di scambio convenzionale, istituito tra privati allo scopo di saldare il corrispettivo dell'acquisto di beni e servizi.

Il tentativo di considerare le criptovalute quale risultante del processo di dematerializzazione monetaria non appare convincente. Tale processo rappresenta soltanto un diverso sistema di circolazione della moneta, intesa nella sua tradizionale accezione che, a sua volta, è la conseguenza di una convenzione sociale o, meglio, di un'informazione. Quest'ultima, che si manifesta proprio nel biglietto di banca o nel dato telematico, è garantita dalla banca centrale che l'ha emessa, assicurandone la corrispondenza alla suddetta convenzione sociale. Tale corrispondenza, in altri termini, permette alla moneta di avere un valore di legge – mediante la citata autorità pubblica – che le conferisce la piena capacità solutoria dell'obbligazione cui è sottesa[13]. Occorre, infatti, sottolineare come il possesso di criptovaluta non accordi, di per sé, il diritto al pagamento del suo equivalente in moneta legale. Peraltro, qualora ciò fosse possibile – e ribadiamo, non lo è – risulterebbe sostanzialmente impossibile individuare un debitore emittente della criptovaluta. In ogni caso, appare evidente come possa escludersi un divieto legale alla creazione e all'impiego – su base privata – di un mezzo di pagamento alternativo alla moneta avente corso legale[14]. La mancanza di un'Autorità centrale preposta al monitoraggio delle criptovalute compromette, comunque, l'affidabilità delle stesse.

---

[10] Sul punto, cfr. la ricostruzione di E. Girino, *Criptovalute: un problema di legalità funzionale*, www.dirittobancario.it, 4/2018 p. 2.

[11] «*La Banca centrale europea ha il diritto esclusivo di autorizzare l'emissione di banconote in euro all'interno dell'Unione. La Banca centrale europea e le banche centrali nazionali possono emettere banconote. Le banconote emesse dalla Banca centrale europea e dalle banche centrali nazionali costituiscono le uniche banconote aventi corso legale nell'Unione*».

[12] «*Conformemente all'articolo 128, paragrafo 1, del trattato sul funzionamento dell'Unione europea, il consiglio direttivo ha il diritto esclusivo di autorizzare l'emissione di banconote in euro all'interno dell'Unione. La BCE e le banche centrali nazionali possono emettere banconote. Le banconote emesse dalla BCE e dalle banche centrali nazionali costituiscono le uniche banconote aventi corso legale nell'Unione*».

[13] E. Girino, *Criptovalute: un problema di legalità funzionale*, cit., p. 12.

[14] E. Girino, *Criptovalute: un problema di legalità funzionale*, cit., p. 13.

3. Le criprovalute negli Stati membri dell'UEM

Diverse Banche centrali nazionali e Autorità di vigilanza hanno evidenziato i rischi associati alla circolazione e all'impiego di criptovalute. Per esempio, la *Bundesanstalt für Finanzdienstleistungsaufsicht* (*BaFin*), la *Banque de France*, la *Nederlandsche Bank* e la *Banque Nationale de Belgique* hanno manifestato le loro preoccupazioni sul possibile impiego delle monete virtuali nel riciclaggio di denaro e nel finanziamento del terrorismo nonché sulla mancanza di una politica comune di vigilanza e sui rischi connessi alle loro oscillazioni[15]. La *Finlands Bank* ha comunicato che il *Bitcoin* – in particolare – non soddisfa i criteri propri di una valuta, né quelli di uno strumento di pagamento. Anche la *Sveriges Riksbank* ha osservato come il medesimo *Bitcoin* non soddisfi la definizione di valuta – poiché questa è emessa da una Banca centrale e riguarda un'area geografica ben definita. Il governo svedese, peraltro, ha deciso di tassare la suddetta moneta virtuale al pari di una risorsa finanziaria. Il Ministero delle Finanze tedesco, invece, la considera un'unità di conto. La *BaFin*, peraltro, ha aggiunto che le unità di conto che non hanno corso legale – come, appunto, i *Bitcoin* – si qualificano come strumenti finanziari.

Un certo numero di Autorità ha specificamente sottolineato che, sotto il profilo giuridico, il *Bitcoin* non è una valuta, non ha lo *status* di moneta avente corso legale e/o non soddisfa la definizione di strumento finanziario.

Inoltre, alcuni Stati membri stanno valutando la possibilità di concedere autorizzazioni e di organizzare, conseguentemente, un'attività di supervisione su alcuni servizi relativi ai *Bitcoin*. Per esempio, in Svezia, gli operatori concernenti i *VCS* hanno dovuto registrarsi presso l'Autorità di vigilanza finanziaria a partire dal 2012, dato l'impiego della moneta in oggetto come mezzo di pagamento. In Germania, la *BaFin* ha dichiarato che l'uso, la vendita e l'acquisto della suddetta moneta, di per sé, non necessitano di autorizzazione, sebbene questa possa essere richiesta per alcuni servizi aggiuntivi. Anche in Danimarca, i fornitori di servizi connessi ai *Bitcoin* non sono attualmente soggetti ad autorizzazione. In Francia, l'*Autorité de contrôle prudentiel et de résolution* ha precisato che, nel quadro di un'operazione di acquisto o di vendita della menzionata moneta contro un'altra avente corso legale, l'attività di intermediazione consistente nel ricevere fondi dall'acquirente della prima per trasferirli al venditore della stessa configura un'erogazione di un servizio di pagamento e che per l'esercizio abituale di tale attività è richiesta la relativa autorizzazione.

Appare, pertanto, evidente come la mancanza di una disciplina comune, nell'UEM, concernente le criptovalute, e di un'Autorità centrale preposta alla vigilanza sulle stesse, oltre a generare i menzionati problemi, ne implica un altro, ancora più complesso. Trattasi della scomposizione – con riferimento alle valute virtuali – del sistema dell'UEM stessa configurato con il Trattato di Maastricht. In altri termini, se il quadro normativo per gli Stati membri che hanno aderito alla moneta comune si caratterizza per la sua unitarietà e per una gerarchia istituzionale

---

[15] Informazioni reperibili sui siti *web* delle rispettive Autorità nazionali.

puntualmente definita dalle disposizioni primarie, i medesimi Stati membri sono liberi di intraprendere le azioni che reputano opportune e, di conseguenza, di legiferare in maniera assolutamente indipendente dall'Unione, in un settore – quello delle valute virtuali – sempre più connesso al sistema finanziario tradizionale.

La conseguenza dell'assenza di una disciplina comune è che il sistema finanziario dell'UEM, che include, in maniera unitaria, sia gli strumenti finanziari tradizionali sia quelli originati dalla rete, risulta integrato sotto il profilo geografico e, con riferimento agli strumenti ordinari, sotto quello giuridico ma è disarticolato con riferimento alle criptovalute.

In definitiva, se gli Stati membri dall'area euro hanno trasferito, *in toto*, la loro sovranità in materia monetaria a favore dell'UEM, con riferimento alle valute virtuali essi non hanno operato alcuna armonizzazione normativa. Le diverse situazioni interne, inoltre, hanno condotto le rispettive Autorità nazionali ad assumere, nei confronti delle valute in questione, degli atteggiamenti che, sebbene caratterizzati da una comune preoccupazione circa la loro diffusione, si sono rivelati alquanto eterogenei finendo per frammentare, sempre sotto il profilo giuridico, un quadro normativo già scarno e debole di per sé.

4. La possibile interazione tra le Autorità nazionali

Considerato che l'attuale assenza di norme europee non consente neppure una qualificazione giuridica uniforme delle criptovalute, determinando piuttosto una percezione differenziata della fattispecie da Stato membro a Stato membro, il primo presupposto ineludibile per una visione condivisa delle valute virtuali è l'introduzione, quanto meno a livello europeo, di una disciplina comune che, stante l'odierno scenario di frammentazione, dovrebbe concretarsi inizialmente in un'armonizzazione delle discipline legislative nazionali, da perseguire verosimilmente con lo strumento della direttiva.

Una volta armonizzate le singole discipline nazionali, potrebbe essere affrontato anche il problema della vigilanza sulle criptovalute e sui soggetti che vi operano.

A tal fine, una prima soluzione potrebbe contemplare un duplice intervento volto, da un lato, a rafforzare e specificare i poteri attribuiti alle Autorità nazionali e, dall'altro, a rafforzare la collaborazione fra le stesse in ragione della "internazionalità" del fenomeno. Anzi, è proprio questa caratteristica a rendere superflua la devoluzione di poteri a un organismo centrale dell'UEM, la cui competenza territoriale, comunque, non consentirebbe di presidiare in maniera ottimale la creazione e lo scambio di criptovalute negli Stati membri senza deroga.

L'istituzione di un ente incaricato di assicurare il coordinamento centrale richiederebbe l'emanazione di un atto di diritto derivato, in particolare un

regolamento, da adottarsi sulla base degli artt. 114 e 352 TFUE. La prima delle suddette norme, peraltro, è stata già impiegata per l'istituzione dell'ENISA[16] e delle agenzie che costituiscono il SEVIF[17].

Tuttavia, occorre sottolineare che l'art. 114 TFUE permette soltanto l'istituzione di organismi che contribuiscono alla realizzazione dei processi di armonizzazione nei casi in cui, allo scopo di agevolare l'attuazione e l'applicazione uniformi di atti fondati su tale base giuridica, risulti appropriata l'adozione di misure di accompagnamento e di inquadramento non vincolanti[18]. Mediante la norma in questione, pertanto, non potrebbero essere istituiti organismi suscettibili di emanare atti vincolanti a meno che gli stessi non contribuiscano all'armonizzazione del mercato interno, nell'accezione utilizzata dal diritto dell'Unione[19].

---

[16] Regolamento (CE) n. 460/2004 del Parlamento europeo e del Consiglio, del 10 marzo 2004, che istituisce l'Agenzia europea per la sicurezza delle reti e dell'informazione.

[17] Acronimo di Sistema europeo di vigilanza finanziaria, il SEVIF comprende: il Comitato europeo per il rischio sistemico (ESRB), l'Autorità bancaria europea (ABE), l'Autorità europea delle assicurazioni e delle pensioni aziendali e professionali (EIOPA), l'Autorità europea degli strumenti finanziari e dei mercati (ESMA), il Comitato congiunto delle Autorità europee di vigilanza (AEV) e le Autorità competenti o di vigilanza degli Stati membri indicate negli atti istitutivi delle AEV. Essi sono stati istituiti, rispettivamente, con Regolamento (UE) n. 1092/2010 del Parlamento europeo e del Consiglio, del 24 novembre 2010, relativo alla vigilanza macroprudenziale del sistema finanziario nell'Unione europea; Regolamento (UE) n. 1093/2010 del Parlamento europeo e del Consiglio, del 24 novembre 2010, che istituisce l'Autorità bancaria europea; Regolamento (UE) n. 1094/2010 del Parlamento europeo e del Consiglio, del 24 novembre 2010, che istituisce l'Autorità europea delle assicurazioni e delle pensioni aziendali e professionali; Regolamento (UE) n. 1095/2010 del Parlamento europeo e del Consiglio, del 24 novembre 2010, che istituisce l'Autorità europea degli strumenti finanziari e dei mercati; Direttiva 2010/78/UE del Parlamento europeo e del Consiglio, del 24 novembre 2010, recante modifica delle direttive 98/26/CE, 2002/87/CE, 2003/6/CE, 2003/41/CE, 2003/71/CE, 2004/39/CE, 2004/109/CE, 2005/60/CE, 2006/48/CE, 2006/49/CE e 2009/65/CE per quanto riguarda i poteri dell'Autorità bancaria europea, dell'Autorità europea delle assicurazioni e delle pensioni aziendali e professionali e dell'Autorità europea degli strumenti finanziari e dei mercati.

[18] Sentenza della Corte del 2 maggio 2006, *ENISA*, causa C-217/04, ECLI:EU:C:2006:279, p.to 44. Sulla questione cfr. M. Chamon, *EU Agencies: Legal and Political Limits to the Transformation of the EU*, Oxford, 2016, p. 52 ss.

[19] Alcune perplessità sul ricorso all'art. 114 TFUE quale fondamento giuridico delle Autorità istituite in occasione della crisi sono state espresse da N. Moloney, *EU Financial Market Regulation after the Global Financial Crisis: "More Europe" or More Risks?*, in *Common Market Law Review*, 2010, p. 1317 ss., p. 1341. Dello stesso avviso è E. Fahey, *Does the Emperor Have Financial Crisis Clothes? Reflections on the Legal Basis of the European Banking Authority*, in *The Modern Law Review*, 2011, p. 581 ss., p. 593. Di parere opposto sono F. Hänle, *Die neue Europäische Finanzaufsicht*, Hamburg, 2012, p. 40 ss., nonché A. Frank, *Die Rechtswirkungen der Leitlinien und Empfehlungen der Europäischen Weltpapier – und Markt aufsichts behörde,* Baden-Baden, 2012, p. 53 ss.
Il problema della vincolatività delle misure da adottare non sarebbe superato con sicurezza neppure ricorrendo all'art. 352 TFUE che, per lungo tempo, ha rappresentato la base giuridica per l'istituzione delle agenzie europee. Nell'ipotesi di cui si discute infatti, occorrerebbe fondarsi su un'interpretazione estensiva della disposizione *de qua*, in base alla quale l'istituzione di un organismo dotato di poteri specifici nella vigilanza prudenziale rientrerebbe nell'obiettivo del rafforzamento della coesione economica e sociale. Senza contare poi che il ricorso alla norma in oggetto non deve rappresentare il fondamento giuridico per ampliare la sfera dei poteri dell'Unione al di là dell'ambito generale risultante dal complesso delle disposizioni dei Trattati, con particolare riferimento a quelle che definiscono i compiti e le azioni dell'Unione medesima: cfr. sentenza del 3 settembre 2008, *Kadi e Al Barakaat International Foundation* c. *Consiglio e Commissione*, cause C-402/05 P e C-415/05 P, ECLI:EU:C:2008:461, p.to 203.

Ragioni, quindi, di carattere operativo e giuridico sconsigliano la creazione di un'Agenzia sovranazionale, dovendosi più proficuamente farsi capo alla sperimentata collaborazione fra le Autorità nazionali. Il disegno potrebbe essere costituito, come anticipato, dall'attribuzione ad esse di un ruolo di rilievo nella vigilanza prudenziale concernente le criptovalute dal momento che, sebbene il relativo mercato sia caratterizzato dall'anonimato degli operatori e dall'irrilevanza dell'area geografica di riferimento, proprio per questo è necessario "presidiarne" le varie zone in modo da controllarlo senza soluzione di continuità. A tal proposito, occorre sottolineare come l'efficacia del suddetto sistema – soprattutto a causa della natura delle operazioni che lo caratterizzano – possa essere garantita, pur con evidenti limiti, ma altra soluzione non pare divisarsi, soltanto attraverso il controllo dei "tratti europei" delle medesime operazioni, in un'azione coordinata fra le varie Autorità nazionali. A tale scopo, mutuando prassi e regole già adottate, potrebbero crearsi protocolli di intesa, documenti congiunti che armonizzino interventi e procedure e che aumentino lo scambio di informazioni, in modo da rendere più efficiente la risposta alle necessità di una vigilanza integrata.

Il ruolo delle Autorità nazionali appare fondamentale in tale contesto, dovendosene solo perfezionare la collaborazione reciproca, dal momento che soltanto l'integrazione degli interventi e delle regole può costituire un valido riferimento per un efficace controllo della tratta nazionale ed europea delle transazioni in criptovalute.

5. Osservazioni conclusive

Il Parlamento europeo, con la Risoluzione del 26 maggio 2016[20], ha rappresentato le opportunità e i rischi connessi alle valute virtuali. Esso, preliminarmente, ha osservato come non sia stata ancora formulata una definizione unitaria delle stesse le quali sono, talvolta, considerate denaro digitale oppure, come ritenuto dall'*European Banking Authority* (EBA), delle rappresentazioni di valore digitali che non sono emesse da una banca centrale o da un ente pubblico né sono, necessariamente, legate a una valuta a corso legale. Esse, piuttosto, sono accettate da persone giuridiche e fisiche quale mezzo di pagamento e possono essere trasferite, archiviate o scambiate elettronicamente.

Il documento, tra le opportunità offerte dalle valute virtuali, annovera la riduzione dei costi di transazione e di quelli operativi per i pagamenti – con particolare rilievo ai trasferimenti transfrontalieri di fondi – la riduzione del costo di accesso ai finanziamenti, anche in mancanza di conto bancario tradizionale, il potenziamento della resilienza e della velocità dei sistemi di pagamento dei beni e servizi nonché l'istituzione di sistemi che permettano di preservare la riservatezza degli operatori senza giungere all'anonimato totale.

---

[20] Risoluzione del Parlamento europeo del 26 maggio 2016 sulle valute virtuali (2016/2007(INI)).

Non sono sottaciuti, tuttavia, gli intrinseci rischi che esse comportano. I principali consistono nell'elevata volatilità delle valute virtuali e nelle possibili bolle speculative che possono generare, nella limitata capacità delle autorità preposte al controllo che potrebbe ostacolare la configurazione di apposite garanzie per gli investitori e i risparmiatori, nella mancanza di trasparenza delle relative operazioni e nella possibile instabilità finanziaria che potrebbe scaturire dalla loro diffusione.

Soprattutto, il Parlamento europeo constata l'incertezza giuridica che le concerne. Esso, tuttavia, si limita a proporre l'adozione di un quadro normativo proporzionato a livello dell'Unione, in modo da non compromettere i risultati attesi dall'innovazione apportata dalle criptovalute, né da aggiungere costi superflui per gli investitori e i risparmiatori nella fase iniziale di diffusione delle stesse. Tale quadro normativo dovrebbe avere come riferimenti degli importanti atti di diritto derivato dell'Unione, quali i regolamenti EMIR[21], CSDR[22] e MiFIR[23], nonché le direttive SFD[24], MiFID[25], OICVM[26] e GEFIA[27].

Sorprende come il Parlamento europeo non proponga l'emanazione di apposite regole concernenti la vigilanza sugli operatori nel settore delle criptovalute. Considerando l'importanza della sorveglianza, in generale, al fine di preservare la stabilità del sistema finanziario – peraltro riconosciuta proprio dal Parlamento europeo nel regolamento MSU[28] – e come esso, si è detto, annoveri tra i rischi connessi alle valute in esame quello di generare l'instabilità finanziaria, non si comprende l'assenza dell'auspicio all'adozione delle suddette regole.

Si ritiene, invece, che la disciplina della materia debba contenere, sin dalla prima fase della sua previsione, anche delle regole specifiche attinenti alla vigilanza prudenziale sugli operatori di tale settore. L'obiettivo di tali disposizioni sarebbe quello di garantire, in maniera integrata, la stabilità di un sistema finanziario in costante evoluzione che non può essere scisso tra un *coté traditionnel* (regolamentato del MSU) e un altro *virtuel*, privo di riferimenti normativi per non compromettere l'innovazione o aggiungere costi superflui nella fase di diffusione delle criptovalute.

---

[21] Regolamento (UE) n. 648/2012 del Parlamento europeo e del Consiglio, del 4 luglio 2012, sugli strumenti derivati OTC, le controparti centrali e i repertori di dati sulle negoziazioni.

[22] Regolamento (UE) n. 909/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, relativo al miglioramento del regolamento titoli nell'Unione europea e ai depositari centrali di titoli e recante modifica delle direttive 98/26/CE e 2014/65/UE e del regolamento (UE) n.236/2012.

[23] Regolamento (UE) n.600/2014 del Parlamento europeo e del Consiglio, del 15 maggio 2014, sui mercati degli strumenti finanziari e che modifica il regolamento (UE) n. 648/2012.

[24] Direttiva 98/26/CE del Parlamento europeo e del Consiglio del 19 maggio 1998 concernente il carattere definitivo del regolamento nei sistemi di pagamento e nei sistemi di regolamento titoli.

[25] Direttiva 2014/65/UE del Parlamento europeo e del Consiglio del 15 maggio 2014 relativa ai mercati degli strumenti finanziari e che modifica la direttiva 2002/92/CE e la direttiva 2011/61/UE.

[26] Direttiva 2009/65/CE del Parlamento europeo e del Consiglio, del 13 luglio 2009, concernente il coordinamento delle disposizioni legislative, regolamentari e amministrative in materia di taluni organismi d'investimento collettivo in valori mobiliari (OICVM).

[27] Direttiva 2011/61/UE del Parlamento europeo e del Consiglio, dell'8 giugno 2011, sui gestori di fondi di investimento alternativi, che modifica le direttive 2003/41/CE e 2009/65/CE e i regolamenti (CE) n.1060/2009 e (UE) n. 1095/2010.

[28] Regolamento 1024/2016, cit., considerando 5 e 6.

Criptovalute e l'applicazione della normativa antiriciclaggio

Eugenio Maria Mastropaolo

1. Innovazione digitale e teoria dei beni – 2. Le valute virtuali in relazione alla funzione della moneta: valute o beni – 3. Il potenziale uso delle valute virtuali rispetto ad un'operazione di riciclaggio o di finanziamento del terrorismo – 4. La risposta dell'ordinamento giuridico – 5. Considerazioni conclusive

1. Innovazione digitale e teoria dei beni

1.1. L'innovazione digitale ha permesso la creazione di nuove categorie di beni o ha comunque consentito di trasformare ciò che prima era rappresentato da oggetti, in qualcosa di virtuale basato non su di una trasposizione della realtà attraverso elementi materiali, ma attraverso numeri e dunque algoritmi capaci di tradurre una realtà in informazioni elettroniche ed algoritmi capaci di ritrasformare tali informazioni in qualcosa di disponibile per l'utente finale.

L'innovazione digitale apre a mio avviso ampi spazi di ricerca giuridica in materia di diritto dei beni (Libro III, Titolo I c.c.) ed il rapporto tra questi ed i diritti reali (Libro III c.c.). La questione è stata infatti affrontata più sotto il profilo della proprietà intellettuale e delle opere dell'ingegno ed artistiche che sotto il profilo della proprietà in sé e per sé considerata, riconducendo alle categorie esistenti ciò che appunto l'innovazione digitale ha prodotto, grazie fondamentalmente alla flessibilità del nostro diritto, limitando però in questo modo l'esigenza dell'elaborazione di un'ampia ed esaustiva teoria dei beni digitali e dei contratti che hanno per oggetto gli stessi.

Si pensi al fenomeno, possibile oggi grazie alla digitalizzazione e alla *blockchain,* della cd. "tokenizzazione"[1], cioè della riduzione ad un codicenumerico di qualunque diritto a valere su di un bene per renderlo scambiabile: vi sarebbe da chiedersi il senso di attributi dei beni quali "fungibilità" e/o "consumabilità", ma anche quali contratti riguardano tali beni e se ancora abbia senso parlare per es. del contratto di deposito in custodia ed amministrazione di strumenti finanziari dematerializzati rappresentati neanche più da una scrittura contabile (oggetto appunto della custodia), ma da un codice numerico assolutamente unico che identifichi il singolo strumento, il singolo diritto, il suo titolare e i precedenti titolari.

In buona sostanza, solo dopo un'attenta analisi sul diritto dei beni, effettivamente potrà essere possibile un'analisi delle tipologie contrattuali applicabili per la trasmissione e/o la conservazione e gestione di tali beni di nuova concezione.

1.2. Vivendo ancora in un mondo fatto di cose, la scarsa attenzione al fenomeno è però comprensibile: infatti a ben pensarci l'innovazione digitale ha cominciato ad incidere ormai da alcuni decenni su aspetti non banali della vita quotidiana, dalla lettura di un giornale alla possibilità di vivere un'esperienza virtuale o magnificata con emozioni simili a quelle reali, fino ad arrivare a riguardare aspetti più complessi quali la conservazione di ciò che si è ricavato e non si è speso, dunque il risparmio, ed i meccanismi attraverso i quali si vede riconosciuto un guadagno dalla vita lavorativa o dalla messa a frutto di beni

---

[1] Sulla questione si è soffermata CONSOB nel documento di discussione "*Le offerte iniziali e gli scambi di cripto-attività*" del 19 marzo 2019 disponibile sul sito istituzionale ricercando le seguenti parole chiave "CONSOB, *token*".

e diritti e si effettuano le spese. In tale ultimo caso l'innovazione digitale ha colpito l'elemento che caratterizza buona parte della vita umana: la moneta e fondamentalmente due delle sue tre funzioni, cioè la funzione solutoria e la funzione di riserva di valore.

Come tutti i processi umani complessi, l'innovazione digitale non emerge per caso e soprattutto non determina la scomparsa di ciò che prima esisteva: semplicemente si sovrappone e trasforma determinati fenomeni da reali ed analogici appunto a digitali, rendendo ancora più evidente l'applicabilità di teorie e meccanismi economici e finanziari. Sempre con riferimento alla moneta, si pensi a tutto il percorso fatto dalla moneta cartacea, alla moneta bancaria, passando per la moneta scritturale, per arrivare alla moneta elettronica, con l'intersecarsi di tali forme, concetti o definizioni della moneta per es. con il meccanismo del moltiplicatore dei depositi o la composizione delle varie forme di massa monetaria.

Applicata alla moneta, l'innovazione digitale ha così creato nuove forme di mezzi di pagamento e nuove modalità di esecuzione di un pagamento, non più rappresentate da monete metalliche, banconote o un credito scritturale verso una banca, ma rappresentate da dispositivi elettronici o sistemi elettronici di registrazione del valore monetario potenzialmente utilizzabile con funzione solutoria o con funzione di conservazione del risparmio accumulato.

L'emersione di nuove forme di moneta elettronica, cioè del valore monetario rappresentato e memorizzato in uno strumento di pagamento virtuale, cioè *software–based*, come un'applicazione istallata su di un telefono cellulare alla quale corrisponda una registrazione presso l'emittente, e l'emersione di valute virtuali, non sono altro che le due facce della stessa medaglia: l'utilizzo di strumenti digitali basati su algoritmi e chiavi crittografiche che permettano la detenzione, memorizzazione e trasferimento con funzione solutoria a qualunque titolo di valori monetari.

2. Le valute virtuali in relazione alla funzione della moneta: valute o beni

2.1. Le valute digitali e/o elettroniche diverse da quelle emesse da un'autorità pubblica alla quale sia riconosciuto per legge il diritto di battere/emettere moneta, sono definite in blocco "criptovalute" o "valute virtuali".

L'etimologia appare chiara: si tratta di valute – almeno le persone le percepiscono come tali – la cui emissione avviene privatamente, sulla base dell'adesione delle persone a regole stabilite e racchiuse in un algoritmo, la cui detenzione e custodia avviene attraverso la custodia delle chiavi digitali (basate sulla crittografia) attraverso le quali è possibile ricostruire la titolarità ed il valore rappresentato. Il loro trasferimento avviene tramite l'aggiunta di nuovi elementi alla stringa numerica di dati che rappresenta l'unità valutaria o suoi frazionamenti.

Sulla base di quanto sopra, vi è da chiedersi rispetto alle tre funzioni della moneta (intermediario di pagamento, numerario e riserva di valore), quali di queste funzioni la valuta virtuale assolve.

Al momento nessuna delle tre, anche se la risposta purtroppo non è certa ed è in funzione fondamentalmente di due fattori: uno intrinseco e l'altro non governabile. Il primo è che geneticamente le valute virtuali possono essere emesse fino ad un massimo numero di unità, per ragioni in parte connesse al fatto che non essendo collegate all'economia reale o finanziaria del paese emittente, un'espansione infinita della base monetaria determinerebbe meccanismi inflattivi ed in parte tecnologiche in quanto la stringa numerica di dati non può essere allungata all'infinito, in quanto la sua elaborazione presupporrebbe una potenza di calcolo altrettanto infinita. Il secondo fattore è quello temporale: qualunque definizione è infatti influenzata da un'analisi di ciò che al momento le valute virtuali rappresentano comunemente per coloro che le usano, a prescindere dal loro *status* giuridico (che segue e descrive la realtà economica).

Dato il ridotto utilizzo di una singola valuta virtuale (si pensi per es. al *bitcoin*), la sua accettazione è molto limitata (in certi casi appare più come una trovata pubblicitaria). Chi accetta di essere pagato in una determinata valuta virtuale, infatti, ha tre opzioni: potrebbe spenderla, anche se rimane il tema sul dove e per acquistare cosa oppure potrebbe convertirla in valuta avente corso legale, ma a questo punto tanto vale esser pagati direttamente con una valuta più agevolmente convertibile ed il cui rapporto di conversione rimanga più o meno costante nel tempo e non sia suscettibile di fluttuazioni di valore significativo oppure ancora potrebbe conservarla e dunque considerarla come una forma di risparmio, ma sul punto vale quanto sopra in riferimento alla scarsità dell'accettazione come mezzo di pagamento (si rammenta come economicamente il risparmio venga considerato una spesa differita nel tempo) e alla conservazione del valore nel tempo.

Data la fluttuazione del suo valore nel tempo, una valuta virtuale non assolve alle funzioni di numerario, cioè non riesce ad esprimere un valore chiaro nel tempo che consenta ad un potenziale acquirente di percepire il valore di un bene o servizio da acquistare, comparandolo con un bene o servizio analogo, soprattutto se la produzione o offerta degli stessi avvenga in tempi diversi (si pensi a due paia di scarpe: la differenza di prezzo potrebbe essere data dal differente valore delle stesse, ma anche dal fatto che un paio è stato prodotto in un momento diverso con costi diversi delle materie prime e delle unità di lavoro).

Data sempre la fluttuazione del suo valore nel tempo (più che l'ancora scarsa accettazione), una valuta virtuale non assolve alla funzione di riserva di valore, proprio perché chi desidera conservare quanto risparmiato (inteso come differenza tra quanto guadagnato e quanto speso), tra i tanti investimenti possibili andrà a selezionare quello che quanto meno non sia soggetto a svalutazione e a scarsa liquidabilità.

2.2. A prescindere quindi dall'elemento etimologico e dalla percezione del pubblico, le valute virtuali non sono considerabili economicamente "valute" o "monete", mentre invece possono essere considerate beni, in quanto cose che possono formare oggetto di diritti, secondo la definizione data dall'art. 810 c.c.

A questa definizione è giunto il Legislatore europeo nella Direttiva (UE) 2018/843 del Parlamento europeo e del Consiglio del 30 maggio 2018 (c.d. V Direttiva antiriciclaggio) che ha modificato la Direttiva (UE) 2015/849 del Parlamento europeo e del Consiglio del 20 maggio 2015 relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo (cd. IV Direttiva antiriciclaggio).

Il Legislatore europeo (art. 1 della V Direttiva antiriciclaggio che ha introdotto nell'elenco delle definizioni di cui all'art. 3, il punto n. 18) ha infatti definito le valute virtuali ai fini dell'uso delle stesse per operazioni di riciclaggio o finanziamento del terrorismo come la rappresentazione di un valore in forma digitale "che non è emessa o garantita da una banca centrale o da un ente pubblico, non è necessariamente legata a una valuta legalmente istituita, non possiede lo status giuridico di valuta o moneta, ma è accettata da persone fisiche e giuridiche come mezzo di scambio e può essere trasferita, memorizzata e scambiata elettronicamente".

La definizione offerta dal Legislatore europeo è estremamente interessante, ancorché strumentale rispetto all'ambito normativo dell'impianto legislativo antiriciclaggio e di contrasto del finanziamento del terrorismo, argomento del presente scritto: il Legislatore europeo infatti considera la valuta virtuale come un "valore" quindi qualcosa che può avere funzione di tesaurizzazione e dunque un bene che potrebbe mantenere un suo valore intrinseco nel tempo, proprio perché le persone lo usano come mezzo di scambio, ancorché la stessa valuta virtuale non abbia lo *status* giuridico di una "valuta" o di una "moneta" nel significato offerto dalla dottrina economica[2]. È chiaramente una soluzione intermedia che propende per una definizione delle valute virtuali come "beni" di valore (e non beni di consumo), ma che lascia ampi margini per intercettare modifiche comportamentali e fenomeni simili, economicamente rilevanti. Soprattutto è una soluzione molto equilibrata che come vedremo cerca di intervenire chirurgicamente rispetto ad un potenziale uso distorto (*rectius*, illecito) delle valute virtuali.

3. Il potenziale uso delle valute virtuali rispetto ad un'operazione di riciclaggio o di finanziamento del terrorismo

I comportamenti, i presupposti e le finalità perseguite da chi desideri porre in essere un'operazione di riciclaggio sono completamente diverse da chi intende porre in essere un'operazione di finanziamento del terrorismo.

---

[2] Sulla definizione di valuta virtuale adottata dalla V Direttiva antiriciclaggio, cfr. in questo *Quaderno* il contributo di N. De Giorgi.

3.1. In un'operazione di riciclaggio fondamentalmente chi la pone in essere cerca di convertire il prezzo o la refurtiva derivante dalla commissione di un reato in un altro valore rappresentato da un bene o da un valore monetario che nasconda la natura criminale originaria, attraverso l'anonimato o la presenza di prestanome, al fine di poterlo reimmettere nell'economia legale in un tempo successivo, senza che sorgano dubbi sulla sua origine.

Chi ricicla ha dunque fondamentalmente l'esigenza di nascondere la vera titolarità del bene (anonimato), di diminuire il rischio che l'intero prezzo o la refurtiva, ancorché convertiti, siano intercettati e di nascondere l'origine criminale dei fondi utilizzati per acquistare una valuta virtuale o l'origine criminale della valuta stessa (alcuni criminali soprattutto informatici chiedono di essere pagati in valute virtuali). Avendo ingenti somme a disposizione, chi ricicla non ha esigenze e limiti temporali: anzi più il tempo passa, più dell'origine criminale si perde la memoria.

Le valute virtuali hanno tutte queste caratteristiche: sono anonime o meglio la loro titolarità non è trasparente, infatti l'identità del titolare si nasconde facilmente dietro soprannomi, ancorché tutti i passaggi di titolarità siano registrati dalla stringa; permettono una differenziazione del rischio trattandosi fondamentalmente di beni virtuali intestabili a chiunque e trasferibili liberamente, alla stessa stregua del denaro contante; la loro conservazione e memorizzazione non è di facile accesso; dato il numero di transazioni che possono avere ad oggetto, l'origine dei fondi utilizzati per il loro acquisto o la loro stessa percezione criminale si possono perdere nel dettaglio dell'elemento digitale.

Chi ricicla invece non si cura dell'eventuale perdita di valore alla quale una determinata valuta virtuale potrebbe andare incontro. Non essendo valori guadagnati lecitamente (si pensi al prezzo della corruzione o di un fenomeno estorsivo), oppure essendo il frutto di illeciti il cui ritorno sull'investimento iniziale è moltiplicato per numeri importanti, un'eventuale perdita di valore è un'eventualità assolutamente sopportabile e messa in conto da chi voglia riciclare. Chi ricicla infatti non ragiona secondo criteri di economicità e logicità di un'operazione finanziaria, ma esattamente all'inverso. Egli sarà disponibile a pagare un qualunque prezzo pur di poter nascondere abilmente l'origine criminale dei fondi utilizzati per l'acquisto di una valuta virtuale oppure la sua percezione. L'eventualità che il prezzo dell'illecito e ciò in cui è stato convertito siano confiscati, rende più conveniente appunto l'accettazione del rischio che il non porre in essere l'operazione stessa.

3.2. Nel finanziamento del terrorismo al quale possono essere equiparate tutte le situazioni in cui una valuta virtuale è utilizzata al fine di aggirare sanzioni internazionali e/o embarghi e/o divieti e sanzioni amministrative o giudiziarie (si pensi al caso di *Wikileaks* dove per aggirare il blocco del suo finanziamento attraverso donazioni con carte di credito, i cui circuiti sono sostanzialmente riconducibili a soggetti collegati agli Stati Uniti d'America, i finanziatori hanno inviato alla stessa *bitcoin*), l'utilizzo di una valuta virtuale risponde ad esigenze molto diverse.

Anzitutto, le singole operazioni di conversione e/o trasferimento sono di piccolo ammontare, vuoi perché coloro che finanziano sono persone indottrinate/ideologizzate, tuttavia spesso dalle modeste condizioni economiche, vuoi perché in tal modo si dissimula l'uso finale delle valute virtuali, vuoi poi perché l'ausilio alle organizzazioni terroristiche, offerto da alcuni Stati o Paesi, avviene direttamente in natura (fondamentalmente armi acquistate con triangolazioni internazionali, scambio petrolio contro armi), vuoi infine perché logisticamente l'atto terroristico per essere impiantato, drammaticamente, non necessita di investimenti importanti (v. l'attentato di Nizza del luglio 2016 – dove è stato sufficiente rubare un camion), anzi sociologicamente risponde ad un principio di ottimizzazione delle risorse (poche persone coinvolte nell'organizzazione ed esecuzione dell'atto, il cui sviluppo deve essere eclatante al fine di ingenerare il massimo terrore).

Poi le organizzazioni terroristiche (*Al Qaeda*, *Daesh*, *Hitzbullah*, *Hamas*…) o singoli terroristi che si riconoscano in movimenti terroristici, non hanno necessariamente l'esigenza di convertire le valute virtuali in valori accettati nell'economia legale. Il terrorismo infatti utilizza direttamente ed attraverso una circolazione parallela le valute virtuali al fine di preparare le operazioni terroristiche, acquistando armi ed esplosivi, finanziando l'indottrinamento dei terroristi ed il mantenimento delle truppe presenti su determinati territori. Le esigenze dei terroristi presenti sul territorio dove andranno a colpire possono essere soddisfatte con pochi soldi ed attraverso un'immediata conversione delle valute virtuali in moneta corrente e valuta legale.

Infine, per le organizzazioni terroristiche mediorientali che commerciano illegalmente petrolio e prodotti oppiacei e che devono poter essere pagate aggirando l'ostacolo dei trasferimenti monetari verso tali Paesi e da tali Paesi di valute legali, le valute virtuali rappresentano un ottimo sistema.

Sulla base di queste considerazioni, le organizzazioni terroristiche e chi finanzia il terrorismo non si curano del fatto che le valute virtuali possano o meno mantenere immutato il valore nel tempo, in quanto lo scopo non è quello di tesaurizzare un valore, ma di spenderlo o di convertirlo immediatamente. La valuta virtuale dunque, nell'ambito del finanziamento del terrorismo, assume una funzione di intermediario di pagamento in un'economia illecita e parallela che risponde a logiche diverse da quelle di un soggetto che intenda riciclare. Infatti, nel finanziamento del terrorismo il fattore temporale è cruciale sotto un duplice aspetto: velocità del trasferimento ed accettazione nell'ambito dell'economia illegale (semmai saranno i venditori illegali di armi i soggetti interessati ad un'eventuale tesaurizzazione oppure alla reimmissione nell'economia lecita dei proventi derivanti dal commercio delle armi) e rapida convertibilità in moneta avente corso legale per finanziare le operazioni sul territorio da colpire.

Anche l'anonimato che le valute virtuali offrono ad un terrorista/organizzazione terroristica ha una valenza diversa rispetto ad un soggetto che intenda riciclare. Il terrorismo internazionale si è infatti evoluto (si parla di terrorismo internazionale 3.0). Slegate da qualunque istanza politica, le

organizzazioni terroristiche hanno fallito l'obiettivo di costituire entità statali indipendenti (v. Stato del *Daesh*), di conquistare uno Stato (v. Somalia, Iraq e Siria) o, comunque di istallare una presenza operativa (v. Libia) oppure condizionarne la vita (v. in parte Afganistan e Libano, meno la Nigeria ed ancora una volta Iraq e Somalia), dunque non è più necessario percepire finanziamenti dai paesi cc.dd. occidentali per proseguire la "lotta terroristica" in forma di guerriglia sovversiva in un determinato territorio, ma semmai è necessario finanziare il ritorno nei paesi di origine (dunque nei paesi cc.dd. occidentali) dei *foreign fighters*, di occultarne i trascorsi e di permettere loro di colpire nei territori obiettivo. Come il senso dell'operazione ("da" in inglese "*inbound*" contro "verso" in inglese "*outbound*"), anche l'anonimato ha un senso ed uno scopo: preservare l'identità del terrorista che colpirà e non preservare l'anonimato di colui che abbia simpatie per una determinata organizzazione terroristica in quanto ne condivide i "valori" e che quindi finanzia i terroristi all'estero a partire dagli stati cc.dd. occidentali.

4. La risposta dell'ordinamento giuridico

Rispetto a quanto sopra e al potenziale utilizzo delle valute virtuali per porre in essere un'operazione di riciclaggio o di finanziamento del terrorismo, l'ordinamento giuridico – inteso come impianto normativo europeo in materia di contrasto del riciclaggio e del finanziamento del terrorismo, rappresentato dalla IV Direttiva antiriciclaggio – ha reagito in maniera estensiva e non puntuale con una normativa dedicata.

Anzitutto, si è partiti dal riconoscere che sul punto esiste comunque un uso proprio delle valute virtuali. Infatti, l'VIII considerando della V Direttiva Antiriciclaggio ritiene che non vada vietato l'uso delle valute virtuali in assoluto. Se posto, tale divieto da un lato non farebbe altro che far ricadere nell'oscurità l'uso delle valute virtuali, che circolerebbero come monete parallele, quasi ritornando alle origini delle stesse (sociologicamente nate in contrapposizione o a prescindere dall'esistenza di un'autorità statale di emissione) ma dall'altro lato non farebbe altro che determinare un rallentamento dello sviluppo tecnologico e dell'uso di piattaforme alternative di finanziamento e della diffusione dell'imprenditorialità con ricadute sociali. Infatti, il Legislatore europeo ha preferito demandare alle autorità preposte (individuate nelle Financial Intelligence Unit (FIU) – o unità nazionali di informazione finanziaria; in Italia, la UIF) il monitoraggio circa l'uso delle valute virtuali, cioè l'analisi dei flussi da e verso le stesse provenienti dalle valute aventi corso legale e demandare sempre a tali autorità la possibilità di richiedere i codici digitali delle singole valute virtuali agli snodi che detengono tali informazioni. Di qui l'assoggettamento a vigilanza dei cc.dd. "prestatori di servizi di portafoglio digitale" cioè di quei soggetti che conservano le chiavi digitali private di accesso per conto dei propri clienti alla titolarità delle singole quantità di valuta virtuale, allo scopo di permetterne la detenzione, la memorizzazione (della titolarità e della quantità) ed il loro uso in termini di trasferibilità (v. la nuova definizione *sub* n. 19 all'art. 3 della IV Direttiva Antiriciclaggio).

Lo stesso Legislatore europeo in considerazione della situazione ha poi riconosciuto come l'utilizzo di tali snodi sia facoltativo e dunque la stessa volontà di regolamentazione potrebbe determinare un occultamento dell'utilizzo delle valute stesse o comunque l'impossibilità di intercettare la titolarità ed i trasferimenti delle valute virtuali in assenza dell'intervento di un prestatore di servizi di portafoglio digitale.

In funzione di tali analisi, la risposta ordinamentale è stata quella di non emanare norme particolari, ma di utilizzare l'impianto esistente di cui alla IV Direttiva Antiriciclaggio per contrastare l'uso illecito delle valute virtuali.

È stato quindi previsto come i cc.dd. snodi, cioè i prestatori di servizi di portafoglio digitale debbano essere soggetti a registrazione (cfr. nuovo testo dell'art. 47, Paragrafo 1, IV Direttiva Antiriciclaggio), il che non vuol dire assoggettare a vigilanza prudenziale tali soggetti, ma vuol dire fare in modo che gli stessi rispettino gli obblighi di adeguata verifica all'atto della registrazione digitale delle chiavi private relative alla titolarità della quantità "X" di valuta virtuale, che registrino le transazioni aventi ad oggetto la stessa, che conservino le informazioni e se del caso che inviino una segnalazione di operazioni e/o comportamenti sospetti. Rispetto a tale scelta, il Legislatore europeo a ben vedere, ha di fatto esteso sotto il profilo comportamentale, gli obblighi e le attività che qualunque soggetto deputato alla conservazione di un bene (per es. i depositari centrali di strumenti finanziari) dovrebbe adempiere o svolgere.

Poi sono stati estesi gli obblighi di identificazione di coloro che richiedano la prestazione di servizi di cambio (ovviamente in parte digitale) tra valute virtuali e valute aventi corso legale e viceversa, alla stessa stregua di qualunque attività di cambiavalute. Parallelamente sono stati estesi gli obblighi di conservazione delle informazioni e scritture contabili e segnalazione all'ingrosso delle operazioni di conversione da e verso le singole valute virtuali.

Infine, e mi appare la misura più innovativa, è stata prevista la possibilità in sede di prima relazione della Commissione europea al Parlamento europeo e al Consiglio (dovuta entro l'11 gennaio 2022) di accompagnare tale relazione con misure normative che eventualmente permettano l'istituzione di un registro centrale dei titolari di valute virtuali (partitamente per ciascuna valuta) e gli indirizzi dei portafogli ove siano detenute, memorizzate e a partire dai quali possano essere trasferite quantità di valuta virtuale.

5. Considerazioni conclusive

L'impressione che si ricava è un tentativo non troppo convinto da parte del Legislatore europeo di emanare una normativa di contrasto dell'uso delle valute virtuali a fini illeciti.

Gli strumenti prescelti e l'impianto normativo sembrano più volti a tracciare le operazioni tra diversi portafogli di valute virtuali e tra valute virtuali e valute

aventi corso legale o lo *status quo* (dunque la detenzione e la memorizzazione delle valute virtuali), che a contrastarne l'uso illecito.

Il tentativo appare più quello di isolare l'uso illecito dall'uso lecito delle valute virtuali, riducendo gli spazi del primo e di contaminazione del secondo, in maniera tale da dissuadere chi intenda procedere all'immissione nell'economia legale, rappresentata e fondata sulle valute aventi corso forzoso dei valori ricavati illecitamente e conservati in valute virtuali, che quello di contrastare l'uso della valuta virtuale per ricevere e pagare oppure scambiare il controvalore di beni o servizi prestati o ricevuti.

In fin dei conti, chi fa uso illecito delle valute virtuali, probabilmente continuerà in tale uso attraverso altri canali, appunto paralleli ed una loro circolazione, ancorché ampia, sarà comunque limitata a tale situazione. Chi invece ne fa un uso lecito, continuerà in tale uso senza che ne abbia a risentire dall'eventuale assoggettamento alla normativa di contrasto del riciclaggio e del finanziamento del terrorismo dei prestatori di portafoglio digitale o di cambiavalute. Chi al contrario dovesse mirare a mettere in comunicazione tali due "mondi", sarà invece soggetto ad identificazione e dunque analisi economico-finanziaria delle ragioni che al tempo determinarono la scelta di convertire valute aventi corso legale in valute virtuali (acquistandone una quantità) o di essere pagato in tali valute oppure che determinano la conversione attuale di valuta avente corso legale in valuta virtuale.

Difficilmente, ed è l'ultima considerazione, il tentativo del Legislatore europeo sarà contrastato sotto il profilo sociologico e comportamentale. Anche qui se è pur vero che le valute virtuali in parte nascono come forma "antitetica" all'autorità statale e di opposizione al "ceto bancario", una forma anarchica di autoregolamentazione democratica di aspetti economici, è anche vero che difficilmente gli utilizzatori attuali abbandoneranno appunto l'impiego delle valute virtuali più diffuse (*in primis* il *bitcoin*), in virtù del fatto che tale utilizzo divenga limitatamente soggetto ad una normativa specifica. Se dovesse avvenire il contrario (cioè un ritorno alle origini anarchiche e di contrasto dell'autorità statale e del ruolo delle banche), probabilmente (e potrebbe essere la scommessa del Legislatore europeo – v. XI considerando della V Direttiva Antiriciclaggio) le valute virtuali sarebbero ricacciate nell'uso limitato e potrebbero, dunque, essere trattate come valute locali o monete complementari che, per uso regionale o municipale e per numero di utenti, non portano rischi e non si prestano a fenomeni illeciti.

Criptovalute e l'applicazione delle disposizioni tributarie

Daniela Conte

1. Natura giuridica e regime impositivo delle c.d. "valute virtuali": lo stato dell'arte a legislazione vigente

La creazione delle valute virtuali e la loro crescente diffusione come strumento di negoziazione o di investimento ha favorito la nascita di un sistema economico-finanziario che, rispetto a quello tradizionale, si modella secondo uno schema innovativo ma "anarchico" perché deregolamentato[1]. Uno schema in cui non solo non è presente un'autorità centrale che emetta o controlli la moneta ma la stessa moneta, in quanto virtuale, non ha corso legale e il suo valore intrinseco, essendo regolato unicamente dai meccanismi della domanda e dell'offerta, è costantemente in fluttuazione a causa delle fortissime oscillazioni di prezzo. Ma vi è di più. Le operazioni di acquisto e di vendita di moneta virtuale, pur lasciando una traccia indelebile nel c.d. registro *blockchain*, garantiscono l'anonimato degli utenti e, dunque, si prestano ad operazioni illecite e a finalità criminali che dovrebbero essere contrastate con una specifica disciplina[2]. La regolamentazione delle valute virtuali rappresenta, tuttavia, per il legislatore italiano, un difficile "banco di prova" soprattutto se si considera che la mutevole natura delle criptovalute, cangiante a seconda del contesto di riferimento, ne impedisce la collocazione nelle tradizionali categorie giuridiche[3] con evidenti effetti non solo sotto il profilo civilistico[4] ma anche sotto il profilo fiscale, tenuto conto che dall'inquadramento giuridico delle valute virtuali in una determinata categoria dipendono le disposizioni applicabili per la tassazione dell'attività di produzione, utilizzo e scambio di criptovalute e per il monitoraggio fiscale[5]. Non è, dunque, un caso se la regolamentazione delle valute virtuali è stata "incasellata" nella più ampia disciplina del contrasto al fenomeno del riciclaggio e del finanziamento di attività illecite.

---

1 Per un approfondimento, cfr. G. Palumbo, *Le criptovalute: tra evasione fiscale e reati internazionali*, in *Dir. prat. trib.*, n. 1, 2019, p. 42; Id., *Il trattamento tributario dei bitcoin*, *ivi*, n. 1, 2016, p. 286 ss.; I. Bixio, *Le valute virtuali nella V Direttiva antiriciclaggio*, in *Corr. trib.*, n. 25, 2018, p. 1987 ss.

2 Su questi aspetti cfr. in questo *Quaderno* il contributo di E. Mastropaolo.

3 Se la collocazione sistematica del fenomeno (o di una qualsiasi delle sue manifestazioni) all'interno delle tradizionali categorie dogmatiche avrebbe senz'altro il pregio di consentire una più agevole ricostruzione dei suoi risvolti giuridici, occorre comunque guardarsi dal rischio "*di forzare un piolo quadrato in un foro rotondo*". In questi termini, G. Rinaldi, *Approcci normativi e qualificazione giuridica delle criptomonete*, in *Contr. impr*., n. 1, 2019, p. 260.

4 La questione assume rilevanza sotto il profilo dell'adempimento delle obbligazioni pecuniarie mediante tali schemi: è opinione comune che la valuta virtuale non abbia efficacia solutoria legale, ma solo su base convenzionale, cioè laddove il beneficiario accetti la predetta valuta come mezzo di estinzione dell'obbligazione pecuniaria. Manca, dunque, la qualificazione legale, da parte dell'autorità statale, quale mezzo di pagamento non rifiutabile dal creditore ed idoneo ad adempiere l'obbligazione pecuniaria liberando il debitore.

5 Per un approfondimento, C. Sacchetto e F. Montalcini, *Diritto tributario telematico*, Torino, 2015, p. 165 ss.

In occasione della recente riforma della disciplina antiriciclaggio[6], il legislatore italiano – nel dare attuazione alla IV Direttiva antiriciclaggio – è intervenuto, con il d.lgs. n. 90/2017, sulla disciplina contenuta nel d.lgs. n. 231/2007 introducendo nel nostro ordinamento la definizione di "valuta virtuale"[7]. In particolare, l'art. 1, comma 2, lett. qq), del d.lgs. n. 231/2007 ha definito la valuta

---

[6] Questa riforma è stata realizzata attraverso il recepimento, con il d.lgs n. 90/2017, della Direttiva n. 2015/849 del Parlamento europeo e del Consiglio del 20 maggio 2015 relativa alla "*prevenzione dell'uso del sistema finanziario ai fini di riciclaggio o finanziamento del terrorismo*" (c.d. IV Direttiva antiriciclaggio) che, come è noto, ha modificato il Regolamento UE n. 648/2012 del Parlamento europeo e del Consiglio nonché la Direttiva 2006/70/CE della Commissione.

[7] In tempi non sospetti, la Banca d'Italia, riprendendo quanto affermato dalla Banca Centrale Europea, aveva già definito, nella *Comunicazione* del 30 gennaio 2015, le valute virtuali come «rappresentazioni digitali di valore non emesse da una banca centrale o da un'autorità pubblica. Esse non sono necessariamente collegate a una valuta avente corso legale, ma sono utilizzate come mezzo di scambio o detenute a scopo di investimento e possono essere trasferite, archiviate e negoziate elettronicamente. Le valute virtuali non sono moneta legale e non devono essere confuse con la moneta elettronica». Nello stesso anno, la Banca d'Italia, nell'*Avvertenza sull'utilizzo delle cosiddette valute virtuali* (Roma, 30 gennaio 2015), aveva altresì indicato alcuni elementi distintivi che accomunano la maggior parte delle valute virtuali presenti sul mercato: sono create da un emittente privato (nel caso delle cc.dd. valute centralizzate) o, in via diffusa, da utenti che utilizzano *software* altamente sofisticati (nel caso delle cc.dd. valute decentralizzate, come il *bitcoin*); non sono fisicamente detenute dall'utente, ma sono movimentate attraverso un conto personalizzato noto come "portafoglio elettronico" (*wallet*); sono scambiate in apposite piattaforme, che offrono il servizio di conversione delle valute virtuali in moneta legale; possono essere acquistate con moneta tradizionale su tali piattaforme ovvero ricevute online direttamente da qualcuno che le possiede, per poi essere detenute su un "portafoglio elettronico"; sono utilizzate dai titolari per effettuare acquisti presso esercizi commerciali o persone fisiche che accettano le valute virtuali, rimesse in favore di altri soggetti titolari di portafogli di valute virtuali, nonché riconvertirle in moneta legale. Inoltre, i titolari dei portafogli elettronici e i soggetti coinvolti nelle transazioni rimangono anonimi e le transazioni tramite le quali vengono trasferite sono tecnicamente irreversibili, nel senso che una volta fatta la transazione non è possibile chiederne l'annullamento. Nella citata *Avvertenza*, la Banca d'Italia ha, inoltre, informato gli operatori dei rischi che tale tipo di attività può comportare. In particolare, riprendendo il parere dell'*European Banking Authority* del 2014 sulle valute virtuali (EBA/OP/2014/08, 4 luglio 2014), ha sottolineato che «i rischi individuati superano i possibili benefici che le VV potrebbero fornire ai loro utilizzatori, anche considerando i vantaggi in termini di costi e tempi di transazione e di inclusione finanziaria», scoraggiando le banche e gli altri intermediari vigilati dall'acquistare, detenere o vendere valute virtuali, in quanto, in assenza di adeguati presidi e di un quadro legale certo circa la natura giuridica delle valute virtuali, vi è il rischio di essere esposti a perdite, inficiando, di conseguenza, la consistenza del patrimonio di vigilanza e la stabilità stessa degli intermediari. Pertanto, gli intermediari sono invitati a considerare che «le concrete modalità di funzionamento degli schemi di VV possono integrare, nell'ordinamento nazionale, la violazione di disposizioni normative, penalmente sanzionate, che riservano l'esercizio della relativa attività ai soli soggetti legittimati (artt. 130, 131 TUB per l'attività bancaria e l'attività di raccolta del risparmio; art. 131-*ter* TUB per la prestazione di servizi di pagamento; art. 166 TUF, per la prestazione di servizi di investimento)». Inoltre, la Banca d'Italia ha raccomandato alle banche e agli altri intermediari di rendere edotti «i clienti, persone fisiche o giuridiche, operanti nel settore delle VV, prima di intraprendere operazioni della specie con essi». Ma vi è di più. A distanza di alcuni anni, la Banca d'Italia, nella sua seconda *Avvertenza per i consumatori sui rischi delle valute virtuali da parte delle Autorità europee* (Roma, 19 marzo 2018), sulla scorta di quanto diffuso al pubblico da parte dalle autorità di vigilanza europee (ESMA, EBA, EIOPA, ecc.) ha nuovamente avvertito i consumatori circa l'estrema rischiosità delle valute virtuali e la volatilità dei loro prezzi, la cui formazione è spesso non trasparente, sottolineando l'esistenza di chiari segnali di una bolla nei prezzi di queste valute o di strumenti finanziari a esse collegate e, al contempo, l'assenza di forme di protezione e di specifiche garanzie legali. Per ampi riferimenti, cfr. L. Donato (a cura di), *La riforma delle stazioni appaltanti. Ricerca della qualità e disciplina europea*, in *Quaderni di ricerca giuridica della Consulenza Legale della Banca d'Italia*, n. 80, febbraio 2016.

virtuale come «*la rappresentazione digitale di un valore, non emessa da una banca centrale o da un'autorità pubblica, non necessariamente collegata a una valuta avente corso legale, utilizzata come mezzo di scambio per l'acquisto di beni e servizi e trasferita, archiviata e negoziata elettronicamente*»[8].

Dal punto di vista della qualificazione giuridica, il legislatore non si è preoccupato di escludere espressamente, dalla predetta definizione, la presunta equiparazione fra valuta virtuale e moneta legale evidentemente perché ha ritenuto che non sussistano i presupposti sui quali fondare la predetta assimilazione. D'altra parte, sotto il profilo funzionale, non solo la criptovaluta non ha efficacia liberatoria *erga omnes* (in quanto la sua accettazione come mezzo di pagamento è subordinata alla volontà della controparte) ma l'estrema fluttuazione delle sue quotazioni ne compromette la funzione di riserva di valore. La combinazione di queste due criticità finisce, altresì, per ostacolare l'utilizzo della valuta virtuale come unità di conto[9].

Dunque, la moneta virtuale non può essere assimilata alla valuta legale e ciò sembra confermato anche dalle modifiche apportate dal d.lgs. n. 90/2017 all'art. 17-*bis* (rubricato "Attività di cambiavalute") del d.lgs. n. 141/2010, recante la disciplina dei soggetti operanti nel settore finanziario; modifiche che consentono di distinguere, sotto il profilo operativo, le valute virtuali da quelle legali. Per finalità di contrasto al riciclaggio, il nuovo art. 17-*bis*[10] ha, come è noto, esteso la disciplina prevista per i cambiavalute anche ai prestatori di servizi che operano con valute virtuali[11] e, in più, ha stabilito che tali soggetti, per esercitare la propria attività sul territorio nazionale, devono iscriversi in una

---

[8] È appena il caso di ricordare che il legislatore italiano, con il d. lgs. n. 90 del 25 maggio 2017, ha "anticipato" le disposizioni contenute nella proposta di modifica della IV Direttiva antiriciclaggio presentata dalla Commissione il 5 luglio 2016 (confluita, successivamente, nella V Direttiva perché non approvata in tempo), come modificata all'esito della prima lettura del Parlamento europeo (per una ricostruzione, v. G. Rinaldi, *Approcci normativi e qualificazione giuridica delle criptomonete*, cit., p. 275 ss.). Rispetto alla IV Direttiva che nulla diceva in materia di valute virtuali, la suddetta proposta estendeva parti della disciplina comunitaria in materia di antiriciclaggio alle transazioni eseguite tramite valute virtuali prevedendo obblighi di adeguata verifica della clientela, di conservazione di documenti, dati e informazioni sui clienti, di segnalazioni di operazioni sospette, a carico di soggetti che forniscono a terzi servizi funzionali all'utilizzo, allo scambio e alla conservazione di valuta virtuale e alla loro conversione da o verso valute virtuali (c.d. "prestatori di servizi relativi all'utilizzo di valuta virtuale"). Tutto ciò al fine di garantire il monitoraggio, da parte delle autorità competenti, sia del momento di accesso della moneta legale nel *network* (con la conversione in valuta virtuale) sia di quello di uscita dal *network* stesso (con la riconversione in moneta legale), consentendo così la verifica della congruità delle operazioni rispetto al profilo patrimoniale, economico e reddituale dell'utente e all'attività esercitata dallo stesso.

[9] Cfr. G. Gasparri, *Timidi tentativi giuridici di messa a fuoco del bitcoin: miraggio monetario crittoanarchico o soluzione tecnologica in cerca di un problema*? in *Il diritto dell'informazione e dell'informatica* 2015, p 417 ss., al quale si rimanda anche per la bibliografia.

[10] Come risulta modificato dall'art. 8 del d.lgs. n. 90/2017 con l'introduzione del comma 8-*bis.*

[11] Definiti, nell''art. 1, comma 2, lett. ff), del d.lgs. 21 novembre 2007, n. 231, come «*ogni persona fisica o giuridica che fornisce a terzi, a titolo professionale, servizi funzionali all'utilizzo, allo scambio, alla conservazione di valuta virtuale e alla loro conversione da ovvero in valute aventi corso legale*».

sezione speciale del registro tenuto dall'Organismo degli Agenti e dei Mediatori[12]. Dunque, se il legislatore avesse voluto collocare le valute virtuali all'interno del sistema monetario equiparandole alle valute legali, non vi sarebbe stata necessità alcuna di introdurre una sezione speciale del citato registro in quanto le criptovalute sarebbero rientrate *tout court* nell'alveo dell'oggetto dell'attività dei cambiavalute[13].

In questo contesto, privo di una qualificazione giuridica delle valute virtuali nonostante lo sforzo definitorio del legislatore, la dottrina ha avanzato diverse ipotesi classificatorie[14] senza, tuttavia, giungere a soluzioni univoche[15], in quanto l'attrazione nell'ambito delle possibili categorie giuridiche dipende, in primo luogo, da quale aspetto o funzione, tra quelli che concorrono a formare la struttura delle criptomonete, venga ritenuto prevalente rispetto agli altri[16]. Una svolta in tal senso, potrebbe essere offerta dalla nuova definizione di valuta

---

[12] Cfr. art. 3, comma 5, lett. i) del d.lgs. n. 231/2007, come modificato dal predetto d.lgs. n. 90/2017, che attribuisce ai prestatori di servizi che operano con valute virtuali la qualifica di "operatori non finanziari" al fine di assimilarli ai cambiavalute e, dunque, di estendere ad essi gli obblighi antiriciclaggio.

[13] A supporto di quanto affermato vi è la sentenza n. 195/2017 del Tribunale di Verona che rappresenta, come è noto, il *leading case* italiano in quanto segna una svolta in tema di inquadramento giuridico dell'attività di conversione in valuta ufficiale ad opera di una società di cambio. Il rapporto sinallagmatico nato tra le due parti in seguito alla conclusione *on line* di un contratto di cambio di valuta reale con *bitcoin* configura – secondo il Giudice interpellato – «*un servizio finanziario, in quanto le transazioni* on line *sono state effettuate con uno strumento finanziario costituito da una moneta che può essere coniata da qualunque utente ed è sfruttabile per compiere transazioni, possibili grazie ad un software* open source *e ad una rete* peer to peer».

[14] In particolare, la dottrina si è chiesta se le criptovalute possano farsi rientrare nella categoria degli strumenti finanziari (e, più opportunamente, in quella dei prodotti finanziari) o, in alternativa, nella categoria dei beni mobili immateriali. Per un'analisi cfr. A. Magliocco, *Bitcoin e tassazione,* in *Strumenti finanziari e fiscalità*, n. 22, 2016, p. 27 ss.

[15] È appena il caso di ricordare che le criptomonete non sono assimilabili alla c.d. moneta elettronica, la quale identifica esclusivamente quegli strumenti di pagamento che incorporano nel proprio supporto, digitale o magnetico, un credito nei confronti di un istituto finanziario o bancario. In argomento è intervenuta anche la Banca Centrale Europea (BCE) (cfr. Banca Centrale Europea, *Virtual Currency Schemes*, Frankfurt am Main, 2012, la quale ha chiarito che, mentre all'interno dei sistemi di moneta elettronica il collegamento diretto tra *electronic money* e valute tradizionali è garantito e protetto dall'ordinamento (in quanto i fondi sottostanti sono espressi nella medesima unità di conto, ad esempio l'euro o il dollaro), nel caso di acquisto di valute virtuali l'unità di riferimento non è legata a una moneta legale (dato che quest'ultima, all'atto della compravendita, viene convertita in moneta virtuale), ed il loro valore è regolato unicamente dal meccanismo della domanda e dell'offerta. In argomento v. G. Rinaldi, *Approcci normativi e qualificazione giuridica delle criptomonete*, cit., p. 270 s.

[16] Le criptovalute sono state, invece, oggetto di interventi normativi organici nell'ambito di un ristretto gruppo di ordinamenti (Giappone, Stati Uniti, Germania) che sono stati in grado di coniugare adeguatamente le diversi componenti del fenomeno (ed, in particolare, l'aspetto pseudo-monetario) con quello di risorsa digitale senza, tuttavia, indugiare sul fatto che non si tratta di strumenti che hanno un potere solutorio *ex lege*. Per un'analisi comparata cfr. G. Rinaldi, *Approcci normativi e qualificazione giuridica delle criptomonete*, cit., p. 271 ss.

virtuale adottata dal legislatore europeo nella V Direttiva antiriciclaggio[17], intesa ad agevolare una convergenza a livello europeo della relativa disciplina. A tal fine, la definizione contenuta nell'art. 3 della citata Direttiva – pur essendo molto simile, per alcuni elementi essenziali, a quella contenuta nella disciplina domestica – introduce una fondamentale novità che consente di tracciare un confine netto tra moneta virtuale e moneta tradizionale.

A livello europeo, la moneta virtuale è ora definita come "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 o giuridiche come mezzo di scambio e può essere trasferita, memorizzata e scambiata elettronicamente". Dunque, con l'intervento del legislatore europeo, non dovrebbero esserci più dubbi su cosa non è una valuta virtuale in quanto la disciplina comunitaria ha espressamente stabilito che la criptovaluta non possiede lo *status* giuridico né di moneta né di valuta legale. Ciò nonostante, l'Agenzia delle entrate, nella risposta al recente interpello n. 956-39/2018, ha confermato l'impostazione (errata) contenuta nella risoluzione n. 72/E del 2 settembre 2016 volta ad assimilare, sulla base di una lettura *pro fisco* della sentenza della Corte di Giustizia dell'Unione Europea del 2015, le valute virtuali a quelle estere al fine di applicare alle prime il regime impositivo previsto per le attività estere di natura finanziaria. Da qui il rischio di un palese contrasto tra prassi domestica e norma comunitaria; un contrasto che non può più essere ignorato soprattutto in vista del recepimento della V Direttiva nello Stato italiano[18].

2. La rilevanza fiscale delle operazioni in valuta virtuale: la posizione dell'Amministrazione finanziaria ai fini delle imposte dirette ed indirette

Il primo documento di prassi attraverso il quale l'Amministrazione finanziaria ha reso noto il proprio orientamento in merito al trattamento fiscale delle operazioni in bitcoin è la Risoluzione n. 72/E pubblicata il 2 settembre 2016[19]. Come è noto, la risoluzione in oggetto ha tratto origine da una istanza di interpello presentata da una società di capitali che, intendendo svolgere per conto della propria clientela operazioni di acquisto e di vendita di bitcoin, ha

---

[17] Direttiva n. 2018/843 del Parlamento europeo e del Consiglio del 30 maggio 2018 che modifica la Direttiva (UE) 2015/849 relativa, come è noto, alla prevenzione dell'uso del sistema finanziario ai fini del riciclaggio o finanziamento del terrorismo. Per il recepimento della V Direttiva, all'art. 4 della stessa è previsto che «*gli Stati membri mettono in vigore le disposizioni legislative, regolamentari e amministrative necessarie per conformarsi alla presente direttiva entro il 10 gennaio 2020*». Sulla definizione delle criptovalute contenuta nella V Direttiva antiriciclaggio, cfr. in questo *Quaderno* il contributo di N. De Giorgi.

[18] È appena il caso di ricordare che la bozza del decreto legislativo contenente le prescrizioni necessarie al suddetto recepimento, dopo la consultazione pubblica, è in attesa di approvazione.

[19] Per un commento S. Capaccioli, *Regime impositivo delle monete virtuali: poche luci e molte ombre*, in *Il fisco*, n. 37, 2016, p. 3538 ss.

chiesto all'Agenzia delle entrate di conoscere quale fosse il corretto trattamento applicabile alle predette operazioni, sia ai fini IVA che delle imposte dirette (IRES ed IRAP) e se, in relazione alla predetta attività, risultasse necessario porre in essere gli adempimenti previsti, ai fini fiscali, per i soggetti che ricoprono la qualifica di sostituto d'imposta. Nella risposta, l'Agenzia delle entrate ha innanzitutto precisato che "con riferimento al trattamento fiscale applicabile alle operazioni relative ai bitcoin e, in generale, alle valute virtuali, non si poteva prescindere da quanto affermato dalla Corte di Giustizia dell'Unione europea nella sentenza 22 ottobre 2015, causa C-264/14"[20].

Dunque, in assenza di una specifica normativa tributaria applicabile al sistema delle monete virtuali, la citata sentenza della Corte di Giustizia ha rappresentato per l'Agenzia delle entrate «un punto di riferimento» soprattutto per la sua indiscutibile «portata storica»[21]. In detta sentenza, la Corte di Giustizia europea – dopo aver chiarito che «la valuta virtuale a flusso bidirezionale 'bitcoin' (…) non può essere qualificata come 'bene materiale' ai sensi dell'art. 14 della direttiva IVA» in quanto «non ha altra finalità oltre a quella di un mezzo di pagamento» – ha stabilito che le operazioni che consistono nel cambio di valuta tradizionale contro unità di valuta virtuale bitcoin e viceversa, effettuate a fronte del pagamento di una somma corrispondente al margine costituito dalla differenza tra il prezzo di acquisto delle valute e quello di vendita praticato dall'operatore ai propri clienti, configurano, ai sensi dell'art. 2, par. 1, lett. c) della Direttiva IVA, prestazioni di servizio a titolo oneroso. In particolare, secondo la Corte, tali prestazioni ricadono tra le operazioni, compresa la negoziazione, "relative a divise, banconote e monete con valore liberatorio" le quali, come è noto, sono esenti ai fini IVA a norma dell'art. 135, par. 1, lett. e), della Direttiva 2006/112/CE[22]. A tal fine, i Giudici europei, uniformandosi alle conclusioni esposte dall'Avvocato Generale Juliane Kokott, hanno messo in evidenza che le differenti versioni linguistiche dell' art. 135 della Direttiva IVA – proprio perché recepite in modo non perfettamente coincidente in tutti gli Stati membri – non consentono di determinare, con assoluta certezza, se questa disposizione debba applicarsi solo alle operazioni concernenti valute tradizionali oppure se essa riguardi anche operazioni relative a valute di altra natura.

---

[20] Corte UE, 22 ottobre 2015, C-264/14 Skatteverket contro David Hedqvist.

[21] Con la citata sentenza, per la prima volta, a livello europeo, sono state risolte le incertezze circa la possibilità di applicare le imposte sui consumi anche alle transazioni effettuate in *bitcoin* e, più in generale, alle valute virtuali sebbene in regime di esenzione. Per un approfondimento, v. G. Corasaniti, *Il trattamento tributario dei* bitcoin *tra obblighi antiriciclaggio e monitoraggio fiscale*, in *Strumenti finanziari e fiscalità*, n. 36, 2018, p. 45 ss.

[22] M. Piasente, *Esenzione Iva per i "bitcoin": la strada indicata dalla Corte UE interpretando la nozione "divise"*, in *Corr. trib.*, n. 2, 2016, p. 141 ss. ha affermato che la posizione della Corte di Giustizia risulta coerente alla *ratio* delle esenzioni in esame le quali, come è noto, sono finalizzate ad ovviare alle difficoltà di determinazione della base imponibile e dell'importo dell'IVA detraibile proprie delle operazioni finanziarie.

È proprio questa situazione di ambiguità che, secondo parte della dottrina[23], ha spinto la Corte di Giustizia ad affermare che non è possibile «escludere l'applicabilità della disposizione della lettera e) del citato art. 135 ai bitcoin, anche se privi di valore liberatorio, prevalendo la necessità di interpretare la stessa in funzione del contesto in cui si inserisce, della finalità e del sistema della Direttiva Iva». In altri termini, secondo i giudici europei, le prestazioni di servizio, oggetto del procedimento, sono rilevanti ai fini IVA ma ricadono all'interno delle ipotesi di esenzione, contemplate dall'art. 135, par. 1, lett. e) della Direttiva IVA, in quanto l'espressione «divise, banconote e monete con valore liberatorio» deve essere interpretata in funzione del contesto in cui essa si inserisce; una diversa interpretazione della norma in esame volta ad escludere le valute virtuali dal suo ambito di applicazione perché senza valore liberatorio, anche se riconosciute dalle parti che l'accettano, «si risolverebbe nel privarla dei suoi effetti». Pertanto, secondo la Corte, il principio di neutralità dell'IVA impone che il regime previsto per i mezzi di pagamento legali valga anche per gli altri mezzi di pagamento che hanno la loro stessa funzione, considerando ininfluente nella fattispecie la presenza del "corso legale".

Facendo leva su questa impostazione, l'Amministrazione finanziaria ha risposto alla istanza di interpello, da cui si è originata la Risoluzione in commento, aderendo alla posizione dell'istante secondo il quale l'attività che la società intendeva realizzare avrebbe dovuto configurarsi come prestazioni di servizi esente, ai fini IVA, ai sensi dell'art. 10, comma 1, n. 3 del d.P.R. n. 633/1972. Al riguardo, attenta dottrina[24], ha osservato che le conclusioni cui è pervenuta l'Agenzia delle entrate sembrano superare, in una certa misura, il dato letterale della norma da ultimo citata che, come è noto, lega l'esenzione Iva delle valute estere alla presenza del corso legale. Tanto è vero che l'art. 10, co. 1, prevede l'esenzione dall'Iva «per le operazioni relative a valute estere aventi corso legale e a crediti in valute estere, eccettuati i biglietti e le monete da collezione e comprese le operazioni di copertura dei rischi di cambio». Dunque, l'aspetto che lascia perplessi nella citata risoluzione è la ricostruzione della sentenza della Corte di Giustizia. Sembra, infatti, che l'Amministrazione finanziaria abbia inteso "equiparare" la valuta virtuale bitcoin alla valuta estera, avente corso legale, sebbene nella sentenza della Corte di Giustizia non sia possibile trovare traccia di questa equiparazione. Come è noto, la Corte di Giustizia ha fatto rientrare i bitcoin tra i mezzi di pagamento presupponendo che la loro unica finalità sia quella liberatoria, seppure contrattuale o su base volontaria e, in questa prospettiva, ha finito per "assimilare" i bitcoin alle "divise", ritenendo sostanzialmente ininfluente, ai fini IVA, la presenza del "corso legale" in quanto

---

[23] G. Corasaniti, *Il trattamento tributario dei* bitcoin *tra obblighi antiriciclaggio e monitoraggio fiscale*, cit., p. 55; M. Piasente, *Esenzione Iva per i "bitcoin": la strada indicata dalla Corte UE interpretando la nozione "divise"*, cit., p. 144; F. Fassò, *Il regime fiscale dei bitcoins secondo una recente ed (unica) prassi amministrativa*, in *Strumenti finanziari e fiscalità*, n. 3, 2017, p. 105 ss.

[24] G. Corasaniti, *Il trattamento tributario dei bitcoin tra obblighi antiriciclaggio e monitoraggio fiscale*, cit., p. 57.

ciò che rileva, nella prospettiva comunitaria, è che sia le valute virtuali che quelle legali hanno la medesima funzione di mezzo di pagamento.

Anche con riferimento al regime di imposizione diretta, l'Agenzia delle entrate ha risolto la questione prendendo in considerazione i bitcoin solo come mezzi di pagamento ed affermando che l'attività di intermediazione di valute tradizionali con bitcoin, svolta in modo professionale ed abituale, costituisce attività d'impresa, rilevante ai fini IRES ed IRAP. Al riguardo, la Risoluzione ha innanzitutto chiarito che, analogamente alle altre attività di compravendita, le operazioni che consistono nel cambio di valuta tradizionale contro unità della valuta virtuale bitcoin e viceversa costituiscono per la società interpellante l'oggetto dell'attività svolta in grado di generare ricavi e costi propri del reddito di impresa. In particolare, con riguardo alla tassazione diretta, l'Agenzia delle entrate ha stabilito che la società deve assoggettare ad imposizione i componenti di reddito derivanti dalla attività di intermediazione nell'acquisto e vendita di bitcoin, al netto dei costi inerenti detta attività.

I guadagni (o le perdite) di competenza della società sono rappresentati dalla differenza tra quanto anticipato dal cliente e quanto speso dalla società per l'acquisto o tra quanto incassato dalla società per la vendita e quanto riversato al cliente. Tali elementi di reddito – derivanti dalla differenza (positiva o negativa) tra prezzi di acquisto sostenuti dalla società e costi di acquisto a cui si è impegnato il cliente (nel caso in cui quest'ultimo abbia affidato alla società l'incarico a comprare) o tra prezzi di vendita praticati dalla società e ricavi di vendita garantiti al cliente (nel caso di affidamento di incarico a vendere) – sono ascrivibili ai ricavi (o ai costi) caratteristici di esercizio dell'attività di intermediazione esercitata e, pertanto, "contribuiscono quali elementi positivi (o negativi) alla formazione della materia imponibile soggetta ad ordinaria tassazione ai fini IRES (e IRAP)".

La Risoluzione n. 72/E del 2016 ha esaminato, inoltre, il caso in cui, alla fine dell'esercizio, la Società intermediaria detenga in proprio bitcoin a titolo di proprietà, precisando che gli stessi dovranno essere valutati secondo il cambio in vigore alla data di chiusura dell'esercizio e che tale valutazione assume rilievo ai fini fiscali ai sensi dell'art. 9 T.U.I.R dovendo la Società procedere alla relativa valutazione secondo le regole previste dal Testo Unico con riferimento ai casi di detenzione di valute estere. Pertanto, la determinazione delle valute virtuali detenute dovrà essere effettuata sulla base del valore normale espresso in euro (o in altra valuta legale) applicando il cambio vigente alla data di chiusura dell'esercizio. Per quanto riguarda, invece, la tassazione dei proventi conseguiti dai clienti di una Società che svolge attività di intermediazione nell'acquisto e nella vendita di bitcoin, nel caso in cui tali clienti siano persone fisiche e detengano bitcoin, al di fuori dell'attività d'impresa, l'Agenzia delle entrate, nella risoluzione in commento, ha chiarito che le operazioni di conversione di valuta virtuale, se detenute al di fuori del regime di impresa, generano un reddito diverso di natura finanziaria tassabile, ai sensi dell'art. 67, comma 1, lett. c-*ter*) e comma 1-ter T.U.I.R., alla stregua dei principi che regolano le operazioni aventi a oggetto le valute tradizionali.

Ai fini dell'imposta sul reddito delle persone fisiche, nell'ambito delle operazioni di conversione di bitcoin con altra valuta virtuale (oppure da valute virtuali in euro), occorre distinguere le operazioni realizzate per effetto di una cessione a termine da quelle realizzate per effetto di una cessione a pronti (intendendosi per tale ogni transazione in cui si ha lo scambio immediato di una valuta contro una valuta differente). L'equiparazione tra valute virtuali e valute estere aventi corso legale comporta che, ai sensi del citato art. 67, comma 1, lett. c-*ter*), le plusvalenze derivanti dalle cessioni a termini di valuta virtuale, come redditi diversi di natura finanziaria, sono soggetti ad imposta sostitutiva con aliquota al 26%; le eventuali plusvalenze derivanti dalla cessioni a pronti di valuta virtuale non sono, invece, tassabili a meno che, nel periodo d'imposta, la giacenza media dei conti correnti in valuta estera e dei depositi (siano essi bancari o elettronici) complessivamente detenuti dal soggetto cedente abbia superato il controvalore di 51.645,69 euro per almeno sette giorni lavorativi. Come è noto, l'art. 67, comma 1, lettera c-*ter*, prevede espressamente che «l'imponibilità delle operazioni sulle valute estere riguarda soltanto quelle operazioni espressamente contemplate nella lettera c-ter che si intendono come espressive, per presunzione di legge, di un'attività di investimento e cioè il prelievo della valuta da depositi o conti correnti ovvero la sua cessione a termine». Dunque, le operazioni a pronti di valuta virtuale sono imponibili solo se vengono realizzate per finalità speculative.

A tal fine, vige una presunzione di legge assoluta che opera quando si realizza la condizione prevista dall'art. 67, comma 1-*ter*. In base a questa norma, le plusvalenze derivanti dalla cessione a titolo oneroso di valute estere, rivenienti in depositi e conti correnti, concorrono a formare il reddito a condizione che, nel periodo d'imposta, la giacenza dei depositi e dei conti correnti complessivamente intrattenuti dal contribuente presso tutti gli intermediari sia superiore, come precisato, a 51.645,69 euro. In questo caso, il valore in euro della giacenza media in valuta virtuale va calcolato secondo il cambio di riferimento all'inizio del periodo di imposta e cioè al 1° gennaio dell'anno in cui si verifica il presupposto di tassazione mentre la plusvalenza va calcolata, secondo l'Agenzia delle entrate, utilizzando il rapporto di cambio al 1° gennaio rilevato sul sito dove il contribuente ha acquistato la valuta virtuale o, in mancanza, quello rilevato sul sito dove effettua la maggior parte delle operazioni in quanto manca un prezzo ufficiale giornaliero cui fare riferimento per il rapporto di cambio tra la valuta virtuale e l'euro. Alla luce di tali circostanze, l'Agenzia delle entrate ha escluso che la Società istante fosse tenuta a porre in essere adempimenti in qualità di sostituto d'imposta.

3. Equiparazione delle valute virtuali alle valute estere ed obblighi di monitoraggio fiscale: il corto circuito con la V Direttiva antiriciclaggio

Nelle more di un intervento del legislatore tributario volto a regolamentare organicamente il fenomeno delle criptovalute, l'Amministrazione finanziaria,

ha confermato – in risposta a numerose istanze di interpello, alcune delle quali non pubblicate – il proprio orientamento in materia di trattamento fiscale delle operazioni realizzate in bitcoin[25]. Un orientamento che, come noto, è frutto di un'interpretazione "estensiva" di quanto affermato dai Giudici europei volta a realizzare una equiparazione "arbitraria" dei bitcoin alle valute estere aventi corso legale. Un'interpretazione che non solo lascia perplessi ma che è difficile sostenere soprattutto se si considera che il Parlamento europeo, in sede di approvazione della Risoluzione legislativa del 19 aprile 2018 sulla proposta di modifica della IV Direttiva antiriciclaggio ha, come precisato, espressamente affermato che le criptovalute sono definite come «rappresentazione digitale di valore non necessariamente collegata a una valuta avente corso legale» e che la valuta virtuale "non possiede lo status giuridico di valuta o moneta". Dalla definizione contenuta nella Direttiva 2018/843/UE emerge una nozione di virtual currency priva di qualsiasi accezione "monetaria" o "valutaria", che ha subito, evidentemente, l'influenza di quanto affermato dalla Banca Centrale Europea[26] precisando che l'utilizzo della locuzione "valute virtuali" non produce come effetto un avvicinamento delle criptovalute alla nozione giuridica o economica di moneta, rispetto alla quale esse risultano sostanzialmente diverse.

Non concordano con la natura giuridica delle criptovalute come moneta alternativa a quella tradizionale nemmeno i Giudici nazionali i quali, in quella che sembra essere la prima pronuncia avente ad oggetto tematiche relative ai bitcoin[27], hanno valorizzato la componente di riserva di valore che almeno in parte caratterizza le criptovalute, affermando che la valuta virtuale ha natura di «strumento finanziario utilizzato per compiere una serie di particolari forme di transazioni on line» costituito da «una moneta che può essere coniata da qualunque utente ed è sfruttabile per compiere transazioni, possibili grazie ad un software open source o ad una rete peer to peer». Nel caso in esame, il carattere finanziario dell'operazione sembra discendere, più che dalla semplice attività di compravendita di criptomoneta, dalla presenza di ulteriori profili di rischio/rendimento quali l'acquisto di una partecipazione sociale in una start-up. Non è, dunque, condivisibile l'acritica qualificazione dei bitcoin come strumento finanziario che viene proposta dai giudici nazionali senza sviluppare alcun percorso logico e senza addurre alcuna motivazione a supporto di tale affermazione[28]. In questa prospettiva, l'equiparazione delle valute virtuali a valute estere, posta in essere dall'Amministrazione finanziaria, rappresenta

---

[25] In questo quadro, ha assunto particolare importanza la risposta all'interpello n. 956-39/2018, rilasciato dalla Direzione regionale della Lombardia il 22 aprile 2018 che, sebbene non pubblico, ha fornito indicazioni sulla posizione dell'Amministrazione finanziaria italiana relativa sulla questione in esame.

[26] Banca Centrale Europea, *Virtual Currency Schemes – a Further Analysis*, Frankfurt am Main, 2015.

[27] Si rimanda alla nota 13 di questo lavoro.

[28] Sulla natura delle criptovalute come strumenti finanziari (*melius*: prodotti finanziari) v. P. Carrière, *Le "criptovalute" sotto la luce delle nostrane categorie giuridiche di "strumenti finanziari", "valori mobiliari" e "prodotti finanziari" tra tradizione e innovazione*, in www. dirittobancario.it, n. 2, 2019; G. Greco, *Valute virtuali e valute complementari, tra sviluppo tecnologico e incertezze regolamentari,* in www. dirittobancario.it, n. 5, 2009.

forse il tentativo di trovare una soluzione in attesa di un intervento legislativo che prenda in considerazione le possibili funzioni delle criptovalute, a metà tra l'investimento finanziario e il mezzo di pagamento.

Sotto il profilo fiscale, l'orientamento dell'Amministrazione finanziaria ruota attorno alla (presunta) equiparazione delle criptovalute alle valute estere e produce, come effetto, l'estensione anche ai detentori di valuta virtuale degli obblighi di monitoraggio fiscale contenuti nel d.lgs. n. 167/1990[29]: qualora il contribuente, persona fisica residente nel territorio dello Stato, detenga – nel periodo d'imposta – valute virtuali, lo stesso è tenuto a darne comunicazione nella dichiarazione annuale dei redditi mediante la compilazione del quadro RW. Nella risposta all'interpello 956-39/2018, la Direzione Regionale della Lombardia ha espressamente affermato che "alle valute virtuali si rendono applicabili i principi generali che regolano le operazioni aventi ad oggetto valute tradizionali nonché le disposizioni in materia di antiriciclaggio". In altri termini, se si considera l'investimento in bitcoin come una normale attività finanziaria suscettibile di produrre redditi imponibili in Italia, l'utilizzo di un wallet tramite un intermediario non residente "custode" della chiave privata di accesso al portafoglio elettronico (custodial wallet) configura, quantomeno nella prassi amministrativa, l'obbligo di compilazione del predetto quadro RW. La risposta dell'Agenzia delle entrate all'interpello del 2018 non fornisce, tuttavia, indicazioni riguardo al codice corrispondente allo Stato estero da indicare nel quadro RW. La questione è complessa in quanto le piattaforme on line di gestione delle transazioni e i relativi portafogli elettronici (wallet) sono procedure informatiche collocate su server accessibili via Internet; sicché diventa difficile individuare il soggetto tenuto all'adempimento dell'obbligazione tributaria in base al collegamento territoriale con uno o più Stati esteri[30].

4. Considerazioni conclusive

La natura ibrida delle criptovalute e il loro crescente utilizzo sollevano nuovi interrogativi che, a legislazione vigente, restano senza risposta perché manca una disciplina sostanziale volta a regolamentare i profili giuridici e fiscali.

---

[29] L'art. 4 del d.l. n. 167/1990 prevede che le persone fisiche, gli enti non commerciali e le società semplici ed equiparate ai sensi dell'art. 5 T.U.I.R., residenti in Italia che, nel periodo d'imposta, detengono investimenti all'estero ovvero attività estere di natura finanziaria, suscettibili di produrre redditi imponibili in Italia, devono indicarli nella dichiarazione annuale dei redditi. Sono, inoltre, tenuti agli obblighi di dichiarazione i soggetti indicati nel precedente periodo che, pur non essendo possessori diretti degli investimenti esteri e delle attività estere di natura finanziaria, siano considerati titolari effettivi dell'investimento.

[30] Cfr. E. Mignarri, *Imposizione e monitoraggio delle operazioni in criptovalute: molte questioni aperte*, in *Il fisco*, 39, 2018, p. 3751 ss; I. Bixio, *Le valute virtuali nella V Direttiva antiriciclaggio*, in *Corr. trib.*, n. 25, 2018, p. 1987 ss.; A.E. Giudice, *Bitcoin e criptovalute tra tassazione e monitoraggio fiscale*, in *Strumenti finanziari e fiscalità*, n. 34, 2018, p. 75 ss; G. Giangrande e F. Capogrossi, *La moneta virtuale tra regime impositivo, monitoraggio fiscale e strumento di lotta all'evasione*, in *Strumenti finanziari e fiscalità*, n. 38-39, 2018, p. 75.

Proviamo a fare il punto della situazione in materia di tassazione delle criptovalute alla luce di quanto esaminato nei paragrafi precedenti.

A livello europeo, la Corte di Giustizia ha stabilito che le criptovalute non sono assimilabili a valute "legali" (Sent. Hedqvist, C-264/14), del 2015) e in questo senso si è orientato anche il legislatore italiano nella definizione di "valuta virtuale" introdotta in sede di recepimento della IV Direttiva antiriciclaggio. Al contrario, l'Amministrazione finanziaria – nella risoluzione n. 72/E del 2016 e nell'interpello n. 956-39/2018 della Direzione Regione Lombardia del 2018, su cui ci siamo soffermati nei paragrafi precedenti - ha affermato che le virtual currency possono essere uno «strumento di pagamento alternativo a quelli tradizionalmente utilizzati nello scambio di beni e servizi». In questa prospettiva, l'Agenzia delle entrate ha ritenuto applicabili nei confronti delle criptomonete i principi generali che regolano le operazioni aventi ad oggetto le monete tradizionali e, in particolare, le disposizioni relative alle valute estere; sicché, il privato che matura plusvalenze sulle cessioni di bitcoin produce un reddito diverso di natura finanziaria da assoggettare a tassazione al verificarsi di due condizioni: a) la cessione è avvenuta con operazioni a termine; b) la cessione è avvenuta con operazioni a pronti, ma le criptovalute sono detenute da più di sette giorni sul proprio conto per un controvalore medio superiore a 51.645,69 euro. Ma non basta. Se le criptovalute sono detenute su conti (c.d. wallet) presso piattaforme estere, occorre, secondo l'Agenzia delle entrate, che il contribuente ne dichiari il possesso nel "quadro RW" della propria dichiarazione dei redditi. La ratio di questa impostazione è da ricercare nel fatto che alle valute virtuali «si rendono applicabili i principi generali che regolano le operazioni aventi ad oggetto valute tradizionali nonché le disposizioni in materia di antiriciclaggio».

Ai fini IVA, l'operazione di cambio di bitcoin (e, più in generale, di valuta virtuale) con valuta legale è considerata, dall'Agenzia delle entrate, come una prestazione di servizio a titolo oneroso che ricade nel campo di applicazione dell'IVA, ma tra le operazioni esenti ai sensi dell'art. 10, comma 1, n. 3) d.P.R. n. 633/1972 in quanto, secondo la Corte di Giustizia nella nota sentenza Hedqvist, si tratta di operazioni «relative a divise, banconote e monete con valore liberatorio», di cui all'art. 135, par. 1, lett. e), della Direttiva IVA.

Alla luce delle considerazioni svolte, occorre innanzitutto chiarire che l'interpretazione dell'Amministrazione finanziaria in materia di tassazione delle valute virtuali, contenuta nella risoluzione ministeriale in commento, produce – come è noto – effetti solo nei confronti del contribuente istante e con riferimento al caso concreto prospettato nell'interpello tributario; sicché, per i contribuenti che decidono di uniformare il proprio comportamento alla predetta interpretazione ministeriale non è prevista alcuna tutela in caso di *revirement in peius* dell'Amministrazione finanziaria, fatta eccezione per la possibilità di ricorrere in sede contenziosa, impugnando l'avviso di accertamento contenente la richiesta dell'imposta o della maggiore imposta. Ma vi è di più. Se si tiene conto dell'orientamento del legislatore europeo che nella V Direttiva antiriciclaggio ha introdotto una nuova definizione di valuta virtuale, affermando espressamente

che la stessa non ha lo *status* né di valuta né di moneta, è evidente che non si possa più continuare a navigare a vista in un quadro normativo troppo lacunoso per poter individuare strumenti adeguati a fronteggiare le diverse problematiche sollevate dal fenomeno in esame. Pertanto, è auspicabile un intervento del legislatore italiano che, nell'individuare la natura giuridica delle criptovalute, ne disciplini anche i profili fiscali al fine di evitare, nell'ottica della moderna visione del rapporto tributario ispirata alla c.d. *tax compliance*[31], inutili contenziosi tra contribuente e Fisco.

[31] Per un approfondimento mi sia consentito di rinviare al mio *Dal controllo fiscale sul dichiarato al confronto preventivo sull'imponibile. Dall'accertamento tributario alla compliance*, Ipsoa, 2017.

Strumenti digitali e credito

Michele Bellino

1. La raccolta di capitali tramite piattaforme: il crowdfunding *e la disintermediazione – 2.* Peer-to-peer lending*: focus sulle attività delle piattaforme – 2.1 Le criticità nella selezione dei richiedenti – 2.2 Il* matching *tra gli utenti e la conclusione del contratto – 2.3 La gestione dei flussi di pagamento tra gli utenti – 2.4 La cessione del credito originato tramite la piattaforma – 2.5 I rischi del default della piattaforma – 3.* Invoice trading *– 3.1 L'*invoice trading *a confronto con il* peer-to-peer lending *e lo sconto – 4. Disintermediazione creditizia e riserve di attività – 4.1 L'area della raccolta del risparmio riservata alle banche – 4.2 La raccolta del risparmio tra il pubblico: l'attività delle piattaforme – 4.2.1 L'attività dei prenditori – 4.3 Il* peer-to-peer lending *e la riserva nella concessione di finanziamenti – 4.4 Piattaforme di* peer-to-peer lending *e mediatori creditizi – 4.5 La necessità di un intervento normativo* ad hoc *– 5. L'*investment based crowdfunding *– 5.1 I gestori di portali – 5.2 Gli offerenti e gli strumenti di raccolta – 5.3 La raccolta condotta tramite portali di* investment based crowdfunding *e gli obblighi del gestore – 6. La proposta della Commissione Europea per un Regolamento in materia di* Financial Return crowdfunding *– 6.1 Ambito di applicazione – 6.2 I fornitori di servizi – 6.3 L'attività dei fornitori di servizi – 6.4 La disciplina dell'attività – 6.5 Obblighi informativi e test di "adeguatezza" – 7. Considerazioni finali sull'*investment based crowdfunding

1. *La raccolta di capitali tramite piattaforme: il* **crowdfunding** *e la disintermediazione*

Con il termine *crowdfunding*[1] si indica l'attività di raccolta di denaro condotta da un soggetto nei confronti del pubblico, caratterizzata dall'impiego, da parte dell'investitore, di somme relativamente modeste, al fine di finanziare – insieme ad altri individui – un progetto, un'impresa o un'esigenza di consumo del richiedente. Prescindendo dall'esame di forme di *crowdfunding* in cui l'investimento è legato a scopi benefici o comunque a forme di ricompensa non monetaria, oggetto del presente contributo sarà il *Financial Return crowdfunding* (*FR crowdfunding*), famiglia che raccoglie fattispecie in cui l'investimento è finalizzato ad ottenere un rendimento finanziario.

Il *FinTech*[2] ha infatti investito anche il settore della raccolta e dell'impiego di risparmio e, trasformando le modalità di incontro tra i soggetti in *surplus* ed in *deficit* monetario, comporta la nascita di nuove forme di intermediazione del mercato finanziario[3], con riferimento sia al segmento bancario (*lending based crowdfunding*)[4] che alla raccolta di capitale di rischio e di debito da parte delle imprese (*investment based crowdfunding*)[5].

Al centro di queste nuove forme di raccolta e di investimento c'è la piattaforma[6], che permette agli utenti del mercato dei capitali di soddisfare le proprie esigenze senza la necessaria intermediazione di un operatore tradizionale. Favorendo l'incontro degli utenti "diretto" e "tra pari" sul *web*, questo nuovo tipo di intermediario offre da un lato ai soggetti in *deficit* la possibilità di percorrere – rivolgendosi direttamente al pubblico – una "nuova via" rispetto ai tradizionali canali di finanziamento, dall'altro nuove forme di investimento ai soggetti in *surplus*[7].

---

1 Su questo tema cfr. il contributo di P. Lucantoni in questo *Quaderno*.

2 Il *FinTech* può essere definito come «*technology-enabled innovation in financial services that could result in new business models, applications, processes or products with an associated material effect on the provision of financial services*»: Financial Stability Board (FSB), *Financial Stability Implications from FinTech – Supervisory and Regulatory Issues that Merit Authorities' Attention*, 2017.

3 In tale linea di pensiero cfr. A. Sciarrone Alibrandi, G. Borello, R. Ferretti, F. Lenoci, E. Macchiavello, F. Mattassoglio, F. Panisi, *Marketplace lending – Verso nuove forme di intermediazione finanziaria?*, in *Quaderni FinTech*, CONSOB, 2019, pubblicato successivamente alla conclusione della stesura del presente contributo.

4 Il termine *lending based crowdfunding* è spesso utilizzato come sinonimo di *peer-to-peer lending* (*P2P lending*) o di *social lending*.

5 E. Kirby e S. Worner, *Crowd-funding: an infant industry growing fast*", in *Staff Working Paper of the IOSCO Research Department*, 2014.

6 La piattaforma «*può essere definita tecnicamente come l'infrastruttura di supporto in grado di mettere in comunicazione due parti (generalmente produttori e consumatori) semplificando lo scambio o la fornitura di un servizio attraverso una combinazione di canali di accesso garantiti da un sistema IT*», A. Canepa, *L'era delle piattaforme fra opportunità e rischi*, in *Fintech – Introduzione ai profili giuridici di un mercato tecnologico dei servizi finanziari*, a cura di M. T. Paracampo, Torino, 2017, p. 53.

7 Financial Stability Board (FSB), *FinTech credit. Market structure, business models and financial stability implications*, 2017, p. 31.

Se allo strumento sono state riconosciute le potenzialità per estendere l'offerta di servizi finanziari, favorendo così la concorrenza del mercato e l'ottenimento di fondi da parte di soggetti che potrebbero incontrare difficoltà nel ricorso ai tradizionali canali di finanziamento, su un distinto versante il solo utilizzo di fisionomie operative diverse da quelle tradizionali non consente di escludere che l'attività delle piattaforme necessiti di una regolamentazione *ad hoc* che sia volta a stimolare, indirizzare e regolare tali nuovi fenomeni, contemperando la necessaria apertura all'innovazione tecnologica con il perseguimento dei tradizionali obiettivi della regolamentazione in ambito finanziario.

In tal senso deve essere inquadrata l'iniziativa della Commissione europea che muovendosi nel quadro della *Capital Markets Union* – ove il *crowdfunding* viene individuato come uno degli strumenti attraverso i quali ampliare le possibilità di finanziamenti per le imprese e le PMI europee – ha formulato una Proposta di Regolamento europeo in tema di *crowdfunding*, mirando così a favorire lo sviluppo delle piattaforme su scala comunitaria.

Dato il meccanismo di *opt-in* che connota la Proposta della Commissione, i regimi nazionali in tema di *crowdfunding* non verrebbero sostituiti, ma continuerebbero ad applicarsi alle imprese operanti al solo livello nazionale sicché allo stato, prima di esaminare la Proposta di Regolamento attualmente pendente davanti alle Istituzioni europee, appare opportuno verificare se e quali elementi del quadro normativo vigente incidano sulla fattispecie, contigua ad attività soggette a numerose e penetranti normative che ne riservano l'esercizio ad intermediari specializzati.

2. **Peer-to-peer lending***: focus sulle attività delle piattaforme*

Il *lending based crowdfunding*, diffusamente noto come *peer-to-peer lending* (*P2P lending*)[8], non è, allo stato attuale, oggetto di regolamentazione in Italia.

Partendo dalla definizione del fenomeno fornita dall'EBA[9], è possibile individuare come tratto peculiare del fenomeno l'attività delle piattaforme di *P2P lending*. Si desume, infatti, che la piattaforma è un luogo virtuale tramite il quale l'utente in *deficit* può rivolgersi direttamente al pubblico al fine di ottenere la concessione di un finanziamento.

---

[8] Per un'analisi dei rischi connessi a questa attività cfr. il contributo di C. Porzio e G. Sampagnaro in questo *Quaderno*.

[9] Il *lending based crowdfunding* viene definito come «*open calls to the wider public by fund seekers through a third party, typically an on-line platform, to raise funds for a project or for personal purposes, in the form of a loan agreement, with a promise to repay with (or in certain cases without) interest. The fund raisers may include individuals, start-up companies or existing SMEs that are seeking an alternative means of funding, rather than the traditional credit market*», cfr. European Banking Authority (EBA), *Opinion of the European Banking Authority on lending-based crowdfunding*, 2015, p. 8.

Il ruolo delle piattaforme che, organizzando e gestendo la piazza virtuale di incontro tra richiedenti e prenditori, fungono da intermediari tra gli utenti, appare in ogni caso necessario. Col tempo, l'operatività della piattaforma si è evoluta, arricchendosi di nuove funzioni ed attività, fino a comprendere un composito panorama di servizi offerti agli utenti durante lo svolgimento del rapporto.

Sebbene i servizi offerti dalle piattaforme differiscano a seconda del portale individuato, la piattaforma dapprima raccoglie e verifica le informazioni necessarie alla valutazione del merito creditizio del richiedente e, sulla base dell'elaborazione di tali informazioni, inserisce il richiedente in una classe di rischio, calcolando o gestendo il calcolo del tasso di interesse applicabile all'operazione di finanziamento. La piattaforma inoltre cura il *matching* tra le richieste e le offerte di credito e, nella fase successiva alla conclusione dell'operazione, monitora l'adempimento del prenditore, gestisce i flussi monetari tra gli utenti e, nel caso in cui il prenditore sia inadempiente, cura – su mandato dei prestatori – la procedura per l'eventuale recupero forzoso dei crediti insoluti. Infine, i modelli più avanzati di piattaforma, offrono servizi di garanzia a copertura delle eventuali perdite da parte del prestatore e permettono la cessione dei crediti tra gli utenti.

2.1 Le criticità nella selezione dei richiedenti

Aspetto particolarmente delicato dell'attività del gestore della piattaforma è la valutazione del merito creditizio del richiedente. Le piattaforme di *P2P lending* generalmente condividono scarse informazioni sul richiedente e sul progetto che chiede di finanziare, oppure operano in totale anonimato tra gli utenti[10]; i prestatori devono dunque affidarsi alla *due diligence* operata dalla piattaforma per l'identificazione e per la valutazione del merito creditizio del richiedente, non potendo svolgere in autonomia alcuna verifica.

Mentre alcune piattaforme affidano questo processo a *credit bureau* specializzati, altre forniscono il servizio *in house*[11] e, in assenza di un quadro regolamentare che disciplini la materia, fissano *standard* minimi di *due diligence*[12] e valutano il merito creditizio del richiedente elaborando le informazioni raccolte secondo modelli liberamente plasmabili a seconda della loro politica aziendale, volta a favorire il finanziamento di una platea più o meno ampia di soggetti.

In questo caso, una prima criticità del procedimento attiene alle informazioni raccolte sul richiedente ed all'accuratezza della loro verifica[13].

---

[10] E. Kirby e S. Worner, *op. cit.*, p. 26.

[11] European Banking Authority (EBA), *op. cit.*, p. 11.

[12] M. Bofondi, *Il lending-based crowdfunding: opportunità e rischi*, in *Questioni di economia e finanza*, n. 372, Banca d'Italia, 2017, p. 8.

[13] M. Bofondi, *op. cit.*, p. 8. Vedi anche E. Macchiavello, "*Peer-to-peer lending ed informazione: la tutela dell'utente online tra innovazione finanziaria, disintermediazione e limiti cognitivi*", in *Dir. banca e merc. fin.*, 2015, 29, 2, p. 237.

Alla valutazione di eventuali garanzie prestate[14] ed alla richiesta di informazioni sul richiedente, sul progetto da finanziare, sulle caratteristiche del finanziamento richiesto, solitamente completate dall'interrogazione dei sistemi di informazioni creditizie, si affianca in alcuni casi la raccolta di informazioni ricavate dalla rete *internet* o dai *social network*, della cui accuratezza ed affidabilità appare lecito dubitare. Inoltre, le piattaforme – anche se alcune, per allineare i propri interessi a quelli degli utenti, finanziano con fondi propri una parte dei contratti sottoscritti tramite il portale – solitamente non corrono alcun rischio di credito collegato alle operazioni concluse sul portale: l'unico presidio volto ad assicurare la prudenza nella valutazione della situazione patrimoniale dell'utente è il rischio reputazionale.

Le criticità fin qui evidenziate assumono una connotazione ancora più pregnante alla luce del sistema di remunerazione della piattaforma. Solitamente il percepimento di commissioni da parte del gestore è slegato dall'adempimento degli utenti-richiedenti, ed è calcolato in funzione della quantità di contratti di finanziamento conclusi dagli utenti. Lo sguardo deve dunque spostarsi dall'accuratezza dei modelli di elaborazione del merito creditizio e dall'azzardo morale di un gestore che, non rischiando in proprio, potrebbe effettuare blande verifiche sugli utenti finanziati, ai possibili conflitti di interesse tra le piattaforme – le quali, incassando le commissioni per ogni prestito concluso, potrebbero aver interesse ad allargare la possibilità di ottenere finanziamenti anche a soggetti poco idonei – e i prestatori, sui quali ricade il rischio di credito[15]. Ulteriori conflitti di interesse potrebbero sorgere nel caso di rapporti (personali, professionali, societari…) tra le piattaforme e gli utenti-richiedenti[16], circostanza non a caso pesantemente presidiata nella normativa bancaria (art. 136 t.u.b.).

2.2 Il **matching** *tra gli utenti e la conclusione del contratto*

All'esito della valutazione del merito creditizio dell'utente, il gestore provvede ad inserire la richiesta di credito sulla piattaforma, in modo che gli utenti interessati al prestito possano accordarlo. L'attività, che costituisce il momento centrale dell'attività di *P2P lending*, è andata evolvendosi nel tempo, vedendo l'attribuzione alle piattaforme di un sempre maggior numero di funzioni ed attività, con conseguente avvicinamento della loro operatività a logiche simili a quelle degli operatori creditizi tradizionali.

In questa fase, assumono rilievo due aspetti dell'attività delle piattaforme, entrambi meritevoli di particolare attenzione: il calcolo del tasso di interesse relativo all'operazione e l'incrocio delle domande ed offerte di finanziamento.

---

[14] La maggior parte dei prestiti concessi tramite piattaforme di *peer-to-peer lending* non è assistita da garanzie reali o personali.

[15] Sul punto, cfr. E. Macchiavello, "*La problematica regolazione del lending-based crowdfunding in Italia*", in *Banca, borsa, tit. cred.*, 2018, I, p. 70.

[16] Sul punto, cfr. European Banking Authority (EBA), *op. cit.,* p. 14.

Le modalità di calcolo del tasso di interesse sono andate semplificandosi nel tempo[17], passando da meccanismi basati sull'asta competitiva degli utenti-finanziatori a meccanismi in cui il calcolo del tasso di interesse è demandato integralmente alla piattaforma[18].

Anche il *matching* tra le domande e le offerte di finanziamento ha visto una progressiva espansione del ruolo della piattaforma, con conseguente parallela erosione del modello *peer-to-peer*.

Negli schemi in cui l'interazione tra pari appare più pura (c.d. *segregated account model*), il gestore della piattaforma si limita a svolgere alcuni servizi essenziali quali la verifica dell'identità degli utenti, il monitoraggio del credito, il trasferimento delle somme tra gli utenti – comunque segregate rispetto a quelle della piattaforma – e l'apertura di procedure volte al recupero dei crediti in caso di inadempimento del debitore. La conclusione del contratto avviene direttamente tra il richiedente e il prestatore, che sceglie tra uno o più richiedenti sulla base delle informazioni – più o meno ampie – condivise tramite la piattaforma.

Negli schemi più evoluti di tale modello, il contratto viene sempre concluso tra gli utenti, ma è la piattaforma a scegliere, sulla base delle indicazioni dei prestatori, quali richieste di prestiti finanziare. Ogni prestatore dunque indicherà alcuni parametri (durata del prestito, rendimento atteso o classe di rischio) e la piattaforma selezionerà le richieste di prestito compatibili con le sue esigenze[19]. Vantaggio essenziale di questo modello operativo è la diversificazione dell'investimento e la riduzione del rischio di credito, che non è legato all'adempimento di un unico debitore. Il risultato viene anche raggiunto vincolando i prestatori ad investire non più di una certa quota del loro investimento in un'unica richiesta, ma senza che sia la piattaforma a selezionare le richieste da finanziare.

In un altro modello (c.d. *notary model*), il rapporto tra gli utenti appare ancora più labile e mediato: la piattaforma funge da luogo di incontro tra prestatori e richiedenti, ma il contratto di finanziamento non verrà concluso direttamente tra gli utenti della stessa. Quando le somme dei prestatori, depositate in una banca, raggiungono un certo ammontare, la banca depositaria erogherà il finanziamento in favore del richiedente, mentre la piattaforma, dopo aver acquistato il credito dalla banca, provvederà ad emettere una "nota" in favore dei prestatori[20], che riceveranno la restituzione di quanto investito ed il rendimento solo se il debitore salderà il proprio debito.

Infine, nel *guaranteed return model*, al prestatore viene garantita la restituzione (in tutto o in parte) del capitale investito o, in alcuni casi, un rendimento

---

17 Per una trattazione più approfondita di tali meccanismi, si rinvia ancora a M. Bofondi, *op. cit.*, p. 9, e a Financial Stability Board (FSB), "*FinTech credit…*", *cit.*, p. 12.

18 E. Macchiavello, "*Peer-to-peer lending ed informazione...*", *cit.*, p. 231. A seconda dei diversi metodi di calcolo del tasso di interessi cambia anche la modalità di accettazione da parte del debitore.

19 E. Macchiavello, "*Peer-to-peer lending ed informazione...*", *cit.*, p. 228.

20 La nota, in alcuni ordinamenti, viene considerata una *security* (cfr. E. Kirby e S. Worner, *op. cit.*, p. 18).

minimo[21]. A tal fine, solitamente il gestore della piattaforma crea dei fondi di garanzia che, alimentati tramite commissioni versate dagli utenti, operano fino a capienza, essendo solitamente esclusa la possibilità che la piattaforma risponda dell'inadempimento degli utenti.

2.3 La gestione dei flussi di pagamento tra gli utenti

Di vitale importanza per il corretto funzionamento dei sistemi di *P2P lending* è la gestione dei flussi monetari tra gli utenti, attività in cui il ruolo di un intermediario appare essenziale.

Innanzitutto, bisogna operare una distinzione tra le piattaforme che gestiscono direttamente tale segmento di attività e quelle che – in base ad appositi accordi – ne demandano la gestione ad intermediari autorizzati (v. *infra*, § 4.2).

La gestione dei fondi degli utenti inizia solitamente prima che il contratto di mutuo venga concluso: l'utente registratosi come prestatore, per poter offrire denaro sulla piattaforma, deve innanzitutto trasferire i relativi fondi su un apposito conto tenuto dal gestore del portale o dall'intermediario suo *partner*. La provvista così creata verrà vincolata ad una richiesta di prestito al momento del *matching* tra richiedente e prestatore. L'effettivo trasferimento delle somme dal conto del prestatore al conto del richiedente avverrà quindi al termine del periodo di raccolta. Nelle raccolte organizzate secondo il modello "*all or nothing*", il mancato raggiungimento di una soglia minima di raccolta impedisce la conclusione del contratto di finanziamento ed implica lo svincolo delle somme dei prestatori dalla richiesta di prestito.

2.4 La cessione del credito originato tramite la piattaforma

Finanziata la richiesta tramite la piattaforma, il prestatore avrà diritto alla restituzione del capitale mutuato ed alla corresponsione del tasso di interesse secondo le modalità ed i termini previsti dal contratto concluso con il richiedente e dal relativo piano di ammortamento. Il contratto tra la piattaforma ed il prestatore contiene sovente clausole che vietano all'utente la cessione del credito al di fuori della piattaforma[22], implicando così l'impossibilità per il prestatore di liquidare autonomamente il proprio investimento prima della sua scadenza naturale. Al fine di andare incontro alle esigenze degli utenti, alcune piattaforme permettono al prestatore di cedere i propri crediti ad altri utenti desiderosi di subentrare nella posizione del cedente. La cessione del credito è tuttavia subordinata all'esistenza di un'offerta di finanziamento compatibile (per durata, importo, ecc.) con lo stesso, ed al ricorrere di particolari requisiti fissati dalle piattaforme che, al fine

---

[21] E. Macchiavello, "*Peer-to-peer lending ed informazione…*", *cit.*, p. 230.

[22] Chiara la funzione di questo tipo di previsioni contrattuali: la piattaforma gestisce i flussi monetari tra creditori e debitori e non potrebbe svolgere questa essenziale funzione nei confronti di un cessionario non registrato sulla piattaforma.

di tutelare gli interessi del cessionario, non permettono la cessione di crediti parzialmente insoluti. Sebbene tali circostanze siano rappresentate nei contratti tra la piattaforma e il prestatore, esiste il rischio che si crei un'aspettativa di facile cessione del credito che porti il prestatore a sottostimare il rischio di illiquidità connesso all'operazione conclusa[23].

Anche nel sistema di cessioni, il ruolo della piattaforma può essere più o meno marcato a seconda che sia l'utente a scegliere le richieste di acquisto dei crediti o la piattaforma ad incrociare le richieste di cessione dei crediti con le offerte di acquisto.

2.5 I rischi del default della piattaforma

Come appena illustrato, il *servicing* offerto dalla piattaforma è composito ed appare essenzialmente votato non solo a favorire la conclusione del contratto tra gli utenti, ma anche a gestire il credito dei prestatori, monitorando l'adempimento dei prenditori e gestendo i flussi di capitale tra gli utenti. Oltre a tali servizi, le piattaforme spesso si incaricano del recupero forzoso dei crediti per conto dei prestatori, i quali – data l'esiguità delle somme prestate e l'anonimato generalmente garantito dalla piattaforma – incontrerebbero serie difficoltà nel recupero del proprio credito, attività nella quale sovente non avrebbero un apprezzabile interesse economico[24].

3. Invoice trading

Nel solco della disintermediazione creditizia viene ricondotta l'attività delle piattaforme che prestano il servizio di c.d. *invoice trading*, che permette alle imprese di ottenere rapidamente liquidità a fronte della cessione[25], tramite la piattaforma, di crediti risultanti da fatture emesse nei confronti dei propri clienti.

Anche nell'*invoice trading* le modalità operative variano a seconda della piattaforma esaminata, ma è possibile comunque individuare i tratti comuni dell'attività posta in essere. L'impresa, dopo essersi registrata sulla piattaforma, viene abilitata a caricare *on-line* le fatture emesse nei confronti dei propri clienti, solitamente corredate da dati e informazioni sul cliente[26]; raccolta la richiesta, sarà la piattaforma a svolgere la valutazione del merito creditizio del debitore ceduto e dell'impresa cedente e a presentare la fattura agli utenti-investitori che,

---

[23] Financial Stability Board (FSB), "*FinTech credit…*", *cit.*, p. 25.

[24] E. Macchiavello, "*La problematica regolazione…*", *cit.*, p. 70.

[25] A seconda dei casi, viene prevista la cessione *pro soluto* o *pro solvendo*.

[26] Ad esempio, una piattaforma richiede una copia del contratto tra impresa-utente e cliente destinatario della fattura presentata per la cessione tramite il portale. Il contratto non può essere visionato dagli utenti-investitori, ma la sua presentazione mira a prevenire le frodi.

tramite meccanismi di asta al rialzo o di offerta competitiva[27], decideranno se e a quale prezzo acquistare il credito della cedente. Aggiudicatosi il credito, l'utente cessionario corrisponderà immediatamente all'impresa cedente una quota (solitamente pari all'80%-90%) del prezzo di acquisto del credito, saldando la differenza solo in caso di adempimento del debitore ceduto. In caso di mancato incasso della fattura, l'impresa cedente dovrà tenere indenne l'utente finanziatore solo se la cessione è avvenuta *pro-solvendo*, diversamente trasferendosi il rischio di inadempimento del cliente a carico del cessionario.

L'accesso alle piattaforme di *invoice trading* è solitamente limitato, sia dal lato dell'impresa richiedente i fondi sia dal lato dell'utente-investitore.

Fermo restando che la valutazione del merito creditizio viene svolta per ogni fattura presentata per la cessione, le piattaforme tendono ad effettuare una prima selezione dei richiedenti a monte, fissando precisi requisiti soggettivi e oggettivi per l'iscrizione sulla piattaforma. Solitamente, i requisiti per l'accesso contemplano il fatturato minimo o la forma giuridica dell'impresa cedente o del debitore ceduto (ad esempio, spesso l'iscrizione è possibile solo per s.r.l. o s.p.a., e non vengono accettate fatture emesse nei confronti della Pubblica Amministrazione) ed il taglio minimo delle fatture che è possibile proporre per lo sconto tramite la piattaforma (solitamente individuato tra € 1.000,00 ed € 10.000,00)[28].

Sul versante dell'utente-investitore le piattaforme sono solite limitare a soggetti istituzionali l'acquisto delle fatture presentate dai richiedenti, con ciò discostandosi dalla filosofia *crowdfunding*, aperta ad un pubblico indistinto ed in linea di massima non professionale. La scelta appare legata al fatto che, a differenza di quanto accade nel *P2P lending*, la fattura viene acquistata da un solo investitore, che dunque – dato l'ammontare delle fatture commerciali – dovrà disporre di cifre più consistenti rispetto all'investitore tipico del *P2P lending*.

La remunerazione dell'investitore – cessionario sta nella differenza tra il prezzo di acquisto ed il valore nominale del credito ceduto; generalmente le piattaforme permettono all'impresa cedente di poter fissare un limite minimo di prezzo per l'acquisto del proprio credito, fissando così volta per volta la remunerazione massima da corrispondere al cessionario per l'operazione[29]. Diverso invece il meccanismo di remunerazione della piattaforma, che prevede solitamente il versamento *una tantum* di una somma per l'iscrizione

---

[27] Osservatorio CrowdFunding, Politecnico di Milano – School of management, *2° Report italiano sul crowdinvesting*, 2017, p. 52 (disponibile all'indirizzo: http://www.osservatoriocrowdinvesting.it/portal/minibond/documenti).

[28] Osservatorio CrowdFunding, *op. cit.*, p. 51 e ss.

[29] In altri casi l'impresa cedente può fissare un prezzo-soglia raggiunto il quale l'asta si conclude immediatamente. Chiaramente, in questa circostanza, l'impresa sceglie di pagare un prezzo più alto al cessionario in cambio di una maggiore celerità nell'ottenimento della liquidità.

dell'impresa al portale e la corresponsione di ulteriori somme calcolate in percentuale[30] su ogni fattura ceduta tramite il portale.

*3.1 L'***invoice trading** *a confronto con il* **peer-to-peer lending** *e lo sconto*

Le peculiarità del servizio di *invoice trading* possono essere colte sia confrontandolo con le forme di *P2P lending* precedentemente illustrate, sia con riferimento alle modalità operative con le quali gli operatori istituzionali forniscono il servizio di sconto su fattura.

Riguardo al primo profilo, oltre alla maggior "chiusura" delle piattaforme di *invoice trading*, bisogna rilevare come, a differenza di quanto avviene con il *P2P lending*, nell'*invoice trading* non si assiste alla conclusione di un contratto di mutuo tra gli utenti della piattaforma, ma alla cessione a titolo oneroso dei crediti dell'impresa in favore degli utenti-cessionari.

Il ruolo della piattaforma appare in ogni caso più limitato rispetto a quanto visto nel *P2P lending*: non sono previsti meccanismi di diversificazione del rischio e di *matching* automatico tra le fatture presentate per la cessione e le offerte di acquisto.

Più articolato appare invece il confronto tra *invoice trading* e le tradizionali operazioni bancarie con le quali le imprese realizzano l'obiettivo di ottenimento di liquidità a fronte della presentazione delle fatture emesse.

Avuto riguardo alle caratteristiche essenziali del fenomeno, le operazioni di *invoice trading* appaiono affini allo sconto così come definito dall'art. 1858 cod. civ., il cui elemento qualificante risiede nel collegamento funzionale[31] tra la cessione del credito non ancora scaduto, l'erogazione immediata di liquidità in favore del cedente e la prededuzione dell'interesse dovuto al cessionario per l'operazione. Anche analizzando le operazioni da un punto di vista economico, si evince come lo scopo dell'*invoice trading* è analogo a quello perseguito dallo sconto, ossia procurare all'imprenditore liquidità immediata tramite lo smobilizzo di un credito non ancora giunto a scadenza.

Ricondotto il servizio offerto dalle piattaforme di *invoice trading* alla fattispecie dello sconto, appare evidente la sua lontananza da altri schemi operativi creati dalla prassi bancaria.

Estraneo alla prassi operativa delle piattaforme di *invoice trading* è il c.d. "castelletto di sconto", «*negozio in base al quale la banca si impegna, nel limite e per il tempo concordati, a scontare, a favore dell'impresa, gli effetti che questa le presenterà*»[32]. La dottrina qualifica il castelletto di sconto come un contratto

---

[30] La percentuale varia a seconda della scadenza e dell'importo della fattura ceduta.

[31] B. Sirgiovanni e L. Marcello, art. 1858 cod. civ., in *Codice Civile commentato*, a cura di G. Bonilini, M. Confortini, C. Granelli.

[32] Cass. Civ., 14.7.2010, n. 16560.

normativo[33], volto a disciplinare le modalità con le quali l'impresa potrà presentare alla banca le fatture da scontare senza che a carico di quest'ultima sorga necessariamente un obbligo di scontare – entro i limiti quantitativi e temporali previsti dal castelletto – tutte le fatture presentate dall'impresa, così che ogni successiva operazione di sconto è indipendente dalle altre. Nell'*invoice trading* le piattaforme fissano criteri minimi dei quali le imprese richiedenti dovranno tener conto nel momento in cui presenteranno le fatture per lo sconto tramite il portale, senza tuttavia definire limiti di disponibilità entro i quali l'impresa può presentare le proprie fatture.

D'altronde nell'*invoice trading* la possibilità di scontare le fatture presentate dall'impresa non dipenderà dalla piattaforma, ma dalla concreta disponibilità degli utenti a concludere – volta per volta – l'operazione. Tale ultima circostanza vale ad escludere la possibilità per le piattaforme di *invoice trading* – e più in generale di *P2P lending* – di concedere finanziamenti flessibili come le linee di credito o di rinegoziare i termini dei prestiti per consentire ai debitori di superare momenti di difficoltà[34].

4. Disintermediazione creditizia e riserve di attività

Se il mercato finanziario è caratterizzato dallo scambio di «*prodotti privi di una loro materialità, costituiti dai veicoli contrattuali attraverso cui l'impresa finanziaria svolge la propria attività produttiva*»[35], l'esame dei rapporti che tessono la trama del *P2P lending* consente di affermare che il fenomeno insiste – seppur con modalità operative differenti da quelle tradizionali – sul segmento del mercato finanziario tradizionalmente ricondotto alla funzione di intermediazione creditizia.

L'attività delle piattaforme di *P2P lending* comporta nuove forme di intermediazione delle attività di raccolta di risparmio tra il pubblico ed esercizio del credito.

In assenza di un intervento legislativo che regolamenti il fenomeno, le piattaforme e gli utenti devono operare nel rispetto «*delle norme che regolano le attività riservate dalla legge a particolari categorie di soggetti (ad esempio, attività bancaria, raccolta del risparmio presso il pubblico, concessione del credito nei confronti del pubblico, prestazione dei servizi di pagamento)*»[36].

Tali norme, pensate per intermediari la cui attività è diversa da quella delle piattaforme, mal si attagliano al nuovo fenomeno[37], che peraltro presenta diverse tipologie di rischi e dunque necessiterebbe di una normativa *ad hoc*.

---

[33] I. Demuro, *Lo sconto bancario*, in *L'attività delle banche*, a cura di A. Urbani, Padova 2010, p. 161.

[34] M. Bofondi, *op. cit.*, p. 14.

[35] A. Antonucci, *I contratti di mercato finanziario*, Pisa, 2018, p. 16.

[36] Banca d'Italia, Delibera n. 584/2016, Sezione IX.

[37] E. Macchiavello, "*La problematica regolazione…*", *cit.*, p. 93.

4.1 L'area della raccolta del risparmio riservata alle banche

L'art. 11 t.u.b., dopo aver definito al primo comma l'attività di raccolta del risparmio come "*l'acquisizione di fondi con obbligo di rimborso, sia sotto forma di deposito sia sotto altra forma*", ne vieta l'esercizio nei confronti del pubblico ai soggetti diversi dalle banche, chiudendo così la riserva posta dall'art. 10[38].

Se gli strumenti di raccolta sono connotati da atipicità, dovendosi individuare la sussistenza dell'obbligo di rimborso con «*riguardo alla complessiva struttura finanziaria dell'operazione concretamente posta in essere, indipendentemente dalla formale configurazione giuridica assunta dalla stessa*»[39], per integrare la fattispecie di raccolta riservata alle banche, essa deve essere «*effettuata* in incertam personam*, cioè presso un numero non a priori individuato e potenzialmente elevato di soggetti nonché, di norma, attraverso forme di contrattazione standardizzata e 'impersonale'*»[40], ed essere «*strutturata in modo tale da poter essere accolta da una pluralità di soggetti* (…). *Non basta dunque una offerta indirizzata alla generalità, occorre una articolazione dell'offerta, quindi della raccolta, tale da poter essere eseguita da una pluralità, solo così potendosi avere raccolta 'tra' il pubblico*»[41].

Dunque, l'attività delle piattaforme e degli utenti-richiedenti, potrebbe sconfinare nell'attività di raccolta del risparmio tra il pubblico, riservata alle banche, non bastando ad escludere tale eventualità la circostanza che la raccolta effettuata tramite la piattaforma sia rivolta agli utenti-prestatori della stessa, in quanto deve «*considerarsi avvenuta presso il pubblico anche la raccolta che si effettui esclusivamente presso i componenti di una 'comunità' predeterminata quando, per la 'potenziale vastità ed estensione' di questa, tale raccolta assuma dimensioni e caratteristiche standardizzate e di massa tali da escludere che la stessa possa dirsi 'privata'*»[42].

Tuttavia, nell'attività delle piattaforme di *P2P lending* non è possibile rinvenire quel tratto caratteristico dell'attività bancaria costituito dalla «*attività di organizzazione e coordinamento, strutturale e funzionale, di operazioni di raccolta ed erogazione*» di moneta[43], quanto piuttosto un'attività contigua a quella bancaria consistente nella facilitazione della conclusione di contratti di finanziamento tra soggetti "pari". L'attività fisiologica della piattaforma non implica la disponibilità e l'impiego diretto dei fondi dei prestatori nei confronti dei richiedenti, sicché la piattaforma non assume su di sé il rischio di credito legato al finanziamento né il rischio di trasformazione delle scadenze[44],

---

38 A. Antonucci, *Diritto delle banche*, Milano, V ed., 2012, p. 81.

39 T.A.R. Roma, Lazio, 12 dicembre 2009, n. 12848.

40 R. Lener, *La raccolta del risparmio: profili generali*, in *L'attività delle banche*, *cit*. p. 70.

41 P. Ferro-Luzzi, *Lezioni di diritto bancario*, Torino, 1995, p. 121.

42 P. Ferro-Luzzi, *Lezioni di diritto bancario*, *cit*., p. 211.

43 P. Ferro-Luzzi, *Lezioni di diritto bancario*, *cit*., p. 97.

44 E. Macchiavello, "*La problematica regolazione...*", *cit.*, p. 76.

differenziandosi in tal modo dall'intermediario bancario e dai suoi rischi tipici che ne giustificano la disciplina[45].

4.2 La raccolta del risparmio tra il pubblico: l'attività delle piattaforme

Al fine di chiarire il rapporto tra l'attività delle piattaforme di *P2P lending* e la normativa in materia di raccolta del risparmio tra il pubblico, la Banca d'Italia, alla Sezione IX della Delibera n. 584/2016, recante "*Disposizioni per la raccolta del risparmio dei soggetti diversi dalle banche*", ha analizzato la posizione dei gestori e dei prenditori, fornendo indicazioni sulle condizioni da rispettare affinché la loro attività non integri l'attività di raccolta del risparmio tra il pubblico riservata alle banche.

Preliminarmente, preme sottolineare che l'attività di gestione di una piattaforma di *P2P lending* non è soggetta di per sé a riserva di attività e che dunque, una piattaforma che demandasse – in base ad appositi accordi contrattuali – ad un intermediario a ciò autorizzato la gestione dei flussi monetari tra gli utenti, non sarebbe tenuta ad ottenere alcuna autorizzazione da parte delle Autorità di vigilanza.

Nel caso in cui la piattaforma decida di gestire direttamente tale aspetto operativo, si può ritenere pacificamente che non sarà la scelta dello strumento tecnologico tramite il quale entrare in contatto con gli utenti a determinare la violazione o meno del divieto di raccolta del risparmio tra il pubblico, quanto lo *status* giuridico del gestore della piattaforma e le modalità di gestione dei flussi monetari tra gli utenti[46].

Le piattaforme che gestiscono i flussi monetari tra gli utenti dovranno dunque operare nelle aree di esenzione dal divieto di raccolta del risparmio tra il pubblico previste dall'art. 11 t.u.b., ricevendo «*fondi da inserire in conti di pagamento utilizzati esclusivamente per la prestazione dei servizi di pagamento dai gestori medesimi, se autorizzati a operare come istituti di pagamento, istituti di moneta elettronica o intermediario finanziario di cui all'art. 106 t.u.b. autorizzato a prestare servizi di pagamento ex art. 114-novies, comma 4, t.u.b.*»[47]. La disposizione mira evidentemente ad assicurare la segregazione tra i fondi della piattaforma e quelli degli utenti in funzione sia del rispetto della riserva di attività di raccolta del risparmio tra il pubblico, sia di tutela dell'utente, i cui fondi non verrebbero esposti alle azioni dei creditori della piattaforma in caso di suo *default*.

---

[45] R. Costi, *L'ordinamento bancario*, Bologna, V ed., 2012, p. 209.

[46] Nel 2009 la piattaforma Zopa è stata oggetto di un provvedimento di cancellazione dall'elenco generale dei soggetti operanti nel settore finanziario previsto dall'art. 106 T.U.B., in quanto le modalità di gestione dei fondi degli utenti non ne assicuravano la separazione da quelli della piattaforma, configurando dunque una violazione della riserva bancaria dell'attività di raccolta del risparmio tra il pubblico: cfr. Decreto del Ministero dell'Economia e delle Finanze, Dipartimento del Tesoro, Direzione V, n. 258/385-C e T.A.R. Roma, Lazio, 12 dicembre 2009, n. 12848.

[47] Banca d'Italia, Delibera n. 584/2016, Sezione IX.

4.2.1 L'attività dei prenditori

Oggetto di attenzione è anche l'attività dei prenditori, che tramite la piattaforma possono sottoporre le loro richieste di fondi direttamente al pubblico. Affinché la loro attività non integri una raccolta di risparmio tra il pubblico, l'acquisizione dei fondi deve essere effettuata sulla base di trattative personalizzate con i singoli finanziatori o effettuata presso soggetti sottoposti a vigilanza prudenziale, operanti nei settori bancario, finanziario, mobiliare, assicurativo e previdenziale. Le trattative possono considerarsi personalizzate allorché gli utenti siano in grado di incidere con la propria volontà sulla determinazione delle clausole del contratto tra loro stipulato e la piattaforma si limiti a svolgere un'attività di supporto alla conclusione del contratto[48].

Inoltre, le Disposizioni ritengono sia opportuna la fissazione di «*un limite massimo, di contenuto importo, all'acquisizione di fondi tramite portale* on line *di* social lending *da parte dei prenditori*»[49], affinché la loro attività non sconfini nella raccolta di risparmio tra il pubblico.

Su un distinto versante, stante l'ampiezza della nozione di prodotto finanziario adottata dal t.u.f.[50], l'attività del prenditore potrebbe integrare un'offerta al pubblico di prodotti finanziari, con conseguente applicazione della disciplina di cui agli artt. 94 e ss. t.u.f.

---

[48] Consob, con la Comunicazione n. DEM/10101143 del 10.12.2010, ha rilevato come il carattere standardizzato del mutuo non venga meno a causa della mera possibilità, per il prestatore, di scegliere il tasso di rendimento nell'ambito di un *range* prefissato.

[49] Nell'ambito della consultazione sullo schema delle disposizioni in materia di raccolta del risparmio dei soggetti diversi dalle banche destinate a sostituire il Capitolo 2 del Titolo IX della Circolare della Banca d'Italia n. 229 del 21 aprile 1999, è stata richiesta a Banca d'Italia l'individuazione di limiti precisi alle quantità di fondi acquisibili e prestabili tramite le piattaforme affinché non si integrasse la violazione di alcuna riserva di attività.
Nel Resoconto della consultazione, l'Autorità ha chiarito che «*in via generale si rammenta che la sezione relativa al social lending ha carattere ricognitivo; essa è stata introdotta per fornire chiarimenti agli operatori in merito alle condizioni e ai limiti il cui rispetto è necessario perché il social lending non costituisca violazione della disciplina in materia di raccolta del risparmio tra il pubblico. Le disposizioni non riguardano, quindi, le condizioni che è necessario rispettare per non violare altre riserve che pure vengono all'attenzione nel social lending (es. attività di finanziamento, attività bancaria, etc.). Si ribadisce che l'elenco delle attività riservate che possono rilevare nel social lending è solo esemplificativo.*
Quanto alle richieste di definire, nelle disposizioni, un limite massimo all'acquisizione di fondi, la Banca d'Italia non ha – in base all'attuale quadro normativo – il potere di disciplinare questo aspetto. Spetterà quindi al gestore della piattaforma definirlo, in modo che la raccolta sia nel complesso limitata».

[50] L'art. 1, comma 1, lett. u) t.u.f. dispone che sono prodotti finanziari «*gli strumenti finanziari e ogni altra forma di investimento di natura finanziaria; non costituiscono prodotti finanziari i depositi bancari o postali non rappresentati da strumenti finanziari*».
Per una ricostruzione approfondita della nozione di "prodotto finanziario" si rinvia a F. Annunziata, *La disciplina del mercato mobiliare*", IX ed., Torino, 2017, p. 351, a R. Costi, *Il mercato mobiliare*, Torino, XI ed., 2018, p. 11, e a R. Lener, *Gli strumenti finanziari*, in *Diritto del mercato finanziario*, a cura di R. Lener, Torino, 2011, p. 64.

In linea di principio, dunque, deve ritenersi applicabile al *P2P lending* la disciplina dettata dal t.u.f. in materia, salvo che l'offerta condotta dal richiedente non rientri nei casi di esenzione di cui all'art. 100 t.u.f. e all'art. 34-*ter*, comma 1, lett. c) del Regolamento Emittenti.

L'applicazione della disciplina in materia di offerta al pubblico di prodotti finanziari appare tuttavia lontana, stanti i limiti di raccolta fissati dalle piattaforme, ben al di sotto della soglia di esenzione prevista dalla citata normativa. D'altronde, imporre ai richiedenti l'elaborazione di un prospetto, non solo li graverebbe di costi, ma sottoporrebbe ai prestatori un documento di ostica lettura e di non agevole comprensione per un utente non dotato di particolari competenze in ambito finanziario[51].

4.3 Il peer-to-peer lending *e la riserva nella concessione di finanziamenti*

Su un distinto versante, bisogna considerare che l'attività di concessione di credito delle piattaforme e degli utenti-prestatori potrebbe violare la riserva di attività di concessione di finanziamenti nei confronti del pubblico qualora sia svolta nei confronti di terzi con carattere di professionalità, così come disposto dall'art. 106 t.u.b. e dal conseguente decreto del Ministro dell'economia e delle finanze del 2 aprile 2015 n. 53.

In primo luogo, affinché l'attività del prestatore non invada la riserva disegnata dall'art. 106 t.u.b., deve ritenersi opportuna la definizione, da parte delle piattaforme, di un limite di investimento per il prestatore, dovendosi considerare le clausole contrattuali nelle quali questo dichiara di agire non professionalmente alla stregua di mere clausole di stile.

In seconda battuta, se le piattaforme di *P2P lending* – comprese quelle autorizzate ad operare come Istituti di pagamento – finanziassero usualmente parte dei prestiti conclusi sul portale con fondi propri, si potrebbe configurare una violazione della riserva di attività disegnata dall'art. 106 t.u.b., dato il carattere senz'altro abituale delle operazioni.

Tali considerazioni sono valide anche per quanto riguarda i sistemi di *invoice trading*, dato che ai sensi dell'art. 2, comma 1, lett. b) del decreto n. 53/2015 l'attività di concessione di finanziamenti comprende anche l'acquisto di crediti a titolo oneroso, attività che dunque ricade nella riserva *ex* art. 106 t.u.b. nel caso sia esercitata nei confronti del pubblico.

4.4 Piattaforme di peer-to-peer lending *e mediatori creditizi*

L'operatività delle piattaforme di *P2P lending* potrebbe infine essere accostata all'attività dei mediatori creditizi che – definita indirettamente

---

[51] E. Macchiavello, "*Peer to peer lending e informazione…*", *cit.*, p. 270.

dall'art. 128-*sexies* t.u.b. come l'attività volta a mettere in relazione «*anche attraverso attività di consulenza, banche o intermediari finanziari previsti dal Titolo V con la potenziale clientela per la concessione di finanziamenti sotto qualsiasi forma*» – è riservata ai soggetti iscritti in un apposito elenco se svolta professionalmente nei confronti del pubblico. Data la definizione di cui all'art. 128-*sexies*, la disciplina relativa ai mediatori creditizi potrebbe venire in rilievo «*solo nel caso in cui i prestatori-utenti siano banche o intermediari finanziari non bancari*»[52].

4.5 La necessità di un intervento normativo ad hoc

Partendo dal modello base di piattaforma è possibile tracciare una linea lungo la quale le attività ed il ruolo dell'intermediario diventano sempre più penetranti, facendo così sfumare il carattere di disintermediazione del *P2P lending* e configurando una diversa forma di intermediazione del mercato finanziario, che presenta caratteristiche e rischi differenti da quella tradizionale, ma comunque rilevante dal punto di vista giuridico, sia sul versante della tutela del mercato che della tutela dell'utente.

Date le diversità intercorrenti tra piattaforme di *P2P lending* e intermediari tradizionali, appare opportuna l'adozione di una regolamentazione propria, che tenga conto delle caratteristiche e problematiche peculiari del fenomeno. Perseguendo finalità di tutela dell'utente e di sviluppo del mercato, il legislatore italiano potrebbe disegnare un quadro normativo volto ad imporre requisiti di professionalità e di onorabilità ai gestori delle piattaforme, ad individuare norme sulla trasparenza delle condizioni contrattuali con gli utenti e ad apportare soluzioni in tema di conflitti di interessi, *due diligence* o di continuità operativa della piattaforma, aspetti questi che allo stato attuale non sono regolati da alcun presidio normativo.

*5. L'*investment based crowdfunding

La diffusione e l'affermarsi del modello del *crowdfunding* ha investito non solo l'intermediazione creditizia, ma anche il settore della raccolta di risparmio condotta dalle imprese mediante l'offerta, tramite piattaforme *on line*, di strumenti di capitale di rischio (*equity crowdfunding*) o di debito (*debt crowdfunding*).

A differenza di quanto visto per il *P2P lending*, l'attività di *equity crowdfunding* è stata oggetto di un precoce intervento da parte del legislatore italiano che, primo in Unione Europea[53], ha regolato il fenomeno con il d.l. n. 179

---

[52] E. Macchiavello, "*La problematica regolazione…*", *cit.*, p. 78.

[53] R. Caratozzolo, *L'utilizzo delle nuove tecnologie per il finanziamento delle imprese: l'equity crowdfunding*, in *Fintech. Introduzione ai profili giuridici di un mercato unico tecnologico dei servizi finanziari*, *cit.*, p. 154.

del 18 ottobre 2012 (c.d. Decreto Crescita *bis*, convertito in l. n. 212 del 17 dicembre 2012). La celerità e la natura dell'intervento normativo, nonché la successiva evoluzione della disciplina, indicano un'attenzione particolare del legislatore allo strumento, cui sono state riconosciute le potenzialità per svolgere un ruolo determinante nel favorire la crescita economica del Paese[54].

In particolare, se nell'ottica del legislatore del 2012 lo strumento era posto a servizio dello sviluppo di una particolare tipologia di impresa, la c.d. *start-up* innovativa, le successive numerose modifiche e revisioni hanno esteso la possibilità di farvi ricorso a tutte le piccole medie imprese, trasformando un intervento "settoriale" in un canale di finanziamento a sostegno di una parte rilevante del tessuto imprenditoriale italiano, caratterizzato notoriamente da imprese di piccole dimensioni che frequentemente incontrano difficoltà nell'ottenere finanziamenti tramite il sistema finanziario tradizionale[55].

L'esigenza di creare condizioni favorevoli per il finanziamento delle società, d'altronde, ha radici profonde, ed anzi costituiva uno degli obiettivi centrali della riforma del diritto societario, che ha visto un notevole ampliamento delle possibilità di finanziamento per la s.p.a. – cui è stata riconosciuta la possibilità di emettere strumenti finanziari "atipici", non rientranti nella classica dicotomia azioni/obbligazioni – e la possibilità per la s.r.l. di emettere "titoli di debito", la cui configurazione concreta potrebbe essere del tutto identica a quella delle obbligazioni[56]. D'altronde, la stessa distinzione tra capitale di rischio e capitale di debito è diventata incerta[57], stante la grande duttilità permessa dalla normativa nella creazione di diversi strumenti di raccolta. Nella prospettiva di una sempre maggiore agevolazione del finanziamento alle imprese deve dunque leggersi la storia normativa dell'*investment based crowdfunding* in Italia.

La disciplina della raccolta di capitale di rischio tramite portali *on line*, introdotta in Italia con il d.l. 179/2012, è contenuta anche nel t.u.f., all'art. 1, comma 5-*novies* (che prevede la definizione di "*Portale per la raccolta di capitali per le piccole e medie imprese e per le imprese sociali*"), all'art. 50-*quinquies* (che disciplina l'attività dei gestori dei portali) e all'art. 100-*ter* (che disciplina le offerte attraverso gli stessi portali). Alla normativa primaria si affianca il Regolamento sulla raccolta di capitale di rischio tramite portali *on line* adottato dalla Consob con Delibera del 26 giugno 2013 n. 18592 (Regolamento sulla raccolta di capitali di rischio tramite portali *on-line*).

---

[54] L'art. 25, comma 1, d.l. 179/2012 indica come obiettivi della normativa introdotta «*la crescita sostenibile, lo sviluppo tecnologico, l'occupazione, in particolare giovanile, con riguardo alle imprese* start-up *innovative.* (…) *Le disposizioni della presente sezione intendono contestualmente contribuire allo sviluppo di nuova cultura imprenditoriale, alla creazione di un ecosistema maggiormente favorevole all'innovazione, così come a promuovere maggiore mobilità sociale e ad attrarre in Italia talenti e capitali dall'estero*".

[55] V. Santoro e E. Tonelli, *Equity crowdfunding ed imprenditorialità innovative*, in www.dirittobancario.it, 2014.

[56] F. Corsi, *Le nuove società di capitali*, Milano, 2003, p. 262.

[57] A. Lolli, *Commentario Il nuovo diritto delle società*, d.lgs. 17.1.2003, n.6, in *I libri delle nuove leggi civili commentate*, Padova, 2005, p. 196.

5.1 I gestori di portali

L'attività dei gestori di portali per la raccolta di capitali per le piccole e medie imprese e per le imprese sociali si muove nell'area di esenzione facoltativa disegnata dall'art. 3 della MiFID II, che permette agli Stati membri di non applicare la direttiva ai soggetti le cui attività sono autorizzate e disciplinate a livello nazionale purché tali soggetti non siano autorizzati a detenere fondi o titoli appartenenti ai clienti, non siano autorizzati a prestare servizi di investimento diversi dalla ricezione e trasmissione di ordini in valori mobiliari e quote di organismi di investimento collettivo e/o attività di consulenza in materia di investimenti relativi a tali strumenti finanziari e trasmettano gli ordini raccolti durante la prestazione dei loro servizi solo ad intermediari individuati dalla stessa norma. Inoltre, la normativa nazionale relativa a tali intermediari deve fissare per loro requisiti "almeno analoghi" a quelli richiesti dalla MiFID II per le imprese di investimento, con riferimento alle condizioni ed alla procedura di autorizzazione, alla vigilanza continua, alle norme di comportamento ed ai requisiti organizzativi[58].

Le condizioni imposte dalla MiFID II per l'esenzione condizionano dunque la normativa nazionale in tema di *investment based crowdfunding*, che dovrà imporne il rispetto ai gestori di portali.

Non rientrano nei casi di esenzione dalla disciplina MiFID II le imprese di investimento che gestiscono portali di *crowdfunding*, che saranno quindi soggette alla disciplina propria della loro attività[59].

L'attività di gestione di portali per la raccolta di capitali per le piccole e medie imprese e per le imprese sociali è disciplinata dall'art. 50 *quinquies* t.u.f., che ne riserva l'esercizio ad alcuni "gestori di diritto"[60] e ai soggetti autorizzati dalla Consob a prestare tale servizio (c.d. gestori autorizzati).

Tutti i soggetti abilitati a svolgere il servizio sono tenuti ad iscriversi in un apposito registro tenuto dalla Consob, suddiviso in una sezione ordinaria, che raccoglie i gestori autorizzati da Consob in seguito alla positiva verifica dei requisiti richiesti dalla normativa, ed in una sezione speciale che raccoglie i gestori di diritto.

---

[58] E. Macchiavello, "*La travagliata evoluzione normativa dell'equity crowdfunding in Italia, il nuovo regolamento Consob e la prospettiva di regolazione del crowdfunding a livello europeo: una disciplina destinata a breve vita?*", in www.dirittobancario.it, 2018, p. 5 ss.

[59] E. Macchiavello, "*La travagliata evoluzione...*", *cit.*, p. 7.

[60] Rientrano in tale categoria le Sim, le imprese di investimento UE, le imprese di Paesi terzi diverse dalle banche autorizzate in Italia, i gestori di cui all'art. 1, comma 1, lett. q-*bis*), t.u.f., limitatamente all'offerta di quote o azioni di Oicr che investono prevalentemente in piccole e medie imprese, le banche autorizzate a prestare servizi di investimento.

L'art. 50-*quinquies*, comma 3, t.u.f. richiede che i gestori siano costituiti in determinate forme giuridiche[61], che abbiano la sede legale e amministrativa, o comunque una stabile organizzazione in Italia, e che l'oggetto sociale sia conforme alla definizione di "gestore di portale" indicata dal primo comma. Ancora, sono richiesti particolari requisiti di onorabilità dei soci di controllo e dei soggetti che svolgono funzioni di amministrazione, direzione e controllo; questi ultimi, devono possedere anche requisiti di professionalità, stabiliti dalla Consob.

Anche la disciplina dell'attività dei gestori dei portali varia a seconda che il gestore sia un gestore di diritto o un gestore iscritto nella sezione ordinaria del registro. I gestori di diritto sono tenuti a rispettare, oltre alla disciplina relativa alla loro attività (che potranno continuare a svolgere), anche la normativa in tema di *crowdfunding* dettata dall'art. 100-*ter* t.u.f. e dal Regolamento Consob[62].

Leggendo congiuntamente l'art. 50-*quinquies*, comma 3, lett. c) e l'art. 1, comma 5-*novies* t.u.f. si può ritenere che i gestori iscritti nella sezione ordinaria non debbano avere come oggetto sociale esclusivo lo svolgimento professionale del servizio di gestione di portali per la raccolta di piccole e medie imprese, e che possano svolgere – al di fuori del portale – qualsiasi altra attività non riservata dalla legge ad intermediari autorizzati[63]. In ogni caso, l'attività delle piattaforme deve rimanere entro i binari tracciati dall'art. 50-*quinquies*, che riproduce i limiti e le condizioni posti dall'art. 3 della MiFID II per l'esenzione dalla disciplina della direttiva.

A tal proposito, significativamente l'art. 13, comma 3, Reg. Consob dispone che il gestore debba astenersi dal formulare raccomandazioni riguardanti gli strumenti finanziari oggetto delle singole offerte atte ad influenzare l'andamento delle adesioni alle medesime. Chiara la *ratio* della disposizione, volta ad impedire che l'attività del gestore possa sfociare nel campo della consulenza[64].

5.2 Gli offerenti e gli strumenti di raccolta

Facendo riferimento all'art. 5-*novies* t.u.f., che detta la definizione di "*portale per la raccolta di capitali per le piccole e medie imprese e per le imprese sociali*", si deduce come nell'attuale quadro normativo la raccolta di capitali di rischio tramite offerta di proprie azioni e quote sociali per mezzo portali di *equity crowdfunding* sia riservata: 1) alle piccole e medie imprese così come definite dall'art. 2, par. 1., lett. f), primo alinea, del Regolamento (UE) 2017/1129 (c.d. Regolamento Prospetto); 2) alle imprese sociali, così come definite

---

[61] Possono avere forma giuridica di società per azioni, società in accomandita per azioni, società a responsabilità limitata o società cooperativa.

[62] E. Macchiavello, "*La travagliata evoluzione…*", *cit.*, p. 8.

[63] Per un'analisi approfondita del tema, si rinvia a M. Pinto, *L'equity based crowdfunding in Italia al di fuori delle fattispecie regolate dal 'Decreto Crescita'*, in *Società*, 2017, p. 818 ss., ed in particolare p. 824.

[64] E. Macchiavello, "*La travagliata evoluzione…*", *cit.*, p. 14.

dall'art. 1, comma 5-*duodecies*, t.u.f.; 3) agli organismi di investimento collettivo del risparmio o ad altre società che investono prevalentemente in piccole e medie imprese.

Al fine di estendere la possibilità di ricorrere allo strumento anche alle PMI costituite in forma di s.r.l., è stato necessario derogare a numerose e significative norme della disciplina codicistica della s.r.l., configurata come un modello "chiuso" di società.

L'art. 26, d.l. n. 179/2012 pone numerose e significative deroghe alla disciplina tradizionale, prevedendo innanzitutto che, in deroga a quanto stabilito dagli artt. 2468, commi 2 e 3 e 2479 c.c., l'atto costitutivo della piccola e media impresa possa creare diverse categorie di quote, fornite di diritti diversi, eventualmente prive del diritto di voto o dotate di diritto di voto non proporzionale alla partecipazione stessa o limitato ad alcuni argomenti o condizioni. Ancora, l'art. 100-*ter*, comma 1-*bis*, t.u.f. dispone che le quote di partecipazione delle s.r.l. rientranti nella categoria delle piccole e medie imprese possano essere oggetto di offerta al pubblico di prodotti finanziari anche[65] attraverso i portali per la raccolta di capitali. Infine, viene derogato l'art. 2474 c.c., che pone il divieto per la s.r.l. di compiere operazioni sulle proprie partecipazioni sociali.

Nella stessa prospettiva di facilitazione della sottoscrizione e dello scambio delle quote sottoscritte tramite portali di *equity based crowdfunding* deve essere letta la disciplina tracciata dagli ultimi commi dell'art. 100-*ter* t.u.f., che disegnano un regime alternativo di circolazione delle quote di s.r.l. sottoscritte tramite portali di *equity crowdfunding*[66].

Se il quadro normativo relativo ai soggetti che possono raccogliere capitale di rischio tramite i portali *on-line* è stato modificato da ultimo dal d.lgs. n. 129/2017, la l. n. 145/2018 (c.d. "legge finanziaria 2019") è intervenuta sull'universo *crowdfunding* introducendo nell'ordinamento italiano la possibilità di fare ricorso al *debt crowdfunding*, sicché oggi è possibile parlare, in Italia, di disciplina dell'*investment based crowdfunding*. In particolare, a seguito della modifica degli artt. 5-*novies* e 100-*ter* t.u.f. operata dalla legge n. 145, le piccole e medie imprese possono raccogliere finanziamenti tramite obbligazioni o strumenti finanziari di debito, purché la sottoscrizione sia riservata, nei limiti stabiliti dal codice civile, agli investitori professionali e a particolari categorie di investitori eventualmente individuate dalla Consob e sia effettuata in una sezione del portale diversa da quella in cui si svolge la raccolta del capitale di rischio.

---

[65] La formula legislativa non limita la deroga dell'art. 2468, comma 1, c.c. alle offerte condotte tramite portali di *crowdfunding* e dunque deve ritenersi possibile l'offerta al pubblico di quote di s.r.l. anche tramite diversi canali. Sul punto cfr. P. Benazzo, *Start-up e PMI innovative*, in *Digesto delle discipline privatistiche*, Sezione commerciale, Torino, 2017.

[66] Per un approfondimento della normativa, ed in particolare delle problematiche legate alla legittimazione ed alla circolazione delle quote, si rinvia a M. Cian, *L'intestazione intermediata delle quote di s.r.l. pmi: rapporto societario, regime della circolazione*, in *Nuove leggi civ. comm.*, 2018, p. 1260.

5.3 La raccolta condotta tramite portali di investment based crowdfunding *e gli obblighi del gestore*

L'art. 100-*ter* t.u.f. – oltre alle norme già esaminate in tema di *debt crowdfunding* ed alle deroghe alla normativa generale della s.r.l. – dispone che le offerte relative ai singoli strumenti finanziari emessi da piccole e medie imprese debbano avere un corrispettivo totale inferiore a quanto previsto dall'art. 34-*ter* del Regolamento Emittenti ai fini dell'esenzione dall'obbligo di predisporre il prospetto informativo per l'offerta di prodotti finanziari in Italia.

Al fine di ridurre l'asimmetria informativa, accentuata dall'esenzione per gli emittenti dall'obbligo di redigere il prospetto, la Consob – fissando le regole di condotta che i gestori devono rispettare nei confronti degli investitori, come previsto dall'art. 50-*quinquies*, comma 5, lett. d) t.u.f. – ha introdotto specifici oneri informativi in capo ai gestori di portali, sia sul versante delle singole offerte che su quello della rischiosità dell'investimento in sé.

A seguito della modifica all'art. 13 Reg. Consob, intervenuta con la delibera 19520/2016, è stata attribuita ai gestori iscritti nella sezione ordinaria la possibilità di scegliere se verificare direttamente che l'utente abbia il livello di esperienza e conoscenza necessario per comprendere le caratteristiche dell'ordine impartito – attività loro prima preclusa – o se demandare la verifica al soggetto che riceve e perfeziona l'ordine, momento essenziale del procedimento che porta alla sottoscrizione dello strumento offerto tramite il portale. Sebbene tale possibilità abbia semplificato il processo di conclusione dell'operazione, non appare ragionevole non estendere anche alla valutazione condotta da parte dei gestori di portali le soglie di esenzione dalla verifica dell'appropriatezza dell'investimento previste dall'art. 17, comma 3, Reg. Consob per i soggetti che ricevono e perfezionano gli ordini[67].

Ulteriori misure a protezione dell'investitore sono previste dall'art. 24 del Regolamento il quale, nell'attuare l'art. 100-*ter*, 2° co., t.u.f., impone al gestore di verificare che sia assicurata la protezione del socio investitore non professionale nel caso in cui i soci di controllo della piccola e media impresa trasferiscano il controllo a terzi diversi dagli investitori professionali o dalle altre categorie indicate al comma 2 che abbiano acquistato o sottoscritto l'offerta tramite il portale, indicando le modalità e le condizioni di esercizio del diritto (c.d. *tag-along*)[68].

Il secondo comma dell'art. 24 offre invece una tutela indiretta all'investitore non professionista, disponendo che «*ai fini del perfezionamento dell'offerta sul*

---

[67] E. Macchiavello, "*La travagliata evoluzione...*", *cit.*, p. 21.

[68] «*La clausola di* tag-along *obbliga un socio, normalmente quello di maggioranza, che intende vendere ad un terzo la propria partecipazione, a procurare la vendita delle quote partecipative anche del socio di minoranza, che il terzo acquirente si obbliga ad acquistare alle medesime condizioni*». La definizione è di A. Pavan, *Il crowdfunding: cambia il tradizionale sistema del 'fare impresa'*, Padova, 2018, p. 187.

portale» il gestore debba verificare che una certa quota[69] degli strumenti finanziari offerti sia stata sottoscritta da soggetti qualificati[70].

Similarmente a quanto previsto dalla MiFID II, tra gli obblighi del gestore rientra l'elaborazione di un'efficace politica sui conflitti di interesse che consenta di individuare e gestire tramite procedure e misure adeguate le situazioni di conflitto, in un'ottica di prevenzione di lesione degli interessi degli investitori (art. 13 Reg. Consob).

Particolare attenzione è posta ai casi in cui il gestore conduca sul proprio portale offerte aventi ad oggetto strumenti finanziari di propria emissione o emessi da soggetti controllanti, controllati o sottoposti a comune controllo. In questo caso l'esistenza di un conflitto di interesse appare scontata, sicché l'art. 13, comma 1-*ter* del Regolamento individua le misure minime che il gestore deve approntare per la loro gestione, mentre il comma 1-*bis* dispone che, nel caso in cui non sia possibile gestire il conflitto di interesse, «*tali misure includono l'astensione dal condurre tali offerte*».

6. La proposta della Commissione Europea per un Regolamento in materia di Financial Return Crowdfunding

La Commissione, nel 2018, ha varato il c.d. *FinTech Action Plan*[71] al fine di «*sfruttare i rapidi progressi tecnologici a vantaggio dell'economia, dei cittadini e dell'industria UE, di contribuire a rendere più competitivo e innovativo il settore finanziario europeo e di assicurare l'integrità del sistema finanziario UE*».

Sebbene in passato la Commissione abbia ritenuto che date le ridotte dimensioni del fenomeno non fosse necessario un intervento in materia[72], la successiva espansione dello stesso ha determinato un mutamento di indirizzo. In particolare, la Commissione ha constatato come gli interventi normativi intervenuti in alcuni Paesi presentino disomogeneità tali da ostacolare e scoraggiare la prestazione transfrontaliera dei servizi di *crowdfunding*[73] e, al fine di incentivare la creazione di un mercato europeo di tali servizi, ha presentato – contestualmente al *FinTech Action Plan* – una Proposta di Regolamento volta a creare un sistema normativo che permetta alle imprese che lo desiderino di

---

[69] Il comma 2 dell'art. 24 fissa tale soglia al 5%, che scende al 3% in caso di offerta effettuata da piccole e medie imprese in possesso della certificazione del bilancio e dell'eventuale bilancio consolidato, relativi ai due esercizi precedenti l'offerta, redatti da un revisore contabile o da una società di revisione iscritta nel registro dei revisori contabili.

[70] Investitori professionali, fondazioni bancarie, incubatori di *start-up* previsti dall'art. 25, comma 5, d.l. n. 179/2012, o da investitori a supporto delle piccole e medie imprese (definiti dalla stessa norma).

[71] Comunicazione della Commissione al Parlamento Europeo, al Consiglio, alla Banca Centrale Europea, al Comitato economico e sociale europeo e al Comitato delle regioni – Piano d'azione per le tecnologie finanziarie: per un settore finanziario europeo più competitivo e innovativo.

[72] Commissione UE, *Commission Staff Working Document – Crowdfunding in the EU Capital Markets Union*, 2016, p. 31.

[73] Cfr. considerando (5), (6) e (7) della Proposta di Regolamento emendata dal Parlamento Europeo.

operare in tutti gli Stati membri con un'unica licenza. Contestualmente a tale Proposta di regolamento, la Commissione ha prefigurato l'adozione di una Direttiva di modifica della MiFID II[74], tesa ad esentare dall'applicazione della stessa le imprese autorizzate – ai sensi del Regolamento – a prestare il servizio di *crowdfunding*. Dunque, se tale disegno normativo venisse definitivamente adottato, si realizzerebbe un "doppio regime".

Fermo restando che le imprese di investimento autorizzate ai sensi della MiFID II potranno gestire portali di *crowdfunding* soggiacendo alla disciplina propria della loro attività, i fornitori di servizi di *crowdfunding* non potranno prestare servizi diversi da quelli cui sono autorizzati ai sensi del Regolamento.

La Proposta della Commissione è stata approvata in prima lettura dal Parlamento europeo, che ha tuttavia apportato numerose ed incisive modifiche al testo[75], introducendo una distinzione tra servizi di *crowdfunding* diretto e intermediato e modificando l'assetto della vigilanza sui gestori di portali.

6.1 Ambito di applicazione

L'art. 2 della Proposta definisce e perimetra l'ambito di applicazione della disciplina, includendo tutti i soggetti che abbiano chiesto o ottenuto un'autorizzazione a prestare il servizio di *crowdfunding* ai sensi dell'art. 10 del Regolamento. Esclusi[76] da tale perimetro sono invece i servizi di *crowdfunding* prestati a titolari di progetti che siano consumatori, quelli prestati da imprese di investimento autorizzate ai sensi dell'art. 7 MiFid II,

---

[74] Il testo della direttiva proposta è disponibile all'indirizzo: https://ec.europa.eu/info/law/better-regulation/initiatives/com-2018-99_en

[75] La procedura di adozione è contrassegnata dal numero 2018/0048/COD.

[76] I considerando n. 11 *bis*, 15 *bis* e 15 *ter* della Proposta escludono dall'applicazione del Regolamento i fornitori di servizi di *crowdfunding* che utilizzano le *Initial Coin Offerings* (ICOs) sulla loro piattaforma, auspicando l'adozione, da parte della Commissione, di una Proposta normativa *ad hoc* per tali strumenti. In Italia, il Documento per la Discussione pubblicato in data 19 marzo 2019 dalla Consob riguardo "*Le offerte iniziali e gli scambi di cripto-attività*", mira ad avviare una discussione sulla possibilità di disciplinare le ICOs, la cui promozione ed offerta potrebbe realizzarsi non solo tramite piattaforme aventi come «*finalità esclusiva la promozione e realizzazione di offerte di cripto-attività di nuova emissione*» ma anche da parte dei gestori di portali di *crowdfunding* già esistenti. In tema di ICOs si segnalano i contributi di F. Annunziata, *Speak, If You Can: What Are You? An Alternative Approach to the Qualification of Tokens and Initial Coin Offerings*", in Bocconi Legal Studies Research Paper n. 2636561 (disponibile all'indirizzo: https://www.ssrn.com/abstract=3355329); P. Carriére, *Le "criptovalute" sotto la luce delle nostrane categorie giuridiche di "strumenti finanziari", "valori mobiliari" e "prodotti finanziari"; tra tradizione e innovazione*", in www.dirittobancario.it, 2019; Id, *Possibili approcci regolatori al fenomeno dei crypto-asset; note a margine del documento di consultazione della Consob*, ivi, 2019; E. Franza, *Nuove modalità di finanziamento: la blockchain per startup e piccole e medie imprese. Rischi e possibili vantaggi*, ivi, 2019; M. Nicotra, *Il regime giuridico delle ICOs. Analisi comparata e prospettive regolatorie italiane*, ivi, 2019; A. Sciarrone Alibrandi, *Offerte iniziali e scambi di cripto-attività: il nuovo approccio regolatorio della Consob*, ivi, 2019.

o da persone fisiche o giuridiche autorizzate in conformità al diritto nazionale[77] nonché le offerte superiori ad € 8.000.000,00 per offerta, valore calcolato su un periodo di 12 mesi per un dato progetto di *crowdfunding*. L'esclusione della possibilità per i consumatori di ottenere finanziamenti tramite le piattaforme autorizzate ai sensi del Regolamento appare legata all'obiettivo di favorire il finanziamento transfrontaliero delle imprese[78], così come previsto dalla *Capital Markets Union*, ma a ben guardare sarebbe stato opportuno includere nell'intervento anche i servizi prestati ai consumatori in modo da creare anche per questi un canale di finanziamento alternativo ed indipendente dal sistema creditizio tradizionale, stimolando al contempo la concorrenza nel settore.

6.2 I fornitori di servizi

L'art. 10 dispone che i soggetti che desiderino prestare servizi di *crowdfunding* a norma del Regolamento debbano essere autorizzati dall'Autorità dello Stato membro in cui sono stabiliti[79]. La domanda di autorizzazione deve contenere una gamma di informazioni necessarie affinché l'Autorità possa verificare il rispetto dei requisiti e delle condizioni operative richiesti dalla normativa per l'ottenimento dell'autorizzazione.

All'esito dell'istruttoria, l'Autorità, con provvedimento motivato, può concedere o negare l'autorizzazione allo svolgimento dell'attività, qualora esistano «*ragioni obiettive e dimostrabili per ritenere che la gestione del fornitore di servizi di* crowdfunding *possa compromettere la sua gestione efficace, sana e prudente e la sua continuità operativa, nonché un'adeguata considerazione degli interessi dei clienti e dell'integrità del mercato*» (art. 10, par. 6).

Se l'istruttoria ha esito positivo, l'Autorità informa l'ESMA affinché iscriva il soggetto autorizzato nel Registro tenuto ai sensi dell'art. 11.

Il ruolo dell'ESMA, tuttavia, non si esaurisce nella tenuta del Registro; ancorché spogliata – a seguito delle modifiche apportate dal Parlamento – della

---

[77] Le piattaforme che vorranno operare a livello europeo nella cornice offerta dalla Proposta di Regolamento dovranno dunque rinunciare alla licenza eventualmente ottenuta secondo il regime nazionale. Sul punto, cfr. E. Macchiavello, "*La proposta della Commissione Europea di un Regolamento in materia di crowdfunding*", in www.dirittobancario.it, 2018, p. 4.

[78] Cfr. considerando (8).

[79] Ai sensi dell'art. 4, par. 1, requisito indispensabile per l'ottenimento dell'autorizzazione è l'avere una sede effettiva e stabile in uno Stato membro, essendo per contro vietata la presentazione della domanda di autorizzazione a persone giuridiche stabilite in un Paese terzo. In ogni caso, la sede effettiva e stabile in uno Stato membro è sufficiente affinché il fornitore possa svolgere la propria attività in tutti gli Stati membri, essendo fatto espresso divieto a questi di imporre ai fornitori di servizi la presenza fisica nel loro territorio (cfr. art. 10, par. 9).
Una rilevante modifica apportata dal Parlamento europeo alla Proposta formulata dalla Commissione riguarda l'Autorità competente per l'autorizzazione e la vigilanza sui prestatori di servizi di *crowdfunding*, che la Commissione aveva individuato nell'ESMA. A seguito della modifica, sono state inserite una serie di norme di coordinamento tra le Autorità dei diversi Paesi (cfr. art. 13-*bis*).

competenza in merito all'autorizzazione dei fornitori di servizi, l'Autorità europea conserva il potere di «*chiedere informazioni per garantire la coerenza delle autorizzazioni concesse dalle autorità nazionali competenti* (…). *Se non concorda con la decisione dell'autorità nazionale competente di accogliere o respingere una domanda di autorizzazione* (…), *l'ESMA espone le proprie motivazioni spiegando e giustificando i punti in cui si discosta sensibilmente da tale decisione*» (art. 10, par. 6-*bis*).

Il testo della Proposta non prevede un meccanismo di risoluzione della controversia tra l'ESMA e l'Autorità nazionale, sicché si possono prospettare diverse ipotesi di superamento del contrasto. Una prima ipotesi vedrebbe la decisione dell'ESMA prevalere su quella dell'Autorità nazionale, sicché l'Autorità europea potrebbe iscrivere (o non iscrivere) nel Registro un fornitore di servizi sulla base delle proprie valutazioni, con ciò non limitandosi al controllo dell'attività dell'Autorità nazionale competente, ma sostituendo la propria valutazione a quella dell'Autorità nazionale. A tale ipotesi, che menomerebbe la competenza dell'Autorità nazionale sul procedimento di autorizzazione del fornitore di servizi, sembra preferibile l'ipotesi secondo la quale, a seguito delle determinazioni dell'ESMA, l'Autorità nazionale debba valutare nuovamente la domanda di autorizzazione del fornitore di servizi.

Anche in questo caso, tuttavia, bisognerebbe chiarire se l'Autorità nazionale sarebbe libera di decidere di discostarsi o meno dalle determinazioni dell'ESMA – con ciò mantenendo intatta la propria competenza sul procedimento di autorizzazione – o se il contenuto della comunicazione dell'Autorità europea sarebbe vincolante per l'Autorità nazionale – con ciò attribuendosi all'ESMA un potere di intervento e sostituzione dell'Autorità nazionale analogo a quello della prima ipotesi.

6.3 L'attività dei fornitori di servizi

In seguito all'autorizzazione, i gestori vengono abilitati a svolgere l'attività di "servizio di *crowdfunding*", a sua volta distinto dall'art. 3 del Regolamento tra "*crowdfunding diretto*" e "*crowdfunding intermediato*".

La prima categoria include "*l'agevolazione dell'abbinamento tra uno specifico investitore e uno specifico titolare del progetto e l'agevolazione dell'abbinamento tra uno specifico titolare del progetto e uno specifico investitore*"; la seconda include "*l'agevolazione dell'abbinamento tra un investitore e un titolare del progetto e la determinazione dei prezzi e dei pacchetti di offerte a tale riguardo, oppure l'agevolazione dell'abbinamento tra un titolare del progetto e un investitore e la determinazione dei prezzi delle offerte a tale riguardo, o entrambe*" nonché, ai sensi dell'art. 4-*bis*, il collocamento senza garanzia di valori mobiliari o dell'agevolazione di prestiti emessi da titolari di progetti, l'offerta di consulenza in materia di investimenti per quanto riguarda i valori mobiliari o l'agevolazione di prestiti

emessi da titolari di progetti nonché la ricezione e trasmissione degli ordini dei clienti per quanto riguarda i valori mobiliari o l'agevolazione di prestiti emessi da titolari di progetti.

Confrontando le definizioni di cui all'art. 3, nel *crowdfunding* diretto, il gestore si limita ad agevolare l'incontro tra due specifici utenti; nel *crowdfunding* intermediato, l'attività del gestore si estende anche al *pricing* ed al *packaging* delle offerte nei confronti dell'investitore.

6.4 La disciplina dell'attività

La disciplina dell'attività prestata dai fornitori di servizi di *crowdfunding* appare ispirata alla normativa in materia di servizi e attività di investimento e contempla obblighi di condotta a carico del gestore della piattaforma, norme in tema di conflitti di interessi, obblighi informativi volti ad assicurare una scelta consapevole dell'investitore.

Al fine di svolgere la propria attività senza arrecare danno agli utenti e al mercato, ai sensi dell'art. 5 il gestore deve definire ed applicare politiche e procedure idonee a garantire una gestione efficace e prudente[80]. Nel dettare criteri di massima per la gestione efficace e prudente delle piattaforme, l'art. 5 introduce un primo tratto di discontinuità nella disciplina dei fornitori di servizi di *crowdfunding* diretto ed intermediato; a questi ultimi viene richiesto di predisporre sistemi e controlli adeguati per la gestione del rischio e la modellazione finanziaria in relazione all'offerta dei propri servizi[81].

Particolarmente delicato è l'esercizio di poteri discrezionali da parte del gestore; dispone l'art. 4, par. 4, che i fornitori di servizi possono effettuare scelte discrezionali per conto dei loro clienti in relazione ai parametri degli ordini ricevuti, purché comunichino ai clienti il metodo e i parametri esatti delle scelte, adottando tutte le misure necessarie per ottenere il miglior risultato possibile per i clienti. In ogni caso, ai gestori dovrebbe essere preclusa la possibilità di "*effettuare alcun abbinamento discrezionale o non discrezionale tra gli interessi*

---

[80] Tra questi, particolare importanza rivestono i meccanismi di continuità operativa, la cui implementazione è fondamentale per tutelare l'utente che, in caso di *default* della piattaforma, rischierebbe di vedere interrotta la prestazione del servizio con conseguente difficoltà nel recupero delle somme investite, la separazione delle funzioni e l'elaborazione di un'efficace *policy* in tema di conflitti di interesse.

[81] Gli emendamenti del Parlamento europeo hanno disposto che il gestore effettui almeno un livello minimo di *due diligence* nei confronti del soggetto che intenda raccogliere fondi tramite la piattaforma, fissando a tal fine alcuni requisiti minimi (art. 5 *bis*). Sebbene la scelta di introdurre una regolamentazione in tal senso sia condivisibile, sarebbe auspicabile la determinazione di elementi di valutazione più puntuali e penetranti.

di acquisto e di vendita", attività che richiederebbe un'autorizzazione come impresa di investimento o come mercato regolamentato[82].

Un aspetto particolarmente critico dell'operatività delle piattaforme riguarda la possibilità che queste possano partecipare al finanziamento di progetti presenti sulla loro piattaforma. Il ricorso a tale meccanismo, adottato spontaneamente dalle piattaforme per dimostrare l'affidabilità delle loro valutazioni, era vietato nella proposta formulata dalla Commissione, mentre il Parlamento europeo guarda con favore alla possibilità che le piattaforme finanzino i progetti proposti purché la politica di allineamento degli interessi venga presentata ed approvata dall'ESMA[83], sia illustrata chiaramente sul sito *web* della piattaforma e il finanziamento della piattaforma non superi il 2% del capitale raccolto per il progetto.

L'art. 17 della Proposta di Regolamento prevede che i fornitori di servizi di *crowdfunding* possano permettere agli utenti di interagire tra loro «*per l'acquisto di contratti di prestito o valori mobiliari che sono stati inizialmente oggetto di* crowdfunding *sulle loro piattaforme*», informandoli tuttavia che tale servizio, essendo distinto dall'attività delle sedi di negoziazione, non è soggetto alla disciplina dettata dalla MiFID II in materia. In ogni caso, l'attività di vendita o acquisto sul mercato secondario è a discrezione del cliente, che ne è responsabile[84].

6.5 Obblighi informativi e test di "adeguatezza"

Particolare attenzione viene dedicata dal Regolamento alle informazioni veicolate agli investitori tramite la piattaforma, che vengono disciplinate sia sotto il versante dell'informativa contrattuale, che dal punto di vista delle comunicazioni pubblicitarie, oggetto di una disciplina specifica.

Il Regolamento dispone che i fornitori di servizi devono fornire agli utenti tutte le informazioni su loro stessi, sui rischi finanziari, sui costi ed oneri connessi al servizio prestato o all'investimento, compresi i rischi di *default* della piattaforma

---

[82] Cfr. considerando (35).
Particolare attenzione è dedicata dall'art. 7 del Regolamento alla gestione dei conflitti di interesse. I gestori di piattaforme devono definire norme interne e adottare tutte le misure opportune per evitare, individuare, gestire e comunicare i conflitti di interesse che possono sorgere tra loro stessi (e i soggetti a loro legati individuati dalla norma) e gli utenti o tra utenti diversi. In ogni caso, la piattaforma non può accettare come clienti i propri azionisti che detengono il 20% o più del capitale azionario o dei diritti di voto, i propri dirigenti o qualsiasi persona direttamente collegata a tali azionisti e dirigenti. I gestori comunicano su supporto durevole, in maniera dettagliata, la natura generale e le fonti dei conflitti di interesse e le misure adottate per attenuare tali rischi.

[83] Non appare chiaro perché tale verifica debba essere effettuata da ESMA, se competenti per l'autorizzazione del richiedente sono le Autorità nazionali.

[84] Nel caso in cui i gestori forniscano un prezzo di riferimento per l'acquisto o la vendita, sarebbero obbligati ad indicare la vincolatività o meno di tale prezzo e la base sulla quale è stato individuato. Un ulteriore requisito di trasparenza è previsto nel caso di cessione di un credito concesso tramite la piattaforma: in questo caso i fornitori di servizi di *crowdfunding* dovrebbero fornire informazioni sui risultati dei prestiti generati.

e i criteri di selezione dei progetti. Oltre a questo nucleo di informazioni, il Parlamento – con l'evidente intento di responsabilizzare la piattaforma nella selezione di progetti validi e di sensibilizzare l'utente sui rischi dell'investimento – ha introdotto l'art. 14 *bis*, che impone al gestore di pubblicare, con cadenza annuale, i tassi di *default* dei progetti offerti tramite la loro piattaforma nel corso dei 24 mesi precedenti[85]. Tutte le informazioni veicolate tramite la piattaforma devono essere eque, chiare e non fuorvianti, preferibilmente presentate in maniera disaggregata[86], concisa, precisa e facilmente accessibile. Le informazioni devono essere fornite ogni volta risulti appropriato, anche prima che sia effettuata l'operazione di *crowdfunding*.

Il disegno di un'informazione fruibile per l'utente-tipo di un servizio di *crowdfunding* passa per l'esenzione dall'obbligo di redigere un prospetto informativo, sostituito da una scheda contenente le informazioni chiave sull'investimento la cui comprensione dovrebbe risultare più semplice[87].

Il contenuto della scheda, disciplinato dall'art. 16, diverge a seconda che il gestore presti un servizio di *crowdfunding* diretto o intermediato.

La scheda deve contenere una segnalazione di rischio di perdita del capitale e di illiquidità degli strumenti, nonché una formula che dichiara preliminarmente che l'offerta di *crowdfunding* non è stata verificata né approvata dall'ESMA o dalle Autorità nazionali competenti[88]. Infine, la scheda deve avvertire l'investitore che non è stata condotta alcuna verifica circa l'adeguatezza dell'investimento alle sue conoscenze.

All'ESMA è affidato il potere di elaborare progetti di norme tecniche di regolamentazione al fine di specificare meglio i contenuti della scheda informativa, anche mediante l'utilizzo di alcuni indici finanziari, tenendo in debita considerazione le differenze tra i servizi di *crowdfunding* diretto e intermediato.

L'art. 15 impone la raccolta di informazioni circa l'esperienza finanziaria del cliente, i suoi obiettivi di investimento, la sua situazione finanziaria e la comprensione dei rischi legati all'investimento[89]. Sebbene l'art. 15 oneri di tale valutazione "i fornitori di servizi di *crowdfunding*", il terzo paragrafo dell'art. 16 sembra voler escludere da tale onere i fornitori di servizi di *crowdfunding* diretto, imponendo l'inserimento nella scheda informativa destinata al cliente di una formula volta ad avvertirlo che la sua formazione e la sua conoscenza non sono state valutate al fine di concedergli l'accesso all'investimento. Tale lettura appare indirettamente confermata dal quarto paragrafo dell'art. 15 che,

---

85 All'ESMA è demandato il compito di individuare norme tecniche di regolamentazione al fine di specificare i metodi di calcolo del tasso di default.

86 Cfr. considerando (29).

87 Cfr. considerando (12-*bis*).

88 Simile avvertimento è previsto dalla normativa italiana. In ogni caso, è fatto espresso divieto alle Autorità nazionali di richiedere la notifica o l'approvazione *ex ante* della scheda.

89 L'ESMA è incaricata di meglio specificare tali requisiti mediante norme tecniche di regolamentazione.

nel regolare la simulazione della capacità di sostenere perdite, si rivolge a "*tutti i fornitori di servizi di* crowdfunding", mentre come già anticipato, i primi paragrafi si riferiscono semplicemente a "*i fornitori di servizi di* crowdfunding".

Nel caso in cui la valutazione della comprensione e dell'adeguatezza dell'offerta all'investitore abbia esito negativo, il gestore deve informarlo della non appropriatezza, emettendo a tal fine una segnalazione di rischio che indichi chiaramente il rischio di perdita del capitale investito. In ogni caso, emesso l'avvertimento, il gestore potrà dare seguito all'investimento, su scelta dell'investitore.

A norma del par. 5, tutti i fornitori di servizi di *crowdfunding* offrono, in qualsiasi momento, ai potenziali investitori e agli investitori, la possibilità di simulare la loro capacità di sostenere perdite, quantificata pari al 10% del loro valore netto.

Un breve cenno, infine, va fatto alle disposizioni dettate in tema di comunicazioni di *marketing* delle piattaforme, che mirano a delineare un regime facilitato per la conduzione delle campagne pubblicitarie. Le comunicazioni di *marketing* devono essere chiaramente identificabili come tali, non devono dedicare un'attenzione sproporzionata ad un progetto piuttosto che ad un altro[90] e devono essere redatte in inglese o in una o più lingue ufficiali dello Stato membro in cui è attivo il gestore[91].

*7. Considerazioni finali sull'***investment based crowdfunding**

Analizzando il *P2P lending*, bisogna osservare che dato il regime di *opt in* che caratterizza la Proposta di Regolamento, il legislatore italiano potrebbe intervenire sul *P2P lending* anche in caso di approvazione della Proposta pendente in sede europea. In ogni caso quest'ultima, determinando requisiti minimi in tema di *due diligence*, fissando l'obbligo di redazione di una *policy* in tema di conflitti di interesse, regolamentando le pratiche di allineamento degli interessi tra piattaforma e utente e dei flussi informativi tra piattaforma e utente, e imponendo l'adozione di dispositivi di continuità, fissa misure idonee a gestire i rischi caratteristici dell'operatività delle piattaforme di *P2P lending*.

Sul versante dell'*investment based crowdfunding*, il confronto tra la normativa italiana e la adottanda normativa europea mostra – sebbene l'approccio sia in generale piuttosto simile – alcune differenze.

Innanzitutto, la Proposta individua un regime disciplinare diverso a seconda che il fornitore presti un servizio di *crowdfunding* diretto o intermediato, così graduando i requisiti di gestione e alcuni obblighi (es. di condurre il *test* sulla conoscenza del cliente) in base all'attività più o meno

---

[90] Chiara declinazione dell'obbligo del gestore di agire in modo "equo".

[91] Il considerando (34) auspica che le comunicazioni di *marketing* non siano soggette a traduzione.

pervasiva del gestore. Nella complessiva economia della disciplina, pare che i fornitori di servizi di *crowdfunding* diretto debbano fornire all'investitore più informazioni riguardanti il titolare del progetto affinché possa valutare autonomamente l'opportunità dell'investimento, mentre i fornitori di servizi di *crowdfunding* intermediato – onerati della valutazione dell'appropriatezza dell'investimento al cliente – possano condividere minori informazioni sul titolare del progetto, dovendo tuttavia fornire maggiori informazioni sulla propria operatività.

Inoltre, i prestatori di servizi di *crowdfunding* intermediato che opereranno con licenza europea, potranno svolgere le attività di consulenza e di collocamento senza impegno irrevocabile precluse alle piattaforme sottoposte al regime normativo italiano.

Altre differenze tra il regime disegnato dalla Proposta di Regolamento europeo e la normativa dell'*investment based crowdfunding* attengono all'obbligo per tutti i fornitori di servizi di *crowdfunding* autorizzati dalla normativa europea di sottoporre i clienti ad un *test* di simulazione delle perdite.

Un'ultima considerazione riguarda la possibilità che nasca un vero e proprio mercato europeo dell'*investment based crowdfunding*. Dato il regime di *opt in*, saranno le piattaforme a decidere se chiedere o meno l'autorizzazione ad operare a livello comunitario, scegliendo in definitiva se operare a livello europeo, con una licenza ottenuta secondo quanto previsto nella Proposta di Regolamento, o se limitare la propria attività a livello nazionale, magari con una legislazione più favorevole.

Strumenti digitali e finanza

Paola Lucantoni

1. Digitalizzazione dei servizi finanziari e democratizzazione del mercato – 1.1 Il trading on-line *e le sue principali evoluzioni: l'*high frequency trading *– 1.2* Robo-advisor*: aspetti definitori e classificatori – 1.3* Crowdfunding*: funzionamento e tipologie "finanziarie" – 2. Regolamentazione della piattaforma – 2.1* Trading on-line *e principio di neutralità tecnologica – 2.2* High frequency trading*: una proposta di vigilanza algoritmica semplificata – 2.3* Robo-advisor*: dalla neutralità tecnologica all'*algo-governance *– 2.4* Crowdfunding*: il caso dei gestori dei portali – 3. Verso una nuova regolamentazione delle piattaforme – 4. Conclusione*

1. Digitalizzazione dei servizi finanziari e democratizzazione del mercato

La recente crisi finanziaria seguita dall'attuale rivoluzione digitale ha favorito l'implementazione di sempre più nuove tecnologie anche nel mondo della finanza[1]. Si è di fronte a un panorama finanziario in cui è possibile scorgere l'introduzione di strumenti digitali nuovi e innovativi con lo scopo di facilitare l'accesso ai servizi finanziari, di ridurre i costi di prestazione dei servizi o, addirittura, di sopperire alla crisi che ha coinvolto, dal 2008, i canali di finanziamento tradizionali[2].

La digitalizzazione semplifica indubbiamente l'accesso ad un determinato servizio finanziario. Alcuni strumenti, come il "*trading on-line*" e i "*robo-advisor*", ad esempio, hanno fatto acquisire la possibilità al cliente di poter godere dei servizi, rispettivamente, di ricezione e trasmissione di ordini e di consulenza in materia di investimenti comodamente da casa o nel diverso luogo in cui lo stesso si trova. Altri, come il *crowdfunding*, hanno facilitato l'accesso ai servizi di finanziamento, individuando "nuovi" finanziatori fra la "folla" dei risparmiatori.

Tutto ciò è possibile solo grazie a vere e proprie "piattaforme" digitali: "basi" virtuali dalle quali gli intermediari finanziari posso offrire i propri servizi con una disponibilità e capillarità mai vista nel passato. Non è più, dunque, necessario aprire filiali o assumere numeri elevati di consulenti finanziari; ciò che è sufficiente è, ormai, solo un buon programma per elaboratore, ergo un "algoritmo", collegato a *Internet* che faccia acquisire onnipresenza al servizio fornito, fornendone una sempre maggiore facilità di accesso.

L'utilizzo di *Internet* già prima e le nuove tecnologie – quali l'intelligenza artificiale o la criptografia – ora, favoriscono anche una maggiore apertura nonché una vera e propria democratizzazione del sistema finanziario. I servizi che

---

[1] Le grandi rivoluzioni industriali degli ultimi tre secoli si caratterizzano per una sempre maggiore automazione dell'attività produttiva a seguito dello sviluppo scientifico e tecnologico. Se così nella prima rivoluzione industriale (XVIII sec.) l'utilizzo della forza dell'acqua e del vapore ha consentito la meccanizzazione dell'attività produttiva; nella seconda (XIX sec.), con l'impiego dell'elettricità si è assistito alla produzione di massa attraverso le catene di montaggio; nella terza (XX sec.) invece la comparsa dei computer ha permesso l'automazione di molti processi produttivi. Con l'avvento dell'industria 4.0 tuttavia lo scenario è profondamente cambiato. L'evoluzione tecnologica del primo decennio del terzo millennio, infatti, ha inciso profondamente nei meccanismi produttivi dell'economia globalizzata con l'introduzione dell'intelligenza artificiale nei processi decisionali, finora sede privilegiata dell'attività dell'uomo. Nella prospettiva del giurista, le *smart factories* della quarta rivoluzione industriale si caratterizzano così per la previsione dell'intelligenza artificiale non come mero fattore dell'organizzazione produttiva ma come organizzazione stessa dei fattori produttivi.
In argomento cfr. E. Micheler, *Regulatory Technology – Replacing Law with Computer Code*, (2018), disponibile su https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3210962; D. Zetzsche, R. Bucley, D. Arner e J. N. Barneris, *Regulating a Revolution: From Regulatory Sandboxes to Smart Regulation*, *European Banking Institute Working Paper* Series No. 11 (2017); T.C.W. Lin, *The New Investor*, in 60 *UCLA L. Rev.* 678 (2013).

[2] Sulla correlazione fra la crisi finanziaria e lo sviluppo dello strumento dell'*equity crowdfunding* è possibile rimandare a S.L. Furnari, *Market analysis, economics and success drivers of equity crowdfunding*, in *Proceedings of the 3rd Entrepreneurial Finance Conference*, 2018, pp. 4-8.

una volta non potevano che essere resi da intermediari specializzati all'interno delle proprie sedi fisiche ormai possono essere prestati anche da intermediari più semplici e "nuovi" ma, soprattutto, possono essere messi a disposizione di qualsiasi cliente che può interagirvi comodamente da casa.

Queste sono dunque le maggiori novità che la rivoluzione digitale ha portato con sé: la ridefinizione del ruolo dell'intermediario, soggetto sempre più tecnologico e meno "presente", e la possibilità di offrire i propri servizi a un numero sempre maggiore di clienti. Cliente che, con l'avanzare delle generazioni, diventa sempre più tecnologico e, dunque, attirato, quasi per bisogno, dalla prestazione di servizi finanziari in maniera altrettanto tecnologica.

È in questo incrocio di nuovi fattori che nascono nuovi strumenti per l'investitore: le piattaforme di *trading on-line*, i *robo-advisor* e il *crowdfunding*.

1.1 Il trading on-line *e le sue principali evoluzioni: l'*high frequency trading

Con il termine *trading on-line* si intende la compravendita e la negoziazione di strumenti finanziari tramite *Internet*. Ciò è possibile grazie a una piattaforma *web*, un semplice sito *Internet* che consente al cliente-investitore di accedere, grazie a una *password* personale, a un'apposita sezione in cui potrà acquistare e vendere strumenti finanziari all'interno delle sedi di negoziazione cui l'intermediario, per conto del cliente, invierà gli ordini di compravendita ricevuti[3].

Il nuovo impianto normativo *post* MiFID II consente la partecipazione ai mercati regolamentati e ai sistemi multilaterali di negoziazione unicamente agli intermediari, autorizzati ai sensi del nuovo Regolamento Intermediari[4], cui viene riconosciuto un codice identificativo di negoziazione[5]. La concreta ammissione dell'intermediario autorizzato alle negoziazioni è, poi, di competenza del gestore della sede di negoziazione, nel quadro delle regole disposte dalla sede stessa e sottoposte all'approvazione della Consob. L'accesso ai mercati da parte di soggetti diversi dagli intermediari autorizzati è possibile unicamente nella duplice forma del *Direct Electronic Access* che consente ai clienti di accedere al mercato utilizzando (*Direct Market Access*) o meno (*Sponsored Access*) il codice identificativo di negoziazione dell'intermediario autorizzato a partecipare al mercato e servendosi delle infrastrutture messe a disposizione dall'intermediario stesso.

---

[3] Sul tema v. R. Torino, *La commercializzazione via* internet *di servizi di investimento e strumenti finanziari e il* trading on line*,* in E. Gabrielli e R. Lener, *I Contratti del Mercato Finanziario* a cura di E. Gabrielli e R. Lener, Torino, 2004, vol. I, p. 626.

[4] Adottato dalla Consob con delibera n. 20307 del 15 febbraio 2018.

[5] L'eccezione alla necessità di ottenere una specifica autorizzazione per la negoziazione in conto proprio, di cui all'art. 2, par. 1, lett. d) e j) t.u.f. non si applica nel caso di utilizzazione di una tecnica di negoziazione algoritmica ad alta frequenza.

Grazie alla predisposizione di una piattaforma che opera in maniera automatica, l'intermediario offre principalmente il servizio su base continuativa di esecuzione di ordini per conto dei clienti nonché quello di ricezione e trasmissioni di ordini.

Il *trading on-line* permette dunque al cliente-investitore di allocare le proprie risorse all'interno delle diverse sedi di negoziazione messe a disposizione dell'intermediario in maniera libera e diretta; viene, infatti, meno la necessità di passare per una persona fisica (solitamente l'impiegato della propria banca) al quale dover trasmettere l'ordine. In questo modo, così come l'informazione viaggia velocemente, così anche le scelte di investimento possono viaggiare altrettanto velocemente nonché essere adattate o modificate a piacimento dal cliente-investitore.

Mentre il *trading on-line* non può più essere definito uno strumento "recente"[6], lo stesso negli ultimi anni ha subito alcune importanti evoluzioni. Si parla del trading algoritmico e della sua sub-categoria nota con il nome di *high frequency trading*. Diversamente da quanto accade nel *trading on-line*, nel trading algoritmico le scelte di investimento vengono prese direttamente da un programma informatico sulla base delle istruzioni inserite all'interno della stessa dal relativo programmatore. Quando l'algoritmo alla base del programma di *trading* viene impostato per rispondere in maniera molto rapida agli "stimoli" recepiti all'interno del sistema di negoziazione si parla allora più propriamente di *high frequency trading*.

L'ordinamento contiene delle precise definizioni di negoziazione algoritmica, anche ad alta frequenza[7]. In particolare, si definisce negoziazione algoritmica l'attività di *trading* in cui le decisioni fondamentali della negoziazione, *inter alia,* sul se, quando e a che prezzo inviare l'ordine sono definite da un algoritmo informatizzato. La norma esclude dalla definizione, di per sé vasta, solo i sistemi utilizzati meramente per trasmettere ordini, senza lasciare all'algoritmo la definizione delle "scelte" inerenti l'invio dell'ordine[8].

---

6 La regolamentazione di riferimento, come si dirà *infra*, è, infatti, ascrivibile ai primi anni 2000.

7 Si vedano le definizioni di negoziazione algoritmica e negoziazione algoritmica ad alta frequenza contenute, rispettivamente, nei comma 6-*quinquies* e 6-*septies* dell'art. 1 del Testo unico della finanza in recepimento dei punti 39) e 40) dell'art. 4, comma 1, della MiFID II e dell'art. 20 del Regolamento Delegato (UE) n. 2017/565.

8 Sui profili definitori cfr. M. Gargantini e M. Siri, *Il "prezzo dei prezzi". Una soluzione di mercato ai rischi dell'*high frequency trading, relazione presentata al X Convegno Annuale dell'Associazione Italiana dei Professori Universitari di Diritto Commerciale "Orizzonti del Diritto Commerciale", 22-23 febbraio 2019, p. 3 del dattiloscritto; G. Balp e G. Strampelli, *Preserving Capital Market Efficiency in High-Frequency Trading Era,* 2018, disponibile su https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3097723, R. Veil, *European Capital Markets Law,* Oxford and Portland, Oregon, 2017, p. 481 ss.; P.H. Cognac, *Algorithmic Trading and High Frequency*Tradin *(HTF)*, in D. Busch e G. Ferrarini (a cura di), *Regulation of the EU Financial Markets, MiFID II and MiFIR,* Oxford Press University, 2017, p. 469; D. Leis, *High Frequency Trading: Market Manipulation and Systemic Risks from an EU Perspective*, 2012, disponibile su https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2108344; P. Gomber, L. Björn, M. Lutat, T. Uhle, *High Frequency Trading*, 2011, disponibile su https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1858626 e ESMA, *Final Report, Technical Advice to the Commission on MiFID II and MiFIR,* 19 December 2014, ESMA/2014/1569, p. 342, No. 3.

Nel caso dell'*high frequency trading,* l'algoritmo viene programmato per "agire" in maniera molto rapida agli stimoli individuati dal relativo programmatore; ne risulta che all'elemento della "programmabilità", in comune con il trading algoritmico, si aggiunge anche quello della "velocità", che andrà ad influire su ogni aspetto del suo operare: dalla valutazione delle informazioni circostanti, all'inoltro o l'annullamento di ordini ad esso collegati.

L'automazione dei processi decisionali dell'attività di *trading* non implica però che l'attività decisionale umana sia inesistente. Difatti, la programmabilità, caratteristica tipica di qualsiasi tecnologia che basi il proprio funzionamento su un sistema di algoritmi, comporta che il *trader* (*rectius* l'essere umano che sta dietro la macchina) imposti una serie di regole che stabiliscono *a priori* le reazioni del *trader*-macchina alla ricezione di una determinata informazione. Grazie a queste regole, il programma di *trading* "agisce" inoltrando e/o ritirando ordini al ricorrere delle condizioni prefissate. Ne risulta che, contrariamente a quanto sembrerebbe desumersi dalla definizione normativa, esiste quindi un'attività decisionale umana che però funge solo da "guida" ed "indirizzo" per i compiti e la serie di azioni che verranno poi svolti in concreto dal programma.

Punto di forza dell'algoritmo è la capacità di selezionare e processare le informazioni in tempi molto rapidi. All'interno di un mercato, "tutto" può diventare un'informazione rilevante per l'algoritmo[9]. Ciò è vero in modo particolare con riferimento al comportamento degli altri *trader*, uomini o macchine che essi siano. Da qui, l'osservazione che il comportamento di un *trader* algoritmico è intrinsecamente dipendente da quello di un altro *trader*. Correlazione che, di per sé, non rappresenta una novità del settore delle negoziazioni di strumenti finanziari.

L'importante differenza rispetto al passato risiede, però nella gestione dell'imprevisto o dell'anormalità[10].

Poiché le macchine (ancora oggi) non hanno la possibilità di vedere oltre i propri schemi matematici e cioè, più precisamente, di comportarsi diversamente da come sono programmate, queste non sono in grado di individuare comportamenti anomali all'interno del mercato e quindi non hanno la possibilità di fermarsi di fronte a una particolare situazione in cui un *trader* "umano" smetterebbe di negoziare se quella precisa ipotesi non fosse stata già prevista in maniera specifica dal proprio programmatore (con tutte le difficoltà che questo esercizio di previsione richiede). Conseguenza ultima è quella per cui maggiore è la presenza di *trader* algoritmici all'interno di un mercato e maggiore sarà la correlazione

---

[9] Sul ruolo dell'informazione nel mercato cfr,. *ex multis*, G. Carriero, *Informazione, mercato, Buonafede: il cosiddetto* insider trading, Milano, 1992; A. Perrne, *Informazione al mercato e tutele dell'investitore*, Milano, 2003 e F. Sartori, *Informazione economica e responsabilità civile,* Milano, 2011.

[10] Per un'analisi del *flash crash*, fenomeno di *shock* del mercato originato dall'uso delle negoziazioni algoritmiche v. E. O. Barrales, *Lessons from the flash crash for the regulation of high frequency traders*, in 17 *Fordham J. Corp. & Fin. Law* 1195, 2012, e M. J. McGowan, *The Rise of Computerized High-Frequency Trading: Use and Controversy*, in 16 *Duke L. & Tech. Rev.* 1, 2010.

fra i comportamenti dei soggetti partecipanti all'interno del mercato. Ciò implica una maggior facilità di provocare reazioni a cascata i cui effetti possono essere pericolosi per la stabilità dei mercati e la sicurezza dei loro partecipanti.

L'aspetto che in questa sede preme evidenziare è che grazie alla predisposizione di strumenti digitali, quali le menzionate "piattaforme di *trading*", si è ormai reso possibile mettere a disposizione dei propri clienti un servizio libero da intermediari "fisici". La presenza e il ruolo dell'intermediario degradano, allora, alla mera predisposizione della piattaforma e al controllo del corretto funzionamento della stessa. Il servizio tende, quindi, sempre di più a de-caratterizzarsi dall'intermediario che lo predispone, il quale rimane una figura ormai quasi in ombra.

1.2 **Robo-advisor***: aspetti definitori e classificatori*

Come per lo strumento appena descritto, anche grazie ai *robo-advisor* l'investitore può godere comodamente a casa propria (o in qualsiasi altro luogo) di un servizio finanziario ben preciso. Come è possibile intuire dalla desinenza "*advisor*", quello in questione è il servizio di consulenza in materia di investimenti.

Lo strumento del *robo-advisor* consiste nella prestazione del servizio di consulenza appena menzionato grazie ad una piattaforma *on-line* che riduce al minimo, grazie agli algoritmi di cui la stessa si compone, l'intervento umano. Grazie all'impiego della piattaforma e dei suoi algoritmi, quindi, il servizio offerto diventa assolutamente "spersonalizzato" oltre che disponibile 24h su 24h ed in qualsiasi luogo.

Si è soliti individuare tre modalità di prestazione del servizio di consulenza automatizzata. La prima consiste nel *robo-advice* puro in cui tutte le fasi di prestazione del servizio sono automatizzate. La seconda è il *robo-advice* ibrido in cui, invece, si alternano fasi automatizzate a fasi che vedono la presenza di un apporto "intellettuale" umano. Infine, vi è il c.d. *robo4advisor* in cui il servizio non viene offerto a clienti *retail* ma a un altro intermediario[11].

Il servizio di investimento prestato è dunque quello della consulenza in materia di investimenti. In verità, è doveroso precisare che non tutti gli utilizzi di *advisor* "algoritmici" conducono alla prestazione di un servizio d'investimento riservato. Come è noto, infatti, l'attività di consulenza si declina in tre diverse fattispecie: la consulenza di carattere generale che, sebbene avente ad oggetto un determinato strumento o una precisa operazione, è rivolta ad un pubblico così diffuso da poter essere inquadrata alla stregua di una mera attività promozionale; la consulenza generica, avente ad oggetto una specifica tipologia di strumenti

---

[11] Sul tema cfr. R. Lener, *La "digitalizzazione" della consulenza finanziaria. Appunti sul c.d.* robo-advice, in R. Lener (a cura di), *Fintech: Diritto, Tecnologia e Finanza*, I quaderni di Minerva Bancaria, 2018, p. 45 e, da ultimo, Consob, *La digitalizzazione della consulenza in materia di investimenti finanziari*, Quaderni FinTech, 3 gennaio 2019, p. 10.

finanziari; la consulenza specifica avente ad oggetto un determinato strumento finanziario e un'operazione ben contestualizzata. Solo quest'ultima costituisce attività riservata essendo l'unica dotata del requisito della personalizzazione alle richieste del cliente.

Sulla base della normativa vigente, ad oggi la gestione di una piattaforma che offra servizi di *robo-advice* e offra consulenza specifica può essere effettuata da intermediari bancari, SIM, SGR nonché dai consulenti finanziari di cui artt. 18-*bis* e 18-*ter* del Testo unico della finanza.

Nonostante la "particolare" categoria di soggetti ammessi a prestare il servizio di consulenza in materia di investimenti, anche con riferimento a questo strumento digitale è possibile far notare il fenomeno di "eclissamento" che caratterizza l'intermediario che presta questo servizio. L'individuare questa peculiarità anche nella prestazione del servizio di consulenza in materia di investimenti dovrebbe, per lo meno, far stupire, tenendo presente l'importanza del "capitale intellettuale" proprio della categoria di intermediari appena menzionati.

1.3 **Crowdfunding*: funzionamento e tipologie "finanziarie"***

Il *crowdfunding*[12] è uno strumento di finanziamento innovativo che, grazie ad *Internet*, permette di ampliare enormemente la cerchia dei finanziatori di una determinata impresa. Come per gli altri strumenti appena descritti, anche il suo funzionamento si basa sull'utilizzo di una piattaforma *on-line* che ha lo scopo di dare risonanza a una idea imprenditoriale, riuscendo così a mettere in contatto un soggetto che ha necessità di finanziarsi con una "folla" di clienti-investitori (da cui l'inglese *crowd-funding*).

Il *crowdfunding* è tradizionalmente diviso in quattro "modelli": *donation, reward, lending* ed *equity crowdfunding*. Le differenze fra i diversi modelli possono essere ricostruite sulla base di "cosa" un partecipante alla raccolta riceve in cambio della propria contribuzione. Nel *donation crowdfunding,* la raccolta ha solitamente scopi di beneficienza sicché chi ha donato non riceve in cambio null'altro se non la consapevolezza di aver partecipato al finanziamento di una causa benevola. Nel *reward crowdfunding,* come è possibile intuire già dal nome, il partecipante alla raccolta riceve solitamente un "premio" che può consistere solitamente in un *gadget* creato dall'impresa per l'occasione oppure direttamente in un prodotto che l'impresa si impegna a produrre grazie al finanziamento ricevuto. Nel *lending crowdfunding,* invece, i partecipanti effettuano dei veri e propri prestiti e vengono ricompensati con il riconoscimento di un interesse sulla somma prestata. Infine, l'*equity crowdfunding* è la tipologia di *crowdfunding* in cui il partecipante, definibile propriamente come investitore, riceve in cambio della propria contribuzione azioni o quote dell'impresa che ha partecipato a finanziare.

---

[12] Cfr. sul tema il contributo di M. Bellino in questo *Quaderno*.

L'*equity crowdfunding* è dunque la tipologia di *crowdfunding* che, oltre ad avere caratteri maggiormente finanziari, importa anche maggiori esigenze di regolamentazione. Grazie alla piattaforma predisposta da specifici intermediari (i c.d. gestori di portali di cui si dirà *infra*) all'investitore, cliente *retail* o professionale che sia, viene data la possibilità di addentrarsi maggiormente nelle realtà imprenditoriali nelle quali decide di conferire il proprio denaro, accompagnando un investimento generalmente a lungo termine in società di nuova costituzione con la possibilità di far parte di una *community* e di influenzare, all'interno della "folla", l'impresa o la società cui ha deciso di contribuire.

L'offerta tramite il portale, ai sensi dell'art. 100-*ter* del Testo unico della finanza, viene propriamente qualificata come un appello al pubblico risparmio, caratterizzata però dal fatto che questa è condotta esclusivamente attraverso una "piattaforma *web*", il c.d. portale per la raccolta di capitali. Ad oggi, in esercizio dell'esenzione prevista dalla normativa europea sulle offerte al pubblico risparmio, nel complesso, gli strumenti oggetto di offerta non possono superare il valore complessivo di cui all'art. 100, comma 1, lett. c) del Testo unico della finanza[13]. Questo meccanismo, sottrae l'emittente all'applicazione della disciplina comune sull'appello al pubblico risparmio e, conseguentemente, degli obblighi di pubblicazione di un prospetto informativo. Al riguardo, vale la pena sottolineare che gli strumenti oggetto di offerta possono essere rappresentativi solo di capitale di rischio: deve quindi escludersi che gli emittenti possano offrire al pubblico titoli obbligazionari o altri titoli di debito.

Anche nell'*equity crowdfunding* abbiamo quindi un intermediario il cui ruolo appare ridotto al pari di quanto evidenziato nella descrizione dei due precedenti strumenti digitali. A quanto detto si aggiunge la particolarità che nell'*equity crowdfunding* il legislatore è intervenuto appositamente creando un "nuovo" intermediario, il gestore di portali di cui all'art. 50-*quinquies* del Testo unico della finanza. Sulla scorta della tendenza sopra descritta, questo intermediario ha la peculiarità di essere stato creato quasi sapendo del ruolo "marginale" che lo stesso avrebbe ricoperto. Mentre, infatti, gli intermediari che offrono servizi di negoziazione per conto dei clienti e ricezione e trasmissione di ordini nel *trading on-line* o di consulenza in materia di investimenti nel *robo-advice* non sono intermediari "destinati" per propria natura a gestire piattaforme nelle quali verranno offerti, in maniera autonoma, i propri servizi, i gestori dei portali, invece, nascono già con questo scopo, consci dell'apporto veramente marginale che l'intermediario in questione avrà nell'offerta del servizio.

A dimostrazione di ciò, come si vedrà nel dettaglio *infra,* il legislatore nazionale conferisce la possibilità di acquisire questa qualifica rispettando requisiti legali e patrimoniali molto più semplici rispetto a quelli richiesti ad un intermediario tradizionale. In aggiunta a ciò, l'affievolimento del ruolo ricoperto da questi intermediari si nota già dal nome agli stessi attribuito il quale evidenzia

---

[13] Ai sensi del Regolamento emittenti, adottato dalla Consob con delibera n. 11971 del 14 maggio 1999, l'ammontare massimo che può essere raccolto nell'arco di 12 mesi è pari a 8 milioni di euro.

in maniera chiara il loro ruolo di "gestori" di una piattaforma *web*. Siamo dunque di fronte ad un tipo di intermediario di recente creazione che diventa sempre più digitale e "algoritmico" e sempre meno "umano".

2. Regolamentazione della piattaforma

2.1 **Trading on-line** *e principio di neutralità tecnologica*

Relativamente al *trading on-line*, il fenomeno non ha posto di per sé particolari esigenze regolamentari. Oltre a trovare applicazione le norme del Testo unico della finanza e del Regolamento Intermediari[14] relative al servizio di investimento prestato grazie all'utilizzo della piattaforma (ricezione e trasmissione di ordini oppure esecuzione di ordini per conto del cliente) la normativa di riferimento è stata sintetizzata con la Comunicazione Consob n. DI/30396 del 21-4-2000.

Nonostante la sua pubblicazione risalga a quasi due decenni fa, la Comunicazione in discorso riesce a evidenziare alcuni importanti principi che vale la pena riportare. In primo luogo, si riconosce il principio di neutralità tecnologica, secondo cui le regole applicate ad un determinato servizio di investimento non vengono meno per il solo fatto che "l'impresa si avvale di *internet* per lo svolgimento dell'attività di intermediazione". Si ribadisce poi, semplicemente, il principio secondo cui è onere dell'intermediario quello di assicurarsi che l'utilizzo di strumenti innovativi, quale poteva considerarsi *Internet* a quel tempo, consentano comunque il pieno rispetto della disciplina[15].

La restante parte della Comunicazione si occupa semplicemente di sintetizzare la disciplina applicabile alla prestazione dei summenzionati servizi di investimento. Ciò che deve essere sottolineato, a dimostrazione di quanto si credesse nel ruolo neutrale della tecnologia, è il fatto che il resto della Comunicazione si limita a sintetizzare la normativa applicabile pur conscia del forte divario fra le modalità con cui il servizio veniva svolto e gli adempimenti che la normativa, scritta inizialmente sul presupposto della prestazione "non-digitale" del servizio, prevedeva. Fra gli obblighi riportati si evidenzia, ad esempio, la necessità di concludere il contratto in forma scritta e l'obbligo di identificazione della clientela[16].

Come è possibile vedere, dunque, la normativa relativa al *trading on-line* non ha identificato alcuna novità che valesse la pena di essere tutelata legislativamente rispetto al passato. Il legislatore, in questo caso, non ha fatto alcuno sforzo regolamentare nuovo, ritenendo semplicemente di ribadire che le norme

---

[14] Regolamento Intermediari, adottato dalla Consob con delibera n. 20307 del 15.2.2018.

[15] Consob, Comunicazione n. DI/30396 del 21-4-2000

[16] Insieme a questi la normativa ricorda poi, *inter alia*, gli obblighi in materia di (i) trasparenza; (iv) verifica di adeguatezza; (v) conflitto di interessi.

applicabili prima, ai servizi di investimento "sottesi" al nuovo fenomeno digitale, avrebbero tranquillamente trovato applicazione anche successivamente[17].

2.2 **High frequency trading***: una proposta di vigilanza algoritmica semplificata*

Di fronte ad un fenomeno così tecnologicamente complesso come l'*high frequency trading*, ragionare con i soli strumenti di vigilanza prudenziale sembra difficile. La difficoltà maggiore, difatti, è quella di identificare la strategia migliore per riconoscere l'abuso (*ex ante* o *ex post*) senza impedire o ostacolare l'utilizzo di questo strumento e l'evoluzione delle tecniche di negoziazione.

Nella sostanza, la normativa[18] si caratterizza per approcciare il fenomeno da un doppio punto di vista: quello del "*trader*" e quello della sede di negoziazione. A favore dei primi vengono previste regole comportamentali che si traducono in presidi organizzativi dell'attività, mentre, a favore dei secondi, vengono imposti (pressoché analoghi) requisiti organizzativi con l'obiettivo convergente che tali soggetti si dotino di capacità tecnologiche adeguate, altresì funzionali a testare, monitorare e garantire la resilienza del sistema in ipotesi di scenari di *severe market stress*.

In riferimento alle imprese di investimento, l'obiettivo è scongiurare che il funzionamento dell'algoritmo possa sfuggire di mano e provocare, dunque, dei danni (anche solo in termini di "disordine") all'interno del mercato in cui è utilizzato.

La struttura delle norme di regolamentazione dei requisiti organizzativi delle imprese di investimento che effettuano la negoziazione algoritmica riflette la complessità della materia regolata[19].

In sintesi, la normativa impone che tali società si dotino di un sistema di controlli interni che si concentri principalmente su tre aspetti. Il primo riguarda la "resilienza" del sistema di negoziazione e la sua "capacità", imponendo, se necessario, anche limiti alle negoziazioni, onde evitare che il potenziale volume di ordini inviati possa influire sul funzionamento del mercato, anche solo rallentandone l'attività o influenzandone l'efficienza. Il secondo si preoccupa di evitare l'invio di ordini errati o che possano provocare un funzionamento dei sistemi che possa contribuire o direttamente creare un mercato "disordinato".

---

[17] Sul tema cfr. Consob, Comunicazione n. DI/30396 del 21.4.2000 e L. Bonzanini, *La normativa di riferimento in materia di "*Trading on line*"*, in *I Contratti*, 2000, p. 193 ss.

[18] La disciplina multilivello si ricava dalle disposizioni di cui ai Regolamenti Delegati (UE) n. 2017/584 e n. 2017/589 che ripropongono l'impostazione già proposta nelle Linee Guida dell'ESMA del 2012 e recepita in Italia con Comunicazione congiunta Consob/Banca d'Italia del 30 aprile 2012.

[19] L'interprete, difatti, può ricostruire il sistema dalla lettura di tre livelli di normativa: (i) l'art. 67-*ter* t.u.f., in recepimento dell'art. 17 MiFID II; (ii) gli artt. 48 e 49 del Regolamento Mercati adottato dalla Consob con delibera n. 20249 del 28 dicembre 2017; e (iii) il Regolamento delegato (UE) n. 2017/589 della Commissione.

Simili obblighi sono poi imposti con riguardo all'evitare improvvisi malfunzionamenti, richiedendo che i sistemi utilizzati siano verificati a fondo e soggetti a un adeguato monitoraggio. Infine, si impone alle imprese che utilizzano HFT di vigilare affinché le tecniche di negoziazione utilizzate non vengano usate per finalità di manipolazione del mercato.

Ai fini della vigilanza prudenziale, l'intermediario che intenda avvalersi della negoziazione algoritmica, anche mediante l'accesso elettronico diretto dei propri clienti, dovrà notificarlo alla Consob[20] ed è tenuto ad informare annualmente la Consob circa lo schema e il contenuto del linguaggio di programmazione utilizzato nella creazione dell'algoritmo, onde svelare la tecnica utilizzata e assicurare un controllo di congruità dei presidi apprestati dagli intermediari.

L'intermediario funge altresì da *longa manus* dell'autorità di vigilanza per il monitoraggio del comportamento sul mercato dei clienti che negoziano sul mercato tramite l'accesso elettronico diretto ai fini dell'individuazione di comportamenti riconducibili ad abusi di mercato. Difatti, l'intermediario[21] dovrà, in sede di prima ammissione del cliente al *Direct Electronic Access*, e successivamente una volta l'anno, svolgere una attività di *due diligence* al fine di valutare i tipi di strategia di negoziazione che il cliente intende applicare, i livelli di volume previsti e l'adeguatezza dei sistemi e dei controlli, in particolare la dotazione dei controlli *pre* e *post*-negoziazione[22]. L'intermediario dovrà, infine, comunicare alla Consob gli esiti delle valutazioni annuali effettuate sui clienti, segnalando, in particolare, le violazioni delle regole nonché negoziazioni e comportamenti anomali riconducibili ad abusi di mercato[23].

Con riferimento alle regole applicabili alle sedi di negoziazione, è degno di nota come la maggior parte degli obblighi organizzativi che vengono imposti alle imprese di investimento che utilizzato l'*HFT* siano duplicati nei riguardi delle sedi di negoziazione. In particolare, la disciplina dei requisiti operativi delle sedi di negoziazione in termini di resilienza e capacità del sistema, di gestione ordinata delle negoziazioni e di efficacia dei sistemi e delle procedure di negoziazione ricalcano gli obblighi già imposti alle imprese di investimento[24].

All'esito dell'esame della normativa multilivello sopra riportata appare evidente come in ipotesi di *high frequency trading* i meccanismi di vigilanza sono plurimi e, forse, ridondanti. Se, difatti, il *trader* è un cliente che opera sul

---

[20] La disposizione è contenuta nell'art. 67-*ter*, comma 2, t.u.f. e nell'art. 48 del Regolamento Mercati della Consob.

[21] La norma è posta nell'art. 67-*ter*, comma 8-*bis*, t.u.f., dell'art. 50 del Regolamento Mercati della Consob e degli artt. 19-23 del Regolamento delegato (UE) n. 2017/589.

[22] Si veda l'art. 22 Regolamento delegato (UE) n. 2017/589.

[23] Cfr. l'art. 50 Regolamento Mercati della Consob e art. 23 Regolamento delegato (UE) n. 2017/589.

[24] La disciplina si snoda attorno alle disposizioni di cui all'art. 65-*sexies*t. u.f., in recepimento dell'art. 48 MiFID II, all'art. 12 del Regolamento Mercati della Consob e al Regolamento Delegato (UE) n. 2017/584 della Commissione. Sul tema si veda l'ampia indagine sulle sedi di negoziazione soggette alla vigilanza della Consob presentata in Consob, *Mappatura delle sedi di negoziazione in Italia dopo l'entrata in vigore di MiFID II / MiFIR,* 7 ottobre 2018.

mercato attraverso il *Direct Electronic Access*, la catena dei controlli si dipana tra intermediario, sede di negoziazione e, in ultima istanza, autorità di vigilanza.

Mette conto rilevare come, all'interno del mercato, l'esistenza di una regola in più o in meno da dover applicare non è mai senza conseguenza, poiché ogni norma impone un costo che, quale scelta di politica legislativa, deve essere allocato sulla parte più in grado di sopportalo. In termini di valutazione dei costi della regolamentazione, poi, altro è il funzionamento del mercato, nella prospettiva pubblicista di tutela di interessi del sistema, altro è lo sviluppo del mercato stesso, nella cui prospettiva privatistica diventa invece molto importante individuare il soggetto che si sobbarcherà i relativi costi.

Che senso avrebbe infatti non eliminare un costo già effettivamente sopportato da un altro soggetto? Il problema rimane solo quello di capire quale dei due costi eliminare.

Dal lato dell'impresa di investimento, l'approccio adottato può definirsi misto in quanto coniuga obblighi comportamentali a comunicazioni e possibilità di intervento e controllo *ex post*. Per quello che riguarda le sedi di negoziazione, invece, alle stesse vengono imposti quasi gli stessi obblighi di corretto funzionamento e di registrazione imposti alle imprese di investimento, nonché quelli riguardanti i principi di non discriminazione.

Dall'analisi così effettuata è possibile notare un certo sbilanciamento a sfavore delle imprese di investimento. Il presupposto (e quindi la causa) di questo tipo di approccio sembra potersi individuare in una sorta di leggera sfiducia con il quale il legislatore si approccia a queste tecniche di negoziazione innovativa. È come se queste non siano ancora considerate "normalità" e per questo egli insiste con un approccio normativo che impone severi controlli non tanto su dove vengono usate ma su "chi" le usa. Se, infatti, l'*HTF* fosse considerato come una semplice evoluzione dei meccanismi di "trasmissione" e di "comunicazione" degli ordini, così come l'introduzione del telegrafo nei confronti della "corsa" del *broker* per la trasmissione dell'ordine, il legislatore non si sarebbe curato di imporre obblighi di preavviso e comunicazione sugli utilizzatori di queste nuove tecniche.

Ed infatti, appare di tutta evidenza che gli obblighi imposti alle imprese di investimento possono tranquillamente essere ribaltati con più efficienza sulle sedi di negoziazione. Si pensi all'obbligo di *record keeping*. Chi meglio della sede nella quale l'ordine è stato effettuato può garantire, soprattutto, la "correttezza" e la veridicità della registrazione se non un soggetto diverso da chi ha inviato gli ordini oggetto di registrazione?

A ben vedere, l'imporre obblighi sul partecipante non fa altro che allontanare dalla "normalità" tanto auspicata. Il fatto che chi utilizza gli *HFT* debba incorrere in maggiori obblighi e controlli (e dunque in maggiori costi) di chi non lo utilizza, è probabile che continuerà ad allontanare il momento in cui utilizzare l'*HFT* all'interno di un mercato sarà considerato la normalità, contribuendo alla persistenza di un mercato in cui solo "alcuni" (con più risorse) potranno

accedervi. Quanto detto diventa ancor più importante se si consideri che molte delle tecniche che sono state giudicate come "meno corrette" si basano proprio sullo sfruttare i *deficit* tecnologici dei *trader* tradizionali e meno sofisticati.

Contro quanto detto, si potrebbe affermare che non tutti gli obblighi sono comunque "ribaltabili" sulle sedi di negoziazione. Si pensi all'obbligo di verificare che il proprio sistema non invii ordini errati o non sia soggetto a malfunzionamenti. Nulla di più sbagliato. La tecnologia moderna non è assolutamente di impedimento alla previsione e introduzione di obblighi riflessi di questo tipo esclusivamente alle sedi di negoziazione. Queste, infatti, introducendo veri e propri strumenti di *gate keeping* potrebbero benissimo stabilire delle regole, non discriminatorie, il cui non rispetto porterebbe a segnalare l'ordine ricevuto come erroneo e, dunque, a non elaborarlo.

Quanto detto sembra corretto in quanto è dal mercato (questa volta inteso come singola sede di negoziazione) che dipende l'utilizzo o meno (e anche la diffusione come visto nel paragrafo precedente) di tecniche di negoziazione algoritmica.

Si può allora arrivare al curioso suggerimento secondo cui vi sarebbe la possibilità che proprio lo strumento oggetto di controllo possa divenire lo strumento "controllante". Infatti, un sistema di questo tipo non potrà prescindere dall'introduzione di "algoritmi" ai fini di vigilanza altrettanto veloci ed efficienti quanto quelli utilizzati dai partecipanti al mercato.

Alla luce della natura "necessitata" delle innovazioni tecnologiche che ruotano attorno all'*HTF*, il problema normativo potrebbe spostarsi dalla fase preventiva a quella esclusivamente *ex post*, e dunque sull'assicurare che le condotte manipolative vengano almeno individuate successivamente e quindi sanzionate. Questo alla luce della considerazione, già esposta, secondo cui risulta molto più difficile leggere nel futuro che tipo di comportamenti siano meritevoli di essere sanzionati. In questo senso, grande importanza riveste la precisa tracciabilità degli ordini.

Controllo più diffuso invece, dovrebbe essere richiesto con riguardo all'errore algoritmico, inteso con una specie dell'errore umano, individuabile però nel processo di programmazione dell'algoritmo di *HTF* utilizzato. In questo senso sarebbero allora richiesti maggiori controlli volti ad evitare l'eventuale rischio sistemico derivante da un algoritmo impazzito. In questo senso, il problema si sposta dall'algoritmo al relativo algoritmo che lo controlla. Questo controllore avrebbe, infatti, lo scopo di assicurare una corretta condotta all'interno dei mercati. Alla luce della natura tecnologica e strumentale che caratterizza gli *HTF*, questa sembra la soluzione maggiormente "prevedile". È forse il caso di prepararci, dunque, all'esistenza di sedi di negoziazione in cui gli algoritmi avranno un ruolo prevalente. Un ruolo non solo di meri "partecipanti" ma anche di controllori.

Questo tipo di approccio ha il vantaggio di non sobbarcare di obblighi "inutili" i partecipanti al mercato facendo in modo che gli stessi siano obbligati a comportarsi secondo determinate regole. Esso ha il vantaggio di ammettere l'impossibilità di un controllo preventivo su un tipo di agente la cui operatività,

sebbene preordinata e prevedibile, diventa automaticamente imprevedibile per l'impossibilità di prevedere il comportamento (non per forza ragionevole) anche degli altri partecipanti "robotici" che sarà possibile ritrovare nel mercato.

Spostare l'attenzione sui *trader* anziché sui mercati presuppone che nessun *trader* sfugga al controllo di conformità della vigilanza algoritmica. L'interazione fra gli stessi, infatti, rischia di essere così tanto correlata che se anche uno solo di questi sfugga ai controlli *ex ante* e di conformità anzidetti, tutti i controlli effettuati sugli altri partecipanti sino al quel momento (e tutti i costi sostenuti dalle autorità di vigilanza in tal senso) risulterebbero essere stati vani.

2.3 **Robo-advisor*: dalla neutralità tecnologica all'*algo-governance**

Come per il *trading on-line*, anche la disciplina del fenomeno dei *robo-advisor*[25] tutela non il fenomeno per sé e nel suo complesso, bensì il servizio di investimento che, grazie allo "strumento", viene prestato.

Come già anticipato, l'utilizzo di *robo-advisor* diviene attività riservata solo quando il servizio prestato è inquadrabile nella consulenza in materia di investimenti.

La MiFID II definisce questo servizio come la "*prestazione di raccomandazioni personalizzate ad un cliente, dietro sua richiesta o per iniziativa dell'impresa di investimento, riguardo ad una o più operazioni relative a strumenti finanziari*"[26]. Gli elementi essenziali della fattispecie sono, dunque: una raccomandazione personalizzata; l'adattamento della raccomandazione al destinatario; e il fatto che la raccomandazione abbia a oggetto una o più operazioni relative a strumenti finanziari.

In applicazione del già menzionato principio di neutralità tecnologica, la disciplina di livello primario di riferimento dei *robo-advisor* è dunque quella applicabile al servizio finanziario prestato.

Il ruolo delicato della tecnologia utilizzata per la prestazione del menzionato servizio non è però passato inosservato alle autorità europee. Fra queste, l'ESMA, in parziale superamento del principio di neutralità tecnologica fino ad ora sostenuto, ha deciso di emanare precise *guidelines* di carattere sia informativo che organizzativo[27].

---

[25] Per un'analisi dei rischi connessi a tale attività cfr. il contributo di C. Porzio e G. Sampagnaro in questo *Quaderno*.

[26] Art. 1, comma 1, n. 4, MiFID II.

[27] Il compito è stato svolto dall'ESMA dopo aver promosso una consultazione pubblica sull'argomento, a maggio 2018 ha pubblicato un *Final Report* avente a oggetto le linee guida sul principio dell'adeguatezza della prestazione dei servizi di consulenza. Per ulteriori approfondimenti, si rimanda alla ricostruzione effettuata in M.T. Paracampo, *L'adeguatezza della consulenza finanziaria automatizzata nelle linee guida dell'Esma tra algo-governance e nuovi poteri di supervisione*, in www.dirittobancario.it.

In particolare, l'ESMA, nell'ufficializzare implicitamente l'utilizzo di strumenti automatizzati nella prestazione del servizio di consulenza, fornisce alcune *best practice* a favore dei *provider* di questi servizi[28].

All'interno del report dell'ESMA è allora possibile assistere ad un radicale cambio di prospettiva.

Come è noto, la prestazione di servizi di investimento ha sempre fatto dei principi di trasparenza e degli obblighi informativi un vero e proprio pilastro della protezione dell'investitore. Nonostante l'attenzione rispetto a questi aspetti non sia venuta meno, è come se si inizi a comprendere sempre di più l'inefficacia (se non l'inutilità) di obbligare l'intermediario a "svelare" all'investitore il codice utilizzato della programmazione dell'algoritmo.

Il passo in avanti è stato fatto introducendo obblighi a carico degli intermediari privi di effetti immediati nei confronti dell'investitore ma non per questo meno efficaci. In quest'ottica viene richiesto agli intermediari di monitorare e testare con una adeguata regolarità gli algoritmi utilizzati per la prestazione del servizio di consulenza. Obbligo di monitoraggio e di *testing* che deve coinvolgere tutte le fasi della progettazione dell'algoritmo. Questi obblighi vengono affiancati da uno ulteriore di grande rilevanza che richiede di annotare e di tenere traccia di ogni intervento effettuato sull'algoritmo[29].

Ciò che è possibile osservare è dunque un parziale superamento del principio, fino ad allora sostenuto, di neutralità tecnologia. Superamento realizzato, ancora, con metodi e mezzi diversi dalla disciplina normativa di rango primario.

Oltre a ciò, grande importanza deve essere attribuita al modo in cui viene promosso questo superamento e, in particolare, a ciò con cui è stato sostituito. Dall'analisi dei menzionati obblighi è, infatti, possibile scorgere l'affermarsi di un nuovo principio. Sembra che possiamo dirci di fronte ad un fenomeno di "*algo governance*"[30].

2.4 **Crowdfunding***: il caso dei gestori dei portali*

Come anticipato, l'unica forma di *crowdfunding* che nel nostro ordinamento ha subito una regolamentazione specifica è l'*equity crowdfunding*.

Al contrario di quanto detto sia per il *trading on-line* che per i *robo-advice*, per quanto riguarda l'*equity crowdfunding*, il legislatore ha preferito intervenire in maniera specifica "sullo" strumento, creando quello che, per certi versi, potrebbe

---

[28] M.T. Paracampo, *op. ult. cit.,* p. 2.

[29] Per ulteriori dettagli, si rimanda a M.T. Paracampo, *op. ult. cit.,* pp. 14–16. Per una prospettiva che valorizza le istanze di protezione del cliente si veda. R. Natoli, *Il contratto "adeguato". La protezione del cliente nei servizi di vredito, di investimento e di assicurazione,* Milano, 2012, *passim.*

[30] M.T. Paracampo *La consulenza finanziaria automatizzata*, in M.T. Paracampo (a cura di), *Fintech*, Torino, 2017, pp. 136-138.

essere considerato un servizio finanziario nuovo: la gestione delle piattaforme nelle quali vengono effettuate raccolte di *equity crowdfunding*.

La disciplina di riferimento, introdotta con il c.d. Decreto Crescita 2.0, è sostanzialmente contenuta all'interno dell'art. 50-*quinques* del Testo Unico della Finanza e del Regolamento Consob sul *crowdfundin*g[31].

Per "*portale per la raccolta di capitali per le piccole e medie imprese e per le imprese sociali*" si intende una piattaforma *on line* con la finalità esclusiva di facilitare la raccolta di capitali di rischio da parte dei soggetti ammessi all'utilizzo dell'*equity crowdfunding*. Soggetti il cui numero nel tempo è aumentato grazie a successivi e repentini interventi che hanno trasformato questo strumento da mera agevolazione addizionale prevista per le *start-up* innovative a strumento di finanziamento alternativo per tutte le forme societarie[32].

Nella definizione di quello che abbiamo definito come un "nuovo" servizio di investimento, il regolatore ha distinto fra: "gestori di diritto", ovvero soggetti quali imprese di investimento e le banche, che non hanno bisogno di alcuna ulteriore autorizzazione per svolgere questo servizio; e i c.d. "gestori speciali non professionali" ovvero i soggetti iscritti in un apposito registro tenuto dalla Consob i quali possono svolgere il servizio all'esito di una "semplice" iscrizione ma con alcune rilevanti limitazioni. A differenza dei gestori di diritto, i gestori speciali non professionali non possono eseguire direttamente gli ordini di acquisto o di sottoscrizione degli strumenti finanziari oggetto dell'offerta, dovendosi avvalere di intermediari finanziari autorizzati allo svolgimento di tali attività. Parimenti, agli stessi non è consentito di detenere somme di denaro o strumenti finanziari di pertinenza di terzi provenienti dall'attività di intermediazione svolta a favore dell'emittente[33].

Per poter essere iscritti nel registro dei gestori di portali, tenuto dalla Consob, i gestori non professionali devono comunque possedere alcuni requisiti il cui ottenimento non è eccessivamente dispendioso[34].

---

31 Regolamento sulla raccolta di capitali di rischio tramite portali *on-line*, adottato con delibera Consob n. 18592 del 26 giugno 2013, da ultimo modificato con delibera n. 20264 del 17 gennaio 2018.

32 Inizialmente solo imprese in possesso della qualifica di *start-up* innovative potevano utilizzare l'*equity crowdfunding*. La categoria è stata lentamente ampliata, consentendo dapprima l'ingresso alle PMI innovative e solo di recente a tutte le PMI così come definite dall'art. 2, par. 1, lett. (f), primo alinea, del regolamento (UE) 2017/1129, c.d. Regolamento Prospetti.
Per maggiori approfondimenti, cfr. N. Ciocca e F. Accettella, *Emittente e portale nell'*equity-based crowfunding*,* in *Banca, borsa, tit. cred.,* 2017, I, p. 237 ss e N. De Luca, S.L. Furnari, A. Gentile, voce "*Equity Crowdfunding*", in *Digesto delle discipline privatistiche, Sezione commerciale, Aggiornamento*, Torino, 2017, p. 159 ss.

33 N. De Luca, S.L. Furnari, A. Gentile, *op. cit.,* p. 166.

34 In particolare, i requisiti sono: (i) essere costituiti in forma di società di capitali; (ii) avere la sede legale e amministrativa in Italia; (iii) prevedere come oggetto sociale esclusivo la gestione del portale; e, infine, (iv) dotarsi di organi di amministrazione, direzione e controllo in possesso dei requisiti di professionalità e onorabilità stabiliti dalla Consob.

Con il menzionato Regolamento, inoltre, vengono poi dettagliati gli obblighi cui i gestori dei portali sono sottoposti. Considerando il minore grado di "automazione" che caratterizza le piattaforme di *equity crowdfunding*, il carico di adempimenti è maggiormente spostato verso gli obblighi informativi da fornire alla clientela. Nonostante ciò, è comunque possibile intravedere in queste norme un tentativo di disciplinare la piattaforma più che il "comportamento" dell'intermediario. Infatti, considerando il ruolo di mera "vetrina" che sostanzialmente la piattaforma di *equity crowdfunding* svolge, la regolamentazione secondaria si occupa proprio di disciplinare nel dettaglio le informazioni, ricevute direttamente dall'impresa offerente, che la piattaforma deve mostrare[35]. Gli obblighi informativi così previsti possono facilmente essere considerati più come delle indicazioni su come la piattaforma deve essere programmata e sulle funzioni che la stessa deve svolgere. Anche qui è, allora, possibile intravedere una sorta di "*algo-governance*".

3. Verso una nuova regolamentazione delle piattaforme

All'esito di quanto detto sino a ora, è chiaro come l'avvento di questi nuovi strumenti digitali per la finanza non sia passato inosservato agli occhi del regolatore il quale si è mosso, principalmente a tutela dell'investitore, per regolare questo processo di "democratizzazione" finanziaria caratterizzato, ormai, per l'alto grado di informatizzazione adoperato nella prestazione dei menzionati servizi.

Nonostante ciò, come evidenziato, l'approccio del legislatore ha seguito, in una prima fase, il principio di "neutralità" tecnologia. Secondo questo principio, non rilevava il modo (e, nei nostri casi, gli strumenti tecnologici predisposti) per la prestazione del servizio ai fini della normativa applicabile.

In progresso di tempo e sebbene timidamente, invece, l'approccio appena descritto sembra essere stato sostituito dall'introduzione di regole e norme volte a regolamentare anche la parte digitale del servizio che, sebbene esterna, ne costituisce comunque un'importante infrastruttura.

Infrastruttura costituita, in tutti i casi considerati, da una piattaforma. Nonostante la diversità delle novità "digitali" qui descritte, consistenti sostanzialmente nel diverso servizio offerto, la piattaforma rimane l'elemento che le accomuna. Essa costituisce quasi "l'infrastruttura essenziale" che permette la fruizione digitale dei servizi finanziari, nonostante una prima forma di disinteresse del legislatore, sia europeo che nazionale.

Prima però di ammettere la necessità di questo cambio di approccio e, dunque, di prospettare un completo abbandono del principio di neutralità tecnologica è necessario svolgere alcune riflessioni.

---

[35] Si vedano, ad esempio, gli artt. 14, 15 e 16 del Regolamento Consob sul *crowdfunding* che disciplinano nel dettaglio, rispettivamente, le informazioni da mostrare relative al gestore del portale (e.g. recapiti, attività svolte, data di avvio dell'attività, costi, ecc.), all'investimento (e.g. rischi, divieto di distribuzione utili per *start up* innovative, contenuti tipici di un *business plan* dell'offerente, ecc.) e alle singole offerte.

Il completo abbandono o meno di questo principio dovrebbe infatti essere valutato prendendo in considerazione il tipo di tecnologia utilizzata. Più precisamente sarà necessario analizzare se la tecnologia utilizzata, oltre ad agevolare la prestazione del servizio, introduce o meno degli aspetti di "pericolo" per l'investitore che necessitano di essere tutelati.

Qualora questa valutazione dia esito positivo, diverrà allora necessario individuare sotto quali profili è possibile proteggere al meglio il cliente-investitore. Il nodo centrale diverrà, allora, quello di individuare gli specifici pericoli per l'investitore che possono derivare dal fruire di servizi di investimento prestati attraverso "algoritmi". Infatti, la vera novità risiede non tanto nel semplice fatto che i servizi di investimento citati vengano prestati a distanza quanto più nell'utilizzo di programmi informatici automatizzati.

Sembra corretto suggerire di concentrare l'attenzione del regolatore su uno dei pericoli maggiori nonché comuni a entrambi questi tre strumenti e consistente nella correttezza del codice con il quale la piattaforma è stata realizzata al fine di garantire gli utilizzatori contro "errori" improvvisi o pericolosi malfunzionamenti. Verifica che non deve ritenersi facile per il dispendio di energie sia tecniche che economiche che questa attività potrà richiedere.

Al riguardo, infatti, la prima questione da risolvere può riguardare che "tipo" di controllo svolgere (*ex post* o *ex ante*) e da *"chi"* questo deve essere svolto (dal regolatore o dal cliente).

Lasciare che sia il cliente ad esercitare una qualche forma di controllo ha il vantaggio di fare in modo che sia il "mercato" a decidere il successo o meno dell'intermediario che offre quel determinato servizio. Questo si esplicherebbe, semplicemente, con la scelta, in capo allo stesso, di decidere se usufruire o meno di un determinato servizio. Ma affinché quanto detto sia effettivamente realizzabile, è altresì necessario che questi debba essere in possesso delle informazioni per poter effettuare le proprie valutazioni, ma soprattutto che sia in grado di comprendere le informazioni ricevute. Questo tipo di controllo è stato sempre incentivato tramite la previsione di regole di trasparenza. Trasparenza che, *ictu oculi*, diventa inutile se le informazioni oggetto di *disclosure* sono costituite da "codici informatici" o, comunque, procedure tecnologiche complesse la cui comprensione risulta difficile ai non esperti del settore.

Emerge allora che questo controllo sull'algoritmo debba essere lasciato a soggetti in possesso delle adeguate competenze tecniche per poterlo esercitare. Nonostante i costi che questa scelta può comportare, sembra allora che solo le autorità regolamentari possano, con l'aiuto di appositi tecnici, esercitare un'efficace attività volta alla verifica dei "codici" utilizzati[36]. Diversamente, si potrebbe ipotizzare l'istituzione di appositi "certificatori" ai quali potrebbe essere conferito il ruolo di "marcare" (e rendere pubblico) le piattaforme che rispettino

---

[36] Sulla sfida che pone la rivoluzione tecnologica nel mercato finanziario alle autorità di vigilanza, anche in termini di necessità di selezionare personale tecnico esperto in materia di algoritmi, si veda il contributo di L. Enriques, *Financial Supervision and RegTech: Four Roles and Four Challanges,* in *Revue Trimestrielle de Droit Financier* 53, 2017, disponibile su https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3087292.

determinati standard di sicurezza in modo da ribaltare interamente il costo di "vigilanza" dalle autorità ai singoli intermediari.

Con riferimento al tipo di controllo, non è sicuramente facile individuare il "momento" in cui effettuare lo stesso. È noto infatti che, avendo a che fare con "algoritmi", solitamente gli errori di sistema di una piattaforma possono venire in rilievo solamente dopo un determinato periodo di utilizzo. Questo in quanto è generalmente difficile "prevedere" tutti gli scenari possibili in cui il sistema può riscontrare una problematica.

In questo senso, un'altra soluzione potrebbe essere quella di propendere per un controllo *ex post*. In questi termini, però, l'efficacia di questo controllo sarà strettamente correlata con il regime di responsabilità previsto in caso di errori di "programmazione" che possano causare un danno al cliente. Soluzione che, in generale, non potrà essere diversa dal prevedere la responsabilità in capo all'intermediario e non sul creatore della piattaforma, in linea con i principi ormai consolidati in tema di "esternalizzazione" di funzioni che, nel nostro caso, potremmo arrivare quasi a definire come "essenziali"[37].

4. Conclusione

La rivoluzione digitale cui anche il mercato finanziario sta andando incontro, ci porta inevitabilmente a riflettere. Come visto con l'analisi degli strumenti digitali "per" la finanza sopra trattati, la tendenza nella prestazione dei servizi di investimento sta portando alla progressiva scomparsa dell'intermediario, impresa di investimento, così come tradizionalmente conosciuta. Non più impiegati e consulenti persone fisiche ma sempre di più *robot* e algoritmi.

Questo mutamento di paradigma obbliga il regolatore a ripensare gli strumenti tradizionali di tutela degli investitori e del mercato, dato che, considerate le complessità tecnologiche che iniziano a coinvolgere questo settore, molti dei presidi oggi vigenti (si veda quello della "trasparenza") potrebbero presto rivelarsi inefficaci.

Se prima infatti le autorità potevano contare sugli intermediari, soggetti che fungevano da tramite obbligatorio fra il cliente e il mercato, con l'appassimento progressivo del loro ruolo, sarà necessario individuare altri metodi e meccanismi per esercitare una vigilanza effettiva. Meccanismi che, in un mercato sempre più automatizzato ed algoritmico, dovranno, probabilmente, esserlo "almeno" altrettanto.

---

[37] Consob, *La digitalizzazione della consulenza in materia di investimenti finanziari*, cit., p. 82.

RISCHI DELLE BANCHE CONNESSI A FINTECH

Claudio Porzio e Gabriele Sampagnaro

1. Considerazioni introduttive

Obiettivo del presente lavoro è valutare l'impatto prospettico delle nuove tecnologie utilizzate nell'ambito del fenomeno '*FinTech*' – sul sistema dei rischi degli intermediari finanziari, in particolare le banche. L'analisi sarà prevalentemente riferita alla loro operatività, più complessa perché legata alla possibilità (concessa dalla normativa) di svolgere tutte le attività di intermediazione (con la sola esclusione di quella assicurativa e di gestione del risparmio): di conseguenza, si può affermare che per le altre tipologie di intermediari, i rischi effettivamente sopportati e gestiti rappresentano un sottoinsieme più o meno ampio di quelli bancari.

La letteratura recente, nell'analizzare le attività *FinTech* ne ha messo in luce l'impatto sulle diverse categorie di soggetti coinvolti ponendo particolare enfasi sui *regulators* e la clientela[1], soprattutto *retail*. Meno indagato è stato il tema delle conseguenze delle nuove aree di business sugli intermediari tradizionali vigilati (i cosiddetti *incumbents*)[2]. L'applicazione estesa della tecnologia digitale e dell'intelligenza artificiale è, infatti, destinata a modificare, in modo dinamico e in parte imprevedibile, il contesto di riferimento, richiedendo comportamenti flessibili e adattivi agli intermediari le cui risposte strategiche non potranno non causare una modifica del loro profilo di rischio e degli equilibri gestionali.

In altre parole, *FinTech* determinerà un'effettiva discontinuità rispetto al tradizionale *mapping* dei rischi o, piuttosto, una loro diversa graduazione e importanza che potrebbe giustificare, rendere in prospettiva necessario, un diverso approccio nella misurazione del capitale regolamentare? Lo sviluppo di aree emergenti di innovazione pone alle autorità di vigilanza la necessità di assumere decisioni solo avendo valutato i profili di rischio cui si espongono (e a cui espongono) sia le nuove realtà emergenti sia gli *incumbents*. Con riguardo a questi ultimi, si devono necessariamente assumere almeno due prospettive di indagine, tra esse intersecate, riferite ad un approccio 'verticale', teso ad evidenziare le diverse forme di rischio associate ad ogni

---

[1] Anche con riferimento alle implicazioni del fenomeno in termini di *policy*, l'utilizzo della tecnologia ha suscitato minore attenzione rispetto ai loro fornitori, che, sfuggendo alla regolamentazione, non sono tenuti al rispetto delle norme, in particolare in materia di tutela del consumatore. Cfr. D.A. Zetzsche *et al*., *From FinTech to TechFin: The Regulatory Challenges of Data-Driven Finance,* in *European Banking Institute, WP series*, n. 6, 2017.

[2] «*Innovative Fintech business models typically offer one or more specific financial products or services in an automated fashion through the use of the internet. By doing so, they unbundle the different financial services traditionally offered*. […].*Emerging technologies such as cognitive computing, machine learning, artificial intelligence, and distributed ledger technologies (DLT) can be used to supplement both Fintech new entrants and traditional incumbents, and carry the potential to materially change the financial services industry*». Cfr. International Organization of Securities Commissions (IOSCO), *Research Report on Financial Technologies*, February 2017, p. 4.

area di business, e ad un approccio 'orizzontale', teso ad esplorare in chemodo le tradizionali tipologie di rischio cui sono esposti gli intermediari si conformano ed evolvono.

Il lavoro è così articolato: nel § 2 si fornisce una tassonomia dei rischi 'tradizionali' degli intermediari; nel § 3, dopo aver definito contenuti e contorni di *FinTech*, si è proceduto all'analisi verticale dei rischi di alcune aree di business; nel § 4 l'analisi è stata condotta in modo orizzontale per evidenziare componenti tradizionali e aree emergenti.

2. *Il sistema dei rischi bancari e il loro* **mapping**

Complessità e ampiezza degli elementi che determinano le conseguenze di una qualsiasi decisione, non solo finanziaria, rendono necessario uno sforzo di classificazione delle loro differenti tipologie (*mapping*). In finanza una prima suddivisione distingue, sulla base dei loro effetti: rischi puri (o anche assicurativi) la cui eventuale manifestazione comporta solo conseguenze negative e la cui gestione è oggetto specifico dell'attività assicurativa, definita come la trasformazione dei rischi puri per le unità di domanda (assicurati) in rischi speculativi per le unità di offerta (le compagnie di assicurazione); rischi finanziari (o anche speculativi) la cui manifestazione comporta conseguenze, che possono essere, con diversa intensità, positive o negative, connaturate all'attività finanziaria la quale implica il trasferimento, nel tempo e/o nello spazio, di valori (gli strumenti finanziari e i mezzi di pagamento) per ciò stesso mutevoli. In relazione alla loro natura si individuano rischi sistematici, originati sia da situazioni relative al contesto generale sia dall'andamento delle variabili dei mercati finanziari; rischi non sistematici, originati da fenomeni di diversa natura (operativi, di business, strategici e reputazionali), che dipendono prevalentemente dalle peculiarità della gestione caratteristica di ogni singolo intermediario.

Per qualsiasi impresa, compresi gli intermediari, il rischio complessivo è misurato dalle oscillazioni del valore del capitale economico o della sua redditività: poiché tale approccio è troppo sintetico, è indispensabile individuare i molteplici fattori alla base della manifestazione dei rischi secondo un approccio 'causativo'. Inoltre, qualsiasi definizione delle differenti fattispecie non può prescindere dalla circostanza che i rischi vanno considerati non singolarmente bensì nel loro reciproco interagire ('il sistema dei rischi', appunto) che incide sull'equilibrio patrimoniale, economico e finanziario in funzione del tipo di attività svolta.

A ciascun fattore di rischio corrispondono le aree di impatto, ossia gli aggregati, contabili ed extra-contabili, sensibili: attività e passività finanziarie singolarmente considerate; portafogli di crediti, titoli e derivati (rispettivamente *banking book* e *trading book*); posizioni debitorie e capitale; margini intermedi del conto economico; viceversa, sul medesimo aggregato

possono incidere più fattori in conseguenza di fenomeni di dipendenza e di correlazione che determinano l'esposizione complessiva.

Il *mapping* qui proposto[3] è stato elaborato prescindendo dalla regolamentazione[4], che pure lo ha fortemente condizionato: infatti, l'approccio adottato, rispondendo soprattutto a obiettivi di determinazione dell'adeguatezza patrimoniale, è stato parziale e mutevole nel tempo e alcune fattispecie, *in primis* il rischio di liquidità, sono state a lungo 'ignorate'. La classificazione qui proposta è, pertanto, parzialmente diversa perché finalizzata a comprendere origine e impatto dei rischi sulla gestione dell'intermediario nonché effetti su equilibri e *performance* aziendali.

Le 'fonti' principali dei rischi (fig. 1) possono essere eminentemente esterne – ossia riconducibili al tipo e alla natura delle relazioni instaurate dall'intermediario con le diverse categorie di controparti: datori di fondi (depositanti, finanziatori sul mercato interbancario, obbligazionisti, azionisti); prenditori di fondi e controparti delle transazioni in titoli; mercati finanziari; autorità di regolamentazione e vigilanza – o interne in conseguenza delle scelte strategiche e gestionali e delle modalità di svolgimento dell'attività (propensione al rischio, decisioni di finanziamento e investimento, organizzazione dei processi produttiwwvi, risorse umane)[5]. È evidente che lo schema proposto ha una funzione eminentemente tassonomica poiché qualsiasi decisione produce, sia pure con diversa intensità, effetti diretti e indiretti sul valore del capitale economico.

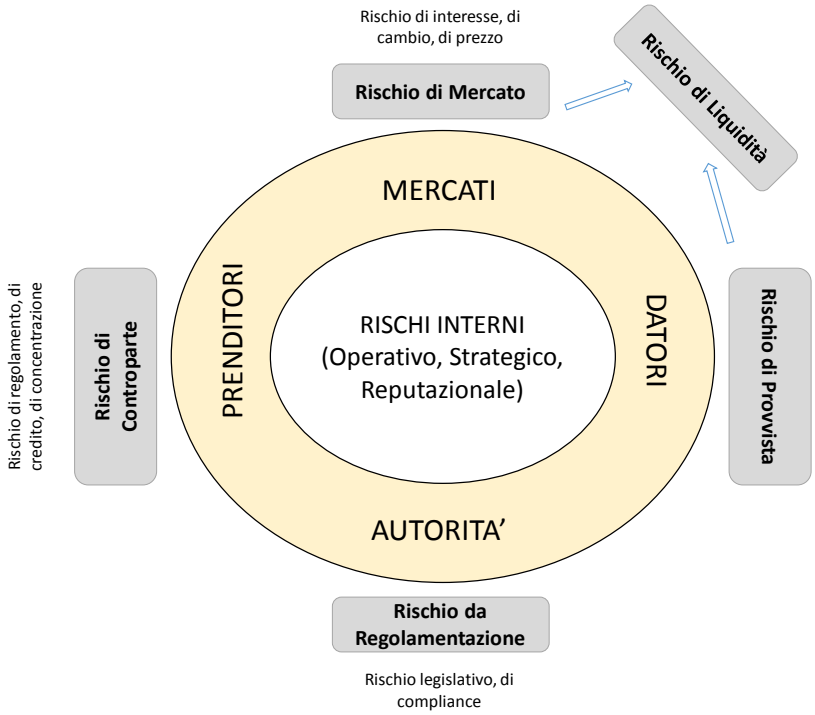
---

[3] Cfr. L. Nadotti, C. Porzio, D. Previati, *Economia degli Intermediari Finanziari*, Mc Graw Hill, 2017, cap. 3.

[4] Come è noto, accanto ai rischi di credito, di mercato e operativo (di I Pilastro), le banche devono sottoporre a valutazione interna rischio di concentrazione, rischio paese, rischio di trasferimento, rischio base, rischio di tasso di interesse derivante da attività diverse dalla negoziazione, rischio residuo, rischi da cartolarizzazioni, rischio di leva finanziaria, rischio strategico, rischio di reputazione (di II Pilastro). Cfr. Banca D'Italia, *Disposizioni di vigilanza per le banche*, Circolare n. 285 del 17 dicembre 2013, 26° aggiornamento 6 marzo 2019, Parte Prima, III, 1, 29, Allegato A.

[5] Non si sono volutamente considerati, in questa sede, gli effetti di *FinTech* sui *macro financial risks*. «*While there are currently no compelling signs of these risks materialising, experience shows that they can emerge quickly if left unchecked. Systemic importance and procyclicality could emerge from a number of sources, including from greater concentration in some market segments and if funding flows on FinTech lending platforms were to become large and unstable. Any assessment of the implications of FinTech for financial stability is challenged by the limited availability of both official and privately disclosed data in the FinTech area*»: Financial Stability Board, *Financial Stability Implications from FinTech. Supervisory and regulatory issues that merit authorities' attention*, June 2017, p. 2.

Figura 1. Tassonomia dei rischi: rischi esterni vs rischi interni.



Fonte: elaborazione degli autori

Sulla base delle peculiarità analizzate in qu Il rischio di provvista (o anche di 'approvvigionamento' o *funding liquidity risk*[6]) dipende dalla capacità dell'intermediario di mantenere relazioni stabili e durature nel tempo con i prestatori di fondi e, quindi, di raccogliere continuativamente (nei tempi richiesti) le risorse finanziarie necessarie (depositi dalla clientela al dettaglio, obbligazioni collocate sul mercato, depositi interbancari, capitale proprio dagli azionisti) per quantità e a prezzi (costi) compatibili con gli obiettivi di crescita, le scelte di composizione dell'attivo e il rendimento degli investimenti, indipendentemente dal verificarsi di situazioni patologiche, specie di origine esterna, che possono dare origine a fenomeni di illiquidità.

Il rischio di liquidità (inteso in senso stretto) è legato alla necessità di far fronte, in presenza di improvvisi squilibri tra entrate e uscite, alle obbligazioni tempestivamente e senza compromettere la solvibilità prospettica (criterio della sostenibilità). Poiché le risorse finanziarie integrative possono provenire, oltre che dalle 'riserve libere' disponibili, da nuova raccolta e/o dal parziale smobilizzo di attività (tipicamente titoli), il manifestarsi di tale rischio dipende dall'interazione tra struttura, caratteristiche e composizione del passivo (*funding liquidity risk*

[6] Il *funding liquidity risk* è distinto dal *market liquidity risk*, connesso, piuttosto, all'eventuale difficoltà di smobilizzo anticipato delle attività detenute con il sostenimento di perdite e ai conseguenti maggiori costi di raccolta.

e rischio di leva finanziaria), del *banking book* (rischi di controparte) e del *trading book* (*market liquidity risk*).

Il rischio di controparte[7] attiene a tutte le operazioni attive e deriva dall'eventualità che alcuni soggetti possano risultare, entro un determinato intervallo temporale, inadempienti rispetto agli impegni contrattualmente assunti. Il rischio di regolamento è legato, nell'attività di *trading,* all'inadempienza della controparte obbligata a consegnare una certa somma di denaro in contropartita di determinati strumenti finanziari e viceversa; nei servizi di pagamento al buon fine dell'operazione. Impatto e possibili conseguenze dell'inadempienza dipendono dalla scadenza dell'esecuzione del contratto (a pronti o a termine) e dalla contestualità (*delivery vs payment* o *delivery vs settlement*) delle prestazioni; in caso di prestazione anticipata, per il beneficiario può manifestarsi un rischio di credito qualora l'inadempimento temporaneo si trasformi in insolvenza[8]. Nella gestione dei servizi di pagamento, il rischio di regolamento è legato al buon fine dell'operazione.

Il rischio di credito – connesso all'attività di finanziamento mediante concessione di fidi e sottoscrizione di titoli – concerne la possibilità che la controparte debitrice non sia in grado di far fronte ai propri impegni di pagamento o che si riduca il suo livello di affidabilità[9]. Data la complessità degli eventi che lo possono generare e le variegate caratteristiche tecniche e contrattuali dell'esposizione dell'intermediario verso le controparti affidate, il rischio di credito assume differenti accezioni in relazione al fattore causale e alla natura della posizione (insolvenza, migrazione, *spread*, tassi di effettivo recupero, paese di insediamento).

Il rischio di mercato identifica l'insieme dei fattori esogeni di incertezza derivanti dalla molteplicità dei 'rapporti' che gli intermediari intrattengono con i mercati finanziari attraverso la detenzione e la gestione degli strumenti negoziabili; essi, pertanto, evidenziano gli effetti sul valore atteso delle attività incluse nel *trading book* e delle passività emesse (azioni e obbligazioni), riconducibili alla variabilità dei tassi (rischio di interesse), delle valute (rischio di cambio), delle quotazioni degli strumenti (azioni, obbligazioni, derivati, *commodities*) e dei mercati (rischio di prezzo). Inoltre, l'esposizione al rischio di interesse (e di cambio) si manifesta nel momento e nella misura in cui – dovendo l'intermediario adattare le condizioni dello scambio finanziario alle divergenti preferenze di

---

[7] Nell'ambito della CRD IV, «*il rischio di credito comprende il rischio di controparte, ossia il rischio che la controparte di un'operazione risulti inadempiente prima del regolamento definitivo dei flussi finanziari di un'operazione*», cfr. Banca d'Italia, *op. cit.*, Parte Prima, III, 1, 29.

[8] Nelle operazioni in cambi, il rischio di regolamento (cd. Rischio *Herstatt*) si può manifestare qualora una delle controparti consegni la valuta venduta ma non riceva quella acquistata. Cfr. G. Galati, *Il rischio di regolamento nei mercati valutari*, in Bank for international Settlements, *Rivista Trimestrale*, dicembre 2002.

[9] «*Con il termine rischio di credito si indica la possibilità che una variazione inattesa del merito creditizio di una controparte nei confronti della quale esiste un'esposizione creditizia generi una corrispondente variazione inattesa del valore di mercato della posizione creditoria*». A. Resti e A. Sironi, *Rischio e valore nelle banche*, Milano, 2008.

prenditori e datori di fondi – si determina una condizione di *mismatching* (di scadenza e/o di rivedibilità delle condizioni contrattuali) tra attivo e passivo.

Il rischio da regolamentazione si articola nel rischio legislativo (da non confondersi con il rischio legale, di natura prettamente operativa, e quindi interna) legato agli effetti derivanti dall'introduzione di nuove regole che modificano l'operatività degli intermediari con effetti negativi sul conto economico, e nel rischio di *compliance*[10] legato al verificarsi di inadempienze interne nel rispetto delle regole o di situazioni nelle quali le norme al cui rispetto è soggetta l'operatività sono ambigue o la loro applicazione non ancora adeguatamente sperimentata. Comportamenti scorretti e il mancato rispetto di norme e procedure, frequentemente all'origine di rischi di credito o di mercato, espongono l'intermediario a sanzioni e richieste di risarcimento danni o annullamento dei contratti e hanno, se resi di dominio pubblico, un effetto sulla reputazione.

I rischi interni attengono a un ampio e variegato insieme di aspetti della vita aziendale, potenzialmente in grado di produrre effetti negativi sui risultati economici. Anche se le numerose declinazioni dei fattori causali si rivelano difficilmente catalogabili, le categorie più 'riconoscibili' sono rischio operativo, strategico e reputazionale: il primo incluso tra quelli di I Pilastro (e quindi nella determinazione del requisito prudenziale), gli altri due tra quelli di II Pilastro, differenza dovuta, forse, non a una maggiore/minore importanza, ma alla diversa diffusione di consolidate metodologie di misurazione.

Il rischio operativo[11] è intrinsecamente connesso allo svolgimento di qualsiasi attività aziendale e considera le perdite inattese causate, oltre che da eventi esterni imprevisti tipicamente di natura non finanziaria (furti, atti vandalici e terroristici, terremoti…), da malfunzionamenti o inefficienze nella gestione dei sistemi interni (rischio informatico, rischio di *trading*), dei processi produttivi (politiche creditizie, sistemi di pagamento), delle risorse umane (comportamenti erronei o dolosi dei dipendenti). Mentre per le imprese non finanziarie il rischio operativo rappresenta il 'vero' rischio legato allo svolgimento del business, negli intermediari finanziari esso viene spesso identificato, in modo residuale rispetto al quelli di mercato e di credito.

Nei sistemi di pagamenti, il rischio operativo assume connotati peculiari: falsificazione, contraffazione e clonazione degli strumenti; frode per la loro appropriazione e indebito utilizzo, il cd. *phishing* che consente di ottenere, in modo

---

[10] «*Il rischio di non conformità alle norme è il rischio di incorrere in sanzioni giudiziarie e amministrative, perdite finanziarie rilevanti e danni di reputazione in conseguenza di violazione di norme imperative (di legge o di regolamenti) ovvero di autoregolamentazione (es. statuti, codici di condotta, codici di autoregolamentazione)*»: Banca d'Italia, *op., cit.*, Parte Prima, IV, 3, 18.

[11] «*Operational risk is defined as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk, but excludes strategic and reputational risk*»: Basel Committee on Banking Supervision, *Basel II: International Convergence of Capital Measurement and Capital Standards: a Revised Framework,* June 2004, § 644. Anche se aiuta a 'fare ordine', tale definizione, tuttavia non è l'unica possibile: cfr. A. Resti e A. Sironi, *op. cit.*, pp. 503 e ss.

ingannevole, l'accesso ai dati necessari per disporre pagamenti fraudolenti[12]. Inoltre, la circostanza che diritti e obblighi delle parti coinvolte possano essere soggetti a incertezza e le situazioni di contrasto circa le relazioni contrattuali tra i soggetti coinvolti nell'esecuzione di una transazione (emittenti, *service provider*, clienti, esercenti ecc.)[13] determinano specifiche fattispecie di rischio legale.

Per le sue manifestazioni, il rischio operativo presenta, rispetto ai rischi finanziari, elementi di differenziazione tali da poterlo assimilare a quelli puri anche se un approccio alternativo lo annovera tra i primi poiché unaa corretta gestione può incidere positivamente su risultati economici, valore e reputazione dell'intermediario[14].

Il rischio strategico, nell'approccio della vigilanza[15], è influenzato da fattori di natura sia esterna (*cambiamenti di contesto*) sia interna (*decisioni aziendali* e *scarsa reattività*) derivanti dall'inadeguatezza degli assetti di *governance*, organizzativi, di controllo. Il rischio strategico puro trae origine da rilevanti cambiamenti nei volumi di attività (raccolta e impieghi, servizi di intermediazione, negoziazione titoli ecc.) a seguito, ad esempio, di differenti comportamenti della clientela; il rischio di business (o commerciale) dagli effetti derivanti da momenti di forte cambiamento aziendale, quali l'entrata in nuovi mercati o aree di attività.

Il rischio reputazionale[16] si manifesta in coincidenza con la diffusione di notizie negative, veritiere o meno, che intaccano la fiducia nell'integrità della banca e nella sua capacità di continuare a soddisfare le aspettative degli *stakeholders.* Tali circostanze sono da attribuire a: comportamenti poco trasparenti, non *compliant*, scorretti; scelte che violano o disattendono le aspettative del mercato/ambiente; errata percezione della natura del business; adozione di strategie dannose per l'immagine esterna. La perdita di reputazione si traduce tipicamente in una riduzione dei volumi di attività e in un aggravio di costi (soprattutto di raccolta).

Il rischio di reputazione ha, quindi, natura consequenziale, quale risultato di una trasformazione di altre forme di rischio che hanno impatto sui processi (rischio operativo e di *compliance*) in presenza sia di una diretta responsabilità della banca nell'adozione di scelte con effetti negativi; sia dell'attivazione

---

[12] La struttura a *network* determina un potenziale di trasmissione all'intero sistema finanziario (effetto sistemico): ad esempio in caso di attacchi alle reti di telecomunicazione in grado di inserire o modificare i messaggi scambiati tra gli operatori.

[13] Ai fini dell'allocazione dei rischi insiti nei processi di regolamento e per la definizione degli standard operativi di gestione del sistema, è, infatti, importante stabilire con certezza il momento in cui i pagamenti immessi nel sistema diventano definitivi e opponibili a terzi.

[14] S. Cosma, *La misurazione del rischio operativo delle banche*, Roma, 2008.

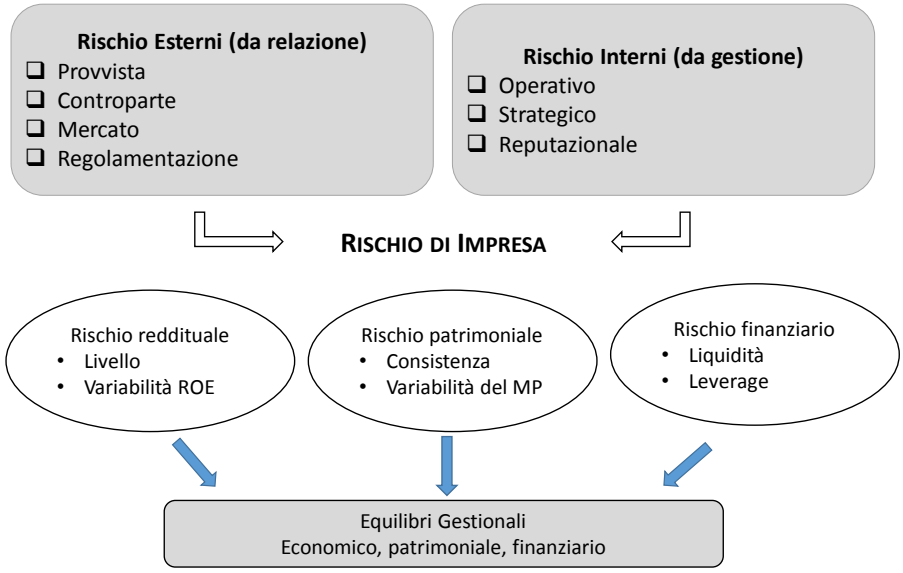
[15] «*Il rischio attuale o prospettico di flessione degli utili o del capitale derivante da cambiamenti del contesto operativo o da decisioni aziendali errate, attuazione inadeguata di decisioni, scarsa reattività a variazioni del contesto competitivo*»: Banca D'Italia, *op. cit.*, Parte Prima, III, 1, 30. Si noti che mentre il modello formale-regolamentare indirizza i comportamenti per evitare/mitigare manifestazioni negative del rischio, in un'ottica aziendale l'assunzione del rischio strategico è 'speculativa' poiché l'obiettivo gestionale è quello di aggiungere valore, definito il livello appropriato di rischio.

[16] «*Il rischio attuale o prospettico di flessione degli utili o del capitale derivante da una percezione negativa dell'immagine della banca da parte di clienti, controparti, azionisti, investitori o Autorità di vigilanza*»: Banca D'Italia, *op. cit.*, *ibidem*.

di specifiche variabili reputazionali (tipologia di business ed esposizione ai processi di comunicazione). Analogamente al rischio operativo, la letteratura ha individuato i molteplici vantaggi derivanti da un più elevato *status* in termini di: capacità di comunicazione, coinvolgimento delle risorse umane, condizioni di accesso al mercato dei capitali, attrazione di nuovi potenziali investitori[17].

Le molteplici categorie di rischio esprimono congiuntamente i principali fattori di incertezza che incidono sull'equilibrio di gestione, inteso come l'insieme delle condizioni necessarie e sufficienti affinché si mantengano nel tempo stabilità e continuità di funzionamento dell'intermediario (fig. 2).

Figura 2. Tassonomia dei rischi ed equilibri gestionali



Fonte: elaborazione degli autori

L'equilibrio va inteso in termini economici (conseguimento di risultati reddituali atti a garantire le relazioni di scambio con datori e prenditori di fondi), patrimoniali (costante mantenimento di un valore dell'attivo superiore al valore del passivo) e finanziari (equilibrio tra flussi in entrata e in uscita nel breve periodo e tra struttura dell'attivo e del passivo nel lungo periodo).

[17] Sul tema ci si limita a rinviare a G. Gabbi, *Definizione, misurazione e gestione del rischio reputazionale negli intermediari finanziari*, in *Banca Impresa e Società*, 2004, pp. 51-80; M. Anolli e F. Rajola, *Il rischio di reputazione e di non conformità*, Roma, 2010 e F. Fiordelisi, P. Schwizer e M.G. Soana *The determinants of reputational risk in the banking sector*, in *Journal of Banking and Finance*, 2013, pp. 1359-1371.

La tassonomia qui proposta non è certamente esaustiva[18] poiché, anche per ragioni di sintesi, non sono state considerate le sotto categorie nelle quali ciascun rischio può articolarsi ma al quale esse sono facilmente associabili: ad esempio: il rischio di riciclaggio è riconducibile al rischio legale e incide su quelli di reputazione e di *compliance*; il *cyber risk*, l'inadeguatezza degli algoritmi, gli errori nella gestione dei dati, la dipendenza da fornitori di servizi tecnologici, hanno tutti natura tipicamente operativa, ma con un forte impatto reputazionale; l'obsolescenza tecnologica e un mutato contesto competitivo attengono al rischio strategico.

Coerentemente con l'approccio adottato, i rischi tipicamente legati alle innovazioni di prodotto e di processo indotte dall'uso intensivo ed estensivo delle tecnologie informatiche e digitali di *FinTech* non sono stati esplicitati[19] poiché si ritiene preliminare la delimitazione e la definizione delle sue principali aree operative.

3. I contorni di FinTech *e l'analisi verticale dei rischi*

Il sistema finanziario, inteso come insieme complesso di transazioni basate su strumenti scambiati attraverso il circuito diretto (i mercati) e il circuito indiretto (gli intermediari), è da sempre esposto agli effetti del processo di innovazione nelle sue molteplici sfaccettature, pur con tassi di accelerazione diversi a seconda del grado di modernizzazione dei contesti di riferimento. Del resto, le prime forme di innovazione tecnologica applicate al sistema finanziario risalgono ai primi anni 50[20] e il settore bancario ha tempestivamente colto, prima di altri[21], le opportunità offerte dalla digitalizzazione dei contatti resa possibile dalla diffusione della rete internet, dando avvio a innovazioni di processo (banca virtuale, *home banking*) e di prodotto (*trading on line*) in grado di migliorare sensibilmente il livello di erogazione dei servizi offerti alla vecchia ed alla nuova clientela.

---

[18] Le Autorità di vigilanza, ai fini Icaap, precisano che «*Le banche effettuano in autonomia un'accurata identificazione dei rischi ai quali sono esposte, avuto riguardo alla propria operatività e ai mercati di riferimento. Al fine di individuare i rischi rilevanti, l'analisi deve considerare almeno i rischi contenuti nell'elenco di cui all'Allegato A. Detto elenco non ha carattere esaustivo: è rimessa alla prudente valutazione di ogni banca l'individuazione di eventuali ulteriori fattori di rischio connessi con la propria specifica operatività*»: Banca d'Italia, *op. cit.*, Parte Prima, III, I, III.

[19] Si veda, a tale proposito, la schematizzazione dei rischi, nell'ottica delle imprese *FinTech* e della clientela proposta da C. Schena, A. Tanda, C. Arlotta, G. Potenza, *Lo sviluppo del FinTech. Opportunità e rischi per l'industria finanziaria nell'era digitale*, Consob, 2018.

[20] Al 1950 risale la prima carta di credito emessa da una *third-party* (Diners Club), vera e propria forma di utilizzo di servizi bancari da remoto, seguita poi dall'introduzione dei primi dispositivi Atm nel 1967 ad opera di *Barclays*. Risale al 1969 il primo tentativo di 'elettronificazione' dei mercati finanziari da parte di *Instinet*, che ha consentito l'avvio nel 1971 del primo mercato elettronico su larga scala con la costituzione della *National Association of Securities Dealers Automated Quotations* (Nasdaq).

[21] Infatti, mentre la prima forma significativa di *e-commerce* risale al luglio 1995 (lancio del primo *bookstore on line* ad opera di Jeff Bezof), la prima iniziativa di *home banking* fu avviata dalla *Stanford Federal Credit Union* nell'ottobre del 1994.

Come è noto, con *FinTech* si intende ogni innovazione di tipo tecnologico in grado di promuovere novità rilevanti in termini di modelli di business, prodotti, processi nonché di modalità di erogazione dei servizi finanziari[22]. L'ampiezza di tale definizione, adottata diffusamente sia nella letteratura di riferimento sia dai *regulators*[23], è spiegata dalla volontà di non confinare un fenomeno così recente, e con una dinamica di sviluppo così fluida, in definizioni puntuali tali da potersi rilevare in futuro restrittive o estremamente parziali. Di certo, l'innovazione digitale riguarda l'intero mercato dei servizi finanziari – inteso come l'insieme delle relazioni, dei comportamenti e delle strategie degli operatori che vi partecipano – oltre che le sue caratteristiche strutturali: barriere all'entrata e all'uscita, numerosità dei *competitors*, apertura e facilità di accesso alle innovazioni tecnologiche[24].

La classificazione delle attività *FinTech* è oggetto di continua revisione anche in considerazione delle possibili interazioni tra le opportunità offerte dai servizi di IT e le linee di business tipiche degli intermediari finanziari (fig. 3).

Il nodo cruciale è però comprendere la reale differenza tra le innovazioni di *FinTech* e quelle precedenti: da questo punto di vista, la 'discontinuità' è legata alla diffusa possibilità di utilizzare processori (*smartphone*) in grado di elaborare volumi di dati di una rilevanza tale da avere uno scarso termine di paragone con il passato. Quale poi il possibile impatto sul mercato finanziario e sulle banche, è questione aperta: pur essendo stati delineati numerosi scenari di mercato, non si è tuttavia ancora giunti ad una condivisa valutazione circa la reale portata della necessità di adattamento del sistema finanziario alle innovazioni digitali, e quindi della nuova dimensione del rischio strategico.

La difficoltà di individuare uno scenario di riferimento è collegata ad una molteplicità di aspetti: la varietà dei segmenti di business e dei processi di mercato collegati al *FinTech*; il diverso grado di permeabilità di ciascuno di essi ai fenomeni di digitalizzazione, le differenze nelle strutture di domanda del canale *FinTech* per le molteplici aree di attività. Se da un lato si è nel tempo assistito a esempi di innovazioni *disruptive*, in grado di arrecare mutamenti radicali all'industria di riferimento e tali da dissolvere anche in tempi brevi modelli consolidati, dall'altro lato, i fattori di specificità delle banche delineano la possibilità che l'impatto del *FinTech* sul mercato finanziario sia più moderato o, per meglio dire, meno futurista di uno scenario *distruptive*, evocativo di una disintermediazione esiziale per la sopravvivenza della banca stessa.

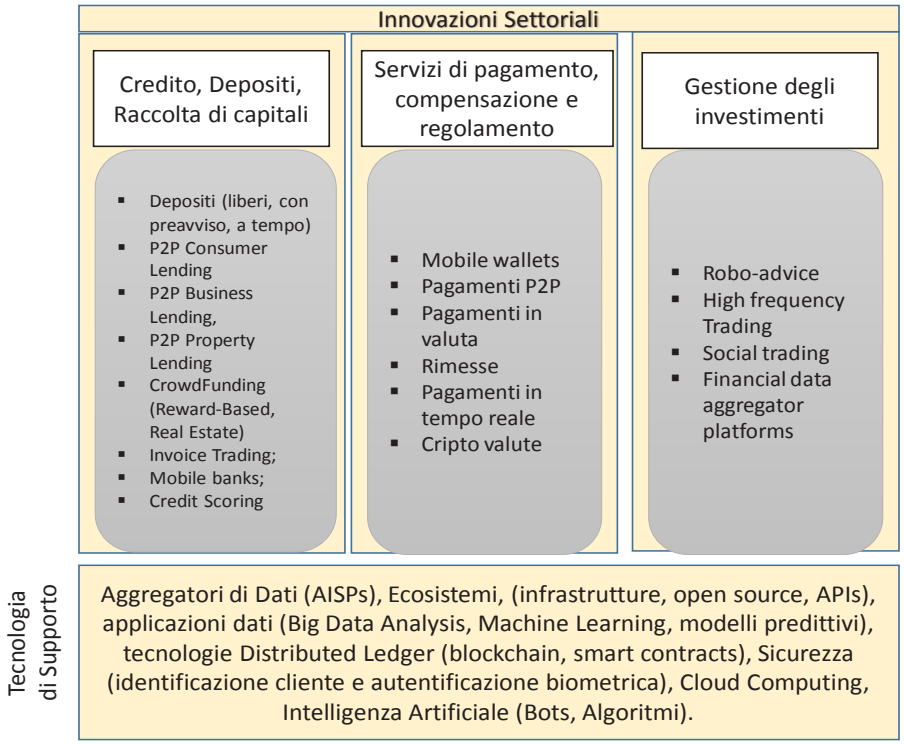
---

[22] «*FinTech is defined as technology-enabled innovation in financial services that could result in new business models, applications, processes or products with an associated material effect on the provision of financial services*»: Financial Stability Board, *op. ult. cit.*, p. 7.

[23] La definizione del Financial Stability Board è stata presa come riferimento ad esempio da Bank for International Settlements, *Implications of fintech developments for banks and bank supervisors*, February 2018, pp. 8-9 e da European Banking Authority, *Report on the Prudential Risks and Opportunities Arising for Institutions from Fintech*, July 2018, p. 9.

[24] Cfr. Financial Stability Board, *FinTech and market structure in financial services: Market developments and potential financial stability implications*, 14 February 2019, p. 3 e ss.

Figura 3. Classificazione delle aree *FinTech*



Fonte: elaborazione degli autori da BIS, 2018, *op. cit*., p. 9.

Lo sviluppo di aree emergenti di innovazione pone alle autorità di vigilanza una serie di sfide, prima tra tutte la ricerca (non semplice) del giusto *trade-off* tra "certezza" delle regole ed incoraggiamento alla rivoluzione digitale[25]: a tal fine, è in primo luogo necessaria una valutazione dei profili di rischio cui si espongono le nuove realtà emergenti con un'analisi di tipo 'verticale' tesa ad evidenziare le diverse forme di rischio associate ad ogni nuova area di business (fig. 4).

Figura 4. FinTech e rischi per gli intermediari

	Settori di Attività FinTech							
Rischio	Crowd-funding	Lending Marketplace	Mobile Banks	Credit Scoring	Mobile payments	Cripto-valute	High Frequency Trading	Robo-Advice
Credito	☑	☑						
Mercato		☑				☑	☑	☑
Operativo	☑	☑	☑	☑	☑	☑	☑	☑
Regolamentazione	☑	☑	☑	☑	☑	☑	☑	☑
Liquidità					☑	☑	☑	
Reputazionale	☑	☑	☑	☑	☑	☑	☑	☑
Strategico	☑	☑	☑	☑	☑	☑	☑	☑

Fonte: elaborazione degli autori

[25] Cfr. C. Barbagallo, *Fintech: Ruolo dell'Autorità di Vigilanza in un mercato che cambia*, Adeimf, Napoli, 8 Febbraio 2019.

Poiché ragioni di sintesi impediscono l'analisi verticale dei rischi per ciascuna delle aree di *FinTech*, in questa sede ci si limiterà solo a due tra le più rilevanti.

Il *Peer to Peer Lending*

Le piattaforme *Peer to Peer Lending* (P2P)[26] costituiscono una delle principali forme di innovazione digitale legata al canale del credito e consentono l'incontro diretto tra prenditori e potenziali datori di fondi a titolo di finanziamento o di mezzi propri, distinguendo *consumer*, *business* e *property lending*. L'attività di P2P, nota anche con il termine di *lending-based crowdfunding*, può articolarsi in diversi modelli di business (in continua evoluzione), che hanno in comune la caratteristica da un lato di agevolare sia la raccolta di informazioni dei prenditori di risorse sia la loro elaborazione da parte dei datori, e dall'altro di essere orientati ad un margine commissionale generato da entrambi i lati del mercato (domanda ed offerta di credito).

Uno dei modelli di business più diffusi (c.d *client segregated accoun*t), prevede che la piattaforma svolga una pura attività di mediazione, provvedendo al *matching* tra debitori e finanziatori, spesso mediante asta. Realizzatosi l'abbinamento, la raccolta avviene attraverso un conto esterno su cui transiterà il credito concesso: il conto è definito '*esterno'* poiché non rientra nelle disponibilità della piattaforma, ciò per garantire l'autonomia patrimoniale dei fondi raccolti e neutralizzare ogni forma di rischio di *default* della piattaforma stessa[27]. Un secondo modello di business (c.d. *notary model*) prevede che, per ciascun prestito, la raccolta di fondi avvenga tramite una banca depositaria, la quale, raggiunto l'importo richiesto, concede direttamente il credito rilasciando ai finanziatori anche un certificato (*promissory notes*) che può essere rinegoziato. Un ulteriore modello-tipico dei paesi in cui c'è un eccesso di offerta di fondi rispetto alla domanda (Cina) è il c.d. *guaranteed return model*, nel quale i fondi sono raccolti presso i finanziatori a fronte della garanzia di un rendimento minimo adeguato al rischio di credito del debitore.

Il ricorso al P2P presenta molteplici vantaggi soprattutto per i *borrowers* per i quali l'offerta di un canale aggiuntivo al tradizionale credito bancario non può che incrementare le probabilità di ottenere un esito positivo nella ricerca di una controparte. La facilitazione di accesso appare ancora più rilevante considerando che tali prestiti sono tipicamente non garantiti. Inoltre, la snellezza della sovrastruttura tecnica e dei processi gestionali consente l'erogazione delle somme in tempi brevi, o comunque inferiori a quelli del comparto tradizionale, mentre i bassi costi operativi determinano la riduzione dei tassi applicati.

---

[26] In materia, cfr. il contributo di M. Bellino in questo *Quaderno*.

[27] Esistono diverse varianti del modello in parola, tra cui quella rappresentata dalla costituzione di un fondo comune di investimento le cui quote vengono sottoscritte da parte dei finanziatori tramite la piattaforma stessa. Cfr. M. Caratelli, U. Filotto, L. Gibilaro, G. Mattarrocci, *Il mercato del peer-to-peer lending nel mondo e le prospettive per l'Italia,* in *Bancaria*, n. 3, 2016, p. 68.

Per i *lenders*, i vantaggi del ricorso a forme di P2P andrebbero invece valutati in termini di tassi di rendimento e, più correttamente, mediante un confronto con investimenti analoghi. Tuttavia, la difficoltà di identificare forme effettivamente comparabili per esposizione al rischio, rende tale approccio poco significativo. Ad esempio, se da un lato la misurazione del differenziale di rendimento tra P2P e *consumer* Abs appare accettabile in linea generale, dall'altro lato la non completa 'nitidezza' di confronto tra le due categorie non garantisce valutazioni corrette di efficienza[28]. Del resto, neanche i confronti tra *performance* di indici rappresentativi di operazioni di *alternative lending* e di investimenti di tipo tradizionale paiono in grado di offrire una valida base di parametrazione dei vantaggi del P2P a favore dei *lenders*[29].

Lo sbilanciamento dei vantaggi a favore dei debitori non può che riflettersi nella prevalenza dei rischi in capo ai finanziatori nella cui ottica la valutazione del rischio di credito assume un ruolo cruciale con effetti anche sul piano, ben più rilevante, della stabilità del sistema finanziario.

La valutazione del rischio di credito, nelle sue due fasi essenziali di *screening* e *monitoring*, viene tipicamente realizzata con metodologie standardizzate di *credit scoring* basate su informazioni provenienti sia dalle schede di accesso compilate dagli stessi debitori, sia dai sistemi esterni di condivisione del rischio (*Credit Bureaux*), oltre che su altre informazioni qualitative e personali desumibili dal web e/o dai *social network*. Il processo di valutazione del merito creditizio non è, in ogni caso, sottoposto ad alcuna validazione, diversamente da quanto avviene per il credito bancario, con conseguenti potenziali rischi di inefficienza nell'allocazione del risparmio.

Inoltre, l'assenza di centrali rischi in grado di monitorare l'esposizione dei *borrowers* congiuntamente sui canali tradizionali e su quelli di *alternative lending,* rende ipotizzabili comportamenti opportunistici da parte dei debitori, con fenomeni di *multi-submission* (richieste simultanee su più piattaforme) e conseguenti rischi di selezione avversa. Peraltro, la mancata segnalazione delle esposizioni sulle varie piattaforme, oltre che aumentare il rischio dei *lenders* che si rivolgono ai P2P, rischia di minare la stessa affidabilità delle centrali rischi esistenti, non essendo esse più in grado di catturare l'esposizione complessiva dei debitori, con una sottovalutazione del rischio di credito non priva di effetti negativi per le banche.

Come visto, nel modello di business tipico del P2P, le piattaforme assumono un ruolo di *broker* senza che ciò comporti alcuna esposizione a

---

[28] Per un approfondimento, M. Bofondi, *Il lending-based crowdfunding: opportunità e rischi*, Banca d'Italia. Questioni di Economia e Finanza, n. 375, marzo 2017, p. 16.

[29] È il caso dei non rari confronti tra l'indice *Orchard US Consumer Marketplace Lending Index* e le tradizionali classi di investimento (azionario vs obbligazionario) che, se da un lato ben rappresentano le differenze di comportamento del comparto in termini di correlazione tra rendimenti, dall'altro non possono evidenziare alcun vantaggio diretto nel ricorso al P2P in considerazione delle diverse esposizioni di rischio a cui ciascuna classe di attività conduce.

rischi particolari, al di là di quelli operativi e reputazionali, ineliminabili in ogni tipo di impresa. Di conseguenza, la redditività è orientata esclusivamente all'ottenimento di un margine commissionale: ciò se da un lato è coerente con lo schema generale di *crowdfunding* di cui il P2P è parte, dall'altro accentua lo scollamento tra l'esigenza di massimizzazione del profitto e l'obiettivo di stabilità del sistema finanziario. Essendo le commissioni complessivamente percepite dalle piattaforme P2P naturalmente legate ai volumi di scambio, la loro massimizzazione potrebbe aumentare il rischio di erogazione di prestiti a soggetti non meritevoli, con conseguente innalzamento dei rischi di selezione avversa e di instabilità del settore.

L'assenza di incentivi per le piattaforme a salvaguardare l'efficienza dell'allocazione (*lack of skin in the game*) genera effetti dal lato sia della domanda, con il rischio di sovra-indebitamento, sia dell'offerta, a causa dell'innalzamento del tasso di insolvenza che, specie in condizioni di mercato avverse (ossia con condizioni di prezzo del credito meno favorevoli di quelle correnti), determinerebbe un rischio di *market failure* per l'intero comparto P2P. La constatazione che molti investitori istituzionali, incluse le banche, hanno previsto e prevedono investimenti in piattaforme fa inoltre emergere il rischio che le eventuali difficoltà del comparto possano propagarsi rapidamente in forma di rischio sistemico.

Nel P2P *lending*, l'assenza di una relazione diretta e continua tra finanziatore e debitore, insieme ad un'attività di *monitoring* debole (o assente) da parte della piattaforma, incrementa il rischio che le risorse raccolte dal debitore possano essere distolte rispetto alle finalità originariamente dichiarate (*moral hazard*). Inoltre, l'assenza di un contatto diretto e la distanza tra finanziatore e debitore paiono impedire il conseguimento dei benefici tipici dei modelli di credito relazionale (*relationship lending*), caratterizzati da una più intensa raccolta ed elaborazione di informazioni di tipo qualitativo sull'imprenditore e la sua impresa (*soft information*), benefici che possono determinare condizioni migliori (per quantità e/o prezzi) nell'accesso al credito[30]. In particolare, anche se in ambito P2P può comunque aversi la 'produzione' di *soft information*, offerte direttamente dal debitore, le maggiori problematiche sembrano risiedere nelle più ampie asimmetrie informative collegate al rischio di manipolazione, o anche falsificazione, delle informazioni rilevanti che i *borrowers*, avendo una maggiore libertà di decisione, effettivamente forniscono ai *lenders*[31].

---

[30] Per una rassegna sulla letteratura dei benefici collegati ai modelli di *relationship lending* si rinvia alla meta-analisi della letteratura proposta da V. Kysucky e L. Norden, *The benefits of relationship lending in a cross-country context: A meta-analysis*, in *Management Science*, 2015, Vol. 62, n. 1, pp. 90-110.

[31] Sulla scorta di alcune evidenze empiriche che sembrano delineare una discriminazione etnica e di genere nei tassi dei prestiti di tipo P2P, si è giunti alla paradossale e provocatoria conclusione secondo cui al debitore converrebbe manipolare il proprio profilo (cfr. B. Käfer, *Peer-to-Peer Lending. A (Financial Stability) Risk Perspective*, *Magks Papers on Economics*, n. 22, Philipps-Universität, 2016, p. 16).

Nella valutazione dei rischi collegati all'attività P2P, occorre poi ricordare che il modello di circuito diretto di intermediazione rende impossibile per il finanziatore realizzare la trasformazione di scadenze che caratterizza e distingue le banche da tutte le altre tipologie di intermediari. Mentre la banca raccoglie tipicamente a breve termine o a vista e riesce a investire in prestiti a medio-lungo termine, gestendo i disallineamenti tra scadenze dell'attivo e scadenze del passivo, nel P2P la scadenza del debito del *borrower* coincide con quella del *lender*, generando una maggiore esposizione al rischio di liquidità per i debiti di medio-lungo periodo[32].

Il servizio di consulenza automatizzata (Robo Advice)

L'automatizzazione indotta da *FinTech* riguarda pressoché tutte le fasi della catena del valore del servizio di *financial advisory*, con particolare riguardo ai suoi due snodi ultimali: *i*) raccolta di informazioni per la profilatura e la segmentazione della clientela; *ii*) proposte di portafogli di investimento ('raccomandazione di investimento di attività finanziarie') coerenti con la propensione al rischio del cliente[33]. L'automazione è quindi a servizio sia del cliente, quale soluzione innovativa per l'identificazione della migliore combinazione rischio/rendimento, sia della stessa società di *robo advice,* in grado di offrire una profilatura tale da aumentare l'efficacia delle iniziative di natura commerciale[34].

Il diverso grado di automazione dei processi nel servizio di *robo-advice* consente l'individuazione di almeno due modelli generali: quelli *puri* caratterizzati da una automazione spinta di tutte le fasi con l'assenza (o la minimizzazione) della relazione fisica con il cliente; quelli *ibridi* che prevedono una combinazione tra la tecnologia digitale e la componente umana in una o più fasi della catena del valore. Nel caso in cui la tecnologia digitale si limita a supportare le scelte del consulente, anziché a comunicare direttamente con il cliente, ci si ritrova, invece, in un modello di tipo B2B noto come *robo4advisor*[35].

In ogni caso, le infrastrutture digitali utilizzate nella fase di *asset allocation*, con particolare riferimento agli algoritmi di costruzione dei portafogli

---

[32] Se da un lato l'implementazione da parte delle piattaforme di opzioni di rimborso anticipato a favore del *lender* ne mitiga la rilevanza, il rischio di liquidità può tuttavia risultare rilevante nei casi in cui l'opzione si rivela particolarmente onerosa, essendo le probabilità di realizzazione di un mercato secondario per i finanziamenti, ancor più se privi di garanzie, molto ridotte.

[33] In argomento, cfr. il contributo di P. Lucantoni in questo *Quaderno*.

[34] Un esempio di automazione dei processi commerciali in ambito di *robo-advice* consiste nella possibilità di raccogliere i dati relativi agli investitori con piccole masse gestite e ricorrere a tecniche di *machine learning* per consentire un *matching* con le informazioni raccolte per gli investitori caratterizzati da un volume di masse gestite più alto. In tal modo, la società investirà maggiori strategie e/o risorse commerciali nei confronti del cliente con piccola esposizione di investimento in considerazione della sua potenzialità a migrare nella categoria dei clienti con maggiore volume di risparmio gestito.

[35] Cfr., Consob*, La digitalizzazione della consulenza in materia di investimenti finanziari*, *Quaderni FinTech* n. 3, 2019, p. 10.

personalizzati proposti alla clientela, assumono un ruolo nevralgico nell'ambito dell'intero processo di produzione del servizio di consulenza.

Gli algoritmi di *portfolio selection* possono essere elaborati *in house* oppure acquistati da soggetti terzi tramite un contratto di licenza d'uso: la scelta non è certamente ininfluente in termini di valutazione delle opportunità e dei rischi per il singolo intermediario nonché per il sistema. A differenza della produzione interna di un software *tailor made*, il ricorso a *provider* esterni potrebbe comportare profili di rischio aggiuntivi collegati alla delega, da parte di una pluralità di intermediari, delle scelte di investimento a uno o pochi soggetti con i relativi modelli proprietari di riferimento.

Finora, i principi di ottimizzazione più utilizzati sono stati coerenti con il *framework* della frontiera efficiente di portafoglio[36] la cui applicazione non è peraltro priva di limiti e complessità tali da rischiare di considerare il portafoglio *à la* Markowitz una combinazione di investimenti contro-intuitiva e/o 'massimizzatrice' degli errori di previsione sull'andamento dei mercati. In estrema sintesi, i limiti metodologici del modello sono riconducibili da un lato alla tendenza a privilegiare, con un effetto di *overweight*, investimenti che rispondono a determinati *trade-off* tra rischio, correlazione e rendimento, generando portafogli concentrati in poche *asset class*, dall'altro a identificare come ottimali portafogli caratterizzati da una forte instabilità[37]. Pur essendo stati proposti, senza peraltro giungere a soluzioni condivise[38], alcuni accorgimenti volti a mitigare la rischiosità del modello, in un contesto di completa automazione dei processi, la diffusione di metodologie algoritmiche standardizzate, ma prive di una chiara e riconosciuta efficacia operativa, genera

---

[36] Sul punto si rinvia all'indagine della Financial Industry Regulatory Authority, *Report on Digital Investment Advice*, 2016, p. 3.

[37] Tale instabilità è l'effetto dell'elevata sensibilità dell'output del modello (i portafogli ottimali) rispetto ad una variazione anche marginale degli input (i rendimenti, i rischi e le correlazioni degli investimenti considerati idonei per il cliente). Giacché l'approccio normativo per l'implementazione del modello di Markowitz prevede una specificazione degli input sostanzialmente basata sulla sola osservazione delle serie storiche, è stato osservato che la frontiera efficiente dei portafogli ottimi si caratterizzi per un'eccessiva sensibilità al valore di "errore di stima" o *estimation error* (definito come la differenza tra il valore stimato di un parametro ed il suo vero valore). Di conseguenza, l'esposizione ad un elevato *estimation error* conduce ad un allontanamento del portafoglio ottimo *ex-ante* dalla zona di efficienza identificata *ex-post*, apre la strada ad un dibattito critico circa la reale capacità dei modelli della frontiera efficiente di minimizzazione del rischio. Cfr. U. Pomante, *Global Asset Allocation: From the efficient frontier to the reduction of the instability due to estimation error*, in G. De Laurentis (a cura di), *Performance measurements frontiers in banking and finance*, Milano, 2004.

[38] Tra le storiche soluzioni di correzione del modello di Markowitz rientra il modello di Black & Litterman (F. Black, e R. Litterman, *Global portfolio optimization*, in *Financial Analyst Journal*, 1992, Vol. 48, n.5) il cui concetto di 'ottimizzazione inversa' non è però scevro da critiche (sul punto si veda ad esempio R.O. Michaud, D. Esch, e R. Michaud, *Deconstructing Black-Litterman: How to Get the Portfolio You Already Knew You Wanted*, in *Journal of Investment Management*, 2013,11 (1), 6-20).

il dubbio (il rischio) circa la capacità del descritto *framework* di riferimento di aggiungere equilibrio ai mercati.

In un contesto di generalizzato ricorso al software per il servizio di raccomandazioni di investimento, ed in presenza di un modello primario di tipo "*one fits size all"* non scevro da limiti, non è difficile immaginare che la crescita dei volumi di servizio erogati tramite *robo advisory,* possa determinare un innalzamento del rischio sistemico in corrispondenza di fasi di mercato negative e perdite diffuse tra i clienti[39].

Le precedenti considerazioni rientrano nell'alveo del più ampio dibattito in tema di *governance* degli algoritmi essendosi posto il quesito circa l'opportunità di assoggettarli a regole chiare di vigilanza[40]: in quest'ottica, è stato imposto alle società *FinTech* di documentare l'intero processo di realizzazione delle raccomandazioni di investimento cui l'algoritmo è sotteso[41], osservando che – ai fini di una corretta implementazione dell'algoritmo stesso e della gestione delle decisioni di tipo *human touch* (ad esempio quelle di ribilanciamento) - rimangono indispensabili competenze e qualificazioni del personale, tali da consentire ed agevolare la comprensione della logica sottostante gli algoritmi[42].

Ulteriori punti di attenzione per il regolatore si riferiscono alle modalità di presentazione al cliente delle possibili scelte di portafoglio. Infatti, indipendentemente dal modello organizzativo prescelto (puro o ibrido) il ricorso all'automatizzazione spinta dà al potenziale cliente maggiori opzioni di scelta anche se le modalità di presentazione delle raccomandazioni possono influire sulla stessa decisione di investimento. La sempre più vasta letteratura sulla finanza comportamentale ha, infatti, evidenziato la rilevanza del tema dell'architettura delle scelte[43] e l'elevata correlazione tra modalità di presentazione e selezione della raccomandazione: in altre parole, il numero di opzioni proposte, le loro peculiarità, il loro ordine di presentazione e, più in generale, il *framing*, possono

---

[39] Pur essendo tale scenario poco realistico, l'eventuale ampia diffusione di *robo advice* centrati prevalentemente su un unico modello algoritmico di riferimento, determinerebbe l'accentuazione della prociclicità di mercato (cfr. European Banking Authority (EBA), *op.ult. cit.* p. 21).

[40] Si veda sul punto quanto richiamato in Consob, *op. cit.*, pp. 52-60.

[41] «*In particular, firms should at least: establish an appropriate system design documentation that clearly sets out the purpose, scope and design of the algorithms. Decision trees or decision rules should form part of this documentation, where relevant; have a documented test strategy that explains the scope of testing of algorithms. This should include test plans, test cases, test results, defect resolution (if relevant), and final test results*»: European Securities Market Authority, *Guidelines, on certain aspects of the MiFID II suitability requirements*, 2018, § 82.

[42] «*Where relevant, when employing automated tools (including hybrid tools), investment firms should ensure that their staff involved in the activities related to the definition of these tools: (a) have an appropriate understanding of the technology and algorithms used to provide digital advice (particularly they are able to understand the rationale, risks and rules behind the algorithms underpinning the digital advice); and b) are able to understand and review the digital/automated advice generated by the algorithms*»: European Securities Market Authority, *ibidem,* § 100.

[43] Con riferimento al tema dell'architettura delle scelte (*choiche architecture*) si rinvia al lavoro pioneristico di R. Thaler e S. Cass, *Nudge, Improving Decisions About Health, Wealth, and Happiness*, Yale, 2008, 3-4, pp. 81-100.

provocare distorsioni cognitive tali da influenzare e concentrare le preferenze su una specifica scelta senza che essa necessariamente corrisponda alla migliore tra le possibili[44]. Di conseguenza, una riflessione in merito all'opportunità di *guidelines* da parte dei regolatori circa l'adozione di modalità neutrali di presentazione della gamma di opzioni possibili per la clientela, non appare inopportuna bensì necessaria.

4. Analisi orizzontale dei rischi: componenti tradizionali vs aree emergenti

L'impatto di *FinTech* sui rischi 'tradizionali' degli *incumbents* deriva in via indiretta dalla presenza sul mercato di nuovi soggetti, in via diretta dal loro ingresso in una o più nuove aree di business attraverso l'ampliamento della gamma di offerta e/o la costituzione di soggetti giuridicamente autonomi ma controllati[45].

Il rischio di provvista e di liquidità

In relazione al rischio di *funding*, è presumibile che le banche tradizionali possano subire gli effetti della crescita dei depositi *on line* – la cui offerta è più elastica al prezzo – che dovrebbero caratterizzarsi, rispetto a quelli tradizionali, per maggiore variabilità (è più probabile il ritiro per passare a un concorrente che riconosce tassi di interesse più vantaggiosi) e/o per minore 'vischiosità' intesa come resistenza ai deflussi in seguito a tensioni quali una crisi bancaria o altro evento economico esterno. Per gli intermediari di nuova costituzione, soprattutto se indipendenti, la bassa redditività iniziale potrebbe influenzare, innalzandolo, il costo del finanziamento tipicamente basato su raccolta all'ingrosso (obbligazioni e depositi interbancari).

La possibile riduzione dei volumi di raccolta (che, peraltro, assume una valenza anche strategica) potrebbe essere la conseguenza sia del tentativo delle imprese *FinTech* di scomporre il pacchetto di servizi finanziari offerti dalle banche,

---

[44] Cfr. E.J. Johnson, S.B. Shu, B.G.C. Dellaert *et al*., *Beyond nudges: Tools of a choice architecture*, in *Marketing Letters*, June 2012, Vol. 23, pp. 487–504.

[45] «*La BCE considera FinTech le banche 'con un modello imprenditoriale in cui la produzione e l'offerta di prodotti e servizi bancari si basano sull'innovazione resa possibile dalla tecnologia'. Data la varietà di enti e tecnologie, questo concetto ampio coglie le diverse attività degli enti creditizi nei vari paesi e comprende: nuove controllate FinTech di enti già esistenti autorizzati all'esercizio dell'attività bancaria; gli enti di nuova costituzione che entrano nel mercato e adottano l'innovazione tecnologica per competere con banche affermate lungo tutta la catena del valore, nonché i fornitori già esistenti di servizi finanziari (istituti di pagamento, imprese di investimento, istituti di moneta elettronica ecc.) che ampliano la propria operatività alle attività bancarie e possono quindi essere considerati nuovi partecipanti al mercato che necessitano di autorizzazione all'attività bancaria*»: Banca Centrale Europea, *Guida alla valutazione delle domande di autorizzazione all'esercizio dell'attività bancaria degli enti creditizi fintech,* marzo 2018, p. 3.

lasciando a queste ultime solo quelli meno redditizi[46] sia, più in generale, della semplificazione delle modalità di fruizione dei servizi finanziari da parte della clientela[47]. Inoltre, non si può escludere che la crescita del *crowdfunding* e del *peer to peer lending* possa determinare una diversa allocazione del portafoglio dei risparmiatori, in particolare di quelli *affluent,* con una potenziale riduzione dell'incidenza delle passività bancarie anche se con un più elevato profilo di rischio.

Gli effetti negativi potrebbero, però, essere 'bilanciati' dai benefici derivanti da un aumento generalizzato del grado di diffusione dei servizi bancari (inclusione) e dal maggiore coinvolgimento delle coorti di popolazione meno alfabetizzate informaticamente. Ciò richiede agli *incumbents*, considerando anche le innovazioni nel sistema dei pagamenti indotte dalla PSD2 e le maggiori possibilità di scelta per gli utenti, la necessità di ricorrere a una nuova, diversa e più articolata profilatura e segmentazione della clientela al dettaglio. Gli eventuali effetti sul rischio di liquidità in senso stretto (v. *supra*) non sono al momento facilmente prevedibili poiché dipenderanno dai mutamenti, se rilevanti, della struttura del passivo delle banche.

Il rischio di credito e di concentrazione

Per la teoria dell'intermediazione finanziaria, la concessione di un finanziamento implica necessariamente elevate asimmetrie informative ex ante (*adverse selection*) e ex post (*moral hazard*) e, quindi, la presenza di un soggetto (la banca) specializzato nella valutazione del rischio e nel monitoraggio dei prestiti comporta minori costi: si tratta di una capacità che i nuovi soggetti *FinTech* devono ancora acquisire.

In termini generali e astratti, la diffusione delle nuove forme di *lending* potrebbe causare, per gli *incumbents*, da un lato la contrazione del credito finora erogato a favore di soggetti *retail* (privati e *small business*), dall'altro la riduzione del razionamento qualora il fenomeno dovesse riguardare prevalentemente soggetti privi di possibilità alternative di accesso al mercato del credito (maggiore inclusione finanziaria)[48].

---

[46] «*Le banche hanno potuto fino a ieri volgere a proprio vantaggio il fatto di essere il principale punto di accesso al mondo della finanza per la maggior parte della popolazione. L'offerta di un prodotto semplice, ma fondamentale, come il conto corrente ha consentito loro di raggiungere una vasta platea di clienti e fare profitti*»: S. Rossi, *Idee per il futuro del sistema finanziario italiano*, Intervento, Courmayeur 23 settembre 2017.

[47] Ad esempio, la diffusione dei servizi di *instant payment* potrebbe comportare la parziale disintermediazione del passivo (riduzione delle giacenze medie sui c/c) e la contrazione dei margini.

[48] L'*instant lending*, pur potendo soddisfare esigenze particolari di fasce di clientela *retail* (famiglie e *small business*) tipicamente attraverso copertura finanziaria anche per pochi giorni garantita da flussi certificati, appare una tipica innovazione di processo poiché la richiesta di credito (tipicamente *paperless*) deve in ogni caso essere preceduta da una valutazione positiva dei requisiti di concessione del prestito. Le nuove tecnologie possono, però, rendere, anche grazie a nuovi e più sofisticati algoritmi, più efficienti modalità e processi a costi ridotti e con tempi di erogazioni più brevi.

È evidente che il complessivo effetto (aumento o riduzione?) sul rischio di credito e di concentrazione, ossia su qualità e composizione del 'tradizionale' portafoglio delle banche, non è al momento prevedibile ma dipenderà dai volumi effettivamente 'intermediati' dalle piattaforme; dalla loro scelta di operare esclusivamente come *marketplace* o concedere, in tutto o in parte, finanziamenti; dalle loro politiche di *scouting;* dalle caratteristiche dimensionali e qualitative dei prenditori.

Maggiori potenzialità di crescita, al momento e nel nostro Paese, sembra presentare l'offerta di modalità innovative di gestione e smobilizzo dei crediti commerciali con erogazione anche istantanea dell'anticipo[49], servizio destinato a una fascia molto ampia di clienti (piccole e medie imprese) in presenza di un volume molto elevato di crediti di fornitura. Infatti, le piattaforme *on line* sono in grado di digitalizzare i processi di: i) *origination*, aprendo nuovi canali distributivi, rapidi ed efficaci per acquisire nuovi clienti senza limitazioni geografiche; ii) *assessment*, determinando *scoring* e valutazioni automatiche del rischio di credito o di frode attraverso l'integrazione di più fonti di dati e algoritmi; iii) *servicing*, interamente digitalizzato. Rispetto al *factoring* tradizionale (che comunque offre un servizio più completo e personalizzato sulla base di una più intensa relazione con il cliente), le soluzioni *FinTech* consentono integrale digitalizzazione e automazione dei processi, elevata velocità di erogazione, minimizzazione dei costi operativi, riduzione della soglia minima di ingresso. Anche in questo caso, l'effetto sul rischio di credito e di concentrazione dipenderà dalla qualità dei clienti *FinTech* (nuovi o 'ex bancari') e di quelli che continueranno a ricorrere al circuito tradizionale.

Nel caso di piattaforme di P2P *lending* che operano esclusivamente quali *marketplace*, il rischio del contratto, e quindi il rischio di credito, ricade interamente sul prestatore. Il frequente ricorso a metodologie standardizzate di valutazione dell'affidabilità della clientela utilizzando servizi di *credit scoring* esterni e/o avvalendosi di fonti di dati di altra natura (algoritmi basati sui *big data*) dipende sia dal perseguimento di obiettivi di riduzione dei costi operativi, sia dalla mancata disponibilità di alcune informazioni essenziali (in particolare quelle di tipo 'andamentale') che rendono difficoltosa la costruzione di un modello proprietario interno. Nel caso di nuovi intermediari vigilati, tale prassi operativa fa emergere, sia un rischio di *outsourcing* (*infra*), sia un rischio di *compliance* in considerazione – soprattutto nella fase di approvazione del metodo di valutazione e governo del rischio da parte delle autorità di vigilanza[50] – della particolare criticità che assumono la tipologia dei dati utilizzati nel processo di affidamento e le modalità con le quali è assicurata la loro qualità.

---

[49] I principali servizi offerti in questo ambito sono: acquisto di fatture per proprio conto (*Digital Factoring*), acquisto di fatture per conto terzi (*Invoice Marketplace*), gestione dei pagamenti per conto del debitore ceduto (*Supply Chain Finance*).

[50] Banca Centrale Europea, *op. cit.*, p. 9.

In un'ottica di sistema, la crescita del P2P potrebbe determinare una minore capacità segnaletica dei dati di Centrale dei Rischi che potrebbero sottostimare l'esposizione debitoria dei *borrowers* con conseguenti rischi di cattiva allocazione del credito, anche di quello bancario tradizionale.

Il rischio di mercato

Tra i rischi 'tradizionali', quello di mercato sembra essere il meno influenzato dalle innovazioni *FinTech*, nel senso che non si rintracciano, allo stato delle innovazioni correnti, settori la cui attività implica, di per sé, un suo significativo innalzamento. Vero è, però, che l'investimento in strumenti finanziari collegati (direttamente o indirettamente) ad imprese o attività *FinTech* espone l'intermediario ad andamenti sfavorevoli dei loro prezzi. In questo senso, l'incremento di volatilità su attività *FinTech*, già di per sé rischiose (si pensi agli investimenti in *crypto asset*, oppure in azioni emesse da piattaforme di *crowdfunding*), e la tendenza a concentrare il portafoglio su iniziative *FinTech* (settore ad elevato tasso di sostituzione delle imprese), possono certamente influire sul rischio di mercato degli intermediari, con conseguenti rischi per la stabilità del sistema.

Il rischio da regolamentazione

L'assenza di una regolamentazione omogenea tra i diversi ordinamenti e l'eterogeneità degli approcci finora emersi[51], rendono palese il rischio legislativo legato, sia pure in misura diversa, alle singole aree di attività *FinTech*. Ad esempio, la vigilanza sulle attività convenzionali svolte dagli *incumbents* può essere aggirata mediante lo svolgimento di attività non regolamentate (*shadow banking*) che pure comportano gli stessi rischi: l'arbitraggio regolamentare tra attività con medesima funzione e profilo di rischio crea, quindi, condizioni di disuguaglianza tra soggetti e pone questioni in ordine all'esigenza di intervento da parte delle autorità.

Il tradizionale *trade-off* tra stabilità ed efficienza appare più intenso nel caso di *FinTech*: se da un lato la regolamentazione delle 'nuove' aree di intermediazione è necessaria, dall'altro gli auspicati interventi si scontrano con l'esigenza di non inibire l'innovazione e l'avvio di nuove iniziative, soprattutto in considerazione dello stadio iniziale di sviluppo del settore; del resto, la scelta in alcuni contesti di seguire un approccio basato sul modello della *regulatory sandbox* va incontro a questa esigenza.

Pertanto, il rischio legislativo potrà assumere contorni diversi in considerazione sia dell'orizzonte temporale di riferimento sia dell'effettivo

---

[51] Si pensi alla diversità di approcci emersa sul tema delle cripto-attività, e che vede il confronto tra tre opzioni: 'isolare'; 'regolare', 'integrare'; cfr. A. Caponera e C. Gola, *Aspetti economici e regolamentari delle cripto-attività*, Banca d'Italia. Questioni di Economia e Finanza, n. 484, 2019.

processo evolutivo del fenomeno: in questa prospettiva, la manifestazione di rilevanti perdite collegate a fenomeni di *FinTech-failure* sarà probabilmente decisiva e potrebbe condurre ad una accelerazione dei processi di regolamentazione.

Il rischio di *compliance* subisce e subirà un impatto sempre più significativo dalla diffusione e dal successo delle nuove iniziative, prevalentemente a causa dell'esposizione ai rischi di mancato rispetto della normativa in tema di protezione dei dati e di antiriciclaggio.

La possibilità di personalizzare l'offerta di servizi di intermediazione attraverso tecniche di *Big Data Analysis* – producendo, ad esempio stime più precise del profilo rischio rendimento e/o dello schema di preferenze del consumatore – determina nuove responsabilità per l'intermediario in caso di alterazione e/o perdita di informazioni sensibili, nel corso della loro trasmissione a terze parti. Ciò rende necessario un più ampio sforzo nei presidi di controllo atti a garantire che le informazioni siano tutelate in termini di divulgazione a utenti non autorizzati (riservatezza dei dati), modifica impropria (integrità dei dati) e inaccessibilità ove necessario (disponibilità dei dati). Cresce, inoltre, il rischio di una diffusione indiscriminata e incontrollata di informazioni tra un numero sempre più ampio di istituzioni attraverso l'uso di *wallet* digitali e aggregatori.

Nella repressione delle attività di *money laundering*, lo sviluppo di criptoattività appare senza dubbio l'area più delicata di commistione in considerazione degli elementi di congenialità tra le infrastrutture sottostanti ai *cryptoasset* e le diverse forme di finanziamento del crimine[52]. Il fenomeno delle criptoattività che operano attraverso un protocollo elettronico gestito in modo decentrato tramite una *permissionless distributed ledger technology* (DLT) detta anche *blockchain*, ha suscitato particolare interesse per l'assenza di una regolamentazione degli aspetti relativi a titolarità, conservazione e circolazione della valuta virtuale, nonché alla tutela dei terzi nei confronti del titolare[53].

I numerosi profili di rischio derivanti dall'utilizzo o dalla detenzione di tali attività sono rilevanti per gli utilizzatori (consumatori[54], investitori e *merchant*), i partecipanti al mercato (piattaforme di scambio e depositari dei portafogli virtuali, i *wallet providers*), il sistema dei pagamenti, l'integrità finanziaria, i regolatori

---

[52] Si è stimato che circa il 46% delle transazioni in *BitCoin* sia finalizzata al finanziamento di attività illecite. Cfr. S. Foley, J. R. Karlsen e T.J. Putniņš, *Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies*, in *The Review of Financial Studies*, 2019, Vol. 32, n. 5, pp. 1798-1853.

[53] Cfr. in materia il contributo di E.M. Mastropaolo in questo *Quaderno*.

[54] Anche di recente, sia le autorità europee sia la Banca d'Italia, hanno messo in guardia i risparmiatori dall'investimento in tali attività sottolineando sia i rischi di perdite permanenti delle somme utilizzate per l'acquisto di valute virtuali a causa di malfunzionamenti, attacchi informatici, smarrimento della *password* del portafoglio elettronico, sia la mancanza di tutele legali e contrattuali, di obblighi informativi e di presidi di trasparenza, oltre che di forme di tutela o garanzia delle somme impiegate. Cfr. Esma, Eiopa, Eba, *Warning on virtual currencies*, 12 febbraio 2018 e Banca d'Italia, *Avvertenza per i consumatori sui rischi delle valute virtuali da parte delle Autorità europee*, 15 marzo 2018.

e, in prospettiva, anche le banche se continuerà la crescita delle piattaforme di *trading* e dei prodotti legati ai *cryptoasset*[55]. Alcuni di tali rischi si sono già concretizzati in gravi perdite o furti per la clientela nonché nel fallimento di piattaforme di scambio.

L'investimento in criptoattività e lo svolgimento dei servizi ad esse connessi, nelle giurisdizioni che lo consentono, espongono le banche a ognuna delle tipologie di rischio sopra definite[56] e si rende indispensabile prestare particolare attenzione: ai processi di *due diligence* del prodotto; al sistema di *risk management* in grado di integrare la valutazione dell'esposizione diretta e indiretta nei processi ICAAP e ILAAP; alla *disclosure* nei confronti del pubblico e all'informativa alle autorità[57].

Gli intermediari più esposti, sia pure indirettamente, a tali rischi sono i *provider* di servizi di pagamento, specie se enti creditizi, qualora operino, congiuntamente con quelle convenzionali, anche nelle valute virtuali, il cui malfunzionamento può determinare un incremento dei rischi di liquidità, di reputazione o addirittura di insolvenza.

Le autorità di vigilanza hanno esplicitamente 'scoraggiato' le banche e gli altri intermediari vigilati dall'acquistare, detenere o vendere valute virtuali e a mitigare i rischi derivanti dall'interazione tra gli schemi di valute virtuali e i servizi finanziari alla cui prestazione sono autorizzati: ciò considerando l'assenza di adeguati presidi e di un quadro legale certo circa la natura giuridica di tali attività (profilo associato all'ampia casistica di eventi illegali connessi al loro uso) e la circostanza che le modalità di funzionamento degli schemi potrebbero integrare la violazione delle disposizioni che riservano l'esercizio di alcune attività (raccolta del risparmio, prestazione di servizi di pagamento e di investimento)[58].

È l'intero fenomeno di *FinTech* a determinare un crescente rischio di *compliance* non solo per l'ampiezza degli adempimenti normativi ma, soprattutto, per la maggiore complessità delle procedure di *risk management* (*mapping*, misurazione, mitigazione) e del sistema dei controlli interni. Tali considerazioni rendono pertanto quanto mai utile la ricerca di soluzioni di digitalizzazione anche dell'attività di *compliance* normativa, attraverso il ricorso a *provider* specializzati nei servizi *RegTech*.

---

[55] Sulla base di questa tassonomia, sono stati individuati circa 70 rischi derivanti dalle valute virtuali, alcuni simili, se non identici, a quelli legati a servizi finanziari convenzionali, come servizi di pagamento o di investimento, altri specifici. Cfr. EUROPEAN BANKING AUTHORITY, *Opinion on 'virtual currencies'*, 4 July, 2014, p. 21.

[56] Il Comitato di Basilea, nel quadro del *Quantitative Impact Study*, ha incluso la raccolta di informazioni sulle cripto-attività che le banche dovranno monitorare e presidiare con riferimento ai rischi di mercato, di credito, di controparte, in caso di posizioni in derivati aventi come sottostante una o più criptoattività, e di liquidità. Cfr. BASEL COMMITTEE ON BANKING SUPERVISION, *Instruction for Basel III monitoring*, February 2019.

[57] Cfr. BASEL COMMITTEE ON BANKING SUPERVISION, *Cryptoassets: Public statement*, March 2019.

[58] BANCA D'ITALIA, *Valute virtuali, Comunicazione del 30 gennaio 2015*, in *Bollettino di Vigilanza*, n. 1, gennaio 2015.

Il rischio operativo

L'analisi svolta ha messo in luce come *FinTech* possa avere un impatto determinante soprattutto sul rischio operativo, contribuendo anche alla sua riduzione attraverso: la modernizzazione di sistemi informatici, applicazioni o componenti obsoleti e retrodatati (*legacy system*) ancora ampiamente utilizzati; la possibilità di automatizzare le procedure più standardizzate e routinarie necessarie allo svolgimento delle funzioni produttive, di *compliance* e *reporting*; l'utilizzo di intelligenza artificiale, *blockchain* e tecniche di analisi predittiva per rendere più sicuri i dati.

All'opposto, il rischio informatico, l'elevata dipendenza da soggetti terzi e le incertezze di tipo legale circa le responsabilità dei diversi soggetti coinvolti nella filiera, possono aumentare la vulnerabilità del sistema finanziario e la permeabilità dei canali di contagio in caso di crollo generalizzato della fiducia[59]. I recenti casi di attacchi cybernetici testimoniano la difficoltà di mitigare questi rischi e l'importanza di predisporre specifici *recovery plans*.

Nell'ambito del generico rischio operativo è possibile enucleare, per la loro criticità e crescente importanza relativa, il rischio informatico (o *cyber risk*)[60], il rischio di esternalizzazione e il rischio legale.

Il rischio informatico, o, per usare una terminologia oggi più diffusa, il rischio cybernetico[61], è connesso alle molteplici conseguenze negative del malfunzionamento dei sistemi di *Information and Communication Technology* (ICT)[62] e, in ottica di *Supervisory Review Evaluation Process* (SREP), deve essere ancora considerato parte indistinta del rischio operativo, salvo il caso in cui le autorità competenti non lo ritengano rilevante, e quindi meritevole di valutazione individuale, come potrebbe accadere per alcuni nuovi operatori *FinTech*. Tale rischio è influenzato dal grado di interconnessione tra gli

---

[59] «*More generally, operational risks associated with maintaining old legacy systems could become greater than the possible risks posed by new technologies*»: Financial Stability Board, *op. cit*., p. 22.

[60] Sui crescenti pericoli del *cyber risk* si rinvia a McAfee Labs, *2019 Threats Predictions Report*, November 2018 e, per l'Italia, a Associazione Italiana per la Sicurezza Informatica, *Rapporto Cusit 2019 sulla sicurezza ICT in Italia*.

[61] «*The term 'cyber risk' refers to a multitude of different sources of risk affecting the information and technology assets of a firm: it can be defined as 'operational risks to information and technology assets that have consequences affecting the confidentiality, availability or integrity of information or information systems'. Following the operational risk frameworks in Basel II and Solvency II, we categorise cyber risk into four classes: (1) actions of people (e.g. inadvertent loss of data by employee), (2) systems and technology failures (e.g. malfunction of hardware), (3) failed internal processes (e.g. insufficiently defined responsibilities), and (4) external events (e.g. fire)*». C. Biener et al., *Insurability of Cyber Risk*, in *The Geneva Association Newsletter*, n. 14, agosto 2014.

[62] Le autorità di vigilanza hanno individuato 5 categorie di rischi ICT – rischi di disponibilità e continuità, rischi di sicurezza, rischi relativi ai cambiamenti dei sistemi, rischi di integrità dei dati, rischi di esternalizzazione – corredate da un elenco non esaustivo di fattispecie di elevata gravità e/o impatto operativo, reputazionale o finanziario: European Banking Authority, *Orientamenti sulla valutazione dei rischi relativi alle tecnologie dell'informazione e della comunicazione (Information and Communication Technology – ICT) a norma del processo di revisione e valutazione prudenziale (Srep),* 11 settembre 2017, Allegato.

operatori basato su legami 'deboli': l'uso della tecnologia e la diffusione di soluzioni digitali accrescono numero e tipologia dei punti di accesso per i cyber *hackers* e quindi la vulnerabilità dei sistemi ad attacchi che possono causare compromissioni del servizio, perdite di dati dei clienti, operazioni finanziarie fraudolente e interruzioni nell'operatività dei sistemi. I fornitori di servizi possono infatti, essere oggetto di attacco informatico da parte di criminali o terroristi, come punto di accesso ai sistemi ICT degli intermediari o per accedere/distruggere i dati fondamentali o sensibili da questi ultimi archiviati presso il fornitore.

Con riguardo al cd. *outsourcing risk*, gli intermediari hanno, prima ancora di *FinTech*, proceduto ad esternalizzare alcune attività tipiche e tradizionali anche al fine di ridurre i costi e migliorare la loro flessibilità ed efficienza. Nel nuovo contesto finora delineato, tale processo rappresenta una scelta organizzativa, talvolta preferita, spesso necessaria se non indispensabile, per avere accesso alle nuove tecnologie, anche se le nuove forme di interconnessione tra soggetti diversi (intermediari finanziari, operatori non vigilati, fornitori di servizi tecnologici) potrebbero determinare una potenziale crescente dipendenza dei primi dai *third party service providers*[63].

Più nello specifico, i rischi di esternalizzazione, in particolare se attuata via *cloud*[64], derivano, oltre che da fattori prettamente di natura tecnologica, da tipologia, portata e complessità dell'accordo contrattuale tra intermediari e fornitori, il quale deve contenere una precisa indicazione dei ruoli e delle responsabilità del *provider*, frequentemente un operatore non finanziario non soggetto ad alcun controllo. L'intermediario, inoltre, deve essere in grado di ridurre al minimo la propria dipendenza da un singolo soggetto, e quindi la propria vulnerabilità connessa a vincoli contrattuali che potrebbero generare rischi per la sua continuità operativa. Si osservi che i servizi di *cloud computing* sono attualmente forniti da un numero limitato di soggetti che potrebbero incidere sulla prestazione di un ampio numero di servizi finanziari in caso di problemi operativi; la medesima concentrazione si riscontra per i fornitori terzi di dati nelle attività di *robo-advice* e di *lending*.

---

[63] «*The risks to be considered include those associated with the institution's or the payment institution's relationship with the service provider, the risk caused by allowing for sub outsourcing, the concentration risk posed by multiple outsourcings to the same service provider and/or the concentration risk posed by outsourcing critical or important functions to a limited number of service providers. The concentration of outsourcing at a limited number of service providers is particularly relevant*»: European Banking Authority, *Guidelines on outsourcing arrangements*, Final Report, 25 February 2019, p. 9.

[64] «*Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction*»: P. Mell e T. Grance, *The NIST Definition of Cloud Computing*, *National Institute of Standards and Technology, US Dept. Of Commerce*, 2011. Sugli aspetti giuridici si rinvia a A. Mantelero, *Il contratto per l'erogazione alle imprese di servizi di cloud computing*, in *Contratto e Impresa*, 2012, pp. 1216-1222.

Un esempio di dipendenza da terze parti è rappresentato dalle innovazioni introdotte dalla PSD2 nel sistema dei pagamenti il quale distingue tre funzioni e tre soggetti che possono anche coincidere: il prestatore di servizi dispositivi (*Payment Initiation Service Provider* – PISP); il prestatore di servizi informativi (*Account Information Service Provider* – AISP); il prestatore di servizi di pagamento di radicamento del conto (*Account Servicing Payment Service Provider* – ASPSP) il quale fornisce e amministra il conto di pagamento dell'utente[65]. In particolare, il 'servizio di disposizione di ordine di pagamento' è offerto «*nel settore del commercio elettronico mediante un software che fa da ponte tra il sito web del commerciante e la piattaforma di online banking della banca del pagatore per disporre pagamenti via Internet sulla base di bonifici*», mentre mediante il "servizio di informazione sui conti" si aggregano *on line* informazioni «*su uno o più conti di pagamento, detenuti presso un altro o altri prestatori di servizi di pagamento*»[66].

È proprio l'architettura complessiva della PSD2 che induce a ritenere sempre più alta l'intensità del legame di dipendenza delle istituzioni finanziarie dalle *third parthies*. Se ciò si rifletterà anche in una concentrazione verso pochi soggetti, appare allora ragionevole attendersi un ulteriore innalzamento del rischio operativo in considerazione della responsabilità sui servizi erogati che, in ogni caso, rimarrà in capo all'istituzione finanziaria.

La maggiore complessità e rischiosità operativa dell'*outsourcing* indotto da *FinTech* fanno prevalentemente riferimento alla necessità (probabile difficoltà) per l'intermediario di valutare l'efficacia delle funzioni di *risk management* approntate dal fornitore, verifica che può risultare problematica in considerazione dell'elevata complessità dei processi tecnologici offerti dalla *third party* e della conseguente barriera di comprensione da affrontare e superare. La *governance* dell'*outsourcing risk* appare ancora più complessa nei casi, non infrequenti, di scelta della stessa *third party* di delegare parte o tutto il servizio ad un ulteriore terzo fornitore, così da allungare ulteriormente la catena del valore ponendo ulteriori sfide alle autorità di vigilanza in tema di opportunità di regolamentazione e/o di definizione di principi guida a cui assoggettare le stesse *third parties*[67].

---

[65] Su questo tema cfr. il contributo di V. Profeta in questo *Quaderno*.

[66] Recentemente il Tribunale di Firenze (sentenza 21 gennaio 2019, n.18) ha dichiarato – a fronte di ammanchi dovuti a indebiti prelievi di fondi (c.d. doppi prelievi), per circa 17 milioni di criptovaluta da parte di utenti che avevano sfruttato la vulnerabilità del software – il fallimento, primo caso in Italia, del gestore di una piattaforma *online* di scambio e deposito di criptoattività, sancendo la sua responsabilità anche se alcuna facoltà di utilizzo delle somme depositate dagli utenti era riconosciuta al medesimo gestore e pur in presenza di accertate falle nel software ad esso non riconducibile perché sviluppato da terzi. Cfr. M. Krogh, *La responsabilità del gestore di piattaforme digitali per il deposito e lo scambio di criptoattività*, in *Diritto di internet*, n. 2, 2019.

[67] L'assoggettamento delle *third parties* alla supervisione di Autorità di Vigilanza è pratica già adottata in alcuni Paesi. Ad esempio, negli Usa possono procedere ad ispezioni presso le *third parties* sia la Federal Reverse System, che la Federal Deposit Insurance Corporation oltre all'*Office of the Comptroller of the Currency*. In Lussemburgo, le terze parti che intendono offrire specifici servizi agli intermediari sono sottoposti ad un particolare regime autorizzativo che li assoggetta alla supervisione *della Commission de Surveillance du Secteur Financier*.

In uno scenario di esternalizzazione spinta si assiste, pertanto, ad una trasformazione della stessa natura di rischio operativo, che da rischio tipicamente interno si evolve verso una forma ibrida in quanto sempre più influenzato da fonti esterne.

Il rischio reputazionale

Sebbene dotato di alcune caratteristiche – pervasività, intangibilità, interrelazione con altri rischi – che ne rendono difficile misurazione e gestione, il rischio reputazionale assume particolare rilievo in considerazione del ruolo che la fiducia dei risparmiatori riveste quale fattore di equilibrio del sistema finanziario.

L'accesso degli *incumbents* al mercato dei servizi *FinTech*, nella misura in cui le innovazioni sono vulnerabili a minacce tecnologiche (frodi, malfunzionamenti delle infrastrutture digitali, mancata protezione di dati sensibili) rappresenta un fattore di innalzamento del rischio operativo, a sua volta legato ad altre forme di rischio (in primo luogo quello di *compliance*). Poiché il rischio reputazionale dipende anche dalla condotta dei *third parties service provider,* il modello di *open banking* e le dinamiche determinate dalla PSD2 costituiscono certamente un elemento, non più trascurabile, anche a fini di misurazione dell'esposizione.

La stessa natura 'indiretta' del rischio reputazionale in quanto possibile forma consequenziale ad altri rischi di tipo diretto (operativo, di credito, di mercato, di *compliance*, ecc.) rende evidente come la sua gestione sia essenzialmente funzione del grado di efficacia dei presidi organizzativi posti in essere dagli intermediari per fronteggiare i rischi diretti.

Allo stesso tempo, le strategie di mitigazione devono necessariamente comprendere anche un sistema di comunicazione continua e trasparente con gli attori del mercato, inclusi i mezzi di comunicazione, tale da affrontare in modo efficace, completo e tempestivo episodi qualificabili come potenziali cause di danni reputazionali.

Il rischio strategico

Nell'ambito di FinTech, il rischio strategico si ricollega alla potenziale riduzione sia degli attivi intermediati sia degli utili in conseguenza delle politiche di innovazione adottate dai newcomers e della conseguente risposta degli incumbents. Il legame tra tale rischio e le opportunità offerte da FinTech può assumere una duplice valenza: da un lato l'esposizione al rischio strategico è tanto più alta quanto più alta è la riluttanza degli intermediari ad intraprendere un piano di investimenti di capitale (finanziario e sociale) in grado di renderli partecipi delle opportunità; dall'altro, non può non evidenziarsi che, a fronte degli elevati investimenti economici e tecnologici inizialmente richiesti, la clientela possa utilizzare solo marginalmente i nuovi servizi offerti.

Appare evidente che l'effettivo impatto sugli intermediari tradizionali dipenda da un'evoluzione ancora molto incerta, potendosi ipotizzare da un lato che i soggetti attualmente esterni al perimetro regolamentare concentrino la propria attività nell'offerta agli intermediari dei servizi tecnologici e/o finanziari propedeutici allo sviluppo di nuove modalità di intermediazione (che rimarrebbero in capo agli intermediari tradizionali), dall'altro che i *giant players* della tecnologia informatica e dei social media decidano di attuare modalità di ingresso diretto nel sistema finanziario[68].

In una più articolata prospettiva, sono stati individuati[69] cinque possibili scenari, né esaustivi né mutuamente esclusivi: (*i*) '*Better bank',* con l'adattamento degli *incumbents* alle sfide dell'innovazione ed una modifica dei loro modelli di business; (*ii*) '*Newbank',* qualora le banche esistenti non riescano ad adattarsi al nuovo modello di riferimento con il rischio di essere sostituite da nuovi *players* in grado di digitalizzare completamente la loro offerta di servizi; (*iii*) '*Distributed bank'*, nel quale le grandi banche riescono a sopravvivere all'innovazione digitale ma, allo stesso tempo, il mercato consente l'emersione di nuove realtà *Fintech* in grado di fornire servizi di nicchia ad elevata specializzazione senza necessariamente competere con gli *incumbents; (iv)* '*Relegated bank'*, nel quale banche tradizionali si limitano a fornire servizi alle realtà *Fintech* emergenti, cui cedono la relazione diretta con il cliente; (*v*) '*Disintermediated bank',* nel quale si assiste ad una completa sostituzione delle banche tradizionali con le nuove realtà *FinTech*.

5. Conclusioni

Il presente lavoro rappresenta un tentativo di descrizione degli scenari evolutivi delle attività di *risk management* delle banche in presenza di un fenomeno dirompente (potenzialmente o effettivamente? E in quanto tempo?) quale *FinTech*. Si tratta, è bene precisarlo, di un contributo parziale, considerando l'impossibilità sia di definire, nell'attuale momento storico, con precisione i contorni di un settore (un fenomeno) in continua evoluzione, sia di riportare in sintesi l'intera gamma delle aree di business emerse ed emergenti.

L'attuale innovazione finanziaria costituisce una sfida, dall'esito ancora incerto, per molteplici attori del mercato. Innanzitutto le banche, chiamate

---

[68] Cfr. Banca D'Italia, *FinTech in Italia*, *op. cit.*, p. 3. «*Nella percezione degli intermediari i potenziali impatti del Fintech riguardano principalmente i servizi di pagamento, i servizi bancari e di intermediazione con la clientela al dettaglio e la gestione patrimoniale, ambiti nei quali si potrebbe verificare un'erosione dei ricavi da commissioni a fronte di benefici relativamente limitati in termini di riduzione dei costi. Ciò è confermato dal fatto che le start-up Fintech attive sul mercato che potenzialmente comportano maggiori ripercussioni per la solidità del business bancario tradizionale riguardano principalmente i servizi di pagamento e l'erogazione di credito, nonché la gestione dei dati e delle informazioni che le banche hanno a disposizione sui propri clienti*»: N.I. Sibilio, M. Boero, L. Salerno, *Banche e Fintech: strategie e modelli di business* in *Bancaria*, n. 2, 2019.

[69] Cfr. Bank for International Settlements, *op. cit.*, pp. 26-27.

ad adeguare le proprie scelte strategiche all'evoluzione tecnologica ed alle conseguenti opportunità offerte dal mercato. I clienti degli intermediari, destinatari di nuovi servizi e nuove metodologie commerciali che, se da un lato, ci si augura, migliorino il grado di adeguatezza e coerenza con il profilo personale e/o offrano combinazioni costi/benefici più appropriate, dall'altro lato potrebbero essere oggetto di adesioni inconsapevoli specie nel caso di servizi caratterizzati da rapidità di esecuzione ed elevato contenuto tecnologico[70].

Inoltre, l'innovazione indotta da *FinTech* pone una sfida alle stesse Autorità di Vigilanza chiamate a trovare il giusto compromesso tra esigenza di regolamentazione e rischio di *discouragement* delle nuove iniziative. In questa prospettiva, la valutazione dei rischi cui si espongono gli intermediari assume un rilievo centrale nella misura in cui gli sforzi di supervisione sulla *capital adequacy* approntati nell'ultimo decennio possano essere, anche solo in minima parte, depotenziati in conseguenza dell'emersione di nuove ed ancora inesplorate componenti di rischio.

---

[70] Cfr. C. Barbagallo, *op. cit*., p. 19.

AUTORI

Michele Bellino è dottore in giurisprudenza ed esperto in valute virtuali.

Teresa Broggiato è avvocato e presta servizio presso l'Associazione Bancaria Italiana.

Daniela Conte è dottore commercialista, revisore dei conti, ricercatore confermato e docente in Diritto Tributario all'Università degli Studi di Napoli "Parthenope".

Nicola De Giorgi è avvocato e presta servizio nella Consulenza legale della Banca d'Italia.

Domenico Gammaldi è Capo del Servizio Supervisione Mercati e Sistema dei Pagamenti della Banca d'Italia.

Roberto Garavaglia è *Management Consultant & Innovative Payments Strategy Advisor* e consulente strategico nel settore dei sistemi di pagamento digitali.

Costanza Iacomini è dottore in giurisprudenza e presiede il settore Fintech nella Divisione Costituzioni del Servizio Rapporti Istituzionali di Vigilanza della Banca d'Italia.

Paola Lucantoni è professore associato di Diritto dei Mercati Finanziari all'Università degli Studi di Roma "Tor Vergata".

Fabrizio Maimeri è avvocato e professore ordinario di Diritto del Mercato Finanziario all'Università "Guglielmo Marconi" di Roma.

Marco Mancini è avvocato e presta servizio nella Consulenza legale della Banca d'Italia.

Eugenio Maria Mastropaolo è avvocato e docente di Diritto dell'Economia e di Diritto Bancario all'Università Telematica "Pegaso" di Napoli.

Raffaella Menzella è avvocato e presta servizio nella Consulenza legale della Banca d'Italia.

Francesco Moliterni è professore ordinario di Diritto delle Assicurazioni all'Università di Bari.

Fabio Porta è dottore commercialista, revisore legale e cultore di Diritto Bancario all'Università degli Studi di Napoli "Parthenope".

Claudio Porzio è professore ordinario di Economia degli Intermediari Finanziari all'Università degli Studi di Napoli "Parthenope" e componente del Collegio di Napoli dell'Arbitro Bancario e Finanziario.

Vincenza Profeta è avvocato e presta servizio nella Consulenza legale della Banca d'Italia.

Nicola Ruccia è dottore di ricerca in Diritto dell'Unione europea presso il Politecnico di Bari.

Gabriele Sampagnaro è professore ordinario di Economia degli Intermediari Finanziari all'Università degli Studi di Napoli "Parthenope".

QUADERNI PUBBLICATI

n. 1 – Francesco Capriglione, *Evoluzione tecnica e disciplina giuridica dell'intermediazione finanziaria,* ottobre 1985 (esaurito).

n. 2 – Francesco Carbonetti, *Moneta,* dicembre 1985.

n. 3 – Pietro De Vecchis, *L'istituto di emissione,* febbraio 1986 (esaurito).

n. 4 – Giuseppe Carriero, *Governo del credito e Regioni a statuto speciale: il quadro istituzionale,* aprile 1986.

n. 5 – Giorgio Oppo, *Una svolta dei titoli di massa (il progetto Monte Titoli),* aprile 1986.

n. 6 – Luigi Desiderio, *Le norme di recepimento della Direttiva comunitaria n. 780/77 in materia creditizia,* maggio 1986 (esaurito).

n. 7 – Giorgio Sangiorgio – Francesco Capriglione, *La legge bancaria: evoluzione normativa e orientamenti esegetici,* giugno 1986.

n. 8 – Vincenzo Mezzacapo, *L'attività bancaria nell'ambito dei movimenti di capitali nella CEE,* giugno 1986 (esaurito).

n. 9 – Francesco Capriglione, *Le gestioni bancarie di patrimoni mobiliari,* luglio 1986.

n. 10 – Francesco Carbonetti, *I cinquant'anni della legge bancaria,* settembre 1986.

n. 11 – *La legge bancaria,* ottobre 1986.

n. 12 – Carmine Lamanda, *L'evoluzione della disciplina del controllo sul sistema creditizio dalla legge bancaria ad oggi,* dicembre 1986 (esaurito).

n. 13 – Giovanni Imperatrice, *L'accertamento dell'illecito amministrativo nel diritto valutario e nel diritto tributario,* marzo 1987.

n. 14 – Giorgio Sangiorgio, *Profilo istituzionale della disciplina pubblicistica del credito,* maggio 1987.

n. 15 – Francesco Capriglione, (a cura di) *La disciplina comunitaria del credito al consumo,* luglio 1987.

n. 16 – Carlo Taglienti, *Il credito documentario: nozione, fondamento, problematica,* settembre 1987.

n. 17 – Pietro De Vecchis, *Aspetti legali delle crisi bancarie in Italia,* gennaio 1988.

n. 18 – Vincenzo Mezzacapo, *Il mercato secondario organizzato dei titoli emessi o garantiti dallo Stato,* agosto 1988.

n. 19 – Francesco Carbonetti, *Il controllo della Banca d'Italia sulle emissioni di titoli atipici,* ottobre 1988.

n. 20 – Francesco Capriglione, *Le polizze di credito commerciale,* dicembre 1988.

n. 21 – Francesco Capriglione, *La responsabilità penale del banchiere: evoluzione giurisprudenziale e prospettive di riforma,* dicembre 1989 (esaurito).

n. 22 – Marcello Condemi, *Le sanzioni amministrative bancarie e la giurisprudenza della Corte d'Appello di Roma,* aprile 1991.

n. 23 – Marco Mancini – Marino Perassi, *I trasferimenti elettronici di fondi,* maggio 1991.

n. 24 – Enrico Galanti, *La crisi degli enti creditizi nella giurisprudenza: la liquidazione coatta amministrativa*, giugno 1991.

n. 25 – Francesco Capriglione, *Note introduttive alla disciplina delle s.i.m. e dell'organizzazione dei mercati finanziari,* giugno 1991.

n. 26 – AA.VV., *La ristrutturazione della banca pubblica e la disciplina del gruppo creditizio,* gennaio 1992.

n. 27 – Giorgio Sangiorgio, *Le Autorità creditizie e i loro poteri,* marzo 1992.

n. 28 – Francesco Capriglione, *Il recepimento della seconda direttiva Cee in materia bancaria. Prime riflessioni,* febbraio 1993.

n. 29 – *Il Sistema dei pagamenti. Atti del Convegno giuridico* (Perugia S.A.Di.Ba., 23-24 ottobre 1992), settembre 1993.

n. 30 – Olina Capolino, *L'amministrazione straordinaria delle banche nella giurisprudenza,* ottobre 1993.

n. 31 – P. Ferro-Luzzi – P. G. Marchetti, *Riflessioni sul gruppo creditizio,* dicembre 1993 (esaurito).

n. 32 – *Testo Unico delle leggi in materia bancaria e creditizia,* marzo 1994.

n. 33 – *Testo Unico delle leggi in materia bancaria e creditizia. The 1993 Banking Law,* marzo 1994.

n. 34 – Giuseppe Carriero, *Struttura ed obiettivi della legge sui fondi immobiliari chiusi,* novembre 1994.

n. 35 – Lucio Cerenza, *Profilo giuridico del sistema dei pagamenti in Italia,* febbraio 1995.

n. 36 – Giovanni Castaldi, *Il riassetto della disciplina bancaria: principali aspetti innovativi,* marzo 1995.

n. 37 – Vincenzo Pontolillo, *L'evoluzione della disciplina dell'attività di emissione di valori mobiliari,* giugno 1995.

n. 38 – O. Capolino – G. Carriero – P. De Vecchis – M. Perassi, *Contributi allo studio del Testo Unico delle leggi in materia bancaria e creditizia,* dicembre 1995.

n. 39 – Francesco Capriglione, *Cooperazione di credito e Testo Unico bancario,* dicembre 1995 (esaurito).

n. 40 – Marino Perassi, *L'attività delle banche in "securities" e la disciplina dei contratti-derivati in Giappone,* aprile 1996.

n. 41 – Enrico Galanti, *Norme delle autorità indipendenti e regolamento del mercato: alcune riflessioni,* novembre 1996.

n. 42 – M. Perassi – R. D'Ambrosio – G. Carriero – O. Capolino – M. Condemi, *Studi in materia bancaria e finanziaria,* novembre 1996.

n. 43 – Convegno *Per un diritto della concorrenza* (Perugia, giugno 1996), dicembre 1996.

n. 44 – *Crisi d'impresa, procedure concorsuali e ruolo delle banche,* marzo 1997.

n. 45 – Donatella La Licata, *La cessione di rapporti giuridici "individuabili in blocco" nell'art. 58 del T.U. bancario,* aprile 1997.

n. 46 – Paolo Ciocca – Antonella Magliocco – Matilde Carla Panzeri, *Il trattamento fiscale dei rischi sui crediti,* aprile 1997.

n. 47 – P. De Vecchis – G.L. Carriero – O. Capolino, M. Mancini, R. D'Ambrosio, *Studi in materia bancaria e finanziaria 1996,* settembre 1997.

n. 48 – Giuseppe Carriero, *Il credito al consumo,* ottobre 1998 (esaurito).

n. 49 – *Fondamento, implicazioni e limiti dell'intervento regolamentare nei rapporti tra intermediari finanziari e clientela*, marzo 1999.

n. 50 – A. Magliocco – D. Pitaro – G. Ricotti – A. Sanelli, *Tassazione del risparmio gestito e integrazione finanziaria europea*, settembre 1999.

n. 51 – Enrico Galanti, *Garanzia non possessoria e controllo della crisi di impresa: la* floating charge *e l'*administrative receivership*,* gennaio 2000.

n. 52 – *Bankruptcy Legislation in Belgium, Italy and the Netherlands* (Brussels, 7 July 2000), giugno 2001.

n. 53 – Vincenzo Troiano, *Gli Istituti di moneta elettronica,* luglio 2001.

n. 54 – Stefano Cappiello, *Prospettive di riforma del diritto di recesso dalle società di capitali: fondamento e limiti dell'autonomia statutaria,* luglio 2001.

n. 55 – Bruna Szego, *Il* venture capital *come strumento per lo sviluppo delle piccole e medie imprese: un'analisi di adeguatezza dell'ordinamento italiano,* giugno 2002.

n. 56 – AA.VV., *Diritto Societario e Competitività in Italia e in Germania*, luglio 2003.

n. 57 – Gianmaria Marano, *I patrimoni destinati in una prospettiva di analisi giuseconomica*, giugno 2004.

n. 58 – Enrico Galanti e Mario Marangoni, *La disciplina italiana dei* Covered Bond, giugno 2007.

n. 59 – Marco Mancini, Vincenza Profeta e Nicola De Giorgi, *La Centrale d'Allarme Interbancaria nella disciplina sanzionatoria dell'assegno*, settembre 2007 (esaurito).

n. 60 – Marcello Condemi e Francesco De Pasquale, *Lineamenti della disciplina internazionale di prevenzione e contrasto del riciclaggio e del finanziamento del terrorismo*, febbraio 2008.

n. 61 – Bruna Szego, *Le impugnazioni in Italia: perché le riforme non hanno funzionato?*, luglio 2008.

n. 62 – Renzo Costi e Francesco Vella, *Banche, governo societario e funzione di vigilanza*, settembre 2008.

n. 63 – Marco Mancini e Marino Perassi, *Il nuovo quadro normativo comunitario dei servizi di pagamento. Prime riflessioni*, dicembre 2008.

n. 64 – Enrico Galanti, *Discrezionalità delle autorità indipendenti e controllo giudiziale*, giugno 2009.

n. 65 – David Pitaro, *Le disposizioni italiane di contrasto all'elusione fiscale internazionale*, luglio 2009.

n. 66 – Cristina Giorgiantonio, *Le riforme del processo civile italiano tra* adversarial system *e* case management, settembre 2009.

n.66en – Cristina Giorgiantonio, *Civil procedure reforms in Italy: concentration principle, adversarial system or case management?*, September 2009.

n. 67 – Olina Capolino e Raffaele D'Ambrosio, *La tutela penale dell'attività di Vigilanza*, ottobre 2009.

n. 68 – Giuseppe Boccuzzi, *I sistemi alternativi di risoluzione delle controversie nel settore bancario e finanziario: un'analisi comparata*, settembre 2010.

n. 69 – AA.VV., *Insolvency and Cross-border Groups. UNCITRAL Recommendations for a European Perspective?*, febbraio 2011.

n. 70 – Bruno De Carolis, *L'Arbitro bancario finanziario come strumento di tutela della trasparenza*, giugno 2011.

n. 71 – Giuseppe Boccuzzi, *Towards a new framework for banking crisis management. The international debate and the italian model*, ottobre 2011 (esaurito).

n. 72 – *Legislazione bancaria, finanziaria e assicurativa: la storia, il presente, il futuro*. Atti della conferenza tenutasi a Roma il 14 ottobre 2011, ottobre 2012.

n.72app – Enrico Galanti, *Cronologia della crisi 2007-2012,* maggio 2013.

n. 73 – Marco Mancini, *Dalla vigilanza nazionale armonizzata alla* Banking Union*,* settembre 2013.

n. 74 – Raffaele D'Ambrosio, *Due process and safeguards of the persons subject to SSM supervisory and sanctioning proceedings*, dicembre 2013.

n. 75 – *Dal Testo unico bancario all'Unione bancaria: tecniche normative e allocazione di poteri.* Atti del convegno tenutosi a Roma il 16 settembre 2013, marzo 2014.

n. 76 – Giuseppe Napoletano, *Legal aspects of macroprudential policy in the United States and in the European Union,* giugno 2014.

n. 77 – Nicola De Giorgi e Maria Iride Vangelisti, *La funzione di sorveglianza sul sistema dei pagamenti in Italia – Il provvedimento della Banca d'Italia del 18.9.2012 sui sistemi di pagamento al dettaglio,* settembre 2014.

n. 78 – Raffaele D'Ambrosio, *The ECB and NCA liability within the Single Supervisory Mechanism,* gennaio 2015.

n. 79 – Marco Lamandini – David Ramos Muñoz – Javier Solana Álvarez, *Depicting the limits to the SSM's supervisory powers: The Role of Constitutional Mandates and of Fundamental Rights' Protection,* novembre 2015.

n. 80 – Luigi Donato, *La riforma delle stazioni appaltanti. Ricerca della qualità e disciplina europea,* febbraio 2016.

n. 81 – Raffaele D'Ambrosio, *Scritti sull'Unione Bancaria,* luglio 2016.

n. 82 – *Gustavo Bonelli, Un giurista in Banca d'Italia,* dicembre 2017.

n. 83 – *Qualità ed efficienza nel nuovo codice dei contratti pubblici. Prospettive e questioni aperte,* aprile 2018.

n. 84 – *Judicial review in the Banking Union and in the EU financial architecture. Conference jointly organized by Banca d'Italia and the European Banking Institute,* giugno 2018.

n. 85 – *The role of the CJEU in shaping the Banking Union: notes on Tercas (T-98/16) and Fininvest (C-219/17),* maggio 2019.

n. 86 – *A 20 anni dal TUF (1998-2018): verso la disciplina della Capital Market Union?,* agosto 2019.