LUISS Guido Carli
LIBERA UNIVERSITÀ INTERNAZIONALE DEGLI STUDI SOCIALI

Dipartimento di Economia e Finanza

Cattedra di Diritto dei mercati e degli intermediari finanziari (corso progredito)

# *FINTECH*: principali innovazioni, sfide regolamentari, *start-up* innovative di successo in Italia

RELATORE

Prof.ssa Mirella Pellegrini

CANDIDATO

Noemi Lombardi

Matricola 680551

CORRELATORE

Prof.ssa Paola Lucantoni

ANNO ACCADEMICO 2017/18

# Indice

# INTRODUZIONE

In poco meno di trent'anni, la digitalizzazione ha pervaso il mondo che ci circonda, dalla rapida diffusione della telefonia mobile alla nascita di internet e, più recentemente, dei social media e dei *Big data*. La "rivoluzione digitale", intesa come la diffusione su ampia scala delle tecnologie digitali, ha modificato radicalmente lo stile di vita e il modo di comunicare e di agire delle persone, con impatti significativi su tutti i comparti produttivi. Tra questi anche il settore dei servizi finanziari si trova attualmente al centro di una rivoluzione di vasta portata e senza precedenti, nota come *FinTech*, derivante appunto dall'applicazione della tecnologia alla finanza. Dall'intelligenza artificiale, agli algoritmi, dal *crowdfunding* alle criptovalute e tutte le nuove tecnologie emergenti applicate alla finanza hanno fatto emergere nuove dinamiche d'innovazione, mettendo in discussione le logiche e i baluardi stessi del mercato finanziario e aprendo scenari inediti e applicazioni illimitate. *FinTech* si mostra in grado di apportare diversi benefici sia ai consumatori che alle imprese, ma parallelamente si paventano rischi che nella maggior parte dei casi non sono stati ancora completamente identificati. In uno scenario in continua evoluzione, nel quale si alternano luci ed ombre sulle potenzialità e sugli eventuali rischi connessi allo sviluppo di *FinTech*, sono scese in campo tutte le Autorità e le Istituzioni a livello internazionale, europeo e nazionale, che si sono impegnate a studiare ed analizzare, in diversa misura il fenomeno che interessa una sempre più ampia gamma di servizi finanziari. Nella consapevolezza che ogni innovazione tecnologica reca con sé una sfida regolamentare, le Autorità si stanno interrogando sul tipo di azione e di intervento da intraprendere per una regolamentazione del fenomeno *FinTech* al fine di gestire eventuali rischi e tutelare i diritti dei consumatori e la stabilità del sistema finanziario. Tale intervento regolatorio non deve tuttavia ostacolare il naturale sviluppo dell'innovazione tecnologico-finanziaria ma anzi supportarlo con l'obbiettivo di dare forma al Mercato unico tecnologico dei servizi finanziari a livello europeo. Il cammino potrà essere agevolato dalla conoscenza e dalla fiducia nelle nuove tecnologie, nonché da processi di educazione finanziaria e soprattutto digitale.

Le innovazioni *FinTech* hanno aperto nuove opportunità di business e ridotto significativamente il costo di nuove iniziative, motivo che ha determinato la nascita di nuove *start-up* innovative che, per loro natura, fanno convergere competenze finanziarie e competenze tecnologiche e che, superata la fase iniziale di sperimentazione, stanno muovendosi sempre più verso obiettivi di business tangibili. Tali *start-up* innovative, attraverso l'uso di nuove tecnologie, propongono un ripensamento dell'esperienza del cliente nella fruizione dei prodotti e servizi finanziari, soddisfacendo le esigenze proprie delle nuove generazioni (in un mercato dalle fattezze sempre più digitali) e favorendo l'inclusione finanziaria. La diffusione delle *start-up FinTech* è stata favorita anche dal progressivo deteriorarsi del rapporto tra banca e cliente, dal venire meno della fiducia nel sistema finanziario tradizionale (soprattutto dopo la recente crisi economica) e dalla stretta creditizia messa in atto dalle banche per fronteggiare tale crisi.

In questo contesto il sistema bancario tradizionale rischia di essere sorpassato dai nuovi operatori *FinTech* e dalle *start-up* innovative, che fruttando le nuove tecnologie, da un lato e, le maglie aperte della regolamentazione dall'altro, stanno erodendo progressivamente la posizione di dominio degli *incumbents* del settore finanziario. Le banche tradizionali hanno quindi risposto alla sfida digitale

ripensando il proprio modello di business e intraprendendo un percorso di *restyling* tecnologico con l'introduzione di nuovi canali digitali.

La soluzione ottimale sarebbe quella di superare la presente contrapposizione tra operatori tradizionali e *start-up FinTech* favorendo al contrario una simbiosi, o "*fintegration*", in modo tale che le banche possano innovarsi e diventare più digitali tramite l'integrazione con le *FinTech companies*, mentre queste ultime potranno accedere alle enormi *customer base* delle banche riuscendo ad accelerare il proprio business e abbattendo i costi di marketing.

Anche l'Italia, come gran parte dei Paesi nel mondo, sta attraversando un periodo di fermento legato alla diffusione del *FinTech* anche se rimane relativamente indietro rispetto ad altre realtà; si posiziona difatti al 12° posto in Europa per investimenti complessivi in *FinTech*, alle spalle di paesi come Belgio, Finlandia e Spagna. L'Italia però, negli ultimi mesi in particolare, secondo una ricerca di Accenture, sta cercando di colmare il *gap* accumulato con il resto d'Europa e registra una tendenza molto positiva: gli investimenti in *FinTech* stanno accelerando e si stima che potrebbero portare ad un aumento di valore fino al 30% nei prossimi cinque anni. In più si registra un aumento delle *start-up* innovative italiane che si stanno affermando all'interno del territorio nazionale e non solo.

Il presente lavoro di tesi, inizia con un focus iniziale sul fenomeno *FinTech* in generale, sulle sfide regolamentari e sugli sviluppi prima a livello internazionale e poi italiano. Passerò poi ad analizzare singolarmente le seguenti principali innovazioni rientranti nel campo *FinTech*: *big data*, *robo advice*, *crowdfunding*, P2P *lending*, servizi di pagamento digitali, valute virtuali e monete complementari, *blockchain*. Per ognuna di esse porrò l'attenzione sul funzionamento, gli sviluppi, i benefici e gli eventuali rischi per i consumatori, gli approcci regolamentari e presenterò le principali *start-up* di successo in Italia per ogni specifico settore. Successivamente esporrò in breve le caratteristiche base di settori paralleli e complementari a quelli del *FinTech* ossia *RegTech* e *InsurTech* (innovazione tecnologica applicata rispettivamente alla regolamentazione e al settore assicurativo). Per ultimo mi concentrerò sul tema della *cybersecurity* e del legame tra il mondo *FinTech* e quello della lotta al riciclaggio e al finanziamento del terrorismo.

# 1. *FINTECH*

## 1.1 Definizione, sviluppi e impatti sul settore finanziario

Con il termine *FinTech*, abbreviazione di tecnologia finanziaria, si indentifica un ecosistema, in continua evoluzione, di innovazioni tecnologiche applicate al settore finanziario, che si concretizzano in nuovi modelli di business, processi e prodotti e i cui effetti sono dirompenti e di carattere rivoluzionario sia per i mercati finanziari che per le istituzioni. *FinTech* comprende alcune tra le principali innovazioni degli ultimi anni che investono tutti i settori dell'intermediazione bancaria e finanziaria: il *crowdfunding*, la *robo advice*, il P2P, le valute virtuali, *lending platforms*, la *blockchain* ecc.

*FinTech* ha segnato l'accesso nel mercato dei servizi finanziari di *start-up* tecnologiche e dei colossi della tecnologia informatica la cui affermazione in questo settore scaturisce dalla loro connaturata capacità di creare innovazione tecnologica e utilizzarla per l'offerta di servizi finanziari ad alto contenuto tecnologico e a prezzi contenuti. Altrettanto importanti per lo sviluppo delle imprese *FinTech* sono i fattori legati alla crescita della domanda di servizi finanziari digitalizzati, contestuale all'aumento della porzione di popolazione familiare con i servizi digitali, in particolare i più giovani. Le innovazioni *FinTech* in più consentono di semplificare il più possibile la fruizione dei servizi finanziari, permettendo di compiere operazioni in qualunque momento e ovunque ci sia connessione, tramite i propri dispositivi mobili; in questo modo esse favoriscono l'avvicinamento ai servizi finanziari digitali anche alle quote di popolazione più anziana e con minori conoscenze informatiche.

L'ingresso di nuovi operatori stimola enormemente la competitività nel settore finanziario obbligando gli intermediari già esistenti a investire nell'innovazione tecnologica, ad automatizzare i processi e rivedere i propri modelli di business per adeguarsi al nuovo fenomeno *FinTech*. Esso quindi può rappresentare un forte stimolo all'innovazione del settore finanziario ma al tempo stesso può delinearsi come un fattore disruptive per l'industria finanziaria tradizionale se questa non si dimostri in grado di adattare la propria attività di intermediazione alle nuove tecnologie.

Le istituzioni europee hanno mostrato in questi anni il loro sostegno nei confronti del fenomeno *FinTech* che potrebbe dare un impulso decisivo alla formazione di un mercato unico tecnologico dei servizi finanziari, superando le barriere esistenti all'operatività *cross-border*. Il Parlamento europeo nella risoluzione del gennaio 2017 su "*Tecnologia finanziaria: l'influenza della tecnologia sul futuro del settore finanziario*" afferma «Gli sviluppi in materia *FinTech* dovrebbero contribuire allo sviluppo e alla competitività del sistema finanziario e dell'economia europei, compreso il benessere dei cittadini europei, migliorando al contempo la stabilità finanziaria e garantendo il massimo livello possibile di protezione dei consumatori», evidenzia poi i principali benefici sia per i consumatori che per le imprese come «servizi finanziari migliori, più rapidi, meno costosi, più personalizzati, inclusivi, resilienti e trasparenti» permettendo così a tutti i cittadini condizioni di accesso al mercato più ottimali e favorendo l'inclusione finanziaria. Oltre ai numerosi benefici *FinTech* ingloba in sé anche rilevanti rischi che possono mettere a repentaglio la stabilità finanziaria tra cui: assetti di *governance* e di sistemi di controllo inadeguati dei nuovi operatori *FinTech* , spesso non soggetti ad alcuna regolamentazione o comunque assoggettati a controlli meno stringenti rispetto agli *incumbents*; rischio di sicurezza informatica legato al furto di informazioni personali, identità digitale o risorse economiche; l'accresciuta interconnessione tra i mercati che incrementa le esposizione a fenomeni di contagio e la portata sistemica di attacchi informatici.

## 1.2 Approcci regolamentari

Al fine di sostenere l'innovazione apportata dalle nuove frontiere del *FinTech* ma nello stesso tempo proteggere i consumatori e la stabilità del sistema finanziario dai rischi ad essa legati è indispensabile innovare il sistema normativo adeguandolo all'evoluzione in atto.

Il Parlamento europeo, nella sopra citata Risoluzione su "*Tecnologia finanziaria: l'influenza della tecnologia sul futuro del settore finanziario*", ha individuato le principali aree di intervento che risultano prioritarie:

- *Cybersecurity* e protezione dei dati con particolare attenzione alla creazione di maggiore consapevolezza tra i consumatori riguardo il valore dei propri dati personali
- Interoperabilità dei servizi *FinTech* all'interno dell'Unione europea
- *Level playing field* e tutela della concorrenza ottenibile facilitando l'ingresso nel mercato alle nuove *start-up* innovative e prevenendo arbitraggi regolamentari tra gli Stati membri.
- Sperimentazione controllata delle nuove tecnologie e strumenti di *stress-testing*
- Promozione dell'educazione finanziaria e digitale e della fiducia digitale. L'obbiettivo di una maggiore inclusione finanziaria dei consumatori considerati *unbanked* infatti, presuppone l'abbattimento di barriere legate alla mancanza di fiducia nei digital tools e a bassi livelli di educazione finanziaria e digitale. Il fine è quello di porre i consumatori nelle condizioni di utilizzare i servizi offerti dai canali digitali, facendone però un uso responsabile in modo da cogliere appieno i benefici dell'applicazione della tecnologica al settore dei servizi finanziari e del mercato unico digitale.

Riguardo al terzo aspetto, quello della concorrenza, il Parlamento europeo ha indicato i principi ai quali dovrebbe attenersi la regolamentazione del *FinTech*: approccio per attività, neutralità tecnologica e proporzionalità ai rischi.

L'approccio per attività prevede l'applicazione delle stesse regole indipendentemente dall'entità giuridica che svolge l'attività e dal grado di automatizzazione della stessa. Tale approccio garantisce il *level playing field* tra *new comers* e *incumbents*, che offrono lo stesso servizio, ma nello stesso tempo può penalizzare le *start-up* innovative che dovrebbero beneficiare di oneri di *compliance* meno stringenti. Per superare il *trade-off* tra la tutela della naturale concorrenza e la necessità di non ostacolare l'innovazione si può optare per un approccio ibrido *princile-based* e *rule-based*[1]; il primo applicato alle *new comers* di piccole dimensioni per garantire ad esse maggior flessibilità, il secondo applicato alle *incumbents*.

La neutralità tecnologica si manifesta nell'astensione dal bloccare o favorire lo sviluppo di una certa tecnologia solo sulla base dei primi effetti e nell'adozione invece di atteggiamento *wait-and-see* basato sul monitoraggio iniziale del fenomeno e sul successivo intervento una volta ottenuti elementi di valutazione sufficienti per orientare l'azione normativa.

Il principio di proporzionalità riguarda l'incidenza della regolamentazione e dei controlli che devono essere commisurati alle dimensioni, alla complessità e alla rilevanza sistemica dei soggetti vigilati e dei rischi ad essi legati.

Con riferimento alla sperimentazione delle innovazioni *FinTech*, essa usualmente avviene tramite le cosiddette *regulatory sandboxes*, ossia ambienti virtuali nei quali operatori e supervisori possono testare e sperimentare nuove tecnologie innovative nel settore dei servizi finanziari in un contesto controllato caratterizzato da requisiti normativi meno stringenti. Tra i vantaggi che la sandbox offre alle società che ne fanno parte c'è la possibilità di ridurre i costi di *compliance* connessi all'avvio dell'attività, l'opportunità di godere di deroghe normative e la possibilità di ottenere consigli e

[1] D.W. Arner, J.N. Barberis, R.P. Buckley, "*The Evolution of FinTech: A New Post-Crisis Paradigm?",* 2016

orientamenti dalle autorità di vigilanza in merito alle modalità di applicazione della normativa attuale. Per i regolatori e le autorità di vigilanza le *sandboxes* permettono di analizzare più da vicino il fenomeno innovativo e raccogliere informazioni utili per un successivo intervento in campo regolamentare nel caso si verificassero le condizioni necessarie. Per tutelare i consumatori e la stabilità del mercato, le *sandboxes* sono soggette a restrizioni sia sul numero e tipo di clienti da coinvolgere nel lancio di un nuovo sevizio o prodotto, sia sulla durata della fase di sperimentazione.

Esistono anche approcci alternativi alle *sandboxes* che prevedono un livello di coinvolgimento delle autorità di vigilanza diverso: le *innovation hub* e gli *incubators*[2].

Le prime rappresentano un luogo di incontro istituzionale degli operatori con le autorità che offrono chiarimenti o indirizzi senza però un coinvolgimento diretto nello sviluppo della tecnologia. Negli *incubators* invece le autorità di vigilanza svolgono un ruolo più attivo, essendo direttamente coinvolte nello sviluppo e nella sperimentazione del progetto, anche tramite forme di partnership e cofinanziamenti.

In seguito alla pubblicazione della Risoluzione su *FinTech*, la Commissione europea ha stilato il "*Piano d'azione riguardante i servizi finanziari destinati ai consumatori: prodotti migliori, maggiore scelta*" pubblicato il 23 marzo 2017 e che preannuncia un successivo intervento della Commissione stessa per l'armonizzazione del quadro normativo europeo e l'adozione di una strategia per il mercato unico tecnologico dei servizi finanziari. Il testo si articola in quattro direttrici generali che rappresentano le quattro macro aree d'azione, individuate in:

- Riduzione dei costi operativi e aumento dell'efficienza
- Maggiore trasparenza in materia di dati personali e di tutela della vita privata
- Maggiore competitività con minori ostacoli nell'accesso al mercato unico
- Promozione dell'accesso ai servizi finanziari per consumatori e imprese

Importante sul piano della regolamentazione del fenomeno *FinTech* è stato anche il contributo del Comitato di Basilea per la vigilanza bancaria *(Basel Committeeon Banking Supervision* - BCBS) che ha istituito una *task force* impegnata nella valutazione dei rischi e delle opportunità che l'innovazione e la trasformazione digitale pongono al sistema bancario. Nell'agosto del 2017, il Comitato di Basilea ha avviato una consultazione pubblica dedicata alle migliori prassi da adottare per contrastare i rischi connessi con *FinTech*. Il documento di consultazione, che fonde ricerche storiche, analisi dei media, indagini sulle attività dei paesi membri del BCBS e analisi dei prodotti *FinTech*, offre una prospettiva sulle probabili traiettorie evolutive di *FinTech* e sul potenziale impatto sull'industria bancaria. Nell'agosto 2017, invece, l'EBA ha pubblicato un "*Discussion paper on the EBA's approach to financial technology (FinTech)*", che illustra differenti modelli di business legati a *FinTech*, mettendo in evidenza rischi e benefici connessi e delineando le attività future dell'autorità. Nel settembre dello stesso anno, la Banca Centrale Europea ha posto in consultazione pubblica le linee guida per la valutazione delle domande di autorizzazione all'esercizio dell'attività bancaria da parte dei soggetti con modelli imprenditoriali *FinTech*. La pubblicazione illustra il processo per la presentazione dell'istanza, i requisiti di autorizzazione per gli enti creditizi e le considerazioni specifiche per i soggetti con modelli imprenditoriali *FinTech*.

[2] Pwc, "*Le aziende del FinTech in Italia 2017*", 2017

## 1.3 *FinTech* nel mondo

La composizione geografica dei capitali raccolti nel settore *FinTech*, mostra come in America e in Asia si siano concentrati i maggiori investimenti. A trainare gli investimenti in America sono state le operazioni concluse negli USA (circa 13 miliardi di dollari per 500 operazioni), dove si è rilevato un interesse crescente verso le *start-up InsurTech* e quelle *blockchain* (con applicazioni in ambito *smart contract* e *cripto currency exchange* in particolare).

In Asia l'ammontare complessivo di capitali raccolti dalle *FinTech* è stato di circa 8,6 miliardi di dollari per oltre 180 deal conclusi, quindi con un valore medio di 47 milioni di dollari, di gran lunga superiore ai 24 milioni di dollari rilevati in Nord America, dove il mercato mostra già segni di maturità.

L'Europa si colloca su valori molto più modesti, sebbene in crescita rispetto allo scorso anno: le *start-up FinTech* hanno raccolto oltre 2 miliardi di dollari per un totale di 318 operazioni prevalentemente su *social lending* e un valore medio di circa 6 milioni di dollari per operazione, sensibilmente inferiore ad America e Asia. Tuttavia, si è rilevato un interesse crescente degli istituti finanziari, banche e assicurazioni, che hanno incrementato i propri investimenti. I *player* tradizionali stanno optando per un percorso di collaborazione con i nuovi entranti per superare e affrontare al meglio le sfide che l'innovazione digitale impone. Da qui il proliferare di *hub* a supporto dell'ecosistema *FinTech*, localizzati principalmente in UK, Germania, Israele e Paesi Scandinavi.

Sebbene Londra continui ad essere la capitale europea del *FinTech*, in UK gli investimenti nel 2016 si sono ridotti del 34% (per un valore di 783 milioni di dollari), principalmente a causa dell'incertezza legata alla Brexit. Il Regno Unito è comunque riuscito a mantenere il terzo posto dopo Cina e US grazie all'operazione relativa a *Starling Bank*, la nuova banca completamente digitale, che ha concluso il deal più rilevante in Europa per un valore di 101 milioni di dollari.

Al rallentamento degli investimenti *FinTech* nella City si contrappone la nascita di nuovi ecosistemi che si stanno sviluppando in Germania, nei Paesi Scandinavi e in Israele. Tra le prime 50 *FinTech* al mondo rientrano la tedesca *Kreditech*, con focus di offerta in servizi di personal financial management.

Anche in Israele, pur crescendo a ritmi meno sostenuti, il *FinTech* si sta affermando, con una forte caratterizzazione tecnologica dell'offerta e soluzioni basate su tecnologie di *advanced analytics* e *cybersecurity* a supporto dei processi antifrode.

In generale, pur essendo diminuiti i capitali investiti, il settore continua ad essere in fase di crescita a livello globale: l'*InsurTech* ha raddoppiato la sua presenza, crescono in numero anche le *start-up* della *blockchain* e si rafforza l'ambito *RegTech*, ovvero *start-up* che ottimizzano gli aspetti legati alla *compliance* mediante le nuove tecnologie digitali.

In sintesi, dall'analisi per geografia emerge che in America gli ambiti su cui si concentrano maggiormente gli investimenti sono l'*InsurTech* e *Blockchain*; in Asia le *FinTech* di maggior successo operano in ambito *payment* (*real time payment nello* specifico), mentre in Europa è il *social lending* l'area che vede il maggior numero di realtà operative e promettenti.

## 1.4 *FinTech* in Italia

In linea con quanto registrato a livello globale, anche in Italia *FinTech* sta attraversando un periodo di fermento, pur caratterizzandosi per numero di realtà costituite e quantità degli investimenti ricevuti più contenuti rispetto a molte realtà internazionali. Il comparto continua a crescere pur rimanendo ancora lontano dalle cifre e dai ritmi raggiunti in USA e Gran Bretagna, dove nel 2016 si sono registrate importanti operazioni di investimento in nuove e promettenti *start-up*.

Nel 2015 le *FinTech* italiane hanno raccolto 19 milioni di euro. Nel corso del 2016 si sono registrate significative operazioni di investimento verso le realtà più promettenti del mercato e si stimano investimenti per 33,6 milioni di €. Secondo i dati del Registro delle Imprese, in Italia sono presenti oltre 7.200 *start-up* innovative (maggio 2017) di cui più di 200 categorizzabili come realtà operanti nel comparto *FinTech*.

Tra le imprese *FinTech* italiane di maggior successo ricordiamo *MoneyFarm*, investimento di maggiore intensità in Italia, *Prestiamoci*, *Borsa del Credito* e *Sardex*, oltre alle *FinTech* italiane che hanno raccolto capitali sia in Italia che all'estero ossia *Satispay*, su cui ha puntato *Banca Iccrea* e ancora *Smartika* che ha raccolto 4,5 milioni di Euro dal fondo *Hamilton Venture Capital*.

Nel contesto italiano è Milano la città che meglio si presta a consentire la nascita e lo sviluppo di *start-up FinTech*, data la presenza di numerosi *hub* a sostegno delle *start-up* innovative, nonché per la presenza di molti investitori e di *big tech companies* come *Google*, *Cisco*, *Microsoft* o *Facebook*.

Ad oggi non si ravvisano sul mercato italiano incubatori o acceleratori che indirizzano i propri servizi a realtà *FinTech* in maniera esclusiva; piuttosto si sta assistendo alla nascita di programmi o sezioni apposite all'interno di hub generici di *start-up* e aziende innovative, volti a supportare anche le realtà *FinTech*.

Analizzando i principali *hub* e incubatori di *start-up* in Italia, tra i più attivi in ambito *FinTech* emerge *Sellalab*: incubatore di realtà digitali di *Banca Sella* indicato anche da *Deloitte* come principale *hub FinTech* italiano. La Banca ha strutturato di recente un processo ben definito al proprio interno per favorire lo sviluppo delle realtà *FinTech* attraverso un percorso di incubazione all'interno di *Sellalab* e di accelerazione (eventuale) in *Sella Ventures*.

*Sellalab* è anche tra i soggetti promotori del recente polo *FinTech* italiano – *FinTech* District, con sede a Milano. Il *FinTech* District nasce con l'obiettivo di permettere alle aziende aderenti, fra *start-up* e imprese in fase più avanzata, di trovare in Italia le condizioni per svilupparsi in un definito ecosistema di riferimento.

Di particolare rilevanza sono anche le attività messe in campo da *CheBanca*, che a partire dalla scorsa estate ha avviato un programma di incubazione e accelerazione di realtà *FinTech* in collaborazione con la piattaforma di riferimento a livello globale Medici.

Dallo studio delle traiettorie di investimento degli operatori di *Venture Capital*, *Dealroom* (società specializzata nell'analisi dei principali *Venture* europei e delle relative operazioni di investimento) posiziona gli italiani molto al di sotto dei peer europei. Emerge però che, se da un lato la quantità di capitali investiti è minima rispetto a quanto avviene in altri paesi UE (circa 200 milioni nel 2016), si

registra nel 2016 un significativo incremento in valore dei capitali investiti rispetto all'anno precedente (+20%).

Tra i 15 fondi più attivi italiani, oltre la metà sta puntando sul mondo *FinTech* e presenta in portafoglio alcune delle più note *FinTech* italiane, tra tali fondi ricordiamo:

- *Innogest Sgr*, società di base a Torino, ha investito 130 volte in *start-up* realizzando 136 *exit* dal 2006 ad oggi. Alcune delle realtà in cui ha investito hanno raggiunto interessanti performance negli ultimi anni, tra queste due *FinTech* protagoniste dello scenario italiano: *Prestiamoci*, *start-up* italiana autorizzata come finanziaria da Banca d'Italia per la gestione di una piattaforma di prestiti fra privati online (microcredito) e *Sardex*, circuito territoriale di moneta virtuale per lo scambio tra aziende di beni e servizi, recentemente inserita dal Financial Times tra le mille società che più crescono in Europa
- *P101*, *Venture Capital* di Milano, 273esima società nella classifica europea, 10 round di investimento nel 2016 e un *exit*. Tra le *start-up* in portfolio emerge la *FinTech Borsa del Credito*, il *marketplace-lending* italiano dove aziende e risparmiatori possono prestare denaro online alle PMI italiane. P101 ha investito 1 milione di euro in questa realtà
- *United Ventures*, investitore milanese, occupa la 327esima posizione in Europa, nel 2016 ha realizzato due investimenti e un *exit*. Di rilevanza l'operazione di investimento realizzata con l'inglese *Cabot Square Capital* nei confronti di *MoneyFarm* (piattaforma di consulenza finanziaria online) in cui hanno versato 16 milioni di euro

Per concludere la rassegna degli *hub* italiani a sostegno del comparto *FinTech* ricordiamo anche l'incubatore di recentissima costituzione *Supernovae Labs*, nato a fine 2016 con sede a Milano e presente anche nei principali poli *FinTech* al mondo, come UK, Francia, Benelux, Spagna, New York e Kuwait City. *Supernovae Labs* si propone sul mercato come un acceleratore *FinTech* per banche e assicurazioni con l'obiettivo di favorire l'incontro tra il mondo *finance* e le *start-up* capaci di innovare il settore. Ad oggi risultano incubate in *Supernovae Labs* 18 realtà con soluzioni che coprono circa due terzi dei principali trend di innovazione in ambito *FinTech* e *InsurTech*, tra cui: *roboadvisor*y, *blockchain*, *digital marketing*, pagamenti, PSD2, *big data*, *criptocurrency*, intelligenza artificiale, *security & KYC system*, *mobile banking*.

Le banche e gli operatori finanziari cominciano a mostrare segnali di preoccupazione sulle *FinTech* e su come queste possano rappresentare una minaccia per il business tradizionale. Il Global *FinTech* Report 2017 di *PWC* mette infatti in evidenza come l'89% delle banche europee e l'82% delle banche italiane dichiari di vedere nelle *FinTech* una possibile minaccia, in particolare su alcune aree della catena del valore come quella dei pagamenti e del *robo-advisoring*.

Per trasformare in opportunità la sfida posta dalle *FinTech* il 41% degli operatori *finance* tradizionali ha avviato partnership con tali *start-up*, mentre l'84% afferma che intende avviarne nei prossimi 3-5 anni. Lo scenario pertanto è in forte evoluzione e la collaborazione con le *FinTech* rappresenta per le banche un'opportunità per accelerare il processo di innovazione.

Le banche italiane più attive in ambito *FinTech* sono:

- *Intesa Sanpaolo* che ha costituito *Neva Finventures* un fondo di corporate venture capital che ha l'obiettivo di investire, in ambito *FinTech*, su realtà innovative sinergiche con le *business unit* del Gruppo o con nuovi *business model*. Il fondo, inizialmente dotato di 30

milioni di euro, potrà raggiungere a breve un valore complessivo di 100 milioni di euro ed effettuare investimenti, congiuntamente ad investitori istituzionali, in *start-up* dei principali paesi tra cui USA, Israele ed Europa. Tra gli esempi di aziende partecipate e integrate nell'offerta del gruppo vi è *Marketwall* che eroga alla clientela di Intesa *Sanpaolo* servizi di informazione finanziaria e *trading*;

- *Unicredit* ha costituito *Evo*, acronimo di *equity venture opportunities*, un fondo appositamente pensato per investire su *start-up* di ambito tecnologico finanziario, in *joint venture* con *Anthemis Group*, società di *advisor*y e raccolta di capitale per i servizi finanziari
- Banca Sella è una tra le prime banche italiane come già detto ad aver costituito un proprio incubatore d'impresa (*SellaLab*) all'interno del quale è attivo un programma di accelerazione specifico di sei mesi, il "FinTech Accelerator Program". Ad oggi aderiscono al programma *Nes* (*e-wallet* sia per valute fisiche che per *criptovalute*), Shapps (piattaforma di finanziamento per gli sviluppatori di app), Vidyasoft (piattaforma *Cloud* per *l'Internet of Thing*) e l'ucraina *Taplend*, che è focalizzata su prestiti istantanei *Peer-to-Peer*;
- *Che Banca*, con *Advise Only* e *Deus Technology*, ha ampliato la propria offerta con il servizio di *robo advisor*y verso la propria clientela.

Per le grandi banche un'apertura verso forme di cooperazione con le *start-up* innovative potrebbe essere la leva per innovare l'offerta di servizi e migliorare la relazione con la propria *customer base*. Le tecnologie su cui le banche italiane sembra stiano puntando concernono i *data analytics*, la *cybersecurity* e la tecnologia *blockchain*. Grazie alle partnership con le società *FinTech*, gli operatori tradizionali potranno esternalizzare parte della *R&S* e realizzare la propria strategia, consentendo infine di offrire più velocemente nuovi prodotti alla clientela.

In conclusione, emerge che il mercato *FinTech* in Italia sia mediamente meno sviluppato rispetto ad altri Paesi, ma l'evoluzione mostra che sia le realtà finanziarie tradizionali che le *FinTech* stiano avviando un percorso di collaborazione comune che potrà portare vantaggi al mercato nel complesso.

# 2. *BIG DATA*

## 2.1 Definizione

Tra le principali innovazioni *FinTech* abbiamo i cosiddetti *Big data*, ossia quel nuovo settore dell'informatica dedicato alla gestione di database di grandi dimensioni. In particolare, la Commissione europea ha definito i *Big data* come quelle situazioni caratterizzate da un notevole volume di differenti tipologie di dati prodotti, da diversi tipi di fonti, ad altissima velocità, spesso in tempo reale grazie all'utilizzo delle tecnologie IT. La Commissione descrive il fenomeno ricorrendo alle cosiddette tre "V", Volume, Varietà e Velocità[3], altri regolatori invece, in altri contesti hanno fatto ricorso anche ad altre due "V" ossia Veridicità e Valore. Con il termine Volume ci si riferisce

[3] V.Mayer-Shoneberger, K.Cukier, "*Big Data. A revolution that will transform how we live, work and think*", 2013

alla notevole quantità di dati in continua crescita grazie a nuovi strumenti, come internet, social media, piattaforme virtuali e altro, passando da misure come i *megabyte* ($10^6$ *byte*) in passato, ai *yottabyte* ($10^{24}$ *byte*) nella realtà attuale. Il termine Varietà evidenzia come questa ingente quantità di dati provenga da numerose fonti differenti; in particolare, i dati possono essere distinti in strutturati, se riconducibili ad uno stesso ambito (come numeri di telefono, indirizzi), semi-strutturati (come email, dati personali) e non strutturati (come video, immagini). La Velocità indica la rapidità con cui un'enorme quantità di dati viene raccolta e rielaborata per trarne il maggior vantaggio possibile. La Veridicità indica la necessità che i dati debbano essere veritieri e affidabili. Il Valore, infine, si riferisce alla possibilità di utilizzare i dati raccolti per effettuare analisi e prevedere eventi futuri attraverso particolari algoritmi predittivi.

Il concetto di *Big data* non si riferisce solo ai dati in sé ma anche e soprattutto alla loro rielaborazione tramite tecniche sofisticate e i risultati della loro analisi. In particolare, il fattore più importante che caratterizza i *Big data* è quello predittivo, ossia la possibilità, attraverso una serie numerosissima di dati diversi, di catalogare e profilare gli utenti secondo una differenziazione tipologica quasi illimitata. La *Big data Analysis* a differenza di altri sistemi di analisi, che permettono di trovare risposta ad una specifica domanda, consente di trovare attraverso particolari algoritmi relazioni statistiche all'interno di un dataset al fine di identificare delle regolarità sulla base delle quali improntare dei modelli utili per sviluppare un processo decisionale[4]. L'algoritmo è tra l'altro capace di individuare e migliorare le categorie e i fattori di interesse per il processo decisionale in base ai dati che sono di volta in volta analizzati[5], senza la necessità di intervento del programmatore.

Esistono tre tipi di *data analysis*: l'analisi descrittiva che utilizza i *big data* per analizzare eventi passati, l'analisi predittiva che, tramite modelli statistici predittivi, utilizza i *big data* per prevedere eventi futuri; l'analisi prescrittiva, più complessa delle precedenti, che permette attraverso l'analisi dei dati di formulare delle raccomandazioni e individuare le possibili conseguenze di un particolare tipo di comportamento.

## 2.2 Il mercato dei *Big Data*

Nel settore finanziario, così come in tutti gli altri settori interessati dal processo di digitalizzazione, è considerata fondamentale per un'impresa la capacità di raccogliere analizzare e trasformare i numerosi dati in loro possesso in informazioni utili per strutturare la propria attività utilizzando algoritmi sempre più sofisticati; i dati infatti sono ormai considerati come fattori di produzione al pari del lavoro e del capitale. I dati di maggior interesse non sono quelli oggettivi quanto quelli personali, ossia quei dati che gli stessi consumatori diffondono attraverso le piattaforme digitali a favore delle imprese o quelli che i consumatori rilasciano inconsapevolmente attraverso le navigazioni informatiche, durante le quali, attraverso i *web cookie*, è possibile memorizzare i siti visitati. Nella *digital economy* il vantaggio competitivo tra le imprese è largamente basato sulla capacità, attraverso l'uso di sofisticati algoritmi, di raccogliere e analizzare i dati dei propri clienti e dei potenziali tali, per meglio comprenderne i gusti e le esigenze, offrendo loro servizi nuovi,

[4] U. Fayyad, "*The Digital Physics of Data mining*", 2001
[5] P. Domingos, "*A Useful Things to Know about Machine Learning*", 2012

personalizzati, qualitativamente migliori e a prezzi più contenuti rispetto a quelli dei mercati tradizionali[6]. L'uso dei dati è funzionale anche alla formulazione di strategie di produzione e commerciali al fine di conquistare nuovi segmenti di mercato e clientela. Le imprese che operano nell'economia digitale possono decidere di raccogliere i dati in proprio oppure acquistarli da soggetti terzi. Per alcune imprese quindi i dati raccolti rappresentano un semplice *input* della produzione per altre invece i dati possono essere il risultato stesso dell'attività economica (*output*) se questa abbia ad oggetto appunto la raccolta e la rivendita dei dati in maniera grezza o già raffinati. Vi sono anche imprese che operano su piattaforme a doppio versante (*two-sided platforms*) o multi versante (*multi-sided platforms*) e dunque su più mercati contemporaneamente. È questo il caso dei motori di ricerca (*Google, Bing, Yahoo!*, ecc.) i quali, su un versante, raccolgono i dati dagli utenti a titolo gratuito, mentre su un altro versante, ossia il mercato della pubblicità online, rivendono tali dati agli inserzionisti che intendano acquistare spazi pubblicitari. Similmente le piattaforme di *e-commerce* (come *Amazon* e *eBay*) operano sul doppio versante della vendita di prodotti ai consumatori e della vendita di spazi pubblicitari agli inserzionisti. Il mercato dei dati viene tra l'altro suddiviso in più segmenti che rappresentano le varie fasi del ciclo dei dati: quello della raccolta (*Big data Capture*), quello dell'immagazzinamento dei dati grezzi (*Big data Storage*), dell'analisi dei dati e estrazione dei metadati (*Big data Analytics*) e infine quello del riutilizzo dei dati (*Big data Utilization*).

L'esigenza che spinge gli operatori a ricercare informazioni sui propri clienti, attuali o potenziali è dovuta al cambiamento del rapporto con i consumatori determinato dall'avvento dell'economia digitale. Essa ha determinato infatti l'ingresso di nuovi competitors in settori precedentemente controllati da pochi dominanti e una smaterializzazione dell'offerta dei prodotti e servizi con conseguente perdita della tradizionale fidelizzazione. I clienti saranno quindi sempre più disposti a cambiare operatore, sentendo meno il rapporto di fiducia, rivolgendosi a chi propone l'offerta migliore che più si adatta alle proprie esigenze. In questo contesto, la conoscenza approfondita della clientela e la sua profilazione diventerà essenziale per difendere la propria posizione nel mercato; ciò giustifica la tendenza odierna alla *customer centricity* dovuta, in ambito finanziario, oltre che a motivi di natura concorrenziale, legati all'evoluzione tecnologica, anche alle nuove recenti disposizioni del regolatore in materia di tutela del consumatore. Tali disposizioni sono contenute nella direttiva MiFID 2, entrata in vigore il 3 gennaio 2018; essa prevede un'applicazione sempre più minuziosa della regola del "*know your customer*" e della tutela dell'investitore che non si limita solo al momento finale, in cui il prodotto viene consigliato e venduto (come previsto del MiFID 1) ma anche nella fase intermedia ossia di ingegnerizzazione, sviluppo e commercializzazione del prodotto o servizio, nell'ambito della "*product governance*".

## 2.3 Benefici sui servizi finanziari

Tra i principali benefici apportati dalla tecnologia dei *Big data* nel settore finanziario è da considerare, come già detto, il contributo al miglioramento della qualità dei servizi, maggiormente personalizzati e adattati alle esigenze dei consumatori e la possibilità di ottemperare agli obblighi di tutela imposti con MiFID 2. Per il settore creditizio, l'utilizzo dei *Big data* consente di rendere più

[6] F. Di Porto (a cura di), "*Big Data e concorrenza*", 2016

efficace il processo decisionale e di estendere l'accesso al credito di soggetti fino ad oggi esclusi perché considerati *unbanked* secondo i tradizionali modelli di stima. I consumatori possono trarre vantaggio dalla tecnologia dei *Big data* anche attraverso una migliore pubblicità, la proposta di servizi gratis e di offerte speciali sempre grazie alla maggior conoscenza della preferenza dei consumatori, ottenibile tramite l'elaborazione dei dati. I *Big data* possono poi contribuire anche alla prevenzione di fenomeni di *cybercrime*, frodi e attività illecite come il riciclaggio e il finanziamento del terrorismo tramite l'uso di algoritmi sofisticati che permettono di rilevare comportamenti sospetti grazie al controllo delle operazioni di pagamento.

## 2.4 Rischi per la tutela della *privacy*

Tra i principali rischi legati alla tecnologia dei *Big data* vi è quello della tutela della *privacy* e dei dati personali. Il Parlamento europeo ha affermato che nell'utilizzo di tali dati sia le autorità pubbliche che i soggetti privati devono rispettare rigorosamente la normativa a tutela dei diritti fondamentali e della protezione dei dati e in particolare, il regolamento europeo 2016/679, entrato in vigore il 25 maggio 2018. Attraverso tale regolamento il Parlamento europeo ha consentito l'instaurazione di un clima di fiducia, indispensabile per sostenere lo sviluppo di un'economia digitale, garantendo ai singoli di mantenere un controllo sul trattamento dei propri dati da parte di soggetti terzi, soprattutto nel processo di profilazione. Esso, tramite l'elaborazione dei dati, permette di suddividere gli utenti in gruppi omogenei sempre più particolareggiati, accomunati da stesse caratteristiche, al fine di risalire all'utente reale che utilizza quel determinato terminale. Il regolamento pone alla base della disciplina sul trattamento dei dati il principio di finalità e il principio del consenso informato da parte dell'utente; il titolare dei dati deve cioè dare espressamente il proprio consenso al trattamento dei dati personali, dopo essere stato informato circa le finalità per le quali tali dati verranno utilizzati. L'applicazione rigorosa di tale normativa potrebbe ostacolare l'applicazione della tecnologia dei *Big data* che presuppongono l'esistenza di numerosi fini. Sono esenti dall'applicazione della normativa sulla tutela dei dati personali solo i dati anonimizzati cioè quei dati riferiti ad una persona fisica resi sufficientemente anonimi da impedirne l'identificazione. Nel caso in cui l'anonimizzazione non sia possibile, ossia quando il trattamento tramite *big data* è necessariamente ed espressamente finalizzato all'identificazione dei comportamenti e delle caratteristiche di determinate persone o gruppi, allora è d'obbligo applicare le garanzie a tutela della *privacy* previste dal regolamento. In particolare, il titolare del trattamento deve mettere in atto delle tecniche di pseudoanonimizzazione che permettono di "allontanare" il dato dalla persona, rendendo difficile l'identificazione della persona stessa attraverso il dato, senza però eliminare del tutto il legame esistente tra essi[7] (cosa che invece avviene con la tecnica della anonimizzazione). Infine, con l'obbiettivo di tutelare ulteriormente i consumatori, il regolamento prevede il diritto alla portabilità dei dati[8], il quale comporta che gli interessati possano ricevere i dati personali, che sono stati da loro forniti al titolare del trattamento, in un formato strutturato semplice e leggibile da un dispositivo automatico, e che tali dati possano essere trasmessi ad altri operatori senza impedimenti, consentendo agevolmente il passaggio ad un altro servizio.

[7] G. D'Acquisto, M. Di Nardo, "*Big Data e privacy by design*", 2017
[8] WP29, "*Guidelines on the right on data portability*", 2016

## 2.5 Rischi per la concorrenza: intese e pratiche collusive

Di notevole importanza è anche il problema dell'impatto dei *Big data* sulla concorrenza che pone nuove sfide regolamentari nel settore del diritto della concorrenza e della legislazione antitrust. Su tale tema il Parlamento europeo, nella Risoluzione sulla tecnologia finanziaria del 17 maggio 2017, ha evidenziato la necessità di finalizzare la disciplina di settore alla «promozione della concorrenza leale, la neutralizzazione delle eventuali rendite economiche e la creazione di condizioni di parità» e ha inoltre invitato la Commissione europea a verificare «l'adeguatezza del quadro normativo in materia di concorrenza per affrontare le sfide dell'economia digitale in generale e del settore *FinTech* in particolare» e individuare al contempo le misure più idonee da adottare per sostenere l'innovazione tecnologica. Si prevede quindi nell'immediato futuro un intervento delle istituzioni comunitarie su tale tema con strumenti di *hard law* che prenderanno il posto delle misure di *soft law* finora adottate.

Tra gli effetti più preoccupanti dell'economia digitale fondata sui dati si annovera la tendenza alla concentrazione del potere di mercato nelle mani di pochi operatori e la conseguente creazione di barriere all'ingresso da parte di questi ultimi a danno degli aspiranti concorrenti (*foreclosure effect*). Le Autorità Antitrust francese e tedesca, in un *report* congiunto, hanno messo in luce il circolo vizioso creato dalla cessione dei dati personali, da parte degli utenti, ai maggiori motori di ricerca e social network (*Google, Facebook, Twitter*, ecc.). Ciò determina un incremento dei Biadata da questi detenuti, dei loro investimenti pubblicitari e quelli per la creazione di sempre nuovi e migliori servizi gratuiti, marginalizzando al contempo le imprese più piccole per carenza di dati. Il risultato di questa tendenza è quella di aumentare sempre di più il gap esistente nella qualità dei servizi offerti e nelle quote di mercato tra piccole e grandi imprese, fenomeno definito con il termine *snowball effect*.

Pericolose sotto il profilo della concorrenza e dell'antitrust sono inoltre le intese e le pratiche collusive. Nonostante fino ad ora non si siano riscontrate nella prassi intese tra operatori concorrenti nello stesso mercato digitale, sono invece avvenute intese fra imprese che operano in mercati diversi, volte a rafforzare la posizione di dominanza di una delle due nel rispettivo mercato. Esemplare è il caso di *Google/Android*, finito sotto indagine della Commissione europea, per la formazione di un accordo collusivo di preimpostazione della stringa di ricerca *Google* su tutti i dispositivi *Android*, che ha avuto l'effetto di rafforzare la posizione dominante di *Google* nel mercato dell'*engine research* a scapito dei concorrenti; pratica che ha costretto *Android* al pagamento di una multa di 5 miliardi di dollari inflitta dalla Commissione europea. A tal proposito il già citato report delle Autorità francese e tedesca ha evidenziato che la maggiore trasparenza sui mercati online possa avere effetti sia positivi che negativi. Da un lato infatti essa permette ai consumatori di conoscere con più facilità le caratteristiche e i prezzi dei servizi e prodotti offerti sulle piattaforme telematiche da imprese concorrenti e compararli più agevolmente; dall'altro lato però la maggiore trasparenza favorisce lo scambio di informazioni tra imprese concorrenti. Tale fattispecie viene tradizionalmente annoverata tra le pratiche facilitanti [9] ossia pratiche che agevolano il raggiungimento di accordi collusivi taciti sui prezzi dei prodotti o servizi forniti dalle imprese, le quali dovrebbero invece essere indipendenti sul mercato diversificando il più possibile le loro offerte. Tale maggiore trasparenza e lo scambio di informazioni tra i concorrenti provoca infatti l'effetto di

[9] M. Motta, "*Competition Policy. Theory and Practice*", 2004

indurre le imprese ad un allineamento dei prezzi e la fissazione di una soglia di prezzo unitaria e più alta, in modo da garantire una rendita costante alle imprese stesse e il mantenimento nel tempo degli equilibri preesistenti.

Un trattamento differente viene riservato allo scambio di informazioni riguardanti il rischio delle attività essenziali per il mercato dei servizi bancari e le informazioni sui sinistri essenziali per le statistiche di rischiosità nel mercato creditizio. La già citata Risoluzione del Parlamento europeo sulla tecnologia finanziaria mette in evidenza che «i servizi bancari aperti e la condivisione dei dati contribuiscono a garantire che tutti i modelli economici del settore *FinTech* possano crescere insieme a beneficio dei consumatori». È probabile quindi che in futuro vengano elaborati regolamenti di esenzione con riguardo allo scambio di informazioni bancarie e finanziarie essenziali come input nella produzione di servizi del ramo *FinTech*. È possibile inoltre che i risultati di eventuali studi statistici di natura finanziaria svolti dalle imprese di maggiori dimensioni possano essere riconosciuti, in sede regolamentare, come informazioni essenziali, al fine di standardizzarli e porre l'obbligo di condivisione e cessione della relativa licenza d'uso alle imprese di minori dimensioni.

Con riguardo alla trasparenza dei mercati digitali, bisogna tenere presente che il suo effetto anticoncorrenziale appena esaminato possa comunque essere controbilanciato dalle offerte personalizzate e dalla discriminazione dei prezzi largamente praticata in questi mercati che consentono ad alcuni consumatori di ottenere un notevole risparmio rispetto al prezzo comunemente praticato sul mercato dai concorrenti.

## 2.6 Rischi per la concorrenza: abuso di posizione dominante

Altra grande preoccupazione per il diritto antitrust legata alla *digital economy* è lo sfruttamento abusivo della posizione dominante, acquisita sul mercato grazie ai *Big data* e i *data-set*, sia quando questi costituiscono un *input* della produzione, sia quando rappresentano l'*output* stesso dell'attività economica svolta. In particolare, il problema riguarda perlopiù le imprese che non sono in grado di raccogliere da sé i dati degli utenti e debbano quindi necessariamente, per competere su mercato, acquistarli da altre imprese in maniera grezza o già sotto forma di metadati. Tale fattispecie pone questioni di carattere regolamentare riguardo la titolarità dei dati, l'accesso agli stessi, le regole sul loro trasferimento, la possibilità di considerarli o meno come *essential facility* e le relative problematiche sulle barriere all'ingresso, le pratiche escludenti e il rifiuto di licenza. Normalmente se un'impresa investe nella raccolta e analisi dei dati al fine di aumentare la competitività sul mercato, il patrimonio di dati così acquisito diventa parte integrante del proprio avviamento commerciale e principale asset competitivo del proprio business, quindi in quanto tale non vi sarebbe ragione di ritenere che l'impresa in questione lo debba condividere con i propri concorrenti. Le imprese titolari di *Big data* dunque al pari di quelle titolari di brevetti o altri diritti di proprietà intellettuale o industriale, avranno il diritto di usufruire in maniere esclusiva dei propri *data-set* e del risultato dei propri investimenti in *R&S*, essendo l'esclusività d'uso parte integrante del diritto di privativa sui propri beni aziendali. Un'eccezione a questa regola è rappresentata dall'*Essential Facility Doctrine* (EFD), nata con riguardo alle grandi infrastrutture materiali irreplicabili o difficilmente replicabili e successivamente estesa al settore dell'*information technology*. L'EFD impone al monopolista o titolare esclusivo del bene il dovere di consentire

l'accesso all'input essenziale nei casi in cui: detto *input* sia a tutti gli effetti insostituibile; l'impresa che ne richieda l'accesso intenda utilizzarlo per produrre un bene diverso da quello commercializzato dall'impresa che ne è titolare, collocandosi dunque su un diverso mercato; non vi siano cause che possano giustificare il rifiuto di fornire tale bene essenziale. In questi casi il *refusal to supply* può essere considerato come abuso di posizione dominante e quindi essere soggetto a sanzioni antitrust che prevedono di solito, tra le altre cose, l'imposizione dell'obbligo di contrattare per concedere all'impresa richiedente la licenza d'uso dell'essential facility a condizioni FRAND ossia *fair, reasonable and not discriminatory*.

Non è possibile dare una risposta univoca riguardo la possibilità o meno di considerare i dati come *essential facility input*, ma è necessario valutare le singole fattispecie concrete caso per caso, verificando la presenza o meno dei requisiti di essenzialità e insostituibilità della risorsa in questione, nonché la relazione tra le due imprese e la collocazione sul mercato dei rispettivi prodotti o servizi. Caso esemplare dell'applicazione dell'EFD per abuso di posizione dominante è il caso *Magill TV Guide*, in cui tre emittenti televisive britanniche (*BBC*, *RTE* e *ITV*) si erano rifiutate di comunicare i loro palinsesti alla società irlandese *Magill*, impedendole così di realizzare una guida televisiva settimanale generale. La Corte ha affermato in quella sede che il rifiuto di cedere tali informazioni costituiva un abuso di posizione dominante in quanto: ostacolava l'emergere di un prodotto nuovo, non offerto dalle emittenti britanniche e dunque la creazione di un nuovo mercato; non sembrava giustificato rispetto alla tutela del diritto di privativa; infine la licenza era condizione indispensabile per l'ingesso nel mercato e quindi assimilabile ad un'infrastruttura irreplicabile. In realtà diverse indagini hanno dimostrato che non sia affatto agevole qualificare i *Big data* come input insostituibile, in ragione della loro ubiquità, non rivalità, facilità d'acquisizione, dinamicità e velocità di raccolta e aggiornamento e infine per effetto della portabilità dei dati personali esercitata dagli utenti. Detto questo, non potendo, se non in casi rari, applicare l'EFD per abuso di posizione dominante relativa al possesso di *Big data* e *data set*, è stata riconosciuta una nuova fattispecie di abuso ossia l'abuso di dipendenza economica che non richiede la prova di condizioni tanto stringenti come quelle richieste dall'EFD. Si tratta di una fattispecie trans-tipica applicabile a tutti i rapporti tra imprese che si trovino in posizione di squilibrio economico e giuridico e ricorre secondo l'articolo 9 comma 1 e 2 quando «un'impresa sia in grado di determinare, nei rapporti commerciali con un'altra impresa un eccessivo squilibrio di diritti e di obblighi. La dipendenza economica è valutata tenendo conto anche della reale possibilità per la parte che abbia subito l'abuso di reperire sul mercato alternative soddisfacenti. L'abuso può anche consistere nel rifiuto di vendere o nel rifiuto di comprare, nella imposizione di condizioni contrattuali ingiustificatamente gravose o discriminatorie, nella interruzione arbitraria delle relazioni commerciali in atto» Tale fattispecie si adatta perfettamente a quelle situazioni di asimmetria di potere economico che caratterizzano le relazioni tra le piccole e le grandi imprese nei mercati digitali, legate in particolare alla detenzione da parte delle grandi imprese di data set essenziali di cui potrebbero aver bisogno le imprese di piccole dimensioni, non essendo queste ultime in condizione di sostenere i costi di *R&S* per procurarsi i dati autonomamente. Mentre per l'abuso di posizione dominante è necessario dimostrare sia l'insostituibilità della risorsa essenziale sia il rapporto non direttamente concorrenziale tra le imprese, per l'abuso di dipendenza economica il rifiuto di vendere o di dare in licenza la risorsa posseduta potrà considerarsi illecito laddove si dimostri semplicemente che non sia possibile reperire sul mercato risorse alternative soddisfacenti. Questo implica che se il titolare dei *Big data*, a cui venga richiesto il rilascio di una licenza, non sia l'unico a possedere quei dati, ma i suoi *data-*

*set* siano notoriamente i migliori e i più aggiornati e completi presenti sul mercato, ciò può essere considerato sufficiente a ritenere insoddisfacenti le altre alternative reperibili sul mercato. L'abuso di dipendenza economica comprende anche i casi di accesso discriminatorio ai dati da parte delle imprese che li detengono nel momento in cui queste ne concedano l'uso ad una pluralità di imprese ma a condizioni differenti e non paritarie così da favorire alcune imprese e sfavorirne o addirittura escluderne altre.

Tra le possibili condotte di sfruttamento di posizione dominante legata alla titolarità dei *Big data* ricordiamo anche quella delle pratiche leganti. Queste si verificano qualora un'impresa imponga di acquistare i propri dati in abbinamento ai servizi di *data analytics*, costringendo le imprese, che invece necessitano dei soli dati grezzi, ad una maggiore spesa per il servizio (non richiesto) di elaborazione degli stessi.

## 2.7 Rischi per la concorrenza: concentrazioni tra imprese

Particolare attenzione da parte della Autorità antitrust viene posta ai casi di concentrazioni tra imprese nel settore della *digital economy*, legate alla detenzione dei *Big data*. La Commissione europea ha tuttavia deciso finora di autorizzare le operazioni concentrative poste sotto la sua attenzione (*Google/DoubleClick, Microsoft/Yahoo!SearchBusiness, Microsoft/Skype, Microsoft/LinkedIn, Facebook/WhatsApp*) non riscontando rischi di abusi legati alla creazione o al rafforzamento di posizioni dominanti. Il motivo per il quale la Commissione europea non ha finora bloccato nessuna operazione concentrativa potrebbe essere legato all'utilizzo degli schemi operativi del cosiddetto test di dominanza, basati per lo più sul valore delle quote di mercato delle imprese coinvolte e non adatti quindi a stimare l'impatto che, in senso dinamico, l'ampliamento dei *data-set* aziendali (dovuto all'operazione concentrativa) possa avere sul business delle imprese coinvolte e sul relativo mercato. È quindi auspicabile l'adozione di un nuovo sistema antitrust che porti le autorità ad assumere decisioni sulla base di un'indagine accurata degli effetti economici, prospettici e dinamici che il comportamento delle imprese può avere sul mercato, piuttosto che sulla base dello stato delle cose al momento della decisione.[10] Se questo fosse stato fatto nelle precedenti occasioni, probabilmente non tutte le operazioni concentrative sopra elencante sarebbero state autorizzate, come nel caso della fusione tra *Facebook* e *WhatsApp*, autorizzata nel 2014, che ha iniziato subito dopo a produrre effetti negativi per i consumatori. Nel 2017 infatti l'AGCM è intervenuta a sanzionare *WhatsApp* per pratiche commerciali scorrette (PCS) in quanto colpevole di aver indotto i consumatori ad accettare la clausola di condivisione dei propri dati con *Facebook* nella fase di accettazione dei termini di utilizzo di *WhatsApp Messenger*, facendo credere agli utenti che, senza l'accettazione di tale clausola, non avrebbero più potuto continuare ad utilizzare il servizio offerto da detta app. Tale caso ha dimostrato che vi possano essere abusi conseguenti all'acquisita dominanza su un certo mercato (quello dei social network per *Facebook*) capaci di estendersi anche su altri mercati (quello delle comunicazioni in cui opera *WhatsApp*) per effetto della fusione realizzata tra due colossi.

[10] R. Podszun, "*The More Technological Approach: Competition Law in the Digital Economy*", 2015

## 2.8 Rischi per la concorrenza: discriminazione dei prezzi

Problemi di carattere commerciale e concorrenziale, legati all'uso dei *Big data*, sono causati anche dalla tendenza nella *digital market economy* alla personalizzazione delle offerte da parte degli operatori, in quanto porta alla cosiddetta discriminazione dei prezzi. Tale espressione indica la pratica messa in atto dalle imprese, di differenziare il prezzo di un prodotto o servizio per determinati consumatori, sulla base della loro disponibilità a pagare prezzi più alti, a fronte del risparmio di spesa riservato a quei consumatori che, pur appartenendo al medesimo target, sono disposti a pagare un prezzo più basso per il medesimo bene. Tale condotta di discriminazione dei prezzi può avere sia effetti positivi che negativi. Sul piano della domanda, in senso pro-concorrenziale, viene riscontrata la tendenza all'aumento ed alla massimizzazione del benessere generale dei consumatori, intesi nella loro totalità (*social welfare*) e un incremento della competizione tra le imprese[11]; mentre in senso anti-concorrenziale si registra una perdita del benessere individuale per quei consumatori inclini a pagare un prezzo più alto per un determinato bene e un vantaggio di costo soltanto per quelli che pagherebbero un prezzo più basso per lo stesso bene. La discriminazione dei prezzi praticata da un'impresa in posizione dominante, se rivolta nei confronti di altre imprese sul mercato, costituisce sicuramente un illecito *antitrust*. Nel caso in cui è rivolta ai consumatori invece, la discriminazione dei prezzi derivante da offerte personalizzate viene considerata come pratica commerciale scorretta se operata all'insaputa del cliente poiché carente di trasparenza e contraria alla correttezza professionale. Questa pratica infatti è capace di incidere in modo rilevante sulle scelte di consumo del singolo, inducendolo all'acquisto inconsapevole o non sufficientemente informato, di un determinato prodotto o servizio, che magari non sarebbe stato acquistato o sarebbe stato acquistato a condizioni differenti, se il consumatore stesso fosse stato maggiormente edotto sulla natura discriminatoria e personalizzata dell'offerta. Studi di marketing condotti sui consumatori, hanno difatti dimostrato non soltanto la percezione delle offerte personalizzate come scorrette e sleali, ma hanno fatto emergere inoltre una certa propensione degli utenti a modificare le proprie decisioni di consumo, una volta informati della natura personalizzata del prezzo loro praticato, soprattutto se più alto di quello di mercato.

## 2.9 Altre questioni

Oltre ai problemi riguardanti la tutela della *privacy* e quelli relativi all'antitrust vi sono anche altri rischi, legati alla tecnologia dei *Big data*. Il *Financial Stability Board*[12] ha messo in evidenza la complessità e l'opacità dei sistemi di *Big Data Analysis* e che le analisi, a causa di dati errati o di procedure sbagliate, possono portare a risultati scorretti e talvolta anche discriminatori. La profilazione degli utenti e la loro maggiore segmentazione granulare infatti, può condurre, soprattutto nel settore bancario e assicurativo, all'individuazione di una categoria di consumatori considerati indesiderabili, determinandone la loro esclusione da determinati prodotti e servizi[13].

[11] M. Maggiolino, "*Big Data e prezzi personalizzati*", 2016
[12] Financial Stability Board, "*Financial Stability Implications from FinTech. Supervisory and Regulatory Issues that Merit Authorities' Attention*", 2017
[13] FSUG, "*Paper on Assessment of current and future impact of Big Data on Financial Services*", 2016

L'esclusione può tra l'altro interessare anche quelle categorie di soggetti che non sono in grado di utilizzare internet e le nuove tecnologie e quelli che non sono disposti a condividere i propri dati personali.

Recenti indagini hanno evidenziato che gli *incumbents* del settore finanziario tendono ancora ad uso tradizionale dei dati e delle informazioni, al contrario molto più innovativo è l'approccio usato dalle *start-up*, che fanno ormai ampio uso della tecnologia dei *Big data*. Il motivo della resistenza degli *incumbents* alle nuove tecnologie sull'analisi dei dati, è dovuta sia alla grande mole di informazioni che essi già detengono rispetto ai nuovi operatori sia alle incertezze sul piano normativo, soprattutto riguardo il tema della tutela dei dati personali. L'uso dei *Big data* è comunque in continua crescita, per cui sarà necessario un futuro intervento del regolatore volto a disciplinare tale fenomeno, in ragione delle numerose problematiche che esso comporta e dei rischi per la tutela dei consumatori. In particolare, sarà indispensabile rendere note le modalità di funzionamento degli algoritmi, che dovranno quindi essere sviluppati in modo più semplice e comprensibile, per meglio adattarli ai meccanismi di controllo e agli standard legali della normativa europea.

# 3. *ROBO ADVICE*

## 3.1 La consulenza automatizzata

Tra le maggiori innovazioni dell'ecosistema *FinTech* annoveriamo la *robo advice*, ossia la prestazione di servizi finanziari attraverso strumenti automatizzati. Tale definizione comprende diverse fattispecie accomunate dal fatto di utilizzare delle piattaforme online che, sulla base di sofisticati algoritmi, permettono di offrire ai risparmiatori soluzioni di investimento precostituite e di creare, gestire, monitorare e, se necessario, ribilanciare portafogli di investimento da raccomandare ai clienti in base a un processo di consulenza. Quest'ultimo si ottiene dall'analisi dei dati inseriti dal cliente in un questionario volto a valutare il suo profilo di rischio e individuare la combinazione rischio-rendimento che meglio gli si adatta. Si tratta di un vero e proprio consulente finanziario virtuale che, sfruttando la tecnologia, offre servizi di consulenza al pubblico in modo efficiente e a costi contenuti rispetto a quelli connessi alla prestazione del servizio *face-to-face* (si passa da una commissione media attuale di 1,5% applicata dagli istituti tradizionali a circa lo 0,3%-0,5% delle piattaforme) puntando sulla semplicità e sulla qualità dell'esperienza online per il consumatore. Il principale punto di forza della *robo advice* è la capacità di colmare un gap nel mercato dei servizi di consulenza consentendone l'accesso ai segmenti della clientela mass market grazie ai costi più contenuti e l'assenza di limiti di portafoglio. I *robo advisor*[14] rispondono quindi ad un tentativo di democratizzazione dei servizi di consulenza (riservati dai canali tradizionali per lo più alla sola clientela private) al fine di favorire l'inclusione finanziaria di soggetti considerati *unbanked*. Nonostante ciò vi sono però nell'ambiente finanziario numerosi oppositori preoccupati soprattutto dell'impatto disruptive del *robo advice* sul settore dell'intermediazione finanziaria. I maggiori timori riguardano: l'ingresso nel mercato di *start-up FinTech* non soggette a nessun controllo o

[14] BlackRock, "*Digital Investment Advice: Robo Advisors Come of Age*", 2016

regolamentazione che rappresentano pericolosi competitor per gli operatori tradizionali; il rischio di disintermediazione umana a favore di un'intermediazione digitale; la molteplicità delle fattispecie che possono essere ricollegate al settore della *robo advice*, tali da creare problematiche normative diverse da un caso all'altro. Per far fronte al primo di tali rischi le imprese tradizionali, al fine di mantenere la propria posizione sul mercato, hanno intrapreso un percorso di rinnovamento tecnologico attraverso la digitalizzazione dell'intero o solo di parte del processo distributivo direttamente all'interno dell'azienda stessa o esternalizzandolo a imprese *FinTech*. Per evitare il fenomeno di disintermediazione umana, ultimamente si tende ad una scelta di conversione dei *robo advice* in *robo* for *advisor*; in particolare, il modello del *cyborg advisor* (non del tutto umano, né esclusivamente digitale) permette di raggiungere una soluzione intermedia tra umano e digitale, due componenti originariamente presentate come alternative ma che in realtà risultano complementari. In questo modo è possibile soddisfare da un lato l'esigenza di adattarsi ad un mondo sempre più orientato al digitale, dall'altro il bisogno di molti consumatori di relazionarsi con una persona fisica, soprattutto per scelte di investimento complesse.

## 3.2 Interventi normativi: fase conoscitiva

Tra le prime autorità internazionali ad intraprendere un percorso conoscitivo del fenomeno dei *robo advice* annoveriamo la IOSCO che, con il report su "*Social media and automation advice tools Survey*" pubblicato nel luglio del 2014, ha riportato i risultati di un sondaggio svolto tra le autorità nazionali, che mostra le modalità di utilizzo delle nuove tecnologie in campo di *robo advice* da parte degli intermediari e il relativo controllo dei supervisori. I risultati di questo sondaggio mettono in luce una situazione fortemente disomogenea sia per grado di diffusione del fenomeno sia per grado di regolamentazione; non è stato quindi possibile identificare sfide e soluzioni uniche riguardo l'uso e il controllo dei *robo advice*. La IOSCO ha così deciso di temporeggiare in attesa di ulteriori evoluzioni del fenomeno, continuando nel frattempo a monitorare i futuri sviluppi della tecnologia in questione per giungere ad una più approfondita conoscenza della stessa, in vista di un futuro intervento regolamentare efficace su base internazionale.

All'interno dell'UE i primi interventi esplorativi delle autorità europee sul fenomeno della consulenza automatizzata ebbero inizio nel 2015 con l'obbiettivo di una maggiore comprensione delle caratteristiche distintive e l'individuazione dei potenziali rischi, al fine di mitigarli o neutralizzarli con un successivo intervento regolamentare o di altra natura. Tale processo esplorativo si è concluso con la pubblicazione il 4 dicembre del 2015, del *"Joint Committee Discussion Paper on automation in finance advice"* in cui le ESAs , sulla base delle informazioni raccolte, hanno definito il fenomeno in questione ancora ad uno stato iniziale con un differente sviluppo territoriale nei diversi stati membri, più diffuso nel settore finanziario che in quelli creditizio ed assicurativo e basato su una netta prevalenza del modello ibrido rispetto a quello totalmente automatizzato. Le ESAs hanno inoltre dichiarato di voler continuare a monitorare il fenomeno in futuro ma di astenersi al momento da qualsiasi intervento regolamentare, come richiesto tra l'atro dagli appartenenti al settore che hanno invocato il ricorso al principio di neutralità tecnologica, secondo il quale deve essere applicata la stessa normativa ad un determinato servizio prestato, a prescindere dal mezzo utilizzato per svolgerlo. Le ESAs hanno ritenuto quindi la normativa vigente

in materia di consulenza finanziaria capace di proteggere adeguatamente il consumatore anche dai rischi legati alla prestazione di tale servizio attraverso strumenti automatizzati.

All'interno del discussion paper le ESAs hanno poi stilato una lista di benefici legati all'uso di automated advice tools e dei connessi rischi per la tutela dei consumatori. Tra i benefici ricordiamo il già citato ampliamento delle possibilità di accesso ai servizi finanziari a una platea più estesa di consumatori, un più diversificato range di prodotti, costi più contenuti e l'assenza di limiti di portafoglio rispetto alla consulenza *face to face*. Per quanto riguarda i rischi invece ricordiamo: la mancanza di informazioni sul funzionamento degli *automated tools*; errori nella profilatura del cliente con il rischio di raccomandazioni inadeguate; malfunzionamenti del *tools* a causa di limitazioni e manipolazioni degli algoritmi utilizzati; mancanza di chiarezza sull'allocazione delle responsabilità. Tutti questi rischi rimandano al funzionamento degli algoritmi, alla loro mancanza di trasparenza e affidabilità, alla difficoltà di comprensione da parte dei consumatori e ai non chiari profili di responsabilità relativi alla formulazione di raccomandazioni errate da parte degli algoritmi.

## 3.3 Interventi normativi: lo statuto dei *robo advice*

È stata l'ESMA, nell'ambito della consultazione sulla revisione delle "*Guidelines on certain aspects of the* MiFID *2 suitability requirements*" del 13 luglio 2017, a tentare di fornire le prime risposte alle problematiche sollevate dal *Joint Commitee*, contribuendo alla formazione di un vero e proprio statuto dei *robo advice* costituito da misure di terzo livello o di *soft law*. I *robo advice* divengono soggetti ad un regime più severo dovendo sottostare sia alle norme relative ai servizi di consulenza in generale (in base al sopracitato principio di neutralità tecnologica) sia a specifiche guidelines aggiuntive di carattere informativo e organizzativo che tengono conto delle criticità legate all'uso degli algoritmi alla base dei *robo advice*. In particolare, l'ESMA ha posto l'attenzione su tre obbiettivi fondamentali ossia: maggiore trasparenza degli algoritmi, maggiore comprensione delle loro modalità di funzionamento da parte sia dei consumatori che delle autorità di vigilanza, maggiore chiarezza sui profili di responsabilità legati all'uso degli algoritmi. La strada intrapresa dall'ESMA sembra andare in direzione di una *robo advice governance* che, utilizzando *guidelines*, raccomandazioni e misure di *soft law*, fornisce chiarimenti e indicazioni agli intermediari finanziari a partire dalla stessa ideazione e progettazione degli algoritmi fino al loro utilizzo finale per la prestazione del servizio al cliente. L'applicazione delle *guidelines* è comunque subordinata al carattere più o meno automatizzato del servizio di consulenza, al grado di interazione umana e alla tipologia di algoritmi utilizzati. Viene pertanto rimesso all'impresa il compito di spiegare al cliente, in modo chiaro e comprensibile, le modalità di funzionamento del *robo advice*, il modello automatizzato utilizzato e le possibilità di contatto, se necessario, con un consulente umano e la precisazione che le raccomandazioni di investimento potrebbero essere basate principalmente (se non esclusivamente) sulle informazioni fornite dal cliente stesso nel questionario online. In particolare, le informazioni che le imprese che forniscono consulenza automatizzata sono obbligate a formine al cliente sono:

- una dichiarazione sulla quale viene specificata l'esistenza di un algoritmo utilizzato per raccogliere e analizzare le informazioni fornite dal cliente e per formulare, sulla base di queste, raccomandazioni di investimento e consulenza

- una spiegazione riguardo il grado di coinvolgimento umano nel servizio di consulenza e nel controllo dei servizi di investimento
- una descrizione di come l'impresa farà uso delle informazioni fornite dal cliente, per l'elaborazione di una consulenza di investimento o per la gestione di un portafoglio
- una spiegazione di come e quando lo status del cliente viene aggiornato

Un'ulteriore tema da tenere in considerazione è quello del rischio di overconfidence tipico dell'investitore, che si amplifica nel caso dell'utilizzo di un sistema automatizzato o semi-automatizzato di un servizio di consulenza. Per prevenire tale rischio, le imprese dovrebbero inserire nel questionario online anche domande riguardanti le caratteristiche e i rischi legati a particolari tipi di strumenti finanziari, al fine di impedire ai clienti la sovrastima delle proprie conoscenze in materia finanziaria.

## 3.4 *Moneyfarm*

*Moneyfarm*[15] è una Società di intermediazione mobiliare (SIM) che offre servizi di consulenza finanziaria automatizzata a livello europeo, è stata fondata nel 2011 a Cagliari da Paolo Galvani e Giovanni Daprà, in cinque anni ha raccolto oltre 22 milioni di euro di investimenti e oggi conta oltre 80 professionisti operanti nelle sedi di Londra, Milano e Cagliari. Gli investimenti pianificati e offerti della *Moneyfarm* riguardano esclusivamente gli EFT (*Exchange Trade Found*) ossia particolari tipi di fondi che replicano passivamente un indice finanziario; rispetto ai fondi comuni tradizionali, essi sono quotati in borsa, permettendo quindi una più agevole diversificazione dell'investimento, un basso costo di gestione e una maggiore liquidità. Per poter usufruire dei servizi offerti dalla *Moneyfarm* è necessaria l'iscrizione gratuita al portale e la successiva compilazione di un questionario di profilazione per identificare il livello di propensione al rischio del cliente; sulla base di ciò, *Moneyfarm* poi indirizza il cliente su un determinato tipo di portafoglio che più si adatta alle sue esigenze. I vari portafogli disponibili si differenziano:

-per livello di rischio-rendimento, attraverso un diverso mix di *asset class* (azioni, obbligazioni, materie ecc) che coprono svariate arre geografiche valutarie e settoriali;

-per numero di strumenti, a seconda dell'ammontare dell'investimento, comprendendo da un massimo di 7 fondi per investimenti sotto i 50000 euro a un massimo di 14 per investimenti superiori.

*Moneyfarm* offre anche la possibilità di creare piani di accumulo. Dopo aver versato la somma iniziale, che non ha un limite minimo di importo, è possibile effettuare ulteriori versamenti in qualsiasi momento e di qualsiasi ammontare, così come è possibile interrompere il versamento o estinguerlo senza vincoli e costi aggiuntivi. Il cliente ha inoltre la possibilità di scegliere, a parità di costo, tra un portafoglio con servizio in amministrato o in gestito. Con la prima soluzione il cliente riceve, durante l'anno da un team di esperti di *Moneyfarm*, consigli di ribilanciamento del portafoglio che il cliente è libero di accettare, rifiutare o modificare. Con il portafoglio in gestito invece il ribilanciamento sarà eseguito in automatico, senza il bisogno di autorizzazione da parte del

[15] www.moneyfarm.com

cliente. *Moneyfarm* fornisce anche un servizio di consulenza generale gratuita tramite un team di specialisti che possono essere contattatati in qualsisia momento per delucidazioni sui propri investimenti. Per quanto riguarda i rendimenti, essi generalmente nell'arco di tre anni oscillano dai 10-12% fino ai 33-35% per i fondi più rischiosi, per i costi di gestione invece sono previste commissioni su base annua che variano dall'1,25% allo 0,5% per investimenti di maggior ammontare. Non sono invece presenti costi di accesso, di transazione e di uscita. In totale i costi di *Moneyfarm* risultano essere circa la metà dei costi richiesti per l'investimento in un fondo standard. Si può affermare quindi che *Moneyfarm* ha reso di fatto accessibile a tutti il servizio di gestione patrimoniale e, a conferma della sua eccellenza tra le realtà *FinTech*, sono i numerosi premi ricevuti. Nel gennaio 2017 *Moneyfarm* ha vinto lo *Uk-Italy Business Award* riservato alle aziende italiane che più si sono distinte come esempio di eccellenza nel Regno Unito, dove *Moneyfarm* opera dal 2016. Questo riconoscimento va ad aggiungersi ai due consecutivi Sigilli d'oro ottenuti nel 2015/6 e 2016/7 da parte dell'Istituto Tedesco Qualità e Finanza come Migliore Consulente Finanziario Indipendente in Italia.

# 4. *CROWDFUNDING*

## 4.1 Caratteristiche e principali modelli

Un'altra rilevante innovazione in ambito *FinTech* è il *crowdfunding*, una particolare tecnica che permette il finanziamento (*funding*) di iniziative di vario genere (umanitarie, politiche, culturali, scientifiche, sociali, imprenditoriali ecc.) attraverso la raccolta di capitali tra la folla (*crowd*), effettuata tramite l'utilizzo di una piattaforma online. Le caratteristiche fondamentali di questa innovativa operazione sono:

- finanziamento dal basso. Il finanziamento non proviene da un soggetto specializzato, come una banca o un istituto di credito, ma dalla gente che sostiene economicamente un progetto di interesse comune, generalmente con somme non elevate e non necessariamente per motivazioni strettamente economiche
- Uso di nuove tecnologie. La raccolta di denaro avviene tramite piattaforme online che facilitano l'incontro tra domanda e offerta di finanziamenti, grazie alla possibilità di presentare progetti ai potenziali finanziatori in modo semplice, veloce e a costi contenuti
- Uso innovativo del web. Le persone interessate al finanziamento di un determinato progetto e accomunate quindi da medesimi interessi si raggruppano dando vita a delle communities che utilizzano Internet in maniera consapevole e moderna poiché non si limitano ad un utilizzo passivo delle informazioni ricevute tramite web ma partecipano attivamente alla realizzazione del progetto presentato.
- Incontro di interessi di diversa natura. Il finanziatore di un determinato progetto potrebbe essere mosso esclusivamente da interessi economici, avendo un'aspettativa di rendimento dal progetto finanziato, ma potrebbe anche essere mosso da interessi diversi (sociali, culturali, umanitari ecc.) connessi alla natura del progetto stesso.

Il *crowdfunding* si presenta quindi come un moderno strumento per finanziamenti sostenibili, grazie alla sua capacità di unire esigenze e interessi di natura diversa, sia di carattere individuale/privatistico sia collettivo/pubblicistico. Esso rientra nell'ambito della *sharing economy* e, passando dalla "*firm production*" alla "*common-based peer production*", ribalta il tradizionale rapporto tra produttore e consumatore; quest'ultimo infatti non si limita al semplice acquisto di un bene o servizio prodotto da altri ma partecipa attivamente alla sua produzione assumendosi il rischio connesso al finanziamento. Prende vita quindi una nuova figura quella del *prosumer* che rappresenta l'aggregazione in capo ad un unico soggetto delle due identità, solitamente distinte, del produttore (*producer*) e consumatore (*consumer*) di un determinato bene o servizio[16].

Esistono diverse tipologie di *crowdfunding* che si differenziano per la modalità di remunerazione prevista per il finanziatore.

- *Donation based crowdfunding*. Il finanziamento avviene tramite donazione di una somma di denaro in favore di una specifica iniziativa in genere di carattere benefico, culturale o sociale, senza ricevere nessun tipo di ricompensa
- *Reward-based crowdfunding*. A fronte dell'erogazione di una somma di denaro, i finanziatori ricevono una remunerazione non finanziaria, ossia un riconoscimento sociale o personale. Questa tipologia di *crowdfunding* presenta due varianti: la "*all or nothing*" in cui il denaro raccolto andrà a finanziare il progetto solo se raggiungerà la cifra inizialmente determinata; la "*keep it all*" in cui le somme raccolte finanzieranno il progetto a prescindere dal raggiungimento o meno dell'ammontare fissato
- *Lending-based crowdfunding*. Imprese o individui privati ottengono fondi dalla gente sotto forma di contratti di prestito. Ne esistono due varianti: il *consumer lending*, in cui individui privati (*consumer-to-consumer*) o istituzioni (*business-to-consumer*) prestano fondi ad altri privati, di solito senza alcun tipo di garanzia da parte dei mutuatari; il *business lending*, in cui individui privati (*consumer-to-business*) o istituzioni (*business-to-business*) prestano alle imprese, solitamente con garanzie.
- *Invoice trading crowdfunding*. Le imprese, tramite la piattaforma online, cedono fatture o crediti impagati, singolarmente o raggruppati sotto forma di pacchetti, ad un gruppo di investitori che di solito sono istituzioni o soggetti specializzati e il corrispettivo viene stabilito tramite aste online.
- *Royalty based* o *profit-sharing crowdfunding*. Il finanziamento di un'iniziativa imprenditoriale viene ricompensata con le partecipazioni ai futuri profitti della stessa attraverso strumenti contrattuali come le *silent partnership* che non attribuiscono il titolo di socio.
- *Investment based crowdfunding*. Particolari tipi di imprese emettono azioni o obbligazioni e li offrono al pubblico tramite una piattaforma online. Rientra in questa categoria l'*equity crowdfunding* in cui i finanziatori acquistano sulla piattaforma azioni dell'impresa diventandone soci a tutti gli effetti e quindi esposti all'andamento della stessa e al rischio di impresa.
- Modelli ibridi di *crowdfunding*. Presentano delle caratteristiche comuni a due o più dei modelli precedenti.

[16] A. Troisi, "*Crowdfunding e mercato creditizio: profili regolamentari*", 2014

- *Do It Yourself* (DIY) o *crowdfunding* indipendente. Una nuova forma di *crowdfunding* che si sta sviluppando negli ultimi anni e che consiste nel creare autonomamente una campagna di raccolta fondi, promuovendola al pubblico attraverso un proprio sito web. Tale tipologia di *crowdfunding* risulta particolarmente utile per quei progetti che non riescono a trovare spazio in una piattaforma specializzata.

A livello normativo le diverse tipologie di ricompensa relative ai vari modelli di *crowdfunding* comportano l'applicazione di una disciplina differente. Per il *donation-based* e il *reward-based crowdfunding* per esempio si applicano le regole dettate per i corrispondenti istituti civilistici; per l'*equity crowdfunding* è prevista in Italia una specifica disciplina che si differenzia sia da quella applicata agli investimenti finanziari sia da quella inerente alle partecipazioni nelle società commerciali.

## 4.2 L'*equity crowdfunding*: potenzialità e rischi

Il modello di *crowdfunding* di maggiore interesse per le Autorità europee è l'*equity crowdfunding* per la sua valenza di efficace strumento che, supportando l'affermazione di nuove imprese e la ricerca di nuovi investimenti, può contribuire notevolmente alla ripresa economica sfruttando le potenzialità del web. L'*equity crowdfunding* rappresenta infatti un'efficace fonte di finanziamento alternativa che assume particolare rilevanza soprattutto per le imprese che tipicamente sono escluse dal mercato del credito per l'assenza di asset tangibili da porre a garanzia oppure semplicemente perché troppo piccole e rischiose. Per quanto riguarda gli investitori, tra le opportunità principali che l'*equity crowdfunding* offre loro, abbiamo sicuramente l'elevato potenziale di rendimento; le persone fisiche possono godere di una detrazione fiscale pari al 30% di quanto investito e le persone giuridiche di una deduzione dei ricavi pari al 30% dell'investimento. A fronte di tali benefici vi sono però anche diversi rischi da tenere in considerazione come la perdita di capitale nel caso, non improbabile, in cui il progetto della *start-up* non vada a buon fine; per tale motivo è consigliabile investire somme di cui si possa sostenere la perdita e differenziare il più possibile gli investimenti. Va considerato poi il divieto di distribuzione di utili (secondo la normativa vigente in Italia in materia di *equity crowdfunding*) per tutto il periodo in cui la società mantiene i requisiti di *start-up* innovativa e cioè per un massimo di 4 anni dall'iscrizione nella sezione speciale del registro delle imprese, per cui gli eventuali utili, in questo caso, devono essere reinvestiti nella società. Ulteriore rischio riguarda il fatto che questi strumenti finanziari risultano molto illiquidi non potendo essere negoziati su mercati secondari.

I primi interventi regolamentari a livello europeo sono stati apportati dall'ESMA con la pubblicazione a settembre 2012 di un'Avvertenza rivolta soprattutto agli investitori retail in cui illustrava le possibili insidie dell'*equity crowdfunding*[17]. Ad essa è seguita poi la pubblicazione nel dicembre 2014 di un Opinion per le autorità Nazionali e una *Advice* per le Istituzioni europee, con la finalità di realizzare una maggiore convergenza e razionalizzazione regolamentare e di vigilanza tra i gli Stati membri. La Commissione europea invece ha adottato una comunicazione del 2014 a cui è susseguita

[17] ESMA, "*Avvertenza per gli investitori relativa alle insidie degli investimenti online*", 2012

la formazione di gruppi di studio tra esperti del settore e la pubblicazione di una guida[18] e altri documenti di approfondimento[19]. Gli interventi delle Autorità europee fino ad ora risultano per lo più di carattere esplorativo e conoscitivo del fenomeno, per cui, in assenza di una regolamentazione uniforme a livello europeo, gli Stati membri si sono dotati di regimi domestici che, seppure somiglianti nell'approccio generale, presentano notevoli differenze nella progettazione e attuazione delle regole, determinando una forte frammentazione del mercato europeo. In generale i regimi adottati dagli Stati membri presentano il duplice obbiettivo di promuovere il *crowdfunding* come nuova fonte di finanziamento per le piccole imprese, garantendo al contempo la difesa degli investitori dai possibili rischi che esso comporta.

### 4.2.1 L'*equity crowdfunding*: la normativa italiana

L'Italia è stata il primo paese europeo a dotarsi di una displica specifica in materia di *equity crowdfunding* con l'emanazione nel 2013 da parte della Consob del Regolamento N.18592/2013. Quest'ultimo riservava le operazioni di *equity crowdfunding* esclusivamente alle *start-up* innovative, ma successivamente con il d.l. n. 3/2015, il cosiddetto *Investment Compact*, ha esteso tale forma di finanziamento anche alle piccole e medie imprese innovative, agli organismi di investimento collettivo del risparmio e alle società di capitali che investono prevalentemente in *start-up* e PMI innovative. Un ulteriore estensione si è avuta con il d.l. n 50/2017, Decreto Correttivo, che ha aperto l'utilizzo di portali online per la raccolta di capitale a tutte le PMI, indipendentemente dal carattere innovativo dell'attività svolta, agli organismi di investimento collettivo del risparmio e alle società di capitali che investono in PMI. La Consob, a seguito del citato decreto correttivo e del decreto legislativo di attuazione della direttiva MiFID 2, ha avviato una consultazione con il mercato finanziario per una revisione del precedente regolamento del 2013. Le principali modifiche riguardano:

- L'obbligo per i gestori dei portali online di aderire ad un sistema di indennizzo a tutela degli investitori o, alternativamente, di stipulare un'assicurazione a copertura della responsabilità civile per i danni derivanti dalla negligenza professionale
- L'espressa regolamentazione del procedimento di decadenza e cancellazione e l'introduzione della rinuncia volontaria all'autorizzazione
- Il rafforzamento degli obblighi in tema di conflitto di interesse per i gestori autorizzati ai quali è vietato pubblicare sui propri portali offerte di strumenti finanziari di propria emissione o emessi da soggetti appartenenti al medesimo gruppo
- La possibilità di recesso e di co-vendita per tutte le tipologie societarie entro un limite temporale di solito di tre anni
- La necessaria sottoscrizione da parte di investitori qualificati, ai fini del perfezionamento dell'offerta, di una quota pari ad almeno il 5% degli strumenti finanziari offerti

Tutti i richiamati interventi correttivi sono funzionali al raggiungimento di alcuni obbiettivi fondamentali: ampliare le tipologie di società finanziabili e le gli strumenti oggetto di offerta,

[18] Commissione europea, "*Il crowdfunding cos'è? Una guida per le piccole e medie imprese*", 2015
[19] Commissione europea, "*Crowdfunding in the EU Capital Markets Union*", 2016

semplificare le condizioni di accesso, ridurre i costi e garantire la qualità e l'affidabilità del servizio. Particolare attenzione è posta alla tutela degli acquirenti poiché, mentre un tempo questi appartenevano ad una limitata élite di benestanti ben informati e consapevoli, più di recente la partecipazione ai mercati finanziari ha interessato fasce sempre più ampie della popolazione che spesso non hanno un'adeguata cultura finanziaria, né sono sufficientemente informate riguardo la portata delle operazioni finanziare.

### 4.2.2 L'*equity crowdfunding*: presidi a tutela dei risparmiatori

L'attività di gestione dei portali online per l'*equity crowdfunding* è riservata a due tipologie di soggetti: le imprese di investimento e le banche autorizzate ai relativi servizi di investimento (c.d. gestori di diritto) e i soggetti iscritti in un apposito registro tenuto dalla CONSOB (c.d. gestori autorizzati); questi ultimi sono però obbligati a trasmettere gli ordini ricevuti a banche o imprese di investimento. La gestione dei portali online da parte dei gestori di diritto è sottoposta alle regole previste dal TUF per la prestazione dei servizi di investimento, i gestori autorizzati invece sono sottoposti alle regole previste dal citato regolamento della CONSOB.

L'*equity crowdfunding* ha tutte le caratteristiche di un investimento di natura finanziaria (impiego di capitali, aspettativa di rendimento, assunzione di rischio) e per tale motivo è indispensabile porre dei presidi a tutela dell'investitore in modo tale che questi possa avere le informazioni necessarie per compiere delle scelte di investimento consapevoli. Per le modalità di investimento finanziario tradizionali lo strumento principale a tutela dell'investitore è il prospetto informativo, documento che contiene le principali informazioni riguardanti l'investimento proposto, il soggetto proponente e il rischio dell'operazione. La relativa disciplina contenuta nel TUF si articola in una serie di obblighi molto stringenti per le società offerenti, relativi alla tipologia, alla quantità e la qualità delle informazioni da inserire nel prospetto e le tempistiche e le modalità di pubblicazione dello stesso. Le operazioni di *equity crowdfunding* sono invece esenti dalle disposizioni relative al prospetto informativo in quanto il legislatore, per incentivare l'utilizzo di tale strumento innovativo, ha voluto semplificare la posizione delle imprese senza tralasciare però la tutela dei risparmiatori. Per fare ciò ha organizzato un percorso, per l'utilizzo delle piattaforme online diviso in varie fasi che prevedono particolari obblighi di comportamento e di trasparenza per gli offerenti, i gestori e i risparmiatori.

Nella prima fase la società offerente fornisce al gestore le informazioni riguardanti il progetto proposto, la natura dell'investimento, la tipologia di strumenti offerti e il rischio connesso. Nella seconda fase è il gestore a dover fornire informazioni riguardo il tipo di attività svolta, le modalità di selezione delle offerte, i costi a carico degli investitori, le misure adottate per ridurre i rischi di frode e per gestire i conflitti di interesse. Il gestore è inoltre tenuto a fornire una spiegazione al cliente riguardo le caratteristiche generali degli investimenti finanziari effettuati tramite portali online e i relativi rischi a ad essi legati, in particolare: il rischio di perdita dell'intero capitale, il rischio di illiquidità, l'eventuale divieto di distribuzione degli utili, il diritto di recesso e di co-vendita. Le ultime informazioni che il gestore deve fornire al cliente sono quelle inerenti alla singola offerta; esse devono essere rese disponibili agli investitori in maniera dettagliata, chiara, comprensibile e tale da consentire la comparabilità con le altre offerte svolte sullo stesso portale. La terza fase è costituita dal procedimento di adesione all'offerta e prevede particolari obblighi per i risparmiatori

che sono tenuti a: prendere visione delle informazioni di *investor education* presenti sul sito della CONSOB e di quelle relative alla singola offerta, presenti sulla piattaforma del gestore; fornire informazioni in merito alla propria conoscenza ed esperienza in ambito finanziario, per comprendere le caratteristiche e i rischi degli strumenti oggetto dell'offerta; dichiarare di essere in grado di sostenere economicamente l'eventuale perdita dell'itero ammontare investito. A questo punto il gestore dovrà assicurare l'accesso alla sezione del portale dedicata all'adesione all'offerta esclusivamente a quegli investitori che hanno eseguito correttamente la procedura appena descritta. Infine, le ultime modifiche al Regolamento hanno introdotto la possibilità, per i gestori autorizzati che presentino determinati requisiti organizzativi, di effettuare la valutazione di appropriatezza (*opt-in*). Essa consiste nel verificare che il cliente che abbia inoltrato la richiesta di adesione all'offerta abbia un livello di esperienza sufficiente per comprendere le caratteristiche e i rischi che l'investimento comporta sulla base delle informazioni da lui stesso fornite. Se la valutazione di appropriatezza non viene svolta dal gestore dovrà necessariamente essere effettuata dalle banche o dalle imprese di investimento che hanno ricevuto l'ordine di acquisto dal gestore; questo nel caso in cui gli ordini abbiano un controvalore: superiore ai 500 € per singolo ordine e ai 1000 € per ordini complessivi annuali se impartiti da persone fisiche; superiore ai 5000 € per singolo ordine e ai 10000 € per ordini complessivi annuali se impartiti da persone giuridiche. Successivamente il perfezionamento dell'operazione di investimento deve essere svolto in via esclusiva dalle banche o imprese di investimento, che dovranno poi provvedere all'apertura di un conto indisponibile intestato all'offerente in cui far confluire le somme raccolte. Tali soggetti professionali sono dotati di apparati organizzativi e procedurali tali da garantire elevati standard di affidabilità, correttezza e trasparenza, a garanzia della posizione dei risparmiatori. A conclusione del processo è previsto che, per ogni singola offerta, almeno il 5% degli strumenti finanziari offerti venga sottoscritto da investitori professionali. Tale pratica può far aumentare il grado di affidamento che l'investitore retail pone sulla proposta di investimento in quanto gli permette di conoscere i soggetti professionali sottoscrittori e di consultare la valutazione tecnica sulla fattibilità e qualità del progetto imprenditoriale svolta da tali soggetti.

## 4.3 *Startsup*

*Startsup*[20] è stata la prima piattaforma di *equity crowdfunding* in Italia ad aver ottenuto dalla Consob l'iscrizione al registro dei portali online per la raccolta di capitale di rischio da parte di *start-up* e PMI innovative. La società è stata fondata a Livorno nel luglio 2013 da Carlo Piras, Matteo Piras e Alessandro Scutti e ad oggi ha finanziato progetti per un volume superiore ai 2,9 milioni di euro, posizionandosi come prima piattaforma in Italia con 347 investitori attivi (306 persone fisiche e 41 persone giuridiche). *Startsup* offre alle *start-up* e le PMI innovative di raccogliere capitale di rischio, pubblicando su un portale online il proprio progetto, per il quale si richiede il finanziamento previa analisi (da parte di un team di professionisti di *Startsup*) del progetto stesso e della presenza dei requisiti necessari per la pubblicazione sul portale. In caso di esito positivo dell'operazione qualora cioè venga raccolto l'ammontare di capitale richiesto, l'operazione viene conclusa e a *Startsup* è riconosciuto un compenso su base annuale dell'ammontare raccolto. La società inoltre supporta le

[20] www.startsup.it

aziende sia durante le fasi di raccolta di capitale che di sviluppo e gestione del progetto. Per quanto riguarda gli investitori invece, le modalità di utilizzo *Startsup* prevedono passaggi molto semplici; dopo la registrazione al portale, l'investitore è chiamato a rispondere ad un questionario per dimostrare di essere consapevole dell'azione di investimento che sta per compiere, comunica poi la cifra che intende investire e, se il progetto va a buon fine, diventa a tutti gli effetti comproprietario pro quota dell'impresa finanziata. Le campagne di offerta hanno una durata molto variabile che va da pochi giorni fino a molti mesi, spesso con estensioni del periodo utile. In genere l'estensione della scadenza viene decisa o per terminare la raccolta di una campagna molto vicina al target o per dare più tempo agli investitori nel caso di campagne partite con poche adesioni. Prima dell'apertura ufficiale della campagna di solito viene effettuata un'attività di pre-marketing presso un selezionato pubblico di possibili investitori in modo da avere già un certo numero di sottoscrittori informati e pronti al momento della pubblicazione ufficiale sul portale. La *mission* di *Startsup* è quella di promuovere e valorizzare l'innovazione italiana, proporre progetti di "*new economy*" soprattutto se in grado di fornire un servizio utile per la collettività e sostenere le aziende più meritevoli e innovative, capaci di conquistare i mercati.

## 4.4 *Invoice trading crowdfunding*

Per *invoice financing* (o *invoice trading*) si intende l'insieme delle modalità attraverso cui le piattaforme specializzate consentono alle imprese di monetizzare le fatture emesse e non ancora scadute, attraverso la cessione ad investitori online, senza così dover attendere il pagamento da parte del cliente. Questo permette alle imprese (soprattutto PMI) di ottimizzare la gestione del capitale circolante, di proteggere il portafoglio crediti dai mancati pagamenti e migliorare così la propria solidità finanziaria. La cessione delle fatture avviene online attraverso le piattaforme ed il modello di business del settore è il seguente: l'azienda interessata all'anticipo di una fattura inviata ad un'altra società privata presenta la propria richiesta ad una piattaforma di *invoice trading*; il portale valuterà le proposte ricevute sulla base di alcuni indicatori (come il merito creditizio) relativi a tutti gli operatori coinvolti e attribuirà un *rating*, incrociando i dati a disposizione con quelli presenti nelle banche dati di alcuni *provider*; una volta accettata, la fattura viene pubblicata sulla piattaforma di *invoice trading*. A questo punto vi sono tre differenti meccanismi di acquisto per gli investitori[21]: asta al rialzo, offerta competitiva o acquisto diretto da parte della piattaforma e cartolarizzazione delle stesse tramite asset *backed securities*. L'investitore che compra la fattura deve anticipare all'azienda un importo pari all'85-90% del corrispettivo, mentre il saldo sarà liquidato alla scadenza.

Lo sviluppo di queste piattaforme ha subito una forte accelerazione a partire dal 2008 quando, con l'acuirsi della crisi economica, le dilazioni nei tempi di pagamento da parte delle imprese da un lato e la contrazione delle erogazioni di prestiti da parte degli istituti bancari dall'altro, hanno portato a un rinnovato interesse delle imprese verso le forme di finanziamento alternative. Questo scenario, unito alla crescente digitalizzazione della contabilità, ha creato l'opportunità per lo sviluppo delle piattaforme online di *invoice trading* in grado di connettere direttamente imprese ed investitori,

[21] Politecnico di Milano, "*2° Report italiano sul Crowdinvesting*", 2017

disintermediando così il settore bancario. In genere ricorrono all'*invoice trading* le PMI con difficoltà di accesso al classico canale bancario e che sono disposte a pagare un tasso di interesse non sempre vantaggioso a fronte dei benefici legati a questa tipologia di *crowdfunding*. Quest'ultima garantisce infatti rapidità nell'erogazione della liquidità per finanziare il capitale circolante senza bisogno di garanzie e senza segnalazioni alla Centrale Rischi. Come emerge dalla ricerca dell'Università di Cambridge, l'*invoice trading* è il segmento *FinTech* dalla crescita più rapida in Europa: tra il 2014 ed il 2015 il mercato europeo è balzato da un volume d'affari di 7 milioni di euro a 81,6, con un aumento percentuale pari all'877%. In testa alla classifica per giro d'affari troviamo Belgio, Francia e Danimarca. In Italia, sebbene il mercato dell'*invoice trading* sia nato solo recentemente, si è dimostrato tra i più promettenti d'Europa, grazie anche a condizioni di mercato favorevoli per il suo sviluppo.

L'istituto giuridico italiano alla base dell'*invoice trading* è la cessione dei crediti, la cui disciplina si trova negli artt. 1260 ss. del Codice Civile, i quali statuiscono che «il creditore può trasferire a titolo oneroso o gratuito il suo credito, anche senza il consenso del debitore, purché il credito non abbia carattere strettamente personale o il trasferimento non sia vietato dalla legge». Nella sostanza si tratta di un accordo tramite cui il soggetto cedente trasferisce al soggetto cessionario il suo credito verso un debitore. La cessione del credito può essere effettuata *pro-soluto* oppure *pro-solvendo*. Nel primo caso il cedente non garantisce al cessionario la solvibilità del debitore ma solo l'esistenza e la validità del credito, il rischio di insolvenza viene trasferito insieme al credito ed il cessionario non può esercitare alcuna azione di regresso verso il cedente. Nella cessione *pro-solvendo* invece, il cedente risponde dell'eventuale insolvenza del debitore e pertanto potrebbe subire un'azione di regresso da parte del cessionario. Si tratta di un'operazione comunemente offerta dalle società specializzate nel factoring o da istituti bancari ma la digitalizzazione e lo sviluppo di portali dedicati sta portando ad una profonda trasformazione nel settore.

Come già detto in precedenza, la possibilità di cedere crediti commerciali a titolo definitivo costituisce un'esigenza particolarmente stringente in sistemi produttivi dove, a fronte di tempi di pagamento estremamente lunghi, si sperimenta anche una contrazione del tradizionale credito bancario. Da questo punto di vista l'Italia è storicamente un terreno fertile in quanto nonostante un piccolo miglioramento nel 2017, le imprese italiane pagano a 52 giorni quando la media europea è 24 giorni (Germania 19 giorni, Regno Unito 26). Più gravi i ritardi della pubblica amministrazione dove si registra in Italia una media a 95 giorni contro i 41 a livello europeo. Ai ritardi nei tempi di pagamento dobbiamo sommare le difficoltà del sistema bancario nazionale, caratterizzato da un NPL (*Non Performing Loans*) lordo pari al 16,4% dei prestiti totali, tre volte più elevato di quello spagnolo e sette volte di quello tedesco e tale percentuale è destinata ad aumentare. L'aumento dei crediti in sofferenza, unito ai requisiti sempre più stringenti in termini di capitale, ha portato le banche a ridurre i rischi imponendo condizioni più impegnative per l'accettazione delle domande di finanziamento e implicando così una diminuzione costante delle erogazioni. Le condizioni sopra descritte hanno permesso al settore dell'*invoice trading* di crescere con percentuali a doppia cifra raggiungendo oggi un valore pari a 88,5 milioni di euro, circa 8 volte maggiore di quanto risultava un anno fa. Il modello dell'*invoice trading* sta sempre più convincendo imprese ed imprenditori e si candida a diventare uno dei canali principali dell'*alternative finance* perché, da un lato, garantisce l'anticipo di cassa immediato e dall'altro l'assicurazione sul mancato pagamento del proprio credito commerciale.

## 4.5 *Workinvoice*

*Workinvoice*[22] è una *start-up* innovativa fondata nel dicembre del 2014 a Milano da Matteo Tarroni, Fabio Bolognini, Ettore Decio e Luca Spampinato. Si tratta di un portale su cui le aziende, soprattutto di piccola e media dimensione, possono vendere all'asta le proprie fatture *pro-soluto* (ovvero senza dover rispondere delle eventuali inadempienze da parte dei debitori) ricevendo liquidità immediata e gli investitori possono acquisirle, mirando a rendimenti potenzialmente più vantaggiosi rispetto a quelli ottenibili da altri asset di breve termine. La piattaforma si propone come un intermediario tra le PMI e gli investitori in quanto seleziona le aziende che vogliono vendere i propri crediti, controlla che le transazioni esistano realmente e valuta il *rating* del debitore, ma non agisce come finanziatore diretto.

Il cedente, una volta iscritto al portale, inserisce le fatture che vuole scontare insieme ad un valore minimo che vuole ottenere. *Workinvoice*, attraverso il suo modello di analisi, elabora poi per ogni fornitore e per i suoi clienti un "*WIT Score*" che gli consente di sintetizzare in un unico indice: le informazioni elaborate da terze parti (ad esempio *credit rating agency* come *ModeFinance*, la quale fornisce a *Workinvoice* un giudizio sul merito di credito dell'azienda quasi in tempo reale); informazioni finanziarie pubbliche (ottenute dai bilanci); informazioni specifiche sul rapporto di fornitura (rilevate da documenti e questionari); dati storici generati dalle transazioni sul mercato. Il modello seleziona poi, sulla base dello *scoring*, le coppie di fornitori/debitori che necessitano di ulteriori indagini o di specifiche approvazioni da parte della *Risk Unit*, prima di essere ammesse sul mercato.

Una volta a settimana si apre l'asta sulle fatture inserite fino a quel momento; il miglior offerente, o più spesso chi raggiunge il prezzo "preferito" indicato dall'azienda cedente, si aggiudica il credito ed effettua, direttamente sul conto corrente dell'impresa, un versamento a titolo di acconto pari al 90% della somma dovuta. Quando il cliente dell'azienda cedente paga la fattura viene poi accreditata la parte rimanente, alla quale va sottratto uno sconto proporzionale al periodo trascorso tra acconto e incasso ed al rischio del credito (tipicamente il saldo è tra l'8-9% della fattura). Il portale *Workinvoice*.it addebita una commissione pari a 0,4% per fatture con scadenza fino a 60 giorni, 0,65% da 61 a 90 giorni e 0,9% oltre 90 giorni mentre, dal lato degli investitori, il 20% del profitto generato. Inoltre, è prevista una *fee* di adesione iniziale di 450 euro. Il vantaggio fondamentale per l'azienda è il tempo di incasso: c'è la possibilità di completare l'intero processo, e quindi di ricevere il denaro, in 5 giorni lavorativi, mentre una banca impiega qualche settimana.

Al momento la piattaforma non prevede un fondo di garanzia per eventuali *default*, ma ha attivato un accordo con una società di recupero crediti per supportare i clienti qualora dovesse verificarsi un qualche evento sfavorevole. Ultimamente *Workinvoice* ha avviato inoltre collaborazioni con compagnie assicurative che si sono rese disponibili a coprire i rischi di mancato pagamento delle fatture. In questa direzione va l'accordo con *Wills Towers Watson*, multinazionale del *brokeraggio* assicurativo e della consulenza sui rischi (anche di credito). Se per caso la fattura non venisse incassata, l'impresa che ha ricevuto il credito non riceverà il saldo e concorrerà alla perdita in misura ridotta, tipicamente compresa tra 7% e 8%. Questa è una differenza importante rispetto all'anticipo

[22] www.workinvoice.it

fatture praticato tipicamente da una banca, la quale non si accolla il rischio di insolvenza ma andrà a rivalersi sull'impresa.

Le aziende finanziate operano in tutti i settori e sono molto diverse per dimensioni, con ricavi che vanno dai 500mila euro ai 120 milioni. Tra i requisiti richiesti da *Workinvoice* per accedere alla piattaforma troviamo: l'impresa deve essere una società di capitali, S.p.a o S.r.l con fatturato superiore a 100mila euro; le fatture non devono essere scadute e devono avere un importo unitario di almeno 10.000 euro; le fatture devono essere emesse verso S.r.l o S.p.a private (non pubbliche) con un fatturato di almeno 10 milioni di euro. In media le aziende cedono fatture con scadenze comprese tra i 25 e 140 giorni ed importi di 70mila euro, ma con minimi di 10mila e massimi di 250mila. Ad oggi gli investitori attivi sono 31 di cui il 90% sono istituzionali. L'investimento minimo richiesto per accedere alla piattaforma è di 50mila euro, inoltre la singola fattura non può essere suddivisa tra più investitori ma va acquistata in toto, e questo, in ottica di diversificazione del rischio, rende il business senz'altro più adatto ad investitori istituzionali. Si tratta in genere di piccoli fondi chiusi esteri specializzati negli investimenti in fatture su piattaforme web a livello internazionale e in genere hanno tra i 30 ed i 50 milioni di euro di *asset* in gestione; sono presenti anche fondi aperti *Ucits* e veicoli di cartolarizzazione dedicati all'acquisto di questo tipo di crediti che vengono poi cartolarizzati. I rendimenti, al netto di eventuali *default*, hanno dei tassi medi pari al 7-8%.

## 4.6 *Royalty crowdfunding*

Il *royalty-based*, o semplicemente *royalty*, è un tipo di *crowdfunding* in cui si finanzia una determinata iniziativa ricevendo in cambio una parte dei profitti. In pratica chi lancia una campagna di *crowdfunding* di questo tipo offre delle quote dei guadagni futuri del progetto per il quale richiede il finanziamento. Consiste quindi nella vendita da parte del proprietario del business e nel contestuale acquisto da parte dell'investitore, di una parte dei ricavi che saranno generati in futuro dall'attività economica finanziata. Gli investitori possono, quindi, ottenere un reddito regolare garantito dalle vendite ed al contempo i proprietari del business, restandone i soli titolari, mantengono interamente il controllo sull'andamento dell'attività. Tuttavia, a livello pratico le *royalties* devono essere detratte dal fatturato e, pertanto, aggiungono costi al business. Per questa ragione il *royalty crowdfunding* è principalmente consigliabile a tutte quelle attività che hanno alti margini di profitto.

Nel *royalty crowdfunding* viene offerta una ricompensa di natura monetaria che consiste in una condivisione dei profitti o dei ricavi associati all'investimento, ma senza alcun titolo di proprietà sul progetto né di rimborso del capitale. La disciplina del modello è quindi riferibile alle norme sull'associazione in partecipazione (artt. 2549 ss. c.c.3), nella quale chi finanzia partecipa in quota agli utili generati. Infatti, il finanziatore, in questo particolare modello di *crowdfunding*, percepisce, sulla base dell'importo investito, delle royalties che possono riguardare ad esempio: diritti di autore, diritti di proprietà intellettuale, brevetti, licenze, marchi registrati e così via. Nella sostanza, si tratta di un'associazione agli utili e alle perdite, nei limiti del conferimento effettuato dall'investitore, che prevede l'associazione di un numero aperto ed indeterminato di investitori. L'associato in partecipazione non ha i diritti del socio ma ha poteri di controllo che devono essere definiti contrattualmente e che in genere si limitano all'analisi del rendiconto. L'aspetto più problematico è

l'indeducibilità fiscale degli utili attribuiti agli associati in partecipazione, che finisce per pesare notevolmente sulla redditività netta del progetto imprenditoriale.

## 4.7 *BandBakers*

*BandBackers* è una piattaforma italiana di *royalty crowdfunding* fondata da Roberto Calabrò, Salvatore Martino, Valeria Barile e Lorenzo Lucherini attiva dalla fine del 2015. *BandBackers* opera come *Social Music Label*, ovvero un'etichetta discografica che viene finanziata dai fan dei vari progetti e dagli appassionati attraverso il *crowdfunding*[23]. Si presenta quindi come uno strumento di sharing economy, che opera sul mercato discografico e consente di rendere sostenibili le carriere degli artisti, fornendo fondi per produrre e promuovere la loro musica. La particolarità della piattaforma risiede nell'utilizzo del *royalty crowdfunding* per far partecipare i *backer* (micro-finanziatori) agli utili del progetto che finanziano. L'immissione di un progetto sulla piattaforma avviene attraverso più fasi: analisi del progetto per valutarne i punti di forza, le debolezze e il rientro economico previsto; analisi del *feedback* del *network* del progetto attraverso la collezione di Like; allo scattare del 100esimo Like la campagna si trasforma in una raccolta fondi effettiva per finanziare il progetto e la band si presenterà con un video in cui racconterà se stessa e spiegherà come utilizzerà la cifra raccolta; dopo due mesi di raccolta fondi al raggiungimento del *Goal* verrà fatto il prelievo sui conti dei *backers* per la collezione degli investimenti. Il *backer* riceverà un corrispettivo sulla base dell'importo che ha finanziato, in sostanza parteciperà agli utili generati dall'artista/dalla band. Tendenzialmente *BandBackers* riesce a garantire un rendimento sull'investimento che si aggira intorno al 20%, al quale si aggiunge un'altra variabile dello 0-20% calcolata in base alla viralità generata della pubblicità fatta dal *backer*. *BandBackers* ricorre alla raccolta fondi nella modalità *all-or-nothing* (in quanto rappresenta l'orientamento prevalente tra i *player* del settore) senza però consentire l'over*funding*. Quanto ai guadagni della società la *fee* richiesta dalla piattaforma ammonta al 10% dell'importo raccolto tramite la campagna di *crowdfunding*. Oltre a questo, però, *BandBackers*, divide le *royalty* con i micro-finanziatori e, in aggiunta, in quanto il portale è anche un'etichetta discografica iscritta in SIAE e in *Soundreef*, guadagna anche una percentuale sulle vendite e sui live. In pratica, in qualità di *Social Musci Label*, il portale partecipa a tutti i vari flussi economici che l'attività di un artista genera. Attualmente il pagamento delle *royalty* ai sostenitori, sulla base dei termini d'uso, è definito, in ambito giuridico, come procacciamento d'affari. Per far questo *BandBackers* restituisce ai micro-finanziatori parte degli utili generati, sino al raggiungimento della cifra sottoscritta, attraverso la restituzione con la ritenuta d'acconto. Dal lato degli artisti, invece, il rapporto con *BandBackers* è disciplinato tramite contratti discografici.

Gli iscritti sono circa 500, con una conversione tra utenti registrati e *backer* dell'80%. Il *backing* medio (ossia l'investimento medio) si aggira intorno a € 40 e, in un anno, sono stati transati circa € 20.000. In quest'ultimo valore fornito sono inclusi anche gli importi che non sono, poi, stati effettivamente erogati, in quanto non tutte le campagne hanno raggiunto l'importo minimo da finanziare per farle andare a buon fine (caratteristica tipica del modello *all-or-nothing*, di cui si è detto prima).

[23] www.bandbackers.com

## 4.8 *Donation* e *reward crowdfunding*

La prima forma originaria di *crowdfunding*, che ha dato il via al fenomeno, è quella del donation-*based* ossia, come già detto, un modello tipico di donazione in cui si devolve altruisticamente il proprio denaro a sostegno di una causa specifica non ricevendo in cambio alcuna ricompensa o, al massimo, ricompense simboliche, spesso intangibili. Il funzionamento del modello è piuttosto semplice. I donatori, che in gergo vengono chiamati *backer*, possono visualizzare le campagne di raccolta fondi all'interno di specifiche piattaforme online (i cosiddetti portali di donation *crowdfunding*), fra i progetti disponibili essi possono scegliere quale oppure quali sostenere. Non è, per altro, insolito trovare siti Internet rivolti alla raccolta di denaro per un'unica finalità: è il caso di *#UnAiutoSubito*, dedicato al supporto delle popolazioni terremotate del Centro Italia. La disciplina giuridica delle elargizioni tramite donation *crowdfunding*, in generale, fa riferimento al Codice Civile italiano, al cui interno le donazioni sono definite come contratti attraverso i quali, per spirito di liberalità, una parte arricchisce un'altra andando a disporre a favore di questa di un suo diritto oppure andando ad assumere una obbligazione verso la stessa. La donazione è, quindi, un atto 'liberale'. Chi la effettua non si aspetta alcun beneficio materiale in cambio e tanto meno alcun tipo di ricompensa, se non simbolica. Piuttosto vi è una esplicita volontà di dare il proprio contributo allo scopo di partecipare alla realizzazione di progetti rivolti a finalità sociali, culturali, ambientali, assistenziali e così via. Spesso sono motivazioni filantropiche a spingere i benefattori a offrire le somme necessarie al completamento delle campagne; sono difatti le organizzazioni no-profit le realtà che ricorrono principalmente al modello *donation-based*, fra tutte le tipologie di *crowdfunding* esistenti. Per di più le donazioni verso organismi costituiti in forma di Onlus (Organizzazioni non lucrative di utilità sociale), possono consentire ai donatori di godere di alcune agevolazioni fiscali per dedurre le somme versate all'ente, proprio in virtù delle caratteristiche stesse dell'istituto dell'Onlus.

Il reward *crowdfunding*, invece, consiste nella raccolta di finanziamenti via internet a fronte di una ricompensa proporzionale all'importo investito dal sostenitore. Si tratta di una pratica che ha origini molto remote, tradizionalmente si identifica la nascita di questo modello di *crowdfunding* con la costruzione della Statua della Libertà: nel 1880 il magnate dell'editoria Joseph Pulitzer lanciò una pubblica sottoscrizione tramite i suoi giornali per raccogliere i 250.000 dollari che servivano per completare il basamento, come ricompensa offrì la menzione dei sottoscrittori che avrebbero contribuito.

Oggi, sulla base della tipologia di ricompensa, è possibile classificare i vari tipi di *reward crowdfunding* in diverse categorie omogenee (ciascuna soggetta ad una specifica disciplina dell'ordinamento giuridico italiano) tra cui:

- Regalo o riconoscimento. Il proponente offre ai finanziatori una menzione o un piccolo regalo di modico valore. Il tipo di *crowdfunding* in esame rientra nel paradigma della donazione modale, prevista e regolamentata dall'art. 793 del Codice Civile. La ricompensa è un obbligo che grava sul donatario ed il cui eventuale inadempimento potrebbe avere un effetto decisamente deleterio: la revoca della donazione. È dunque necessario che chi propone una reward *crowdfunding* di questo tipo accantoni sufficienti risorse per eseguire quanto promesso.

- Pre-ordine. Prevede la possibilità di prenotare un bene non ancora prodotto, versando anticipatamente o promettendo di versarne il prezzo. In genere chi finanzia ha un ruolo determinante anche nello stabilire le caratteristiche del futuro prodotto/servizio. Dal punto di vista legale si tratta a tutti gli effetti di una compravendita con la particolarità che il bene non è ancora esistente e che l'acquisto verrà perfezionato soltanto se si raggiunge l'importo necessario per andare in produzione. A tal proposito è frequente il modello "*all or nothing*". Laddove il pagamento venga effettuato all'ordine il denaro viene conservato in *escrow* ed utilizzato solo dopo il raggiungimento dell'obiettivo. Trattandosi a tutti gli effetti di una compravendita questo tipo di *reward crowdfunding* è sottoposto alla normativa sull'*e-commerce* ed alla protezione dei consumatori nei contratti a distanza.

## 4.9 *Eppela*

*Eppela*[24] è una tra le principali piattaforme di reward *crowdfunding* in Italia ed è specializzata in progetti di arte, tecnologia, cinema, musica, fumetto, innovazione sociale, scrittura, moda, no-profit. È stata fondata nel 2011 a Lucca da Nicola Lencioni e Chiara Spinelli e ad oggi ha finanziato più di 3000 progetti, raccogliendo più di 20 milioni di offerte. Gli utenti registrati hanno superato la soglia dei 200.000 e tra questi sono presenti anche enti pubblici come il Comune di Milano e la Regione Piemonte mentre il contributo medio è di 50 euro.

Il suo funzionamento è piuttosto semplice: ci si iscrive gratuitamente, si invia una breve sintesi del progetto indicando anche il periodo in cui si vuole rimanere online (tra i 30 ed i 120 giorni) e l'ammontare del finanziamento richiesto; infine si aggiungono i riconoscimenti previsti per coloro che sosterranno economicamente il progetto. Gli utenti che saranno interessati, potranno donare il proprio contributo tramite *Paypal* ed il passaggio di denaro avverrà solamente se il budget sarà raggiunto entro la scadenza (se non viene raggiunto, i contribuenti riceveranno indietro le somme). Qualora i contributi raggiungano, prima della scadenza, l'obiettivo prefissato la campagna non si ferma ma continua fino al termine del periodo stabilito permettendo così anche un eventuale *overfunding*. In caso di successo della campagna, *Eppela* tratterrà il 5% della somma raccolta. Grazie alle partnership che *Eppela* ha instaurato con importanti aziende ed istituti di credito (come *Poste Italiane*, *Fastweb* ed *Unipol*), su alcuni progetti è prevista la possibilità, qualora non venga raggiunto il budget prefissato ma sia superata la soglia del 50%, di un cofinanziamento della parte restante per raggiungere la soglia prefissata. Ad oggi il totale dei cofinanziamenti ha superato i 3.500.000 milioni di euro. *Eppela* inoltre effettua una selezione dei progetti che vengono presentati alla piattaforma e secondo quanto riportato dall'azienda, solo il 10% va online. Tra i criteri principali che vengono presi in considerazione oltre alla fattibilità del progetto è necessaria la presenza del soggetto richiedente sui social network ed in generale sulla rete internet, essendo questo un fattore importante per la diffusione della campagna.

[24] www.eppela.com

## 4.10 *Crowdfunding* indipendente o *Do It Yourself* (DIY)

Il *Do-It-Yourself* (DIY) è una nuova forma di *crowdfunding* che consente di realizzare una campagna all'interno del sito stesso dell'organizzazione senza dover passare su di una piattaforma specifica di *crowdfunding*: si crea quindi una propria campagna personale su un proprio sito web e lo si promuove al pubblico. Detto anche *crowdfunding* indipendente, sta diventando abbastanza di moda ultimamente, a causa del fatto che molti siti di *crowdfunding* stanno restringendo il numero di progetti approvati modificando le regole e le norme delle loro piattaforme, rendendo di conseguenza non idonei progetti che magari in precedenza avevano le giuste qualifiche. Sempre più progetti si trovano le porte delle piattaforme di *crowdfunding* sbarrate e sono costretti a ricorrere al DIY. Questo metodo di *crowdfunding* è un po' più complesso rispetto all'utilizzo di piattaforme specializzate in quanto occorre essere abbastanza tecnologici, avere conoscenze SEO e di marketing, studiare e creare un modo per indirizzare il traffico verso il sito web e, cosa molto importante, mantenere tale traffico. Il sito web dovrà essere sempre aggiornato, deve avere contenuti interessanti per gli utenti ed essere in grado di collezionare le informazioni in maniera appropriata.

Il *crowdfunding* indipendente presenta diversi benefici tra cui: la possibilità di personalizzare al 100% e amministrare senza restrizioni; l'assenza di categorie proibite; si evita la commissione da dare al portale intermediario; si possono effettuare campagne più lunghe. Vi sono però anche diversi difetti e problemi legati a questa forma di *crowdfunding* ossia: meno esposizione (il marketing è tutto sulle proprie spalle); investitori meno accessibili e credibili; eventuali difficoltà nella creazione di *landing page* e nella gestione dei pagamenti; problemi tecnici da dover risolvere da sé.

## 4.11 *Starteed*

*Starteed*[25] è una *crowd-company* italiana fondata da Claudio Bedino e attiva dal 2012 che sviluppa soluzioni nel mercato del *crowdfunding* e della co-creazione con l'obiettivo di fornire infrastrutture tecnologiche personalizzate e servizi specializzati per chi vuole creare campagne *Do-It-Yourself* di ogni genere, dalle donazioni alla partecipazione in *equity* nelle *start-up*. *Starteed Crowdfunding* rappresenta quindi una soluzione professionale ideale per aziende, istituzioni, associazioni o privati che cercano flessibilità e controllo nel creare una o più campagne di raccolta fondi. *Starteed* permette di ospitare direttamente sul proprio sito una campagna di *crowdfunding* totalmente personalizzata, con un potente sistema di gestione e con una maggiore flessibilità rispetto alle tradizionali piattaforme. Per ogni campagna è infatti possibile decidere liberamente il metodo di pagamento, la durata, la modalità di raccolta e la personalizzazione di ogni aspetto grafico; il tutto con un semplice costo fisso e senza percentuali trattenute sul totale raccolto. I punti di forza di *Starteed* sono:

- L'assenza di commissioni, in quanto *Starteed* non trattiene nessuna percentuale sulle somme raccolte durante la campagna di *crowdfunding*, qualunque sia l'obiettivo impostato.

[25] www.starteed.com

- La possibilità per il cliente di utilizzare il proprio *brand*, ospitare la campagna direttamente sul proprio dominio e di personalizzarne l'aspetto grafico in ogni sua parte, dal logo ai colori, passando per *font* ed icone.
- Un potente pannello di controllo attraverso il quale è possibile analizzare l'andamento della campagna in tempo reale, gestire gli utenti, verificare le transazioni e modificare i contenuti testuali e multimediali in piena autonomia.
- Tutti i dati relativi a utenti e contenuti rimangono di proprietà del cliente, con la possibilità di esportarli in qualunque momento e utilizzarli in applicazioni di terze parti.

*Starteed* offre inoltre al cliente: eventuali servizi aggiuntivi per tutta la durata del progetto; implementazione e aggiornamento della piattaforma, in modo tale da mantenere l'efficienza del servizio; attività di assistenza tecnica e di manutenzione ordinaria e straordinaria della piattaforma e del sito dedicato; il rinnovo delle licenze su *software* e su servizi erogati da terzi necessari per la corretta erogazione del servizio; garanzia del corretto funzionamento dei flussi di pagamento veicolati attraverso il *Payment Provider*. Ad oggi *Starteed* conta più di 90 progetti sviluppati e più di 4.500.000€ transati.

# 5. *PEER TO PEER LENDING*

## 5.1 Origine e sviluppi

Il *Peer-to-Peer Lending* (P2P *Lending*) o *Social lending* è una forma di *crowdfunding* basata sul prestito tra pari tramite una piattaforma online gestita da operatori professionali.[26] Nasce nel 2005 nel Regno Unito quando i fondatori della *Egg* (banca online britannica) ebbero l'idea di disintermediare il processo di erogazione dei prestiti aprendo il sito web *Zopa* (acronimo di *Zone of Possible Agreement*), prima piattaforma virtuale per il prestito diretto tra privati. Dopo il successo di *Zopa* il fenomeno si è poi diffuso in tutto il mondo, in parte modificato ed esteso nelle sue modalità operative, aprendosi per esempio al finanziamento delle imprese (*business lending*). Nella sua forma essenziale però il P2P *Lending* è un prestito personale tra privati svolto senza l'intervento di un intermediario finanziario poiché l'incontro tra domanda e offerta di finanziamenti avviene esclusivamente attraverso la piattaforma virtuale e a condizioni particolarmente vantaggiose in quanto i costi di struttura e di intermediazione sono fortemente ridotti se non addirittura azzerati. Il taglio dei costi di intermediazione è stato uno dei punti di forza per la diffusione del P2P *Lending*, poiché da un lato consente a chi presta denaro di percepire un tasso di interesse superiore sia a quello proposto dagli intermediari finanziari tradizionali sia a quello ottenibile dall'investimento in obbligazioni o depositi a risparmio; dall'altro lato consente a chi richiede il prestito di pagare un tasso di interesse notevolmente più basso rispetto ai tassi del tradizionale credito al consumo. La caratteristica che differenzia nettamente il P2P *Lending* dalle altre forme di *crowdfunding* è che i prestiti erogati attraverso le piattaforme di *social lending* non costituiscono finanziamenti finalizzati in quanto l'interesse del prestatore è esclusivamente legato all'ottenimento di una remunerazione

[26] A. Milne, P.Parboteeah, "*The Business Models and Economics of Peer-to-Peer Lending*" 2016

a fronte del denaro prestato a prescindere dal fine per il quale il finanziamento è stato richiesto. Per le altre forme di *crowdfunding* invece, come visto nel capitolo precedente, i prestatori di fondi sono mossi principalmente dall'interesse alla realizzazione del progetto finanziato a volte anche prescindendo da un ritorno economico.

## 5.2 Modalità di funzionamento

Le richieste di finanziamento presentate online sulla piattaforma vengono vagliate per verificare che abbiano le caratteristiche necessarie per poter accedere al finanziamento. Si passa poi all'analisi della documentazione fornita dal richiedente al fine di verificare la sua affidabilità economica e finanziaria e per la sua assegnazione in una classe di *rating* in base alla quale verrà determinato il tasso di interesse che questi dovrà corrispondere agli eventuali prestatori. Se il richiedente accetta il tasso di interesse proposto dalla piattaforma la sua domanda di prestito viene inserita nel *Marketplace*; il prestito verrà poi erogato in alcuni casi solo se raggiunge una soglia minima di adesione da parte dei prestatori, in altri viene erogato ugualmente nell'ammontare raccolto.[27]

Per quanto riguarda gli investitori invece questi, una volta effettuato l'accesso alla piattaforma, possono scegliere il profilo di rischio-rendimento più adatto alle loro esigenze e investire some anche modeste; l'offerta di fondi da parte dei prestatori può avvenire tramite un'asta al ribasso oppure al tasso fisso stabilito dalla piattaforma. Al fine di mitigare il rischio la somma offerta dal singolo prestatore non viene erogata a un singolo richiedente ma viene suddivisa tra una pluralità di richiedenti diversi. In alcuni casi le piattaforme offrono ai prestatori anche la possibilità di cedere i propri crediti ad altri prestatori dando vita ad una sorta di mercato secondario che permette di poter rientrare rapidamente dall'investimento in caso di necessità. Durante la vita del prestito la piattaforma garantisce ai partecipanti tutti i servizi accessori: gestisce il buon esito dei rimborsi, fornisce alle parti contraenti la reportistica necessaria, gestisce problematiche legate a ritardi o interruzioni nei rimborsi e, in caso di morosità di uno o più richiedenti, attiva programmi di recupero crediti a nome di tutti i prestatori coinvolti.

Le piattaforme vengono remunerate con commissioni pagate in percentuale al finanziamento sia dai richiedenti che dai prestatori (di solito con commissioni *una tantum* per i primi e annuali per i secondi) e con commissioni per specifici servizi accessori (come la cessione del proprio credito ad altri prestatori o la restituzione anticipata del finanziamento).

## 5.3 La disciplina giuridica

A livello mondiale sono stati diversi gli approcci regolamentari al fenomeno del P2P *lending*. In Giappone e Israele l'attività è addirittura vietata ma nella maggior parte dei casi resta invece priva di una disciplina specifica, in genere perché limitata ad un mercato di dimensioni ridotte. Tra i paesi che al contrario hanno deciso di adottare una normativa specifica in materia di P2P *Lending*,

[27] M.Bofondi, "*Il lending-based crowdfunding: opportunità e rischi*", 2017

abbiamo il Regno Unito, dove il fenomeno è nato e si è sviluppato, e la Francia che ha introdotto una riserva di attività per l'esercizio del P2P *Lending* a favore degli *Intermediaires en financement partecipatif*, soggetti che possono operare subordinatamente all'iscrizione in apposito Albo e per la quale sono richiesti specifici requisiti e la sottoscrizione di una copertura assicurativa per responsabilità professionale.

A livello europeo un intervento rilevante è stato quello dell'EBA, che nel febbraio 2015 ha rilasciato insieme all'ESMA un parere sul *lending based crowdfunding* nel quale si è tentato di inquadrare il fenomeno per verificare quale disciplina europea tra quelle esistenti potesse essere applicabile alle piattaforme di P2P in mancanza di una disciplina specifica. Non sono risultate applicabili né le norme sui requisiti patrimoniali degli enti creditizi dal momento che le piattaforme non intermediano, non raccolgono risparmio tra il pubblico e non effettuano attività creditizia, né le norme sul credito al consumo in quanto il credito non viene erogato dalle piattaforme ma dai prestatori. Risultano invece applicabili la disciplina in materia di antiriciclaggio, per pagamenti che eccedono i 15mila euro, e la normativa europea sui servizi di pagamento. Nei documenti ufficiali a livello europeo viene messa in luce la necessità di un intervento degli Stati membri, volto a favorire la convergenza della prassi di vigilanza del fenomeno, al fine di evitare arbitraggi regolamentari e per creare un sistema normativo omogeneo a livello europeo.[28]

In Italia i primi interventi normativi in materia di P2P *lending* si sono avuti con l'ultimo aggiornamento delle disposizioni generali della Banca d'Italia sulla raccolta del risparmio da parte di soggetti diversi dalle banche, pubblicate nel novembre del 2016 ed entrate in vigore nel gennaio 2017. Si tratta di una normativa ancora allo stato embrionale e di carattere ricognitivo, ma rappresenta un primo riconoscimento nell'ordinamento interno del *social lending*, definito dalla Banca d'Italia «uno strumento attraverso il quale una pluralità di soggetti può richiedere ad una pluralità di potenziali finanziatori, tramite piattaforme online, fondi rimborsabili per uso personale o per finanziare un progetto». L'attività viene così legittimata a patto però che venga svolta nel rispetto delle norme che stabiliscono riserve di attività a particolari tipi di soggetti. Ai gestori delle piattaforme è quindi vietata la raccolta di risparmio tra il pubblico in quanto attività riservata alle banche, ma è concessa la raccolta di fondi da inserire in conti di pagamento utilizzati esclusivamente per la prestazione di servizi di pagamento da parte dei gestori stessi. Tale attività infatti nell'ordinamento italiano non viene considerata come raccolta di risparmio tra il pubblico ma come attività riservata agli Istituti di pagamento; i gestori quindi potranno svolgerla se in possesso della necessaria autorizzazione ad operare come tali. Le somme che i prenditori ricevono tramite la piattaforma non costituiscono raccolta tra il pubblico, ma raccolta privata, nella misura in cui l'acquisizione di fondi avvenga sulla base di trattative personalizzate con i singoli finanziatori. Le trattative possono essere considerate personalizzate qualora le controparti dell'operazione di finanziamento sono in grado di decidere autonomamente le clausole del contratto tra loro stipulato. Il gestore deve quindi limitarsi ad un'azione di supporto nello svolgimento delle trattative per la chiusura del contratto ma può predisporre, come base di partenza delle trattative, un regolamento contrattuale standard che può poi essere modificato e personalizzato a piacimento dai contraenti. Il carattere personalizzato delle trattative è quindi condizione necessaria per i gestori affinché non incorrano nel reato di esercizio abusivo della raccolta del risparmio tra il pubblico. Un altro tema delicato sotto il profilo normativo, è infine quello del limite massimo di acquisizione di fondi tramite

[28] IOSCO, "*Research Report on Financial Technologies*", 2017

portali online di *social lending* da parte dei prenditori. Tale limite non è stato quantificato dalla Banca d'Italia, che ha stabilito però debba essere di importo contenuto lasciando quindi al gestore la facoltà di definirlo. La necessità di fissare un limite massimo di acquisizione fondi per le piattaforme di *social lending* è coerente con la *ratio* sottesa alla disciplina della raccolta del risparmio tra il pubblico volta a impedire a soggetti non bancari di raccogliere fondi presso un numero indeterminato di risparmiatori per un elevato ammontare. La decisone delle autorità di vigilanza di non fissare un preciso limite è dovuta all'incertezza sulla posizione da prendere nei confronti del *social lending*. Procedere ad una dettagliata regolazione del fenomeno potrebbe ostacolarne lo sviluppo ma al contempo lasciarlo privo di disciplina espone il sistema finanziario a rischi di instabilità e può determinare un ingiustificato vantaggio competitivo delle piattaforme rispetto agli intermediari finanziari vigilati.

## 5.4 La disintermediazione

Lo sviluppo del P2P *lending* è stato reso possibile dall'evoluzione tecnologica e informatica, che ha consentito, tramite una piattaforma telematica, di mettere in relazione diretta prestatori e prenditori di fondi, rendendo possibile il trasferimento delle risorse in surplus provenienti da una moltitudine di singoli risparmiatori ai singoli richiedenti credito, senza l'intervento di un intermediario finanziario. Le piattaforme quindi, avvantaggiate da una serie di condizioni favorevoli, riescono a eseguire gran parte dei processi della catena di intermediazione che in passato erano appannaggio esclusivo degli intermediari abilitati. La tecnologia applicata alla finanzia in questo caso non si limita a rendere più veloci, semplici ed economiche parti dell'attività di intermediazione ma pone in essere le condizioni per rendere superflua e dunque sostituire del tutto l'intermediazione stessa nella sua forma tradizionale. Il gestore della piattaforma non si configura come intermediario finanziario in quanto il rischio per ogni singola operazione resta in capo al prestatore il quale però grazie alla piattaforma può diversificarlo tra più prenditori. Il gestore della piattaforma si limita infatti ad offrire l'occasione di incontro tra domanda e offerta e una serie di altri servizi che per il singolo prestatore sarebbero troppo onerosi da sostenere a fronte di prestiti anche di importo esiguo. Tali servizi (valutazione del merito creditizio, *pricing*, solleciti di pagamento, recupero crediti ecc.) vengono eseguiti dalla piattaforma a costi ridotti grazie alle economie di scala e a processi automatizzati. La piattaforma, non svolgendo il ruolo di intermediario finanziario, non deve presentare una specifica forma societaria e un determinato patrimonio di vigilanza, né deve assolvere a particolari obblighi informativi e costi di vigilanza.[29]

Oltre a motivazioni di convenienza economica e regolamentare, le ragioni dell'affermazione del P2P *Lending* e del *crowdfunding* in generale sono anche di natura sociologica, riconducibili al venir meno della fiducia dell'opinione pubblica nelle istituzioni finanziarie tradizionali a seguito della crisi e alle misure politiche e regolamentari utilizzate per fronteggiala. La crisi infatti ha portato all'inasprimento degli oneri legali e regolatori imposti alle banche, causando una stretta creditizia dovuta alla difficolta delle banche stesse di far fronte alle richieste di finanziamento; tale situazione ha stimolato così la nascita di fonti di reperimento di capitali alternative ai canali tradizionali. D'altra

[29] U. Filotto, "*Peer to peer lending: mito o realtà*", 2016

parte, se si estendesse il modello di iperregolazione imposto alle banche anche ai nuovi soggetti e alle nuove attività, si condannerebbero le innovative imprese *FinTech* a morte certa.

## 5.5 *Smartika*

La piattaforma di P2P *Lending* attualmente leader in Italia è *Smartika*[30] fondata nel 2011 da Maurizio Sella e Pierluigi Loy Donà. *Smartika* opera come istituto di pagamento ed è quindi un operatore finanziario autorizzato a prestare servizi di pagamento su richiesta dei prestatori e richiedenti di finanziamenti. I prestiti offerti dalla piattaforma vanno dai 1000 ai 15000 euro con scadenza dai 12 ai 48 mesi. I requisiti per i richiedenti prevedono un'età compresa tra i 18 e i 75 anni e l'intestazione di un controcorrente bancario; il debitore deve inoltre essere in grado di dimostrare di possedere una fonte di reddito sufficiente per rimborsare il capitale richiesto. La procedura che porta all'approvazione della richiesta di prestito prevede prima di tutto l'identificazione dell'utente e successivamente la verifica del suo livello di indebitamento e della sua situazione creditizia, utilizzando le banche dati messe a disposizione dalla società partner *Experian*. Terminato il processo di profilazione viene assegnato al prenditore una classe di *rating* (A+, A, B, C e K) e gli vengono comunicate le condizioni contrattuali. In caso di accettazione la somma pattuita viene inizialmente versata sul conto di pagamento *Smartika* e successivamente trasferita sul conto corrente bancario/postale del debitore, il quale oltre agli interessi passivi deve corrispondere anche una commissione fissa di massimo il 3% della somma ottenuta, a pagamento dei servizi istruttori e della gestione del trasferimento del denaro. Le rate di rimborso vengono versate su conti di pagamento accesi presso *Intesa San Paolo*, *Unicredit* o *Banca Popolare di Milano*, intestati ai prestatori e quindi non aggredibili dai creditori di *Smartika*. Sono ammesse a prestare denaro, fino ad un massimo di 50.000 euro, esclusivamente persone fisiche con residenza in Italia che abbiano raggiunto la maggiore età e intestatarie di un conto corrente. Il prestatore può scegliere l'importo, la durata massima del prestito e il rendimento desiderato che dipenderà dalla struttura del portafoglio prestiti, ma in media si aggira intorno al 5-6% al netto delle commissioni. L'utente può poi decidere se reinvestire il capitale rimborsato oppure traferirlo presso il suo conto corrente personale; può inoltre, grazie alla funzione "*Rientro Rapido*", cedere il proprio credito ad altri utenti della piattaforma, a fronte di una commissione fissa di 15 euro e una variabile pari al massimo all'1% della somma erogata. *Smartika* adotta una politica di minimizzazione del rischio che prevede la suddivisione del prestito in 50 tranche da destinare ad altrettanti debitori; inoltre nel 2015 il board della piattaforma ha approvato la delibera di costituzione del fondo a protezione dei finanziatori, chiamato *Smartika Lender Protection*, alimentato tramite piccole trattenute sulle rate di rimborso. Tale fondo interviene subentrando al debitore insolvente nel procedimento di rimborso, decorso un anno dal mancato pagamento e dal fallimento delle azioni di recupero.

[30] www.smartika.it

# 6. SERVIZI DI PAGAMENTO DIGITALI

## 6.1 Strumenti elettronici e *mobile payments*

Tra le attività finanziare sottoposte maggiormente ai cambiamenti generati dall'evoluzione tecnologica si annoverano i servizi di pagamento. Già a partire dagli anni '80, grazie allo sviluppo dell'elettronica e il suo impiego nelle attività finanziarie, si è avviata una vera e propria rivoluzione nel settore dei servizi di pagamento, con un graduale passaggio da servizi di pagamento basati principalmente su strumenti cartacei a metodologie di trasferimento di capitali basate sull'elettronica. Tali strumenti elettronici vennero generalmente definiti EFTS (*Elettronic Fund Transfer Systems*) e considerati come la quarta generazione dei mezzi di pagamento succedendo alla moneta legale, ai titoli bancari e le carte di credito. Negli anni successivi il progresso tecnologico dell'era digitale e il continuo sviluppo delle telecomunicazioni hanno portato alla nascita di servizi e prodotti ancora più innovativi e sofisticati come: la moneta elettronica, metodi di pagamento utilizzabili per l'acquisto di beni e servizi online, l'utilizzo di carte di credito in modalità contactless, la possibilità di effettuare pagamenti tramite cellulare e altri dispositivi mobili. È proprio quella dei *mobile payments* probabilmente la maggior innovazione degli ultimi tempi nel campo dei servizi di pagamento[31], considerato il loro elevatissimo tasso di crescita dovuto per lo più alla massiccia diffusione degli *smartphone*s e altri dispositivi mobili. Gli *m-payments* possono configurarsi come: pagamenti a distanza (*remote payments*), di solito eseguiti tramite internet o con servizi di sms a tariffazione maggiorata e addebitati al pagatore tramite il gestore di telefonia mobile; pagamenti in prossimità (*proximity payments*), in genere eseguiti direttamente nel punto vendita e basati sulla tecnologia NFC che permette si riconoscere il telefono se avvicinato ad un apposito lettore. Tra le più importanti applicazioni in ambito di *m-payments* annoveriamo i cosiddetti portafogli elettronici (*digital wallets*), che sostituiscono i portafogli veri e propri e le carte fisiche. I *digital wallets* consentono di trasferire denaro tra conti di pagamento per l'acquisto di beni e servizi e di effettuare pagamenti con addebito sulle carte o sui conti collegati al servizio, senza comunicare a terzi i dati relativi al pagatore (per l'esecuzione del pagamento è sufficiente infatti effettuare il login, senza la necessità di inserire gli estremi della propria carta di credito). I portafogli digitali apportano notevoli vantaggi al settore dei servizi di pagamento, in quanto permettono di velocizzare le transazioni e ridurre i costi dando così impulso all'attività economica. Gli *e-wallet* inoltre (come in generale tutti gli *m-payments*) hanno contribuito notevolmente all'inclusione finanziaria, in quanto consentono l'accesso ai servizi finanziari anche a quelle fasce di popolazione che non sono in possesso di un conto bancario o residenti in paesi dove il sistema finanziario non è particolarmente sviluppato.

## 6.2 Interventi regolamentari: PSD e PSD2

Nonostante le diversità operative delle varie fattispecie eterogenee rientranti nel settore dei servizi di pagamento elettronici e digitali, vi sono alcune problematiche di carattere regolamentare che

[31] European Payments Council, "*White Paper Mobile Payments*", 2017

investono l'intero settore di riferimento come: la necessità di garantire la protezione dei dati personali e finanziari degli utenti, l'esigenza di assicurare un adeguato livello di sicurezza delle operazioni e il bisogno di porre chiarezza sui profili di responsabilità in capo ai fornitori del servizio. Problematiche di natura regolatoria, sono dovute anche all'ingresso nel mercato di nuovi operatori non finanziari (come compagnie di telecomunicazioni e *start-up FinTech*) che, sfruttando sia l'innovazione tecnologica che i vantaggi regolamentari, stanno erodendo la posizione di dominio incontrastato delle banche nel settore dei servizi di pagamento. L'ingresso di nuovi operatori può apportare indubbi vantaggi sul piano della concorrenza favorendo l'ampliamento dell'offerta di servizi, la riduzione dei costi e spingendo gli *incumbents*, spesso dotati di sistemi tecnologicamente obsoleti, a investire nell'innovazione; ma è pur vero che risulta indispensabile una regolamentazione del fenomeno che garantisca l'affidabilità dei nuovi progetti imprenditoriali, la sicurezza dei consumatori, la stabilità finanziaria e l'integrità del mercato[32]. I primi interventi regolatori a livello europeo si ebbero verso la fine degli anni '80 con forme di *soft law*; solo successivamente sono stati emanati veri e propri provvedimenti normativi caratterizzati tuttavia da un ambito di applicazione limitato (come la direttiva 97/5/CE sui bonifici transfrontalieri e la prima direttiva 2000/46/CE sugli istituti di moneta elettronica). La necessità di disciplinare in maniera completa e organica le diverse fattispecie di servizi di pagamento, raggruppandole in un unico quadro normativo, ha trovato risposta con l'adozione della direttiva 2007/64/CE (*Payment Service Directive* PSD) recepita in Italia col d.l. n. 11/2010. L'obbiettivo di tale direttiva è quello di armonizzare le regole in materia di servizi di pagamento elettronici al fine di agevolare il buon funzionamento del mercato unico dei servizi di pagamento al dettaglio. La PSD costituisce infatti le fondamenta giuridiche della SEPA (*Single Euro Payment* Area), ossia un'area perfettamente integrata e concorrenziale in cui non vi siano differenze di trattamento tra pagamenti nazionali e transfrontalieri in euro. Il fine della SEPA è infatti quello di creare un mercato dei pagamenti armonizzato, che offra ai consumatori strumenti di pagamento comuni basati su standard operativi uniformi, utilizzabili con la stessa sicurezza e alle stesse condizioni in tutto il territorio dell'UE. In quest'ottica, la PSD ha permesso di definire, all'interno di una cornice giuridica unitaria, gli aspetti fondamentali dei servizi di pagamento come: i requisiti di accesso al mercato per i fornitori; la trasparenza delle condizioni relative all'erogazione dei servizi stessi; i diritti, gli obblighi e le responsabilità di prestatori e utenti.

La PSD ha rappresentato senza dubbio un significativo traguardo nella regolamentazione del settore dei servizi di pagamento, ma dalla sua entrata in vigore ad oggi si sono registrate notevoli innovazioni tecniche che l'hanno resa inadeguata e obsoleta. In particolare, si è potuto verificare che: numerosi settori del mercato dei pagamenti, come quello dei pagamenti tramite Internet e dispositivi mobili, rimanevano frammentati lungo le frontiere nazionali; nuovi strumenti di pagamento rimanevano esclusi dal campo di applicazione della normativa; le disposizioni risultavano in molti casi ambigue, troppo generiche e superate rispetto all'evoluzione in atto. È stato quindi necessario un ammodernamento del quadro regolamentare tracciato dalla PSD, operato con la recente direttiva UE 2015/2366 definita PSD2. L'obbiettivo di tale nuova direttiva è quello di garantire un mercato dei pagamenti maggiormente integrato, basato su regole chiare, moderne e uniformi che possa stimolare la crescita economica in tutta l'UE. Più nello specifico la nuova normativa dovrebbe costituire il presupposto giuridico per una più ampia diffusione di nuovi strumenti e servizi di pagamento innovati fermo restando la garanzia di un elevato livello di

[32] A. Enria, "*FinTech: regulatory challenges and open questions*", 2017

protezione dei consumatori, a sua volta necessaria per rafforzare la fiducia nel mercato dei pagamenti. Come tutte le altre normative in materia di *FinTech* anche la PSD2 si fonda sui principi della neutralità tecnologica (stesse regole per un determinato servizio a prescindere dalle soluzioni tecniche utilizzate per svolgerlo) e della proporzionalità (l'azione regolamentare e di vigilanza deve essere commisurata ai rischi correlati all'attività sottoposta al controllo).

## 6.3 PSD2: Ambito di applicazione

Come la direttiva 2007/64/CE anche la PSD2 si applica a tutti i servizi di pagamento elettronici, con esclusione quindi di quei servizi in cui il trasferimento di fondi avviene esclusivamente tramite banconote o strumenti cartacei. Rispetto alla precedente direttiva però nella PSD2 l'ambito di applicazione ha subito delle modifiche includendo nuove tipologie di operazioni e ridefinendo il regime delle esenzioni (precedentemente formulato in modo troppo generico e quindi interpretato e applicato in modo differente negli Stati membri, causando rischi per gli utenti e condizioni non omogenee nel mercato interno per i fornitori di servizi di pagamento). In particolare, la nuova disciplina non trova applicazione:

- alle operazioni di pagamento effettuate tramite un agente commerciale autorizzato a negoziare per conto del solo pagatore o del solo beneficiario (sono invece incluse nell' applicazione PSD2 le operazioni di pagamento in cui l'agente commerciale opera per conto di entrambi i contraenti, salvo il caso in cui detto agente non entri in possesso dei fondi dei clienti o non li controlli)
- ai servizi basati su strumenti di pagamento privi di una spendibilità generalizzata in quanto utilizzabili solo in una rete limitata ossia solo per l'acquisto di beni e servizi presso i punti vendita di determinati rivenditori o per l'acquisto di una gamma molto ristretta di beni e servizi
- ai servizi tecnici a supporto della prestazione dei servizi di pagamento qualora il fornitore non entri in possesso dei fondi da trasferire (registrazione e autenticazione dei dati, manutenzione dei terminali, protezione della riservatezza, ecc.)
- operazioni di pagamento per attività di beneficenza e per l'acquisto di contenuti digitali o biglietti (addebitate tramite relativa fattura), effettuati da un fornitore di servizi di comunicazione elettronica in aggiunta ai servizi base erogati agli abbonati, purché il valore di ogni singola operazione non superi 50 euro e che il valore complessivo delle operazioni per singolo abbonato non superi 300 euro mensili
- ai servizi di prelievo di contante tramite sportello automatico (ATM) forniti da soggetti indipendenti da banche, purché detti soggetti non prestino altri servizi di pagamento e che al cliente vengano fornite adeguate informazioni in merito alle commissioni sui prelievi

La definizione dell'ambito di applicazione della normativa è molto rilevante, in quanto il processo di prestazione di servizi di pagamento presuppone l'intervento di numerosi soggetti. È importane quindi distinguere tra: attività che comportano la prestazione di servizi di pagamento, che come tali devo essere riservate a enti autorizzati e sottoposte all'applicazione delle disposizioni contenute nella PSD2; attività semplicemente accessorie o strumentali alle prime,

che non si traducono nell'erogazione di servizi di pagamento e che quindi possono essere liberamente prestate senza sottostare ai vincoli e le regole relative alla direttiva di riferimento.

### 6.3.1 PSD2: Third-party providers

Tra le principali novità apportate dalla PSD2, si annovera l'apertura del mercato dei servizi di pagamento a due nuove categorie di operatori cosiddetti *third party providers* (TPPs): i prestatori di servizi di disposizione di ordini di pagamento (*Payment Initiation Service Providers,* PISPs) e i prestatori di servizi di informazione sui conti (*Account Information Service Providers*, AISPs). I primi servizi consentono al prestatore (PISP) di disporre per conto dell'utente, un pagamento a valore su un conto trattenuto dall'utente stesso presso un altro intermediario, il cosiddetto prestatore di servizi di radicamento del conto o *Account Servicing Payment Service Provider* (ASPSP) di solito rappresentato da una banca. In termini più pratici i PISP consentono di effettuare pagamenti online attraverso «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» (27°considerando PSD2). Il funzionamento di tali *software* prevede che l'utente-pagatore, dopo aver selezionato il servizio di *payment initiation* tra le opzioni di pagamento presenti sul sito dell'esercente, acceda tramite il PISP al proprio conto online, per poi autorizzare attraverso una *password* il trasferimento dei fondi dal proprio conto a quello del commerciante. Tale servizio garantisce che i dati personali relativi al pagatore non siano condivisi con l'esercente e non siano visibili al di fuori del sistema. I *payment initiation services* si pongono come valida ed economica alternativa ai tradizionali pagamenti con carta in quanto richiedono per il pagatore solo il possesso di un conto corrente mentre per il commerciante non è richiesto l'obbligo di aderire ad una *card scheme* e di sopportarne i relativi costi[33]. Gli AISPs offrono invece, tramite una piattaforma online, un servizio di consolidamento delle informazioni riguardanti i diversi conti intestati al cliente, anche presso diversi intermediari, consentendo al cliente stesso di avere una visione chiara e complessiva della propria situazione finanziaria e delle proprie abitudini di spesa, in modo da gestire al meglio le risorse a disposizione. Entrambe le precedenti categorie di servizi presuppongono l'accesso del fornitore ai conti del proprio cliente, accesso che deve quindi essere garantito dal prestatore di servizi di radicamento del conto (ASPSP); non a caso si parla a tal proposito di servizi bancari aperti o *open banking.* Il rapporto tra TPPs e ASPSP non deve necessariamente esse regolato da un apposito contratto ma è indispensabile che i secondi si dotino di infrastrutture, le cosiddette APIs (*Application Programming* Interfaces), che permettono un'efficace e sicura interazione con i sistemi delle TPPs che chiedono accesso al conto dei propri clienti sotto esplicito consenso di questi ultimi. La PSD2 prevede anche che gli emittenti di carte di pagamento possano ottenere dall'ASPSP la conferma della disponibilità, sul conto del pagatore, dell'importo relativo all'operazione di pagamento, purché il conto sia disponibile on line e il cliente abbia dato il suo esplicito consenso. Tale operazione, definita *fund checking*, è particolarmente innovativa, in quanto permette l'emissione di carte di debito anche a enti che non gestiscono direttamente i conti dell'utente, rendendo accessibili all'emittente le informazioni relativi a tali conti detenuti presso altri

[33] F. Ciraolo, "*Pagamento fraudolento con carta di credito e ripartizione delle responsabilità. Dagli orientamenti attuali alla revisione della PSD*", 2017

intermediari. I TPPs non entrando mai in possesso dei fondi del pagatore, non devono rispettare requisiti prudenziali e di vigilanza minimi, potendo risultare sufficiente un'assicurazione obbligatoria per responsabilità professionale. Al fine di tutelare l'utente, soprattutto sotto il profilo della

protezione dei dati personali, la PSD2 vieta alle TPPs di usare o conservare i dati del cliente per fini diversi dalla prestazione di servizi di disposizione di ordine di pagamento o di informazione sui conti.

### 6.3.2 PSD2: Profili di sicurezza

Tra le problematiche più spinose legate all'utilizzo delle nuove tecnologie nel settore dei servizi di pagamento vi è senza dubbio quella della sicurezza. La crescente complessità tecnica dei pagamenti digitali espone gli utenti a notevoli rischi di frode che minano la fiducia del pubblico nella sicurezza dei servizi di pagamento e incidono pesantemente sul buon funzionamento del relativo mercato. Tra le pratiche più comuni di frode digitale ricordiamo: il *pishing*, attuato di solito tramite un email civetta (apparentemente proveniente da un intermediario finanziario) attraverso la quale si sollecita alla comunicazione di dati riservati; o la più pericolosa tecnica del *man in the browser*, consistente nella immissione, nel sistema informativo del soggetto truffato, di un virus capace di acquisire le credenziali di accesso ai conti e i servizi di pagamento online e di trasmetterle al truffatore.

Occupa quindi, una posizione centrale nella PSD2 il profilo della sicurezza, con un focus particolare sul tema delle frodi e degli abusi nella prestazione dei servizi di pagamento. Per prevenire eventuali operazioni di pagamento non autorizzate la PSD2 impone specifici obblighi di condotta sia a carico del prestatore di servizi di pagamento che dell'utente. Il primo è difatti obbligato a: assicurare che le credenziali di sicurezza personalizzate per l'accesso ai servizi di pagamento siano accessibili esclusivamente all'utente autorizzato all'utilizzo di tali servizi; assicurare che siano sempre disponibili adeguati mezzi che permettano all'utente di poter notificare l'avvenuto furto o smarrimento dello strumento di pagamento; impedire qualsiasi utilizzo dello strumento stesso una volta effettuata detta notifica. L'utente è invece obbligato a: utilizzare lo strumento di pagamento in conformità alle condizioni che ne disciplinano l'uso; adottare le necessarie misure volte a proteggere le credenziali di sicurezza personalizzate dello strumento di pagamento; notificare il prima possibile al prestatore di servizi di pagamento l'avvenuto furto, smarrimento o utilizzo non autorizzato dello strumento di pagamento. Sulla base di tali obblighi si estende il regime delle responsabilità per le operazioni di pagamento non autorizzate, suddivise tra prestatore e utente secondo un criterio basato sulla rispettiva capacità di controllare e prevenire determinanti rischi. Nello specifico, il titolare dello strumento di pagamento subisce le perdite relative alle operazioni non autorizzate compiute prima della denuncia del furto o smarrimento anche se nei limiti di un massimale pari a 50 euro. Tale limite non viene però applicato in caso di condotta fraudolenta da parte del titolare o in caso questi non abbia adempiuto a propri obblighi con dolo o grave negligenza. Le perdite invece gravano interamente sul prestatore di servizi di pagamento successivamente alla denuncia, tranne nel caso in cui l'utente abbia agito in modo fraudolento. In caso di contestazione da parte dell'utente di un'operazione di pagamento, grava sul fornitore di servizi di pagamento l'onere di dimostrare sia che l'operazione sia stata regolarmente autenticata, registrata e contabilizzata, sia che l'utente abbia agito con dolo o grave negligenza.

Le regole presentate finora in materia di obblighi e responsabilità per gli utenti e prestatori di servizi di pagamento riprendono quelle già delineate dalla precedente direttiva del 2007; a queste però si aggiungono nella PSD2 nuove disposizioni di carattere innovativo legate al mutato contesto di riferimento. Di notevole importanza sono le nuove disposizioni in materia di "autenticazione forte" del cliente, cioè una procedura che permette al prestatore del servizio di verificare l'identità dell'utente, fondata sull'impiego di due o più elementi tra loro indipendenti in quanto la violazione di uno non compromette la validità dell'altro. Tali elementi sono classificabili nelle categorie "qualcosa che solo l'utente conosce" ad esempio una *password*, "qualcosa che solo l'utente possiede" ad esempio un *token*, "qualcosa che caratterizza l'utente" ad esempio l'impronta digitale. Secondo le disposizioni della PSD2 il prestatore di servizi di pagamento è obbligato all'applicazione dell'autentificazione forte del cliente quando questi accede al suo conto online, quando dispone un ordine di pagamento e quando effettua una qualsiasi operazione che può comportare un rischio di frode nei pagamenti o altri abusi. La PSD2 stabilisce inoltre che se il prestatore di servizi di pagamento non esige l'autenticazione forte del cliente, quest'ultimo non debba sopportare nessuna conseguenza finanziaria; ma sarà quindi il fornitore del servizio a rispondere in questo caso dei danni derivanti dalle operazioni non autorizzate dall'utente, salvo il caso in cui quest'ultimo abbia agito in modo fraudolento. Tali disposizioni in materia di autenticazione forte sanciscono l'importanza dei presidi di sicurezza e degli accorgimenti tecnici idonei a rendere i pagamenti più affidabili e sicuri. Altra novità introdotta dalla PSD2 è quella riguardante il regime delle responsabilità in capo alle nuove tipologie di prestatori di servizi di pagamento, i già citati TPPs. Questi assumono una responsabilità diretta non solo nei confronti degli utenti ma in alcuni casi anche nei confronti dei prestatori di servizi di radicamento del conto. In caso di un'operazione di pagamento non autorizzata tutti i prestatori di servizi di pagamento intervenuti (sia PISP che ASPSP) si assumeranno la responsabilità di quel segmento di operazione eseguito sotto il rispettivo controllo. L'applicazione di tale norma tuttavia risulta in concreto problematica alla luce della disposizione secondo la quale non è necessario che le relazioni tra PISP e ASPSP siano regolati da uno specifico rapporto contrattuale. La presenza di un contratto infatti renderebbe la risoluzione di controversie tra i due soggetti prestatori di servizi di pagamento più agevole in quanto andrebbe a stabilire con precisione la suddivisione delle responsabilità in caso di operazioni non autorizzate, limitando il rischio di contestazioni e aumentando al contempo la fiducia reciproca tra gli stessi soggetti prestatori[34].

## 6.4 Prospettive future

Il settore dei servizi di pagamento è in continua evoluzione e numerose sono le tecnologie innovative che si stanno sperimentando in questi anni. In particolare, è possibile individuare alcune fondamentali direzioni di innovazione che potranno nei prossimi anni rivoluzionare ulteriormente il mercato dei servizi di pagamento, soprattutto quello del *Mobile Payment*:

- Geolocalizzazione: attraverso un sistema di localizzazione lo *smartphone* può identificare l'individuo all'interno di un punto vendita e abilitare il pagamento in automatico. Esempio lampante è quello del servizio lanciato e poi dismesso da *Google* denominato

[34] F. Cascinelli, V. Pistoni, G. Zanetti, "*La Direttiva (UE) 2015/2566 relativa ai servizi di pagamento nel mercato interno*", 2016

"*Paymentshands free*", il quale permetteva attraverso la geolocalizzazione di pagare senza dover estrarre e attivare il cellulare. Altro esperimento interessante è quello di *Amazon Go*, un negozio reale in cui il pagamento può avvenire tramite l'account *Amazon* dell'utente, il quale viene identificato tramite la geolocalizzazione del proprio *smartphone*. Non è quindi richiesto per il pagamento l'utilizzo della cassa, evitando così al consumatore eventuali code.

- Biometrica: l'attivazione dei pagamenti può avvenire tramite la lettura dell'iride, l'impronta digitale, il riconoscimento facciale; lo *smartphone* può diventare così un utile strumento di riconoscimento. Nel 2016, per esempio, *MasterCard* ha sperimentato il *selfiepayment* con riconoscimento facciale tramite la videocamera dello *smartphone*.
- *InternetofThings* (IoT): l'attivazione del pagamento avviene direttamente dagli oggetti escludendo così anche la necessità di utilizzo dello *smartphone*. Molte case automobilistiche per esempio, stanno integrando i pagamenti dei parcheggi direttamente dal sistema operativo dell'auto.

Lo sviluppo di queste nuove tecnologie e l'affermazione di nuove *start-up* innovative nel settore dei servizi di pagamento pone in essere un interrogativo riguardante l'avvenire delle banche e del ruolo che saranno destinate ad assumere nel prossimo futuro. Per non perdere rilevanti quote di mercato gli intermediari tradizionali dovranno investire nell'ammodernamento tecnologico e nella digitalizzazione dei processi operativi e porre in essere nuove strategie imprenditoriali. La via più efficace da seguire è quella del passaggio da una competizione tra banche e *FinTech* ad una più proficua *co-opetition* attraverso opportune forme di *partnership*. I vantaggi competitivi investirebbero infatti sia le banche che i nuovi operatori digitali: da un lato gli intermediari tradizionali potrebbero compiere quel salto tecnologico altrimenti troppo lungo e costoso da praticare, dall'altro le imprese *FinTech* potrebbero avere accesso alla vastissima platea di clienti bancari cui offrire i propri servizi accessori.

## 6.5 *Satispay*

Tra le principali *start-up* italiane attive nel settore dei pagamenti digitali ricordiamo *Satispay*[35], fondata nel 2013 (ma operativa dal 2015) da Samuele Pinta, Dario Brignone e Alberto Dalmasso. La sua app permette di effettuare micropagamenti con il proprio *smartphone* senza alcun costo per l'utente, mentre per l'esercente l'unica spesa è rappresentata da una commissione di 20 centesimi quando la somma della singola transazione supera i 10 €. L'iscrizione al servizio è gratuita, basta comunicare l'IBAN del proprio conto corrente bancario, il codice fiscale ed effettuare l'*upload* della foto del proprio documento di identità. Il conto corrente indicato sarà la fonte del *budget* settimanale a disposizione del proprio account. Se si decide ad esempio un monte spesa pari a 100 € settimanali, sarà questo il massimale autorizzato per gli acquisti tramite il servizio. Qualora la somma non sia stata raggiunta, *Satispay* preleva semplicemente la parte mancante dal conto corrente per ripristinare la quota a disposizione della settimana successiva. L'invio del denaro è subordinato alla disponibilità di una connessione internet ed all'immissione di una *password*. Una volta effettuato il pagamento l'esercente riceverà istantaneamente una notifica sulla propria applicazione, potendo così verificare seduta stante la sua correttezza ed incassando subito quanto

[35] www.satispay.com

pattuito. A disposizione dei clienti c'è anche un servizio di geo-localizzazione per individuare gli esercizi che aderiscono alla rete di *Satispay*. L'azienda, per incoraggiare l'adozione del servizio da parte di utenti ed esercenti, fa leva su offerte speciali come quella di *cashback*: a fronte di un pagamento effettuato con l'app del servizio, *Satispay* restituisce all'utente parte della somma spesa, offrendo di fatto uno sconto virtuale immediato sulla cifra concordata. Formalmente non si tratta di uno sconto, ma di una vera e propria restituzione; la cifra promessa, infatti, non è decurtata dal totale della transazione ma inviata all'utente con operazione separata e trasparente. A fine 2017 l'app contava oltre 330.000 download, 175.000 utenti privati attivi, circa 3 milioni di euro di transato mensile ed oltre 16.000 esercenti aderenti[36]. Tra questi si annoverano grandi marchi come *Grom, TotalErg, Benetton, Old Wild West, Moleskine* ed *Esselunga*. Per livello di fatturato *Satispay* si è posta come obiettivo un volume di tre milioni di euro entro il 2019 (dai 350mila del 2016) attraverso anche le aperture ai mercati di Germania, Francia, Belgio e Spagna.

# 7. VALUTE VIRTUALI E MONETE COMPLEMENTARI

## 7.1 Tipologie di moneta

A partire dagli anni '70 è nata la cosiddetta moneta bancaria o scritturale rappresentata da assegni bancari o circolari e ordini di accreditamento su conto corrente. Essa costituisce la prima forma di moneta alternativa a quella legale (moneta contante) in quanto consente di trasferire una disponibilità di denaro dal debitore al creditore con effetti analoghi dal punto di vista giuridico a quelli del pagamento per contanti. Nei primi anni 2000 l'innovazione tecnologica ha permesso la nascita della moneta elettronica. Il suo riconoscimento a livello normativo si attua con la direttiva 2000/46/CE del 18 settembre 2000, dove viene presentata come un surrogato elettronico delle banconote e monete metalliche e definita nel considerando 3 della direttiva stessa come «un valore monetario rappresentato da un credito nei confronti dell'emittente che sia: i) memorizzato su un dispositivo elettronico; ii) emesso dietro ricezione di fondi il cui valore non sia inferiore al valore monetario emesso; iii) accettato come mezzo di pagamento da imprese diverse dall'emittente». L'emittente è rappresentato da una banca o un istituto di moneta elettronica e la salvaguardia della sua stabilità rappresenta un elemento essenziale per preservare la fiducia del pubblico nella moneta che questi è in grado di creare e mettere in circolazione e nel sistema finanziario in generale. È per tale motivo che l'emissione di moneta alternativa è riservata a soggetti provvisti di un'autorizzazione amministrativa per l'esercizio della propria attività e vigilati secondo criteri calibrati su quelli stabiliti per le banche, alla luce dei rischi operativi e finanziari ai quali sono esposti. Nell'ultimo decennio la virtualizzazione dei mezzi di pagamento ha favorito la nascita di ulteriori forme di moneta alternativa ossia le valute virtuali e le monete complementari.

[36] www.economyup.it

## 7.2 Valute virtuali: caratteristiche e regolamentazione

Le monete virtuali, tra le quali *Bitcoin* è la più nota e diffusa, si distinguono dalla moneta bancaria in quanto non costituiscono un semplice strumento di pagamento alternativo regolato in moneta legale ma si presentano come una vera e propria moneta a sé stante, non statale, che può essere trasferita, archiviata, negoziata elettronicamente e accettata in via convenzionale dagli operatori per eseguire pagamenti o per finalità speculative. Le monete virtuali quindi, non essendo mere rappresentazioni digitali di valuta legale, non sono rimborsabili in moneta contante nello stesso modo in cui avviene per la moneta scritturale e elettronica[37]. Difatti, al fine di consentire un agevole conversione delle monete virtuali in moneta legale, sono nati veri e propri mercati di cambio con le valute nazionali dove si riscontrano frequentemente fortissime oscillazioni di prezzo, caratteristiche di strumenti finanziari speculativi piuttosto che di valute. La creazione della valuta virtuale così come la sua adoperabilità come strumento di pagamento, non prevede il coinvolgimento delle autorità pubblica in funzione di garanzia; gli emittenti sono infatti soggetti privati e anonimi, per cui l'affidabilità della valuta fa leva esclusivamente sulla tecnologia alla base del funzionamento del *network*. La valuta virtuale non ha efficacia solutoria legale ma solo su base convenzionale e volontaria laddove cioè il beneficiario accetti tale valuta come mezzo di estinzione dell'obbligazione pecuniaria. Nel 2015 la Banca d'Italia in un'apposita Avvertenza ha messo in luce le caratteristiche principali che accomunano la maggior parte delle valute virtuali esistenti:

- sono create da un emittente privato nel caso delle cosiddette valute centralizzate o, in via diffusa, da utenti che utilizzano *software* altamente sofisticati nel caso delle valute decentralizzate come il *Bitcoin*
- non sono fisicamente detenute dall'utente ma sono movimentate tramite un portafoglio elettronico (*e-wallet*)
- sono scambiate in apposite piattaforme che offrono il servizio di conversione delle valute virtuali in moneta legale
- possono essere acquistate con moneta tradizionale o ricevute online direttamente da qualcuno che le possiede e inserite sul proprio *e-wallet*
- sono usate per effettuare acquisti presso esercizi commerciali o persone fisiche che accettano tale tipologia di moneta per effettuare rimesse in favore di altri soggetti titolari di portafogli di valute virtuali o per finalità speculative
- i titolari dei portafogli di monete virtuali e i soggetti coinvolti nelle transazioni rimangono anonimi e le transazioni sono irreversibili (è cioè impossibile richiederne l'annullamento)

All'interno dell'Avvertenza la Banca d'Italia, dopo aver enunciato le suddette caratteristiche riguardo le valute virtuali, ne presenta anche i relativi rischi legati al loro utilizzo. In particolare, sono stati messi in luce i seguenti rischi: assenza di tutele legali e contrattuali; carenza di informazioni; assenza di forme di controllo e vigilanza; assenza di forme di garanzia a tutela delle somme depositate; rischio di perdita permanente della moneta a causa di attacchi informatici o malfunzionamenti; accettazione su base volontaria; elevata volatilità del valore con annesso rischio di elevate perdite; rischio di utilizzo per finalità illecite; rischi fiscali. La Banca d'Italia infine ha sottolineato come i rischi individuati superino i benefici che le valute virtuali possono comportare

[37] N. Mancini, "*Bitcoin: rischi e difficoltà normative*", 2016

ai loro utilizzatori, anche tenendo in considerazione i vantaggi in termini di costi, velocità di transazione e inclusione finanziaria. In questo modo ha scoraggiato le banche e gli altri intermediari finanziari dall'acquistare, detenere e vendere valute virtuali, in quanto, in assenza di adeguati presidi e di un quadro regolamentare definito, vi è il rischio di essere esposti a perdite che potrebbero inficiare la consistenza del patrimonio di vigilanza e la stabilità stessa degli intermediari.

A livello europeo già nel 2014 l'EBA con un *Opinion* aveva auspicato una regolamentazione del fenomeno che prevedesse l'introduzione di: un'autorità di governo degli schemi (piattaforme di creazione e gestione) di valute virtuali; obblighi di verifica su pagatore e beneficiario; requisiti di onorabilità e professionalità per i gestori degli schemi; presidi per la trasparenza nella formazione dei prezzi e per il contrasto dell'abuso di mercato; un'autorizzazione preventiva per la prestazione di servizi relativi alle valute virtuali (che preveda requisiti minimi di capitale, obblighi di separazione patrimoniale dei conti dei clienti e sistemi informativi adeguati); meccanismi di garanzia e rimborsi delle operazioni non autorizzate; obblighi di segretezza tra schemi di valute virtuali e sistemi di pagamento su monete legali. L'EBA inoltre considerata la permeabilità degli schemi di valute virtuali ad attività illecite grazie all'anonimato dei soggetti partecipanti, raccomandava di intervenire nel breve termine in materia di prevenzione di tale utilizzo illecito delle valute virtuali, con particolare attenzione al riciclaggio del denaro e al finanziamento del terrorismo. Nel 2016 con la Risoluzione sulle valute virtuali il Parlamento europeo, escluse al momento dimensioni sistemiche del fenomeno, ha mostrato un atteggiamento tendenzialmente favorevole all'innovazione tecnologica e finanziaria rappresentata dagli schemi di valuta virtuale sviluppatesi spontaneamente sul mercato, evidenziandone alcuni aspetti positivi, come l'abbassamento dei costi di transazione e il contributo all'inclusione finanziaria[38]. D'altra parte, venivano messi in risalto anche alcuni aspetti critici legati alle valute virtuali come: il rischio di condizioni di concorrenza non eque tra i nuovi operatori e gli intermediari finanziari vigilati esercitanti le medesime attività; il rischio di bolle speculative legate all'elevata volatilità di tali valute; i rischi legati al loro utilizzo per attività illecite. In conclusione, il Parlamento europeo pur non considerando ancora opportuni interventi di regolazione, in quanto al momento difficili da graduare, invitava la Commissione Europea a monitorare il fenomeno, adottando un approccio normativo tale da non soffocare l'innovazione in questa fase iniziale, riservandosi però di intervenire in modo deciso nel caso venissero riscontrati pericolosi rischi legati all'uso diffuso delle valute virtuali. A tal fine il Parlamento europeo segnalava che le normative chiave dell'UE in materia finanziaria avrebbero potuto rappresentare un quadro normativo di riferimento efficace per la regolazione delle valute virtuali. La Commissione Europea infatti ha adottato in bozza una direttiva con l'obbiettivo di estendere parti della disciplina comunitaria in materia di antiriciclaggio alle transazioni eseguite tramite valute virtuali e di includere le piattaforme di cambio delle valute virtuali nell'ambito di applicazione della direttiva antiriciclaggio, al fine di eliminare l'anonimato associato a tali piattaforme. In particolare, nella proposta di V direttiva AML è previsto che gli Stati Membri registrino in un database centrale a fini di antiriciclaggio tutti i soggetti che operano nel settore delle valute virtuali. L'estensione degli obblighi in materia di antiriciclaggio risponde all'esigenza di consentire alle autorità competenti di monitorare le operazioni sospette in valute virtuali, preservando al contempo i progressi innovativi offerti da tali valute. D'altronde la riduzione dell'anonimato che caratterizza le valute virtuali può contribuire ad alimentare la fiducia degli utenti in buona fede. Si rilevano, inoltre, iniziative comunitarie finalizzate

[38] Bank of International Settlements (BIS), "*Payment aspects of financial inclusion*", 2016

a rendere applicabile anche agli emittenti di valute virtuali lo statuto introdotto con la PSD in materia di servizi di pagamento. Infine, in questi anni si sta discutendo a livello europeo sulla possibilità di immettere sul mercato una valuta digitale emessa da una banca centrale, che costituisca, non una nuova unità di conto, ma una semplice rappresentazione digitale di una valuta legale basata sulla tecnologia del registro distribuito. Una valuta digitale ufficiale potrebbe garantire una maggiore stabilità e sicurezza rispetto ad una valuta virtuale privata in un analogo contesto di innovazione tecnologica.

Per quanto riguarda l'Italia, il 25 maggio 2017, con il recepimento nel nostro ordinamento della IV direttiva AML tramite decreto legislativo, i prestatori di servizi relativi all'utilizzo di valute virtuali sono stati inseriti nella categoria degli "altri operatori non finanziari" e sottoposti, ai fini della prevenzione del riciclaggio di denaro e del finanziamento del terrorismo, ai relativi obblighi di adeguata verifica della clientela, di conservazione di documenti e informazioni sui clienti e di segnalazione di operazioni sospette, seppur limitatamente all'attività di conversione di valute virtuali in moneta legale e viceversa. Inoltre, i prestatori di servizi relativi all'utilizzo di valute virtuali sono obbligati a comunicare al Ministero dell'economia e delle finanze la propria operatività sul territorio nazionale come condizione essenziale per l'esercizio legale dell'attività e devono essere iscritti in una sezione speciale del registro tenuto dell'Organismo degli agenti e dei mediatori creditizi per coloro che esercitano professionalmente nei confronti del pubblico l'attività di cambiavalute. In realtà, l'inclusione delle piattaforme di cambio di valute virtuale nell'ambito della normativa sull'antiriciclaggio non risolve il problema dell'anonimato delle operazioni, in quanto gli utenti possono effettuare tali operazioni all'interno del *network* senza quindi dover ricorrere a piattaforme di cambio. Nonostante gran parte delle transazioni in valuta virtuale rimanga dunque contraddistinto dall'anonimato, l'intervento legislativo obbliga al monitoraggio del momento di accesso della moneta legale nel *network* con la conversione in valuta virtuale e quello di uscita con la riconversione in moneta legale. Viene in questo modo consentita la valutazione della congruità di tali operazioni rispetto al profilo patrimoniale economico e reddituale nonché all'attività esercitata dall'utente.[39]

## 7.3 Monete complementari: definizione e principali questioni

L'innovazione tecnologica degli ultimi anni ha permesso la nascita e lo sviluppo delle cosiddette valute complementari o locali. Nella Proposta di legge n.2582 del 20 luglio 2014 "*Delega al Governo per la disciplina dell'emissione e della circolazione delle monete complementari*" queste vengono definite come «strumenti di pagamento esclusivamente elettronici volti a facilitare gli scambi di beni e servizi, compreso il lavoro, all'interno di una comunità socio-economica definita utilizzando, anche congiuntamente, criteri di carattere territoriale o funzionale». L'Unità di Informazione Finanziaria nel Rapporto Annuale 2014 le definisce invece «schemi in cui i produttori di beni e servizi e consumatori, legati dall'appartenenza a una medesima comunità, concordano di utilizzare, per il regolamento delle reciproche ragioni di debito e credito, una moneta alternativa a quella ufficiale, realizzando un sistema che favorisce sostanzialmente una forma di baratto tra i soggetti aderenti

[39] J. Nicolaisen, "*What Should the Future Form of our Money Be?",* 2017

all'iniziativa». Seppur accomunate dall'assenza di materialità le monete complementari non possono essere annoverate tra le monete virtuali in quanto le prime sono destinate ad essere usate come mezzo di scambio in un mercato locale e circoscritto, le seconde invece sono aperte al mercato globale. Le monete complementari non vanno confuse neanche con la moneta elettronica in quanto, a differenza di quest'ultima, non costituiscono una mera rappresentazione digitale delle comuni valute legali. Le monete complementari rappresentano quindi strumenti di scambio che si affiancano alle valute legali senza tuttavia sostituirle. Oltre che per l'acquisto di beni e servizi in ristretti ambiti territoriali, le mone te complementari vengono utilizzate anche all'interno di circuiti come moneta scritturale di credito cooperativo, al fine di permettere la compensazione tra crediti e debiti derivanti dalle transazioni commerciali tra i partecipanti del circuito stesso. Nel concreto, tramite una piattaforma, i soggetti gestori di tali circuiti di credito svolgono nei confronti degli aderenti servizi di pagamento che vengono regolati istantaneamente e integralmente in valuta complementare su appositi conti accesi dagli aderenti stessi sulla piattaforma. I gestori forniscono anche servizi accessori alla detenzione del conto da parte degli aderenti e solitamente concedono a questi anche finanziamenti, sempre in valuta complementare e generalmente di importo contenuto, previa verifica del merito creditizio. I gestori di circuiti di credito in moneta complementare non rientrano, in realtà, tra gli enti autorizzati ai sensi del TUB a esercitare professionalmente i servizi di pagamento e concessione di prestiti. Per quanto riguarda però i servizi di pagamento di tali circuiti questi, in quanto caratterizzati da spendibilità limitata, possono essere svolti anche da soggetti non vigilati. Infatti, secondo il d.l. 27 gennaio 2010 n.11 di recepimento della PSD, non rientrano nella riserva di attività i servizi basati su strumenti di pagamento che vengano utilizzati esclusivamente per l'acquisto di beni e servizi presso l'emittente o, sulla base di un accordo commerciale con l'emittente, per l'acquisto di beni o servizi all'interno di una rete limitata di esercenti o per l'acquisto di una gamma limitata di beni o servizi. L'accezione "rete limitata di esercenti" però, come ha specificato la Banca d'Italia, non prevede la spendibilità dello strumento di pagamento presso una lista di esercenti convenzionati poiché in questo caso l'estensione soggettiva della rete di accettazione non sarebbe determinabile a priori e pertanto risulterebbe potenzialmente illimitata. Laddove un circuito fosse indiscriminatamente aperto all'entrata di qualunque nuovo partecipante si può ritenere che la prestazione del servizio sia rivolta al pubblico in generale e che quindi debba essere riservata agli intermediari autorizzati. Per quanto riguarda la concessione di finanziamenti agli aderenti al circuito le considerazioni sono pressoché analoghe a quelle riguardanti la prestazione dei servizi di pagamento. Tali considerazioni fin qui svolte prescindono dal fatto che le transazioni, all'interno del circuito di credito, avvengano in moneta diversa da quella legale in quanto, per la prestazione di servizi di pagamento e l'attività di finanziamento, le esigenze di ordine pubblico, legate all'affidabilità e la stabilità dell'impresa, sussistono indipendentemente dalla tipologia di valuta utilizzata.

Un'altra questione è quella riguardante la possibilità o meno di considerare la moneta complementare come uno strumento di pagamento avente funzione solutoria[40]. Per conferire carattere di moneta a un determinato strumento utilizzato come mezzo di scambio nella compravendita di beni e servizi, come misura del valore o come mezzo regolatore dei rapporti di debito, non è necessaria l'utilità intrinseca dello strumento stesso ma la fiducia del pubblico nella sua generale accettazione. Se ciò ha permesso in passato la diffusione della moneta scritturale, non

[40] S. Sica, P. Stanzione, V. Zeno Zencovich, "*La moneta elettronica: profili giuridici e problematiche applicative*", 2006

si può quindi escludere che nei sistemi economici moderni alcuni operatori decidano di affidarsi a strumenti alternativi come la moneta complementare per regolare i propri rapporti di credito-debito. Seppur sia le monete complementari e virtuali che la moneta scritturale siano prive di valore intrinseco, le prime a differenza della seconda non possono fare affidamento sul potere di solvibilità generalizzata che discende direttamente dalla legge. È quindi necessario verificare se la specifica moneta alternativa conferisca o meno una disponibilità giuridica apprezzabile in capo a chi la detiene, analizzando in primo luogo la dimensione del circuito al cui interno essa è accettata. Tale dato infatti consente di cogliere il grado di spendibilità e affidabilità di tale valuta alternativa e di conseguenza verificare quanto questa, sulla base dei suoi effetti materiali, possa essere paragonabile almeno in un determinato settore o territorio, alla moneta legale. L'attribuzione di funzione solutoria ad una moneta immateriale alternativa risulta quindi un processo spontaneo, che trova terreno fertile nell'evoluzione tecnologica e nella difficoltà degli intermediari tradizionali, a causa della crisi, di rispondere adeguatamente alle esigenze di soggetti in *deficit* di risorse finanziarie. Tuttavia, è da considerarsi del tutto imprudente e pericoloso che tali processi spontanei avvengano in un contesto di assoluta *deregulation* in quanto il *default* di sistemi di pagamento e circuiti di credito alternativi sono comunque capaci di provocare, laddove non circoscritti, crisi di fiducia che potrebbero innestare effetti di contagio sugli altri operatori tradizionali e addirittura, nei casi più gravi, sull'intero sistema finanziario. A questo proposito, con particolare riferimento alle monete complementari, un'iniziativa legislativa di qualche anno fa e ancora nell'iter parlamentare, prevede di definire i requisiti essenziali di tali monete e presidi sull'attività degli emittenti e dei circuiti, tra cui:

- l'obbligo di iscrizione ad un apposito elenco, a seguito di autorizzazione e sorveglianza da parte della Banca d'Italia
- il rispetto di requisiti di equilibrio economico, di solidità gestionale, di professionalità, di onorabilità e di indipendenza da esponenti aziendali
- l'adozione di un organismo di garanzia che assolva a funzioni di supervisione strategica dell'emittente
- la riserva di attività di cambio di moneta complementare in moneta legale e viceversa ai soli emittenti e gestori dei circuiti, vietando il cambio diretto tra soggetti diversi e la negoziazione di moneta complementare su mercati secondari.

## 7.4 *Sardex*

In Italia, tra i più importanti circuiti di moneta complementare, ricordiamo il *Circuito di Credito Commerciale Sardex*[41] nato nel 2010 e consistente in una piattaforma integrata di pagamenti tra gli aderenti progettata per facilitare le relazioni tra soggetti economici operanti inizialmente solo in Sardegna e poi estesa anche in altre regioni italiane. Lo scopo dichiarato del circuito gestito dalla *Sardex* S.p.a. è quello di facilitare la collaborazione e la nascita di nuove relazioni tra gli operatori economici del territorio, di valorizzare le produzioni locali e di riattivare i consumi, attraverso l'erogazione di strumenti di pagamento e di credito paralleli e complementari a quelli tradizionali.

[41] www.sardex.net

L'impresa che intende aderire al circuito, solitamente caratterizzata da condizioni di illiquidità temporanea, chiede al gestore di essere ammessa al circuito. *Sardex*, dopo aver effettuato una verifica del valore dei beni o servizi che l'impresa può apportare al circuito, riconosce a questa un credito nella valuta complementare *Sardex*, che le permette di scambiare tali beni o servizi prodotti con gli altri imprenditori aderenti al circuito, sino a concorrenza del valore stabilito. I corrispettivi dovuti da un'impresa aderente vengono virtualmente addebitati alla stessa con regolamento immediato in valuta complementare, su un apposito conto online ad essa intestato, amministrato dalla società di gestione. Il funzionamento del circuito di credito commerciale viene ricondotto dalla *Sardex* S.p.a. all'istituto della permuta dalla quale tuttavia differisce, in quanto tale contratto prevede lo scambio reciproco di beni o servizi. Nel caso del circuito invece lo scambio non avviene in maniera reciproca tra due o più parti poiché un imprenditore che riceve un bene da un altro imprenditore non è obbligato a scambiare a sua volta i suoi beni o servizi con quest'ultimo ma può effettuare tale scambio con qualunque altro impresario aderente al circuito. Non essendo quindi identificabile il presupposto della corrispettività, proprio del contratto di permuta, il circuito *Sardex* si identifica piuttosto come un sistema di accordi al contempo plurilaterali tra gli aderenti e bilaterale con il gestore, nel complesso riconducibile alla fattispecie atipica del *barter*, appartenente alla famiglia del baratto. Il *barter* consiste in un contratto plurilaterale atipico in cui una pluralità di soggetti si scambiano vicendevolmente beni o servizi concludendo le relative operazioni tramite compensazione reciproca, in presenza di una *barter company*, in questo caso *Sardex*, la quale gestisce il circuito e regola tutte le operazioni in moneta complementare.

Ad oggi il circuito *Sardex* è attivo in 12 regioni italiane e solo in Sardegna conta 4 mila iscritti. Nel 2017 i crediti transati raggiungono 100 milioni, in questo stesso anno è entrata a far parte del *FinTech* District di Milano ed è stata inserita nell'FT1000 del *Financial Times*, *ranking* delle mille aziende a maggior crescita in Europa.

# 8. *BLOCKCHAIN*

## 8.1 Scopi e metodi di funzionamento

La *Blockchain* è la tecnologia ideata da Satoshi Nakamoto (pseudonimo di un individuo o di un gruppo di sviluppatori) che regola il funzionamento della valuta virtuale più diffusa e celebre, ovvero il *Bitcoin*. Il fine della *Blockchain* è quello di consentire lo scambio, sicuro e in tempo reale, di moneta virtuale tra più soggetti senza la necessità che la transazione sia validata da un'autorità centrale. Il principio dominante alla base della *Blockchain* è difatti quello dell'eliminazione del cosiddetto *middleman*[42], ossia di quei soggetti che a livello centrale validano determinate transazioni, scambi e registri. La *Blockchain* permette di sostituire tali soggetti con un meccanismo di consenso basato sulla crittografia che consente a tutti i partecipanti alla rete di poter porre fiducia sulla legittimità di una transazione senza la necessità di una sua validazione da parte di un soggetto centrale di natura pubblicistica o para-pubblicistica. Nella pratica, la *Blockchain* consiste in un database distribuito,

[42] Vinay Gupta, "*The Promise of Blockchain Is a World Without Middlemen*", 2017

condiviso e basato sulla crittografia che serve quale irreversibile e incorruttibile registro di informazioni e dati memorizzati, non su un singolo computer, ma su più macchine collegate tra loro, chiamate nodi. Le unità fondamentali della *Blockchain* sono i cosiddetti blocchi, ciascuno dei quali contiene: una serie di informazioni riferite ad un numero determinato di transazioni; un collegamento con il blocco precedente nella catena dei blocchi; la risposta ad un complesso quesito matematico utilizzato per validare e confermare i dati contenuti nel blocco stesso. In particolare, al fine di validare una transazione nell'ambito della *Blockchain* e quindi per aggiungere un nuovo blocco alla stessa, viene utilizzato un meccanismo di consenso, definito *Proof-of-Work*, il quale prevede che determinati computer all'interno della rete (i cosiddetti *miners*) risolvano, come già detto, dei complessi quesiti matematici, mentre altri nodi della rete verificano che la soluzione offerta non corrisponda ad un'altra precedente transazione all'interno della catena dei blocchi. La validazione delle operazioni nella *Blockchain* avviene tramite un sistema di firma elettronica creato attraverso una specifica funzione di *hash*, la quale racchiude tutte le transazioni contenute in un blocco in una stringa di dati unica e immutabile. Infine, una copia di tutta la catena dei blocchi viene conservata in tutti i computer della rete, i quali vengono periodicamente sincronizzati in modo che ognuno di essi disponga del medesimo registro distribuito. Mentre nella fase iniziale dello sviluppo della *Blockchain* i *miners* erano per lo più singoli sviluppatori, attualmente si parla invece di gruppi di sviluppatori o vere e proprie società specializzate poiché la crescente affermazione dei *Bitcoin* a livello mondiale ha portato negli ultimi anni a una sempre maggiore complessità dei quesiti matematici proposti per aggiungere blocchi alla catena, con un conseguente incremento esponenziale della potenza di calcolo dei computer necessaria per lo svolgimento di tale operazione. I *miners* vengono incentivati ad aggiungere blocchi alla catena e ad investire quindi in potenza di calcolo attraverso una ricompensa in *Bitcoin*. Alcuni sviluppatori stanno esplorando un sistema di consenso alternativo al *Proof-of-Work* al fine di ottimizzare l'energia necessaria per l'aggiunta di nuovi blocchi alla catena e per aumentare il livello di sicurezza delle transazioni. Tale sistema alternativo definito *Proof-of-Stake*, diversamente dal *Proof-of-Work*, non si basa sulla risoluzione di quesiti matematici ma su meccanismi diversi basati sul principio che ogni utente della catena dei blocchi debba dimostrare il possesso di un certo ammontare di criptovaluta.

La *Blockchain* di *Bitcoin* è una *blockchain* pubblica e *permissionless* in quanto tutti gli utenti di internet possono accedervi e operarvi in maniera incondizionata, ma esistono anche *blockchain* private o modelli ibridi di *blockchain* che si stanno sempre più affermando negli ultimi anni. Per *blockchain* privata si intende un registro che, seppur fondato sulla stessa tecnologia della *Blockchain* di *Bitcoin*, differisce da questa in quanto prevede un'autorità centrale (che validi l'aggiunta di blocchi alla catena e le relative transazioni) e un accesso alle informazioni contenute nei blocchi che può essere sia pubblico che ristretto (*permission based*). Queste ultime ossia le *blockchain* private e *permission based* vengono più correttamente chiamate *Distributed Ledger Technology* (DLT). I modelli ibridi di *blockchain* i cosiddetti *consortium blockchain*[43] permettono di superare la dicotomia pubblico/privato e sfruttare al meglio le potenzialità di entrambi i modelli. I *consortium blockchain* basano il meccanismo di consenso sull'adesione di specifici soggetti partecipanti alla rete di computer e possono essere definiti come modelli parzialmente decentralizzati, in quanto tali sono particolarmente adatti a progetti che richiedono l'identificazione dei soggetti partecipanti alla rete di computer e una qualche forma di coordinamento tra gli stessi. Un recente studio, realizzato

[43] Vitalik Buterin, "*On Public and Private Blockchain*", 2015

dall'ufficio studi del Parlamento europeo[44], ha evidenziato come i possibili ambiti di applicazione delle *blockchain* sono pressoché illimitati: dalle valute virtuali, alla distribuzione di contenuti digitali, alla protezione dei diritti di proprietà intellettuale fino ad arrivare agli *smart contracts* e alle *Decentralized Autonomous Organizations* o DAOs. Nello specifico gli *smart contracts* sono protocolli informatici che facilitano, verificano e fanno rispettare, la negoziazione o l'esecuzione di un contratto, permettendo talvolta la parziale o la totale eliminazione di una clausola contrattuale; i DAOs invece, sono fasci di *smart contracts* determinanti un set di regole di *governance* che, in modo

del tutto automatico, controllano il proprio rispetto da parte dei partecipanti all'organizzazione mediante la *blockchain*.

## 8.2 Principali caratteristiche e relativi risvolti giuridici

La *Blockchain* rappresenterà l'infrastruttura tecnologica alla base della quarta rivoluzione industriale, in quanto consente di creare, accanto ad una rete di informazioni (internet), una rete per lo scambio di valore e rappresenta uno strumento funzionale al dialogo e l'integrazione dei sistemi di intelligenza artificiale e di *Internet-of-Things*, destinati ad apportare profondi cambiamenti di carattere economico e sociale alla realtà attuale. Come già detto la *Blockchain* comporta la sostituzione dei sistemi di certificazione e di scambio di valore governati da autorità centrali, con sistemi decentralizzati, all'interno dei quali ciascun componente della rete può potenzialmente validare uno determinato scambio o stato di fatto, utilizzando una tecnologia che assicura il rispetto di alcune condizioni fondamentali. Ed è proprio l'eliminazione del *middleman* (di fatto la premessa fondamentale della *Blockchain*) che dal punto di vista giuridico, rappresenta il principale punto critico di tale fattispecie, in quanto pone una rilevante questione, ossia se possa essere sufficiente affidarsi alla tecnologia, escludendo l'intervento di un autorità centrale di controllo, per assicurare che i dati immessi nel registro distribuito siano veritieri e corretti e che, in quanto tali, possano avere riconoscimento giuridico ed essere vincolanti per i partecipanti al registro e non solo. A questo interrogativo è possibile dare una risposta affermativa sulla base delle caratteristiche stesse della *Blockchain*, che la rendono a tutti gli effetti una tecnologia sicura. Tali caratteristiche sono:

- L'affidabilità. Essendo la *Blockchain* una rete decentralizzata ciascun componente della stessa può esercitare una parte del controllo sulle informazioni e sui valori custoditi e scambiati ma nessuno può essere in grado di modificare o corrompere la rete nel suo complesso. Quindi eventuali attacchi ad uno dei blocchi della catena non saranno mai in grado di incidere sulla piena operatività degli altri blocchi della stessa. Sotto questo profilo la *Blockchain* risulta dunque sicura e idonea per la sua struttura, a risolvere alcune problematiche tradizionali legate alla sicurezza delle reti. Al contempo la stessa propone nuove sfide riguardo, per esempio, ai possibili attacchi al sistema di consenso utilizzato (*consensus hijacking*) che richiederanno opportuni interventi di natura tecnologica e regolatoria.

[44] European Parliamentary Research Service (EPRS), "*How blockchain could change our lives*", 2017

- La piena trasparenza degli scambi. Tutte le transazioni effettuate sulla *Blockchain* sono visibili ai partecipanti alla rete ma al contempo viene assicurato a questi ultimi l'anonimato, rispondendo così, a livello giuridico, sia all'esigenza di assicurare la riservatezza dei partecipanti alla rete sia all'esigenza di garantire il rispetto delle regole di trasparenza, indispensabili in settori delicati quale, ad esempio, quello dei servizi finanziari.
- La solidità e l'irrevocabilità delle transazioni. Le informazioni e gli scambi inseriti nella *Blockchain* non possono essere infatti modificati e sono irrevocabili, in quanto una volta inserito un blocco nella catena questo non potrà più essere rimosso. Tali caratteristiche che hanno permesso la creazione di innovativi strumenti, come i già citati *smart contracts* e DAOs, pongono a livello giuridico una questione riguardo la natura giuridica delle transazioni che avvengono sulla *Blockchain*, ossia se tali transazioni siano da qualificare come atti meramente esecutivi di accordi che prendono forma altrove o come negozi aventi una propria autonomia e individualità, che nascono e si realizzano pienamente all'interno della *Blockchain* stessa.
- Il carattere integralmente digitale e dematerializzato. Tale caratteristica strutturale consente una tendenziale velocità degli scambi che avvengono sulla *Blockchain* e la naturale transnazionalità degli stessi, ma al contempo comporta l'esclusione dai vantaggi legati all'adozione di questa tecnologia di rilevanti fasce di popolazione mondiale che non hanno ancora accesso alle tecnologie dell'informazione (*digital exclusion*).

In definitiva, lo sviluppo della *Blockchain* e il suo successo come infrastruttura fondamentale per la quarta rivoluzione industriale saranno fortemente condizionati dal livello di penetrazione che la stessa riuscirà ad ottenere nel prossimo futuro, condizionando a sua volta anche l'approccio che i legislatori andranno ad adottare nei confronti di tale tecnologia.

## 8.3 Regolamentazione negli USA

Negli Stati Uniti d'America si stanno compiendo, a livello legislativo e regolatorio, percorsi volti ad attribuire giuridicità alla *Blockchain*, sia costruendo un sistema di regole idoneo a riconoscere effetti giuridicamente vincolanti ai fatti che avvengono sulla *Blockchain* e a favorire l'adozione di tale tecnologia, sia fronteggiando e ponendo rimedio alle criticità più consistenti che l'adozione su larga scala della stessa porta con sé. In alcuni Stati americani come le Hawaii e l'Illinois sono stati costituiti gruppi di lavoro a livello governativo con lo scopo di studiare le possibili applicazioni della *Blockchain* e proporre soluzioni, attraverso l'utilizzo di tale tecnologia, per migliorare il funzionamento di determinanti ambiti, quali la gestione dell'identità digitale, il sistema sanitario e i servizi finanziari. In altri Stati come il Nevada, l'Arizona e il Vermont sono state approvate iniziative legislative volte a riconoscere la *Blockchain* e favorirne l'utilizzo, soprattutto per la certificazione di fatti o la gestione di dati e informazioni. Sotto questo aspetto appare rilevante la legge del Vermont, entrata in vigore il 1° luglio 2016, la quale stabilisce vere e proprie presunzioni legali in relazione all'utilizzo della *Blockchain* per dimostrare determinati fatti o transazioni. In particolare, è stato stabilito che la *Blockchain* sia idonea, nei procedimenti giudiziari, ad essere utilizzata come prova circa l'autenticità dei dati e delle registrazioni avvenute tramite essa, la data e l'ora dell'immissione al suo interno della registrazione e il soggetto che l'ha compiuta. Molto importante inoltre, soprattutto per le sue

rilevanti implicazioni sul piano pratico, è la legge del Delaware entrata in vigore il 21 luglio 2017, la quale riconosce piena legittimità all'utilizzo della *Blockchain* per la creazione e il mantenimento dei registri sociali.[45]

Oltre alle richiamate iniziative legislative di carattere promozionale, negli ultimi tempi la crescente diffusione della *Blockchain* ha spinto i legislatori a intervenire anche con attività volte a correggere le principali criticità insite in tale tecnologia, soprattutto sotto l'aspetto della protezione dei consumatori. La *Securities and Exchange Commission* (SEC), per esempio, con un *Investor Bullettin* del 25 luglio 2017, ha messo in guardia i consumatori sulle possibili criticità legate all'adesione alle *Initial Coin Offering* (ICO), offerte abilitate dall'utilizzo della *Blockchain*. In sostanza esse costituiscono una forma di raccolta di capitale utilizzato per finanziamenti imprenditoriali a fronte dell'emissione di monete virtuali o token che ricolano attraverso la *Blockchain*.

## 8.4 Regolamentazione nell'UE

Mentre negli USA, come abbiamo visto, sono numerose le iniziative legislative volte a riconoscere piena validità ed efficacia alla *Blockchain*, in particolare come strumento di certificazione di fatti, nell'Unione europea la legislazione su tale innovativa tecnologia risulta ancora alle prime armi e limitata essenzialmente all'applicazione della stessa nell'ambito dei soli servizi finanziari. Tra gli interventi normativi più recenti ricordiamo la proposta di risoluzione dell'8 aprile 2017 del Parlamento europeo in cui vengono messi in luce i benefici e i rischi relativi alle applicazioni *blockchain* non autorizzate, evidenziando inoltre come queste siano sempre più spesso utilizzate per le attività criminali, l'evasione fiscale e il riciclaggio di denaro; viene dunque invitata la Commissione europea a monitorare attentamente tale questione e organizzare su questo tema una conferenza multilaterale annuale. Dal canto suo la Commissione europea, nell'ambito della consultazione pubblica avviata su *FinTech*, ha messo in luce che le *blockchain* e le DLT hanno ampie possibili applicazioni nell'ambito dei servizi finanziari (dai pagamenti alla reportistica in chiave di *compliance*) e ha inoltre proposto due temi fondamentali da analizzare, in ottica di futura regolamentazione del fenomeno ossia: la legge applicabile e le regole sull'allocazione delle responsabilità per i fatti che avvengono su tali registri distribuiti; il riconoscimento giuridico del valore e della correttezza dei dati custoditi negli stessi. Infine, con l'obbiettivo di approfondire anche sotto il profilo tecnico il fenomeno, la Commissione ha istituito una *task-force* orizzontale sul *FinTech* e le DLT e avviato nel luglio 2017 un progetto pilota per la realizzazione di un Osservatorio europeo sulla *Blockchain* (*EU Blockchain Observatory*) che serva come centro propulsivo delle iniziative europea sul tema. Al fine di dar luce ad una regolamentazione efficace della tecnologia *Blockchain* è necessario comprendere sia il livello che il modello di regolazione auspicabile. Riguardo al primo aspetto, è possibile affermare con certezza che occorre evitare di percorre strade nazionali (al contrario di quanto avvenuto per la rete internet in passato) e di favorire quindi la formazione di una *governance* di livello transnazionale condivisa e armonizzata in tutto il territorio europeo per evitare appunto le criticità che si sono incontrate nello sviluppo della rete internet. Riguardo al modello di regolazione invece, si possono individuare tre strade alternative:

[45] D. Klain, D. De Martino, "*Delware Governor Signs Groundbreaking Blockchain Legislation into Law*", 2017

- Un modello di regolazione “pesante” che riconosca rilevanza giuridica sollo alle *blockchain* e alle DLT che rispondano a determinati standard condivisi di sicurezza, affidabilità e resilienza
- Un modello di regolazione “leggero” che semplicemente favorisca lo sviluppo di questa tecnologia intervenendo sulla legislazione esistente in modo da favorirne lo sviluppo e da consentirne legalmente l’utilizzo in specifici settori della vita economica
- Un modello di regolazione “ibrido” che da un lato stabilisca requisiti minimi che la tecnologia in questione deve avere per poter attribuire rilevanza giuridica alle transazioni e i fatti che avvengono sulla stessa e dall’altro favorisca la diffusione di tale tecnologia consentendone l’utilizzo legalmente riconosciuto in specifici ambiti regolati.

Il modello ibrido risulta il più efficace in quanto permette di soddisfare due interessi contrapposti, ossia facilitare lo sviluppo e la penetrazione della *Blockchain* assicurando al contempo un’adeguata tutela dei soggetti convolti, in particolare consumatori e investitori. Per quanto riguarda le regole minime da mettere in atto tre appaiono gli ambiti di maggiore interesse: stabilire standard comuni che assicurino l’interoperabilità e prevengano la formazione di posizioni dominanti; assicurare la trasparenza dei meccanismi di funzionamento della tecnologia attraverso specifici obblighi di disclosure delle informazioni rilevanti a carico degli operatori; stabilire regole di responsabilità sostenibili in relazione alle caratteristiche della tecnologia analizzata.

## 8.5 *Initial Coin Offering* (ICO)

Oltre che comprando e vendendo su una piattaforma criptovalute già esistenti, oppure creandole attraverso il processo di *mining*, esiste un altro modo per investire nel mondo dei nuovi strumenti finanziari digitali ossia quello di partecipare alle cosiddette ICO. Come già prima accennato, queste sono un nuovo strumento di finanziamento attraverso il quale delle *start-up* raccolgono il capitale necessario per sviluppare i propri progetti legati alla *Blockchain*, creando nel frattempo una nuova criptovaluta con la quale ricompensano i finanziatori. Il termine ICO è l’acronimo di “*Initial Coin Offering*” ovvero “Offerta iniziale di moneta”, una espressione usata in analogia con il termine “*Initial Public Offering*” (IPO), con cui si intende un'offerta al pubblico di azioni di una società che intende quotarsi per la prima volta su un mercato regolamentato. A differenza delle IPO però le *Initial Coin Offerings* non sono regolamentate e non prevedono presidi a tutela degli investitori e, chi investe in una ICO, non ottiene in cambio azioni, ma quelli che nel gergo delle criptovalute si chiamano *tokens*, ossia le singole unità della nuova criptomoneta che viene lanciata. Questa recente tipologia di operazione di mercato viene considerata un’invenzione di un tale J.R. Willet e registrò casi di successo già dal 2013-2014, ma il momento della svolta è stato il 2017 anno in cui i capitali raccolti con questa nuova forma d'investimento hanno superato di ben 40 volte quelli del 2016 raggiungendo la cifra rilevante di 6 miliardi di dollari. Al momento sono oltre 1.400 le criptovalute lanciate e scambiate sul mercato. Quanto ai vantaggi legati alle ICO essi riguardano sia chi lancia la nuova offerta, in quanto permette a chiunque di sviluppare un progetto senza ricorrere alle tradizionali forme di finanziamento bancario; sia gli investitori, capaci di identificare i progetti più promettenti e ottenere significativi ritorni dagli investimenti effettuati. D’altra parte però la promessa di profitti facili non deve far dimenticare che si tratta di un mercato ad alto rischio. Per definizione, infatti, le ICO si riferiscono a progetti non ancora realizzati e di cui nessuno garantisce il

successo con l'aggravante che, a differenza di quanto accade sui mercati regolati, qui l'investitore non ha alcuna forma di protezione nel caso i cui i promotori dell'ICO si dovessero rivelare dei truffatori, o anche se, più semplicemente, nonostante le buone intenzioni, questi non riuscissero a far avanzare il progetto con i finanziamenti ricevuti. Per far partire l'offerta, i promotori di una ICO presentano normalmente un *White Paper*, ovvero un documento che indica gli obiettivi della raccolta e i dettagli del progetto e che, per dare maggiori garanzie, dovrebbe contenere anche informazioni sui membri del team e una roadmap (ossia una calendarizzazione degli obiettivi che si intende raggiungere e una descrizione del modo in cui lo si farà). Nel *White Paper* viene inoltre specificato quanto durerà la fase ICO (di solito qualche settimana o mese) e viene stabilito il prezzo di partecipazione, ossia si stabilisce un'equivalenza tra una quantità di criptovalute già esistenti da investire e una quantità di *token* che saranno offerti in cambio. Oltre che descrivere i suoi obiettivi, il team si sforzerà anche di convincere gli investitori a scegliere la loro ICO e per farlo avvierà dei canali di comunicazione attraverso social *network* come *Reddit* e siti internet su cui veicolare informazioni sul progetto, ad esempio quanti saranno i token emessi e quanti gli sviluppatori ne terranno per sé. Per partecipare ad una ICO, prima di tutto, bisognerà ovviamente sapere come trovare informazioni sulle offerte di nuovi token digitali che si preparano a sbarcare sul mercato, servendosi di uno dei numerosi siti e forum dedicati proprio a questo scopo. Uno di questi è ad esempio Coinschedule.com, ma ce ne sono molti altri *come ICO Bench, Ico Examiner, ICO Stats, ICO Watch List, ICO Alert*, piattaforme che consentono di visualizzare molte delle ICO già lanciate e quelle programmate per i prossimi mesi. Quando si sarà trovata la ICO in programma, si dovrà stare attenti a raccogliere il maggior numero possibile di informazioni per capire se l'ICO in questione è affidabile o meno, e soprattutto se abbia un progetto valido che la sostiene.

# 9. *REGTECH* E *INSURTECH*

## 9.1 *RegTech*

Il *RegTech* viene considerato da molti un sottoinsieme del *FinTech*, al pari dell'*InsurTech* che cavalca l'innovazione nel modo delle assicurazioni. Il termine *RegTech*, contrazione di *regulation* e *technology*, indica l'impiego di strumenti tecnologici per facilitare l'implementazione delle nuove regolamentazioni e della *compliance* nell'ambito dei servizi finanziari[46], per supportare le procedure di adeguamento, conformità, rispetto di norme e regolamenti e per l'automatizzazione dei processi di reportistica alle autorità di vigilanza. Il *RegTech* mira ad aiutare le imprese e le organizzazioni non solo a essere sempre in regola con le diverse normative e regolamentazioni, aspetto non da poco, soprattutto in sistemi altamente burocratici e soggetti a frequenti cambiamenti come quello italiano, ma anche a comprendere meglio come le regolamentazioni possono essere utilizzate per migliorare le prestazioni della stessa organizzazione. *RegTech* sfrutta le nuove tecnologie (algoritmi inclusi) per gestire, in maniera agile ed efficace, le enormi banche dati degli istituti bancari e

[46] Institute for Internarional Finance, "*RegTech in Financial Services: Technology Solutions for Compliance and Reporting",* 2016

assicurativi, rendendo l'attività di *regulatory management* più semplice. L'obiettivo è quello di creare processi standardizzati in modo da accelerare tempi e ridurre costi. Per riuscirci gli specialisti del *RegTech* sfruttano approcci altamente innovativi come quello della biometrica (per la verifica automatica dell'identità), del cognitive computer (per automatizzare i processi di controllo anti-riciclaggio), delle *Application Programming Interfaces* (API; per automatizzare le condivisione dei dati e consentire l'interoperabilità tra *software* diversi), del *cloud computing* (per archiviare , gestire e condividere con più soggetti enormi quantità di informazioni) e della crittografia (per la sicurezza e l'integrità dei dati). Oltre che dalle imprese e dalle istituzioni finanziarie, le innovazioni tecnologiche del ramo *RegTech* vengono ampliamente utilizzate anche dai supervisori e dalle Autorità di vigilanza per la gestione dei dati e delle informazioni, ricevute dai soggetti vigilati, al fine di potenziare l'efficienza e la velocità dei controlli[47]. Le caratteristiche chiave del *RegTech* si individuano nell'agilità con cui dataset non strutturati possono essere combinati, integrati e analizzati, nella velocità di analisi e nella possibilità di estrarre valore da dati altrimenti privi di significato e utilità.

La *RegTech* ha conosciuto un significativo sviluppo dopo la crisi finanziaria del 2008 che ha portato i regolatori a incrementare significativamente gli obblighi a carico dei soggetti vigilati i quali hanno dovuto confrontarsi anche con una certa difformità degli obblighi di *reporting* e di *compliance* tra le giurisdizioni nazionali e ad una notevole incertezza sui possibili futuri sviluppi del quadro normativo, a fronte di un contesto economico e finanziario in rapido cambiamento. È proprio in questo contesto che l'esigenza sempre più urgente dell'industria di contenere l'incremento vertiginoso dei costi di *compliance* ha dato un forte impulso all'automazione dei processi di controllo e gestione del rischio, sia da parte degli *incumbents* che delle *start-up* innovative. Una misura delle dimensioni del *RegTech* si coglie dall'evoluzione degli investimenti di venture capitalists in *start-up* attive in questo settore. Secondo un'indagine svolta da KPMG[48], a livello globale tali investimenti sono cresciuti in maniera esponenziale negli ultimi anni passando dal 275 milioni di dollari nel 2000 ai 994 milioni a fine 2016. Le aree dove più si sono affermate le innovazioni del *RegTech* riguardano: le disposizioni antiriciclaggio e alla connessa *Know Your Customer rule*; la disciplina dei requisiti patrimoniali e gli obblighi di reporting e di stress testing a carico delle istituzioni bancarie ai sensi del Dodd-Frank Act, Basilea 3 e Basilea 4; la gestione dei rischi del *trading book* ai sensi della Volcker rule e della MiFID2; gli obblighi in materia di servizi di pagamento contenuti nella PSD2. Un forte stimolo allo sviluppo del *RegTech* proviene dalle stesse autorità di vigilanza, che si sono dimostrate attive nel sostenere le innovazioni in questo campo. In ambito europeo ad esempio l'ESMA si è fatta promotrice del *RegTech* incoraggiando la digitalizzazione dei processi di trasmissione e gestione dei dati. L'EBA dal canto suo ha auspicato un approccio coordinato al *RegTech* attraverso un'interazione tra supervisori e industria al fine di raggiungere un adeguato livello di standardizzazione e interoperabilità. Molti esperti del settore affermano che, per effetto del *RegTech*, l'attività di vigilanza sarà sempre più improntata alla logica *data driven* e *forward looking*[49], mentre altri addirittura prefigurano un futuro controllo delle autorità sul sistema finanziario in tempo reale. L'accesso diretto ai dati di vigilanza finora filtrati e forniti dagli operatori finanziari potrebbe consentire ai supervisori una valutazione più accurata delle criticità e delle vulnerabilità dei regolati. Il *RegTech* potrebbe inoltre fornire utili

[47] Institute for International Finance, "*RegTech in Financial Services: Technology Solutions for Compliance and Reporting*", 2016
[48] KPMG, "*The Pulse of FinTech Q117*", 2017
[49] P. Armstrong, "*The Adoption of RegTech*", 2017

strumenti e tecnologie, volti a simulare l'impatto di possibili regole e azioni di *enforcement* sul sistema finanziario, consentendo così la piena applicazione della logica della *better regulation*. Il fenomeno *RegTech* dunque pone i presupposti per una radicale trasformazione dell'attuale struttura regolamentare e di vigilanza.

Accenture ha elaborato una ripartizione del tipo di attività in abito *RegTech* basata su quattro categorie: Identity management (che comprende le procedure *Know Your Customer* e la gestione dei processi di autenticazione e gestione dei dati personali in accordo con le nuove linee guida della GDPR), *Risk & Controls analytics* (con elementi quali *Cybersecurity* e *Risk data aggregation* per la rilevazione e gestione dei rischi e delle attività di controllo), *Surveillance* (che annovera le attività di AML (*Anti Money Laundering*) *Screening* delle transazioni, *Fraud detection* e *prevention*) e *Regulatory intelligence & reporting* (con ambiti quali l'*Automated Reporting* e la *Regulation Interpretation*). Dal punto di vista organizzativo, l'ecosistema *RegTech* è composto da quattro attori principali:

- Le *RegTech start-up* che implementano le nuove tecnologie digitali per presentare soluzioni innovative nel settore;
- Gli enti regolatori, che incoraggiano il dialogo e l'interazione tra i diversi *player* del mercato, per valutare le nuove esigenze regolamentari e creare le infrastrutture per una concorrenza sostenibile;
- Le società di servizi *tech* che analizzano le esigenze del mercato e identificano proattivamente nuove soluzioni, supportando le *start-up* nel portare a scala le proprie innovazioni e aiutando gli *incumbents* ad integrarli;
- Le istituzioni finanziarie che possono contribuire allo sviluppo dell'ecosistema tracciando internamente strategie e percorsi per la diffusione di soluzioni *RegTech* e favorendo la sperimentazione.

L'integrazione tra questi *player* sta dando vita a una molteplicità di modelli di collaborazione, che porteranno vantaggi a tutti i *player* del settore e al mercato stesso. In particolare, per le istituzioni finanziare è possibile definire alcuni benefici di breve periodo quali: un abbassamento dei costi di *compliance*, reso possibile dalla semplificazione e dalla standardizzazione dei processi; una maggior opportunità di integrazione, superando le divisioni tra i diversi ambiti dei sistemi di *risk management* con soluzioni scalabili e flessibili in grado di adattarsi alle mutevoli necessità del business; un'accelerazione della trasformazione digitale; la diffusione continua e mirata dell'innovazione e il conseguente raggiungimento di benefici immediatamente tangibili. Sul lungo periodo, invece, si possono prevedere due principali benefici per l'intero mercato: l'offerta di una migliore *user experience* in termini di *privacy* dei dati e fiducia nel brand, resa possibile da processi innovativi di *onboarding*, *cybersecurity* e *surveillance*; una maggiore resistenza agli *shock* del mercato, grazie alla migliorata capacità di analisi dei rischi in tempo reale che permetterà di implementare rapidamente strategie difensive. L'automazione dei processi di *compliance* può tuttavia determinare nuovi rischi che i regolatori devono tenere in considerazione e apprestarsi a mitigare. Una potenziale vulnerabilità è legata all'*outsourcing* degli algoritmi utilizzati dalle istituzioni finanziarie e alla possibilità che queste ultime, affidandosi a diversi operatori esterni specializzati su specifici segmenti della catena del valore, perdano il controllo dell'intero processo di *compliance*, pur rimanendo gli unici responsabili dello stesso. Altra criticità è legata alla sicurezza informatica, la quale può essere messa a rischio da possibili attacchi, furti e frodi ai danni di archivi digitali

centralizzati. Sono da tenere in considerazione anche il rischio di impresa e il rischio operativo derivante dalla migrazione verso *RegTech* sia per gli operatori tradizionali che per le Autorità di vigilanza, tenute ad acquisire risorse e competenze per il passaggio ad un approccio di vigilanza *digital based*.

Tra le società più famose in campo *RegTech* ricordiamo *Fenergo,* con sede in Irlanda fondata nel 2009, che si occupa di *Know Your Costumer* (KYC), ossia l'identificazione e la verifica dell'identità dei clienti dell'azienda. A tale scopo, *Fenergo* monitora le transazioni del cliente e controlla se i clienti sono chi dicono di essere, attraverso processi del tutto automatizzati e con l'aiuto di tecnologie come l'Intelligenza Artificiale e la *blockchain*. Altra famosa azienda è la *start-up ComplyAdvantage*, fondata nel 2014 a New York, che si occupa di *anti-money laundering* (AML) e corruzione. La società è riuscita a costruire il database globale con l'aiuto della tecnologia del *machine learnings* e controlla quotidianamente oltre 5 milioni di pagine di media per verificare se tra i clienti dell'azienda che si affida a *ComplyAdvantage* vi sono soggetti collegati al terrorismo o al crimine.

## 9.2 *InsurTech*

Il neologismo identifica praticamente tutto ciò che è innovazione tecnologica in ambito assicurativo: *software*, applicazioni, *start-up*, prodotti, servizi. Mutuato dal termine *FinTech* che afferisce al mondo più propriamente bancario, l'*InsurTech* è considerato anche un figlio di questo ed è pertanto molto simile sia per l'impatto che sta producendo sulle imprese tradizionali del settore sia per i fondamenti e le specifiche tecnologie (*Blockchain*, *roboadvice*, P2P, ecc.) su cui si basa, sia per la velocità con la quale si sta affermando. Il termine nasce dalla fusione tra le parole *insurance* e *technology* in quanto è, nei fatti, l'incontro e la sintesi tra questi due mondi, quello assicurativo e quello delle tecnologie digitali. Come le banche anche le assicurazioni sono state tra le industrie più lente nell'adattarsi alla digitalizzazione e nel cogliere le opportunità offerte da questo tipo di trasformazione. *CBInsights*, società di consulenza e reportistica che segue da tempo l'*InsurTech*, va indietro nel tempo fino al 2011 nell'individuazione dei primi investimenti nel settore, ma è nel 2015, che avviene internazionalmente (sebbene con forte concentrazione in US) il vero boom. Quello che ha caratterizzato gli ultimi due anni in ambito *InsurTech* è stato, oltre al numero e all'entità degli investimenti, anche il fatto che, con diverse modalità, le compagnie tradizionali hanno finalmente iniziato ad avvicinarsi a questo mondo, a collaborare con le *start-up InsurTech*, spesso a finanziarle con i propri fondi di *venture capital* o ad acquisirle. Sono inoltre sorti negli ultimi anni *innovation lab* aziendali, programmi di accelerazione, incubatori ed eventi dedicati a questo specifico settore.

## 9.3 *Darwinsurance*

Tra le *start-up* italiane attive nel settore dell'*InsurTech* ricordiamo *Darwinsurance*[50] fondata il 27 aprile 2016 da Yuri Poletto, Tommaso Sala, Kumar Gaurav. *Darwinsurance* è una piattaforma web finalizzata a rendere l'assicurazione *social*, conveniente e trasparente. Il progetto è legato

[50] www.darwinsurance.auxledger.com

all'*insurance peer to peer* (primo caso in Italia) e intende distribuire alle persone polizze assicurative costruendo piccoli gruppi mutualistici di amici e di persone di fiducia con cui condividere e controllare i propri rischi. I prodotti offerti sono polizze assicurative non Vita, rivolte alla clientela retail. Accedendo al sito *Darwinsurance.it* è possibile unirsi a un gruppo online di assicurati e sottoscrivere una polizza di uno dei principali *player* assicurativi italiani, al normale prezzo di mercato. Con una parte dei premi pagati dai membri del gruppo *Darwinsurance* crea una sorta di salvadanaio. Se il gruppo di assicurati mantiene basso il livello dei sinistri il denaro nel salvadanaio non verrà speso del tutto, e la somma rimasta sarà rimessa a disposizione degli assicurati sotto forma di un *bonus* (fino al 20% del premio pagato). La somma redistribuita potrà essere poi utilizzata da ogni assicurato per ridurre il premio al rinnovo della sua polizza o per acquistarne di nuove. Attraverso questo modello di business l'assicurato potrà beneficiare di un ritorno economico in caso di comportamento virtuoso del gruppo, mentre i partner assicurativi di *Darwinsurance* possono contare su un canale distributivo che incentiva i clienti a mantenere comportamenti virtuosi garantendo una diminuzione dei costi operativi ed economici dei sinistri. *Darwinsurance* si configura come un broker assicurativo e in quanto tale è sottoposto ai controlli dell'Autorità di Vigilanza assicurativa IVASS; al momento è attiva solo nel mercato delle polizze viaggi ma a breve l'offerta verrà ampliata. Le polizze vendute sulla piattaforma sono sottoscritte da compagnie di assicurazioni e il pagamento dei sinistri è garantito dalla compagnia che ha sottoscritto la polizza. I ricavi per *Darwinsurance* provengono dalle commissioni che le compagnie assicurative pagano per vendere i prodotti sulla piattaforma; tali commissioni sono una percentuale del premio pagato dai clienti che varia in base alla polizza del prodotto.

# 10. *CYBERSECURITY*

## 10.1 Normativa europea

La sicurezza informatica rappresenta oggigiorno un elemento essenziale per l'efficace funzionamento di quei mercati che si fondano sempre di più sulle tecnologie digitali, come appunto quello del *FinTech*, in cui tra l'altro si presentano preoccupazioni ancora più rilevanti rispetto ad altri mercati, alla luce della specifica tipologia di servizi offerti. La corruzione di una rete o di un sistema informatico utilizzato per offerta id servizi finanziari difatti può avere effetti nefasti sull'intero sistema finanziario e corrodere la fiducia dei consumatori in quest'ultimo. Alla luce di queste considerazioni, il quadro normativo relativo alla sicurezza informatica rappresenta un segmento fondamentale del complesso sistema di norme applicabili direttamente o indirettamente ai servizi *FinTech*. Come si verifica in altri settori anche per l'ambito della sicurezza cibernetica i pilastri fondamentali che regolano la materia sono da ricercare nel diritto dell'Unione europea che rappresenta un livello di governo della materia imprescindibile alla luce delle dimensioni sempre più transnazionali e di vasta scala degli attacchi cibernetici. I primi interventi in materia furono avanzati dall'ENISA, l'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione, istituita nel 2004. L'ENISA nel 2012 ha pubblicato un *White Paper* dedicato all'esame delle strategie nazionali

per la cibersicurezza [51] in cui aveva messo in luce le differenze esistenti e formulato alcune raccomandazioni. Nel dicembre dello stesso anno l'ENISA adottava inoltre la "*Practical Guide on Development and Execution"* in cui affermava l'assenza di una comune definizione di *Cybersecurity* a livello europeo, fattore in grado di condizionare i diversi possibili approcci degli Stati membri nei confronti di questa materia e di ostacolare la cooperazione a livello internazionale. In tale guida l'ENISA identificava inoltre una serie di azioni che, se recepite dagli Stati membri, avrebbero potuto portare ad una strategia nazionale coerente in ogni ordinamento e individuava poi quattro fasi di un ipotetico ciclo di vita della strategia di *Cybersecurity*, ossia lo sviluppo, l'attuazione, la valutazione e gli aggiustamenti. Altro intervento regolatorio rilevante in materia di cibersicurezza è la Comunicazione "*Strategia dell'unione europea per la cibersicurezza: un ciberspazio aperto e sicuro"* pubblicata nel 2013 della Commissione europea e dall'Alto rappresentante dell'Unione europea per gli affari esteri e la politica di sicurezza. Contestualmente a tale Comunicazione veniva presentata una proposta di direttiva sulla sicurezza delle reti e dell'informazione: la direttiva (UE) 2016/1148 (direttiva NIS) che rappresenta il primo atto formale dell'Unione europea in materia e impegna gli Stati membri all'adozione di misure finalizzate a definire un livello di tutela adeguato delle reti e dei sistemi informativi. I motivi ispiratori della strategia europea in materia di cibersicurezza, sono contenuti nei principi informatori definiti dalla Comunicazione del 2013 e consistono: nella necessità di garantire l'applicazione dei valori fondativi dell'Unione europea, sia nel mondo digitale che in quello fisico; nella protezione dei diritti fondamentali, della libertà di espressione e del diritto alla *privacy*, inteso sia nella sua accezione negativa (diritto alla riservatezza) sia positiva (diritto alla protezione dei dati personali); nella garanzia dell'accesso per tutti, che testimonia la caratteristiche di fondamentalità raggiunte ormai da Internet per l'esercizio di una moltitudine di diritti e situazioni giuridiche; nella previsione di una *governance* partecipativa, efficiente e democratica; nella responsabilità condivisa tra attori pubblici, privati e cittadini per la gestione della sicurezza. Già nell'individuazione di questi principi ispiratori emerge la stretta correlazione esistente tra la normativa sulla sicurezza cibernetica e le scelte in tema di *governance* di internet, riguardo alle quali il diritto dell'unione europea, senza sovrastare la libera discrezionalità degli Stati membri in materia, mira a stabilire semplicemente alcuni requisiti base al fine di rendere più efficace e armonizzata l'azione complessiva a livello europeo. In particolare, nella Comunicazione sono individuate cinque priorità strategiche da tenere in considerazione nell'affrontare le sfide sopra riportate, ossia:

- Raggiungere la ciberresilienza per contrastare i rischi e le minacce cibernetiche con dimensione transfrontaliera e facilitare l'elaborazione di risposte coordinate da adottare in situazioni di emergenza
- Sviluppare le risorse industriali tecnologiche per la cibersicurezza, sia promuovendo un mercato unico dei prodotti della cibersicurezza, sia incrementando gli investimenti in ricerca e sviluppo e in innovazione
- Ridurre drasticamente il cibercrimine, sia esortando gli Stati membri alla rapida attuazione delle direttive adottate in materia a livello europeo, sia rafforzando le capacità operative di lotta al crimine informatico e il coordinamento tra gli Stati membri
- Sviluppare una politica di ciberdifesa connessa alla politica di sicurezza e di difesa comune (PSDC), in particolare mediante l'elaborazione di capacità e strategie di difesa basate

[51] ENISA, "*Setting the course for national efforts to strenghten security in cyberspace*", 2012

sull'attività di individuazione, risposta e recupero rispetto a minacce cibernetiche di carattere sofisticato
- Creare una politica internazionale coerente dell'Unione europea sul ciberspazio e promuovere i valori costitutivi dell'UE in materia, attraverso l'integrazione delle problematiche relative alla gestione del ciberspazio nelle relazioni esterne dell'UE e nella politica estera e attraverso lo sviluppo di capacità per la cibersicurezza e di infrastrutture resilienti in Paesi terzi

È per risposta alla prima delle priorità appena descritte che la Commissione europea ha elaborato la proposta di direttiva presentata contestualmente all'adozione della Comunicazione e poi definitivamente approvata nel 2016. Su questo specifico ambito la Commissione segnalava infatti la necessità di innalzare significativamente il livello di armonizzazione delle legislazioni degli Stati membri ritenuta necessaria per eliminare le vulnerabilità che ancora resistevano nel contesto europeo in materia di cibersicurezza[52]. La Commissione inoltre, al fine di sviluppare capacità di ciberresilienza, invitava l'ENISA ad assistere gli Stati membri, in particolare stimolando la creazione di competenze in materia e supportando la realizzazione di esercitazioni periodiche paneuropee su ciberincidenti come base di partenza per una successiva partecipazione dell'UE a esercitazioni di livello internazionale. La Commissione chiedeva inoltre all'industria di promuovere investimenti finalizzati a garantire un elevati standard di sicurezza e lo sviluppo di buone pratiche e scambi di informazioni con le autorità pubbliche. Nello specifico la proposta di direttiva presentava i seguenti obbiettivi: fissare in capo agli Stati membri obblighi minimi in materia di sicurezza informatica; stabilire idonei meccanismi di coordinamento funzionali allo scambio di informazioni e all'assistenza reciproca tra gli Stati membri e le rispettive autorità; prevedere un maggior coinvolgimento del settore privato in materia, soprattutto per gli aspetti relativi allo sviluppo di capacità di resilienza informatica, allo scambio di buone pratiche e alla promozione di investimenti, volti a garantire elevati standard di sicurezza informatica, ormai divenuta, da mero costo di *compliance*, un vero e proprio fattore reputazionale, alla stregua di un *asset* concorrenziale. La direttiva 2016/1148 o direttiva NIS ha dunque introdotto stringenti requisiti per diversi attori privati tra cui banche e fornitori di servizi internet al fine di responsabilizzarli nella valutazione dei rischi in materia di cibersicurezza e di imporre meccanismi adeguati di gestione del rischio capaci di garantire la resilienza delle reti e dei sistemi informativi.

## 10.2 Direttiva 2016/1148 (direttiva NIS)

L'ambito di applicazione della direttiva NIS si estende a due diverse categorie di soggetti. La prima è quella degli operatori di servizi essenziali, ossia una serie di soggetti pubblici e privati che operano in determinati settori elencati nell'Allegato 2 (energia, trasporti, fornitura e distribuzione di acqua potabile, settore bancario, infrastrutture dei mercati finanziari e infrastrutture digitali) e che al contempo presentano determinati requisiti enunciati nell'art.5 part. 2, ossia se: «a) un soggetto fornisce un servizio che è essenziale per il mantenimento di attività sociali e/o economiche fondamentali; b) la fornitura di tale servizio dipende dalla rete e dai sistemi informativi; c) un

[52] Financial Stability Board, "*Financial Stability Implications from FinTech. Supervisory and Regulatory Issues that Merit Authorities' Attentions*", 2017

incidente avrebbe effetti negativi rilevanti sulla fornitura di tale servizio». La direttiva inoltre stabilisce all'art.6 che, nella valutazione degli effetti negativi, gli Stati membri devono tener conto di alcuni fattori intersettoriali, ossia: il numero di utenti ed eventualmente di altri settori che dipendono dal servizio fornito dal soggetto interessato; l'impatto degli incidenti, per entità e durata, sulle attività economiche e sociali e sulla pubblica sicurezza; la diffusione geografica e la quota di mercato del soggetto; l'importanza di quest'ultimo per il mantenimento di un livello sufficiente del servizio, tenendo conto anche delle alternative disponibili. È compito degli Stati membri identificare per ciascuno dei settori elencati nell'Allegato 2, gli operatori essenziali aventi sede nel proprio territorio e istituirne un elenco (da aggiornare su base regolare almeno ogni due anni) entro il 9 novembre 2018, data posteriore al termine ultimo di recepimento della direttiva fissata al 9 maggio 2018. La seconda categoria di soggetti rientranti nell'ambito di applicazione della direttiva NIS è quella dei fornitori di servizi digitali che rientrano in una dalle tre seguenti tipologie: mercato online, motore di ricerca online, *cloud computing*.

La direttiva individua gli opportuni strumenti che le legislazioni degli Stati membri devono prevedere per garantire un adeguato livello di tutela della sicurezza delle reti e dei sistemi informativi. In primo luogo l'art. 7, con riferimento alla strategia nazionale in materia di sicurezza informatica, pur riconoscendo un ampio margine di discrezionalità agli Stati membri in merito ai contenuti, individua alcuni elementi che tale strategia è tenuta ad affrontare, tra cui: obbiettivi e priorità; un quadro di *governance* che consenta la realizzazione di tali obbiettivi e priorità, mediante la definizione di ruoli e responsabilità di organismi pubblici e altri attori rilevanti; misure di preparazione, risposta e recupero; programmi di sensibilizzazione e formazione inerenti alla strategia; piani di ricerca e sviluppo relativi alla strategia; un piano di valutazione dei rischi; un elenco degli attori coinvolti nell'attuazione della strategia. In secondo luogo, la direttiva richiede agli Stati membri di individuare: una o più autorità competenti in materia di sicurezza delle reti e dei sistemi; un punto di contatto unico con il compito di garantire la cooperazione transfrontaliera tra le diverse autorità competenti degli Stati membri; uno o più gruppi di intervento per la sicurezza informatica in caso di incidente (CSIRT) con il compito di trattare incidenti e rischi secondo una procedura predefinita. A livello europeo, invece, con lo scopo di favorire tra gli Stati membri una cooperazione strategica rapida ed efficace, lo scambio di informazioni, la fiducia reciproca ed un comune livello di tutela elevato, la direttiva ha definito due strumenti di coordinamento: il gruppo di cooperazione (composto da rappresentanti degli Stati membri, della Commissione e dell'ENISA) e una rete di CSIRT (composta da rappresentati dei CSIRT degli Stati membri e del CERT-UE).

In merito agli obblighi in materia di sicurezza e notifica degli incidenti e alle forme di attuazione e controllo la direttiva prevede una disciplina differente per operatori di servizi essenziali e fornitori di servizi digitali. Per quanto riguarda i primi la direttiva stabilisce in capo agli Stati membri l'obbligo di provvedere affinché questi adottino misure tecniche e organizzative adeguate a gestire i rischi di cibersicurezza e a prevenire e minimizzare l'impatto di incidenti sulla sicurezza delle reti e dei servizi informativi. Inoltre, in base a quanto stabilito dalla direttiva, gli Stati membri devono prevedere l'obbligo per gli operatori di notificare senza indugio all'autorità competente o al CSIRT gli incidenti che presentano un impatto rilevante sulla continuità dei servizi essenziali e fornire le informazioni necessarie per stimare l'impatto transfrontaliero dell'incidente. La direttiva, in particolare, individua tre criteri per la verifica dell'impatto dell'incidente, ossia: il numero degli utenti interessati dalla perturbazione del servizio; la durata dell'incidente; la diffusione geografica dell'area interessata

dall'incidente. Sulla base delle informazioni contenute nella notifica l'autorità compente può informare gli altri Stati membri in cui la continuità del servizio essenziale sia stata interessata dal medesimo incidente. Inoltre, a seguito di una consultazione con l'operatore, l'autorità competente può anche decidere di informare il pubblico, in merito all'incidente, qualora si ritenga necessario sensibilizzarlo per gestire l'incidente stesso o per evitarne dei nuovi.

Per quanto riguarda i fornitori di servizi digitali la direttiva stabilisce in capo agli Stati membri l'obbligo di prevedere per tali soggetti (come per gli operatori di servizi essenziali) l'adozione di misure tecniche e organizzative sia per la gestione dei rischi sia per la prevenzione e minimizzazione dell'impatto degli incidenti. In particolare, la direttiva specifica che è importante tener conto di alcuni aspetti fondamentali quali la sicurezza dei sistemi e degli impianti, il metodo di trattamento degli incidenti, la gestione della continuità operativa, le forme di monitoraggio, *audit* e *test* e infine la conformità con le norme internazionali.[53] Quanto invece ai criteri per la determinazione dell'impatto di un incidente, oltre agli elementi già indicati per i servizi essenziali, bisogna considerare anche la portata della perturbazione del funzionamento del servizio e la portata dell'impatto sulle attività economiche e sociali. A differenza dei servizi essenziali poi, l'obbligo di notifica dell'incidente opera solo quando il fornitore abbia accesso alle informazioni necessarie per valutarne l'impatto e la portata.

## 10.3 Normativa italiana

In Italia le prime attenzioni in tema di sicurezza cibernetica, risalgono al 2012 quando la legge 7 agosto n.133 introdusse un apposito comma 3-bis all'art.1 della legge n. 124/2007 recante la disciplina del sistema di informazione per la sicurezza della Repubblica. Con tale comma 3-bis il Presidente del Consiglio dei Ministri impartisce al Dipartimento delle informazioni per la sicurezza, direttive volte a rafforzare le attività di protezione delle infrastrutture critiche materiali e immateriali, con particolare riguardo alla protezione cibernetica e alla sicurezza informatica nazionali. Nel 2013 poi, a seguito di una mozione che impegnava il Governo alla costituzione di un Comitato interministeriale incaricato dell'elaborazione di una strategia nazionale per la sicurezza cibernetica e della definizione di indirizzi generali, matura il primo provvedimento in materia ossia il D.P.C.M. 24 gennaio 2013, rubricato "*Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale*". A questo primo importante passo si è arrivati per effetto di una crescente percezione di minaccia cibernetica, come fonte di rischio per la sicurezza nazionale, rendendo improcrastinabile l'elaborazione di un piano strategico nazionale. Quest'ultimo avrebbe dovuto definire un'architettura istituzionale, in cui fossero chiaramente definiti meccanismi e procedure rilevanti, individuati i soggetti competenti a intervenire e individuati i rispettivi ruoli e responsabilità in materia di cibersicurezza. Era previsto in particolare che tale architettura istituzionale dovesse svilupparsi su tre livelli di intervento: il primo di indirizzo politico e coordinamento strategico, con lo scopo di definire gli obbiettivi funzionali alla protezione cibernetica e alla sicurezza informatica; il secondo di supporto a carattere permanente, con finalità di raccordo tra le amministrazioni e gli enti competenti, per l'attuazione degli obbiettivi e delle linee d'azione e l'attivazione delle procedure necessarie in caso di crisi; il terzo livello di gestione della

[53] Commissione Europea, "*Strategia dell'Unione europea per la cibersicurezza: un ciberspazio aperto e sicuro*", 2013

crisi, incaricato delle attività di risposta e ripristino dei sistemi. Il D.P.C.M. individua l'organo di indirizzo politico e di coordinamento strategico nel Comitato interministeriale per la sicurezza della repubblica (CISR), il quale ha provveduto ad approvare nel dicembre 2013 il Quadro strategico nazionale per la sicurezza nello spazio cibernetico e il Piano nazionale per la protezione cibernetica e la sicurezza informatica, recentemente sostituiti dalle nuove versioni in vigore da marzo 2017.

Il Quadro strategico nazionale identifica i profili e le tendenze evolutive delle minacce cibernetiche e della vulnerabilità delle reti e dei sistemi informativi; definisce i ruoli e i compiti dei diversi soggetti pubblici e privati e dei soggetti nazionali operanti al di fuori del territorio italiano; individua strumenti e procedure per favorire lo sviluppo delle capacità di prevenzione e risposta, in relazione agli eventi dello spazio cibernetico. Inoltre, il Quadro strategico nazionale definisce sei indirizzi strategici:

- Il miglioramento delle capacità tecnologiche, operative e di analisi degli attori istituzionali secondo un approccio integrato
- Il potenziamento delle capacità di difesa delle infrastrutture critiche e degli attori di rilevanza strategica a livello nazionale
- Il rafforzamento delle capacità di contrasto alla diffusione di attività e contenuti illegali online
- La promozione e la diffusione della cultura della sicurezza cibernetica tra i cittadini e all'interno delle istituzioni
- L'incentivazione della cooperazione tra istituzioni e imprese nazionali
- Il rafforzamento della cooperazione internazionale in materia di sicurezza cibernetica

Questi sei indirizzi strategici sono stati declinati in undici indirizzi operativi sviluppati più dettagliatamente nel Piano nazionale, il cui fine è quello di individuare obbiettivi e linee d'azione per la realizzazione del Quadro strategico nazionale. La sicurezza informatica e la protezione cibernetica non si qualificano quindi solo come un obbiettivo ma come un vero e proprio processo[54] che si snoda in una sorta di roadmap descritta dal Piano. In particolare, gli indirizzi operativi articolati nel Piano sono:

- Il potenziamento delle capacità di *intelligence*, di polizia e di difesa civile e militare, funzionale all'approfondimento delle vulnerabilità e delle minacce cibernetiche, al fine di rendere più resilienti le infrastrutture e più efficace il contrasto delle minacce
- Il potenziamento, a livello nazionale, dell'organizzazione e delle modalità di coordinamento e integrazione tra i soggetti pubblici e privati a cui è affidata la gestione di infrastrutture critiche nazionali
- L'operatività delle strutture nazionali di *incident prevention, response e remediation*; a questo proposito il Piano prende atto delle previsioni della direttiva NIS che richiedono agli operatori di servizi essenziali la costituzione di CSIRT incaricati di offrire consulenza e supporto in caso di evento cibernetico
- La cooperazione internazionale e l'organizzazione di esercitazioni, considerato il carattere transnazionale delle minacce cibernetiche

[54] C. Cencetti, "*Cybersecurity: Unione europea a Italia. Prospettive a confronto*", 2014

- La promozione e la diffusione della cultura della sicurezza informatica, tramite idonee iniziative di formazione e addestramento, rivolta a cittadini privati e al personale delle imprese e della Pubblica Amministrazione
- Gli interventi legislativi e la *compliance* con gli obblighi internazionali; a tal proposito il Piano individua quattro linee d'azione puntuali che si riferiscono (1) alla revisione e il consolidamento della legislazione in materia di sicurezza informatica (2) alla definizione di quadro giuridico adeguato a supportare le attività di cibersicurezza (3) all'attribuzione di responsabilità e alla sanzione delle violazioni (4) al recepimento della direttiva NIS secondo un approccio armonizzato con le disposizioni vigenti in materia di infrastrutture critiche e strategiche
- La *compliance a standard* e protocolli di sicurezza, che garantisce un elevato livello qualitativo di protezione cibernetica e sicurezza di reti e sistemi
- Il supporto allo sviluppo industriale e tecnologico al fine di garantire un innalzamento del livello di affidabilità e sicurezza, già a partire dalla progettazione delle componenti essenziali *hardware* e *software*
- Le risorse, la cui distribuzione presuppone un'adeguata misurazione dei costi riconducibili a eventi di natura cibernetica occorsi o potenziali
- L'implementazione di un sistema di *cyber risk management* nazionale che si occupi della salvaguardia del valore, dell'autenticità, integrità, riservatezza e disponibilità delle informazioni

Al D.P.C.M. del 2013 ha fatto seguito la nuova versione del 17 febbraio 2017 contenente, rispetto al primo, alcune misure di revisione che tengono conto sia delle accresciute competenze di consulenza, proposta e deliberazione in situazioni di crisi, sia dell'entrata in vigore della direttiva NIS. Si è così provveduto ad un'opera di ammodernamento, razionalizzazione e semplificazione della struttura istituzionale che era stata delineata nel 2013. Il D.C.P.M., inoltre, contiene alcune definizioni importanti come quelle di spazio cibernetico e sicurezza cibernetica. Lo spazio cibernetico viene definito come «l'insieme delle infrastrutture informatiche interconnesse, comprensivo di *hardware*, *software*, dati ed utenti, nonché delle relazioni logiche, comunque stabilite, tra di essi»; la sicurezza cibernetica viene definita «condizione per la quale lo spazio cibernetico risulti protetto grazie all'adozione di idonee misure di sicurezza fisica, logica e procedurale rispetto ad eventi, di natura volontaria o accidentale, consistenti nell'acquisizione o nel trasferimento indebito di dati, nella loro modifica o distruzione illegittima, ovvero nel controllo indebito, danneggiamento, distruzione o blocco del regolare funzionamento delle reti e dei sistemi informativi o dei loro elementi costitutivi».

All'interno del D.C.P.M. vengono stabilite, nell'ottica di definire l'architettura istituzionale, le competenze del Presidente del Consiglio dei ministri, il quale adotta sia il Quadro strategico nazionale che il Piano nazionale (nel primo caso su proposta del CISR, nel secondo caso su deliberazione dello stesso) e assume tutte le determinazioni rilevanti quale vertice del Sistema di informazione per la sicurezza della Repubblica. Sono inoltre esplicitati nel DPCR i compiti del CISR che, oltre a proporre l'adozione del Quadro strategico e deliberare il Piano nazionale, può partecipare in caso di crisi cibernetica alle determinazioni del Presidente con funzioni di consulenza, proposta e deliberazione. Il CISR svolge anche funzioni consultive, esercita l'alta sorveglianza sull'attuazione del Piano nazionale, elabora indirizzi generali e obbiettivi fondamentali in materia di

protezione cibernetica e sicurezza informatica nazionali. A supporto del Presidente del CISR, opera il Nucleo per la sicurezza cibernetica istituito presso il Dipartimento delle informazioni per la sicurezza (DIS), presieduto dal vice direttore generale del DIS e composto da rappresentanti dei ministeri competenti e dell'Agenzia per l'Italia digitale. Il Nucleo, che si riunisce almeno una volta al mese, svolge funzioni di raccordo tra le componenti dell'architettura istituzionale nel campo della sicurezza cibernetica. Tra i compiti del Nucleo espressamente elencati nell' art.9 ricordiamo: la promozione della programmazione e pianificazione operativa della risposta da parte di amministrazioni e operatori privati a eventi di crisi cibernetica; l'attivazione all'interno del Nucleo dell'unità per l'allertamento (operativa tutti i giorni h24). Quest'ultima, ricevuta una segnalazione di eventi cibernetico, dirama gli allarmi alle amministrazioni e agli operatori privati, informa il Presidente e valuta se l'evento sia di dimensioni e intensità tali da richiedere decisioni coordinate a livello interministeriale. Al direttore generale del Dipartimento per le informazioni della sicurezza è invece affidata la definizione delle linee d'azione per migliorare il livello di sicurezza dei sistemi e delle reti, nella prospettiva di individuare gli strumenti tecnologici più avanzati e adeguati al compimento delle azioni di prevenzione, contrasto e risposta in caso di crisi cibernetica da parte di amministrazioni, enti pubblici e operatori privati.

## 10.4 Sicurezza cibernetica dei servizi finanziari

Le problematiche inerenti alla sicurezza cibernetica assumono particolare rilievo in riferimento allo specifico settore dei servizi finanziari che, presentando una particolare esposizione nei confronti del pubblico, risultano maggiormente vulnerabili ad attacchi cibernetici. Sebbene la direttiva NIS appaia già presentare le potenzialità per garantire la tutela della sicurezza cibernetica in un campo assai vasto di servizi, rimane l'interrogativo se la tutela da attacchi cibernetici nel settore dei servizi finanziari richieda l'adozione di un approccio specialistico, con un intervento regolatorio *ad hoc*, in ragione delle peculiarità dei rischi in ambito *FinTech*. Un recente studio del *Financial Stability Institute*[55], ha evidenziato che a livello mondiale solo alcuni Paesi (tra cui USA, il Regno Unito, Singapore e Hong Kong) si sono dotati di una normativa *ad hoc* di carattere speciale per far fronte agli attacchi cibernetici relativi al settore dei servizi finanziari. Un approccio specialistico presenta al contempo sia vantaggi che svantaggi. In merito ai vantaggi la presenza di regole *ad hoc*, senz'altro contribuisce a rafforzare, in particolare da parte degli operatori, la percezione e la consapevolezza dell'esistenza di profili di rischio non trascurabili di cui tenere debitamente e obbligatoriamente conto. Quanto ai possibili svantaggi l'adozione di regole *ad hoc* potrebbe risultare controproducente laddove si utilizzasse un approccio di carattere prescrittivo con la definizione di regole puntuali difficili da conciliare con l'evolversi della tecnologia e delle minacce cibernetiche (sarebbe quindi consigliabile, in tal caso, la scelta di una regolazione per principi, più adatta alla fattispecie in questione). È da tenere in considerazione inoltre che un intervento regolatorio specialistico (considerando la dimensione transfrontaliera sia delle infrastrutture utilizzate per la prestazione dei servizi finanziari sia degli attacchi cibernetici) per rivelarsi davvero efficace, dovrebbe condividere la stessa matrice nel diritto dell'Unione europea e non limitarsi ad operare su un piano meramente

[55] Financial Stability Board, "*FSI Insight on policy implementation No 2, Regulatory approaches to enhance banks' cybersecurity frameworks*", 2017

domestico. Quanto maggiore quindi sarà la coerenza nell'approccio di ciascun ordinamento tanto più potrà giovarne la cooperazione tra le diverse autorità e l'efficace opera di prevenzione e contrasto delle minacce cibernetiche.

L'esigenza di un coordinamento a livello internazionale su questo versante è stata di fatti sottolineata anche nel 2016 durante il G7 (che riuniva i Ministri delle finanze e i governatori delle banche centrali dei rispettivi paesi), come testimoniato dall'adozione del documento "*G7 fundamental elements of cybersecuruty for the financial sector*". Quest'atto definisce una serie di capisaldi intorno ai quali ogni istruzione pubblica e privata operante nel settore dei servizi finanziari potrà sviluppare la propria strategia e il relativo quadro operativo in materia di sicurezza cibernetica; il tutto secondo un approccio comune che potrà giovare complessivamente alla sicurezza cibernetica e alla resilienza del sistema finanziario. Gli elementi fondamentali su cui si concentra il documento del G7 riguardano:

- La definizione di una strategia e di un quadro sulla sicurezza cibernetica coerenti con la specificità del settore finanziario e che consentano di identificare gestire e ridurre efficacemente i rischi e le minacce cibernetiche
- la definizione di un adeguato assetto di *governance* che permetta di individuare ruoli e responsabilità dei soggetti competenti ad attuare e monitorare la strategia sulla sicurezza cibernetica
- la valutazione dei rischi e dei sistemi di controllo, al fine di poter stimare l'esposizione ad attacchi cibernetici e di decidere eventualmente di non svolgere attività che presentano rischi troppo elevati o di mitigarli attraverso opportune modalità di controllo, condivisione e trasferimento
- l'istituzione di processi di monitoraggio sistematico che consentano di individuare eventuali incidenti e di verificare periodicamente l'efficacia dei sistemi di controllo tramite attività di testing e di *auditing* affidate preferibilmente a soggetti indipendenti dal personale responsabile dell'attuazione dei programmi di *cybersecurity*
- la pronta e sicura condivisione con altre imprese e autorità pubbliche di informazioni relative per esempio a minacce, vulnerabilità incidenti di natura cibernetica
- l'attivazione di *policy* e misure che permettano un'efficace *incident response* nelle sue varie fasi (individuazione di un incidente, contenimento dei danni, notifica a soggetti interni ed esterni, coordinamento delle attività di risposta necessarie)
- la realizzazione di attività di recupero secondo uno schema che, una volta ripristinata la stabilità e l'integrità operazionale, attribuisca priorità alle funzioni critiche di natura economica; a tale scopo la capacità delle autorità pubbliche e delle imprese di attuare forme di reciproca assistenza accresce la fiducia nel sistema finanziario e l'efficacia della risposta agli incidenti
- l'implementazione di una strategia di *continuous learning*, fondata sulla revisione periodica (e al ricorrere di eventi significativi) della strategia e del quadro sulla sicurezza cibernetica in modo di reagire adeguatamente alla rapida capacità di evoluzione delle minacce e delle vulnerabilità; sotto tale aspetto è importante che siano considerate oltre alle specificità del settore finanziario anche le esternalità determinate dai mutamenti in altri settori quali energia e telecomunicazioni

Altro documento importante riguardante il tema della cibersicurezza nel settore finanziario è quello delle "*Guidance on cyber resilience for financial market infrastructures"* adottato dal *Commitee on Payments and Market Infrastructures* (CPMI) in aggiunta ai "*Principles for Financial Market Infrastructures"* (PDMI), ossia i principi e gli standard sui quali deve basarsi l'attività di vigilanza e supervisione del sistema dei pagamenti e del mercato finanziario. Le *Guidance* definiscono delle linee guida per le infrastrutture del mercato finanziario, che mirano ad orientare l'implementazione di misure necessarie ad un rafforzamento delle capacità di resilienza informatica attraverso un approccio che tenga conto dei rischi crescenti a cui le minacce cibernetiche espongono la stabilità finanziaria.

Il già citato studio del *Financial Stability Institute* dell'agosto 2017 che esplora i diversi modelli di regolazione ha inoltre presentato alcune indicazioni di *policy* utili alle autorità nazionali del settore finanziario che volessero introdurre una regolazione specifica della protezione cibernetica nel settore bancario. Tra tali indicazioni figurano: l'incorporazione del rischio cibernetico nel quadro per la gestione del rischi; la previsione dell'obbligo per gli istituti bancari di dotarsi di standard tecnici e di un quadro di controllo e risposta efficace al rischio cibernetico; la promozione di una maggiore cultura della cibersicurezza tra il personale; il rafforzamento della collaborazione con l'industria; il perseguimento di una maggiore cooperazione e coerenza a livello transfrontaliero nella definizione degli approcci di regolazione e vigilanza.

## 10.5 *Unfraud*

L'unica italiana, su 137 aziende di tutto il mondo che si occupano di *cybersecurity* in ambito finanziario, si chiama *Unfraud*[56], ha sede a Roma ed è una *start-up* fondata nel 2014 da Andrea Puzo, Vincenzo Paduano e Armando Monaco, rispettivamente un economista e due ingegneri di Ariano Irpino. L'obbiettivo di *Unfraud* è quello di migliorare sensibilmente l'affidabilità delle transazioni online attraverso un sistema di intelligenza artificiale in grado di scovare e prevenire le frodi che minacciano le transazioni, con un costante monitoraggio delle attività di business online. Nello specifico *Unfraud* ha sviluppato un *software* che imita i comportamenti del cervello umano, basato sull'intelligenza artificiale e su algoritmi *bio-tech* usati in oncologia per la ricerca sulle cellule. Il programma determina modelli dinamici di comportamento, li discrimina e li segnala al sistema, così da prevenire la frode. Il vantaggio competitivo di *Unfraud*, rispetto a realtà analoghe, è quello di non usare i consueti strumenti antifrode, cioè regole ferree e statiche, ma una tecnologia basata su algoritmi proprietari che riescono a controllare contemporaneamente centinaia di variabili per singola transazione e ad apprendere dall'esperienza.

Per quanto riguarda la *Security Platform* di *Unfraud* essa è stata progettata allo scopo di prevenire e individuare le frodi in tempo reale, ovvero persino prima che accadano, contribuendo ad evitare perdite e migliorare la fiducia dei consumatori. La piattaforma è tra l'altro completamente adattabile al modello di business di qualsiasi azienda o ente e raccoglie, per ogni evento, fino a

[56] www.unfraud.com

migliaia di dati reali, senza un *layout* fisso o prestabilito. Il cliente può scegliere soltanto le funzionalità della piattaforma di cui hai bisogno; può dunque:

- Essere protetto tramite il core di riconoscimento frodi *Tomoko*, costruito con tecnologie di *Deep Learning*, le tecnologie di Intelligenza Artificiale più avanzate del pianeta.
- Scovare *pattern* nascosti grazie ad *Augusta*, strumento di data *augmentation* in grado di scoprire nuovi significati nei dati stessi e da fonti esterne (*databases, social networks*, ecc.)
- Ottenere la protezione massima grazie a *BeA* (*Behavior Analytics*), uno strumento per l'analisi del comportamento dell'utente, capace di effettuare un *device fingerprinting* completo
- Monitorare i dettagli dei dati del cliente sulla *DaViDa* (*Data Visualization Dashboard*), da cui ottenere una panoramica delle frodi ma anche del business, controllando l'attività degli utenti o anche singoli eventi o transazioni.

*Unfraud* è inoltre attenta a ciò che avviene su *Deep Web* e *Dark Web*, patria di frodatori e *hacker*: per questo motivo ha sviluppato *DaWSko* (*Dark Web Scout*), uno strumento in grado di rilevare quali utenti provengono dal *Deep* o *Dark Web* e che quindi potrebbero essere malintenzionati.

Nel 2014 *Unfraud* è entrata nel percorso di accelerazione di TIM #WCap, acceleratore di TIM. Nel 2015 la *start-up* si è classificata fra i finalisti del CheBanca! GrandPrix, competizione lanciata dall'istituto di credito per individuare, premiare e sostenere le *start-up* più innovative d'Italia in ambito *FinTech*. A maggio 2016 TIM *Ventures*, il *Corporate Venture Capital* di TIM, ha deciso di investire 100mila euro sulla *start-up* uscita dal suo programma di accelerazione. Ad oggi *Unfraud*, che ha meno di dieci dipendenti, ha raccolto in tutto più di 130 mila dollari in due round: un primo *grant* da 25mila euro (quello di TIM WCap), più l'investimento *seed* di TIM *Ventures*. Il valore di mercato della *fraud prevention* a settembre 2017 era di 10 miliardi di euro ed è previsto che arrivi a circa 20 miliardi entro il 2019.

# 11. *FINTECH* E ANTIRICICLAGGIO

## 11.1 Il riciclaggio e il finanziamento del terrorismo

Il riciclaggio, qualificato come reato nella maggior parte degli ordinamenti penali nazionali, consiste nella riutilizzazione per attività legali, di denaro frutto di attività illecite. È un fenomeno economico-finanziario di natura transnazionale e incide notevolmente sulle dinamiche della ricchezza di una nazione. I criminali occultano l'origine illecita del denaro, in modo che non possa essere ricondotta ad una azione criminale, mediante la divisione della somma di denaro in piccole quote di importo esiguo, inserite in molteplici conti stabiliti in più Paesi e intestati ad individui o aziende diverse; spesso viene conferita un'origine legale apparente al denaro per poterlo immettere nel mercato creando finti contratti, prestiti, vincite o fatture.

Il finanziamento del terrorismo invece può avere come fonti di denaro attività sia lecite che criminose; ed è proprio l'origine non necessariamente illecita delle disponibilità finanziarie, insieme

all'utilizzo di somme spesso di importo esiguo, che rendono particolarmente complessa l'individuazione preventiva delle condotte finalizzate appunto al finanziamento del terrorismo. La drammaticità degli attentanti statunitensi dell'11 settembre 2001 hanno palesato l'esistenza di una complessa rete terroristica internazionale le cui ramificazioni territoriali provvedono sia al reclutamento degli affiliati che alla raccolta dei mezzi finanziari necessari per il perseguimento degli obbiettivi criminali. Le organizzazioni terroristiche sfruttano abilmente le opportunità offerte dall'integrazione a livello globale dei mercati e le nuove tecnologie in campo finanziario, al fine di veicolare, da un Paese all'altro, in modo occulto, i fondi essenziali per le proprie attività. Gli attentati terroristici statunitensi hanno tra l'atro messo in luce la permeabilità dei sistemi finanziari internazionali all'attività terroristiche e l'esistenza di serie lacune regolamentari[57].

Il riciclaggio di denaro e il finanziamento del terrorismo dunque, rappresentano una grave minaccia per l'integrità e la stabilità del sistema finanziario con conseguenze potenzialmente devastanti sia per la società che per l'economia.

## 11.2 Gruppo di Azione Finanziaria Internazionale (GAFI)

Col fine di contrastare le attività finanziarie illecite, il GAFI (organismo intergovernativo avente il compito di ideare e promuovere strategie di prevenzione e di contrasto del riciclaggio, del finanziamento del terrorismo e della proliferazione di armi di distruzione di massa) ha elaborato le cc.dd. 40 Raccomandazioni, ossia standard riconosciuti a livello internazionale che i Paesi sono chiamati a recepire all'interno dei rispettivi ordinamenti giuridici, amministrativi e finanziari. Le 40 Raccomandazioni, nonostante non abbiano effetti giuridicamente vincolanti, in quanto fonti di *soft law*, influenzano ugualmente le politiche legislative dei singoli Stati delineando l'ossatura dei sistemi antiriciclaggio e dei sistemi di controllo nazionali finalizzati alla prevenzione del finanziamento del terrorismo. A partire dal 2016 il GAFI ha focalizzato la propria attenzione anche su *FinTech* e *RegTech*, annunciando inoltre l'intenzione di sviluppare con esse una *partnership* per supportare l'innovazione dei servizi finanziari e mitigare al contempo i rischi ad essa associati tramite l'elaborazione di *standard guide* e *best practices* sulle nuove tecnologie. A parere del GAFI le innovazioni tecnologiche possono difatti rappresentare un valido strumento per contrastare il riciclaggio e il finanziamento del terrorismo. Ad esempio, i *big data*, l'intelligenza artificiale e il *machine learnings* possono perfezionare il riconoscimento delle operazioni sospette e dei *network* criminali mentre le innovazioni in campo *RegTech* possono rendere più sicuro ed efficiente il processo di verifica della clientela. Bisogna comunque tenere in considerazione che le innovazioni tecnologiche, oltre ad offrire numerose opportunità, presentano anche pericolosi rischi in quanto possono essere utilizzati come nuovi mezzi da criminali e terroristi per trasferire denaro.

Nel corso del "*FATF FinTech and RegTech Forum 2017*" (a cui hanno partecipato più di 150 esponenti del GAFI, delle istituzioni finanziarie e dei settori *FinTech* e *RegTech*) sono stati approvati i seguenti principi guida, cc.dd. "*The San Jose Principles*":

[57] M. Condemi, F. De Pasquale, "*Lineamenti della disciplina internazionale di prevenzione e contrasto del riciclaggio e del finanziamento del terrorismo*", 2008

- L'obbiettivo comune è quello di contrastare i fenomeni di riciclaggio e finanziamento del terrorismo al fine di rafforzare l'integrità del sistema finanziario attraverso una stretta cooperazione e il lavoro congiunto tra i governi e il settore privato
- Va perseguita un'innovazione positiva e responsabile capace di attenuare i rischi e implementare l'efficacia delle misure di contrasto del riciclaggio e del finanziamento del terrorismo
- È necessaria una migliore comprensione di come i vigenti obblighi dettati dalla disciplina di lotta al riciclaggio e al finanziamento del terrorismo si applichino alle nuove tecnologie e ai nuovi prodotti e servizi finanziari
- È necessario adottare regole giuste e coerenti capaci di creare un contesto normativo commercialmente equo, che rispetti il *level playing field* e riduca al minimo le incongruenze regolatorie a livello sia nazionale che internazionale

Il GAFI ha inoltre osservato che nell'ambito delle innovazioni *FinTech* i gruppi criminali organizzati, tra cui anche l'ISIS e i *foreign fighters*, fanno un crescente uso di strumenti quali il *crowdfunding*, le valute virtuali, le carte prepagate, i pagamenti online e i *mobile services*. In particolare, sulle valute virtuali il GAFI, nel *report* "*Emerging Terrorist Financial Risks*" dell'ottobre 2015, ha riportato un case study inerente l'utilizzo di tali valute per il finanziamento del terrorismo.[58] Nell'agosto del 2015 Ali Shukri Amin è stato condannato negli USA a 11 anni di prigione per aver usato *Twitter* al fine di sostenere l'ISIS dando indicazioni su come servirsi dei *Bitcoin* per celare la fornitura di fondi a tale organizzazione terroristica e agevolare il viaggio verso la Siria dei sostenitori della stessa. In merito alla prevenzione e al contrasto della criminalità finanziaria è intervenuta anche Christine Lagarde (*Managing Director* del Fondo Monetario Internazionale), il 22 giugno 2017 all'Assemblea plenaria del GAFI, evidenziando come *FinTech* si mostri come un'arma a doppio taglio: da un lato può essere utilizzato per promuovere e finanziare il terrorismo, dall'altro però può costituire un potente strumento per fortificare le difese contro quest'ultimo, grazie al suo utilizzo per l'individuazione di somme, anche di importo esiguo, destinate ad organizzazioni criminali.

## 11.3 Rischi legati al *crowdfunding* e alle valute virtuali

I recenti attentati terroristici hanno evidenziato l'emergere di nuove tendenze soprattutto riguardo le modalità con cui i gruppi terroristici finanziano le proprie attività. In particolare, alcuni servizi basati sulle moderne tecnologie e utilizzati come sistemi finanziari alternativi, restando al di fuori del campo di applicazione della legislazione dell'UE o beneficiando di minori controlli e ampie deroghe, risultano sempre più appetibili per le organizzazioni terroristiche. La mancanza di una normativa e di controlli adeguati riguardo l'utilizzo di tali servizi finanziari innovativi inoltre permette a chi ricicla denaro di occultarne l'origine illecita più facilmente rispetto a quanto possibile utilizzando i servizi finanziari tradizionali.

L'Unità di Informazione Finanziaria per l'Italia o UIF per l'Italia (l'unità centrale nazionale avente il compito di ricevere, analizzare e trasmettere alle autorità competenti le segnalazioni di operazioni sospette di riciclaggio e di finanziamento del terrorismo) con la Comunicazione "*Prevenzione del*

[58] G. Vangone, "*Il terrorismo islamico nell'era di Internet, fra Bitcoin e dark web*", 2015

*finanziamento del terrorismo internazionale*" del 18 aprile 2016, ha messo in evidenza come le opportunità offerte dall'innovazione tecnologica possano essere utilizzate per finalità di finanziamento del terrorismo con un particolare focus sul *crowdfunding* e sulle valute virtuali. Con riferimento al *crowdfunding*, il 1° luglio 2015 l'ESMA ha pubblicato le "*Questions and Answers – Investment-based crowdfunding: money laundering/terrorist financing*" (Q&A) concernenti i rischi di riciclaggio e finanziamento del terrorismo legati a questa tipologia di *funding* (le piattaforme di *crowdfunding* possono essere utili infatti sia per raccogliere fondi destinati al finanziamento del terrorismo sia per nascondere l'origine illecita del denaro). Tali rischi possono essere attenuati qualora le piattaforme siano obbligate dalla normativa vigente al compimento di controlli minimi che prevedano un'adeguata verifica del titolare del progetto, del progetto stesso e degli investitori, per individuare le situazioni che presentano maggiori rischi e anomalie; indispensabile è anche l'adozione di presidi idonei a identificare e gestire tali rischi. L'ESMA ha inoltre segnalato che non tutte le piattaforme di *crowdfunding* hanno lo stesso *status* regolamentare in tema di contrasto dei fenomeni di criminalità finanziaria in quanto: alcune piattaforme risultano sottoposte alla direttiva MiFID e sono quindi soggette all'obbligo di adeguata verifica della clientela; altre invece, beneficiando dell'esenzione dall'applicazione del MiFID, osservano quanto stabilito dai regimi nazionali. A riguardo l'EBA ha sostenuto quindi la necessità di assicurare che tutte le piattaforme di *crowdfunding* rientrino nell'ambito di applicazione della Quarta Direttiva Antiriciclaggio, così da essere tutte soggette agli obblighi di adeguata verifica della clientela.

Per quanto riguarda le monete virtuali il 30 gennaio 2015 l'UIF per l'Italia ha pubblicato la Comunicazione "*Utilizzo anomalo di valute virtuali*", nella quale, tra le altre cose, ha messo in risalto come tali valute possono esporre a elevati rischi di riciclaggio e di finanziamento del terrorismo, in ragione del maggior grado di anonimato di cui le operazioni in valute virtuali beneficiano rispetto ai classici trasferimenti di fondi, caratteristica che le rende più appetibili alle organizzazioni terroristiche. Altri rischi sono legati inoltre all'irreversibilità delle operazioni, alla natura opaca e tecnologicamente complessa su cui si basa il loro funzionamento e alla mancanza di garanzie regolamentari. L'UIF per l'Italia, nella suddetta Comunicazione, ha inoltre esortato gli intermediari finanziari e gli operatori di gioco ad avere cura di individuare le attività connesse con le valute virtuali esaminandole in relazione al profilo soggettivo del cliente, al coinvolgimento di Paesi a rischio e alle ulteriori informazioni rilevanti disponibili; gli eventuali elementi di sospetto riconducibili ad un uso atipico di valute virtuali dovranno essere segnalate tempestivamente all'UIF per l'Italia. Come già detto nel capitolo relativo alle valute virtuali, in seguito all'emanazione della Quarta Direttiva Antiriciclaggio, l'ambito di applicazione della normativa è stato esteso anche ai prestatori di servizi relativi all'utilizzo di valute virtuali, limitatamente allo svolgimento di attività di conversione di tali valute in moneta legale e viceversa. L'estensione del suddetto ambito di applicazione consentirà alle autorità competenti di monitorare le operazioni sospette in valute virtuali contribuendo così ad accrescerne la credibilità e la fiducia degli utenti in buona fede e preservando al contempo i progressi innovativi offerti da tali valute.

## 11.4 Quarta Direttiva Antiriciclaggio

La direttiva (UE) 2015/849 o Quarta Direttiva Antiriciclaggio, divenuta applicabile del 26 giugno 2017, aggiorna e migliora la previgente direttiva 2005/60/CE (c.d. Terza Direttiva Antiriciclaggio) al fine di potenziare ulteriormente le difese dell'Unione europea contro il riciclaggio di denaro e il finanziamento del terrorismo e garantire la stabilità e l'integrità del sistema finanziario.[59] Essa persegue i seguenti obbiettivi: tutelare gli interessi della società dalla criminalità e dagli attacchi terroristici; salvaguardare la prosperità economica dell'Unione assicurando un efficiente contesto imprenditoriale; contribuire alla stabilità, alla solidità, al regolare funzionamento e all'integrità del sistema finanziario mediante la prevenzione, l'individuazione e il contrasto del riciclaggio e del finanziamento del terrorismo. Detta direttiva prende pienamente in considerazione le già citate 40 Raccomandazioni del GAFI e prevede un approccio più mirato, basato sull'identificazione e la valutazione dei rischi di riciclaggio e finanziamento del terrorismo, insiti nell'esercizio di attività finanziarie e professionali esercitate dai destinatari della normativa. Questa inoltre dispone il consolidamento dei poteri sanzionatori delle autorità competenti stabilendo che le sanzioni e le misure messe in atto dagli Stati membri per la violazione sistematica degli obblighi in essa contenuti (in tema di adeguata verifica della clientela, conservazione dei documenti, segnalazione di operazioni sospette e controlli interni) debbano essere efficaci, proporzionate e dissuasive. Per quanto riguarda le nuove tecnologie la Quarta Direttiva Antiriciclaggio sottolinea la necessità di valutarne i rischi e impone alle autorità competenti e ai soggetti destinatari della normativa in questione di essere proattivi nel contrastare nuovi e innovativi metodi di riciclaggio e di finanziamento del terrorismo basati su tecnologie innovative, nuove pratiche commerciali, nuovi prodotti e meccanismi di distribuzione. Altro obbiettivo della direttiva è quello di garantire l'individuazione e corretta verifica delle parti (siano esse persone fisiche o giuridiche) coinvolte in un'operazione o un pagamento. Le norme sull'identificazione elettronica e i servizi fiduciari sono contenute nel Regolamento eIDAS, applicabile dal 1° luglio 2016, e si adottano per esempio nell'apertura di conti bancari online, nell'accesso a fondi e tracciamento di transazioni elettroniche. Essendo la Quarta Direttiva Antiriciclaggio una direttiva di armonizzazione minima lascia in capo agli Stati membri le decisioni in merito alle modalità di utilizzo degli strumenti digitali innovativi per l'identificazione a distanza dei clienti. Gli Stati membri però devono comunque assicurare che tali strumenti siano sicuri e protetti, che non comportino nuovi rischi per i consumatori e per il sistema e che rispettino la legislazione europea in materia di protezione dei dati personali. La Commissione europea ha istituito un gruppo di esperti di identità degli Stati membri che, con un lavoro congiunto con le autorità di regolamentazione e vigilanza, ha l'obbiettivo di approfondire tali problematiche, sviluppare orientamenti comuni e identificare le migliori pratiche per l'identificazione a distanza e l'adeguata verifica della clientela nell'UE. Parallelamente la Commissione a breve consentirà alle banche l'uso transfrontaliero dei mezzi di identificazione elettronica basati sull'eIDAS con l'obbiettivo di un avanzamento verso la specifica componente dell'*eBanking* che consente l'identificazione digitale a distanza della clientela bancaria.

[59] A. Pezzuto, "*Profili evolutivi della legislazione in materia di antiriciclaggio e contrasto al finanziamento del terrorismo*", 2017

# CONCLUSIONE

Con il presente elaborato, ho voluto mettere in luce quanto l'innovazione e il progresso tecnologico siano capaci di rivoluzionare il mondo in cui viviamo, analizzando gli effetti che l'applicazione della tecnologia al settore dei servizi finanziari (*FinTech*) ha apportato sia a livello economico che sociale. Numerosi sono i benefici riscontrati, sia per il mercato che per i consumatori, grazie all'offerta di servizi finanziari più efficienti, veloci, economici e inclusivi. Accanto ai benefici, si sono delineati però anche numerosi rischi per la tutela del consumatore e per la stabilità e integrità del sistema finanziario. In uno scenario di questo tipo, in continua evoluzione e nel quale si alternano luci ed ombre sulle potenzialità e sugli eventuali rischi connessi allo sviluppo di *FinTech*, sono scese in campo tutte le Autorità e le Istituzioni a livello internazionale, europeo e nazionale, che si sono impegnate a studiare ed analizzare, in diversa misura il fenomeno che interessa una sempre più ampia gamma di servizi finanziari. Risulta quindi necessario l'intervento delle Autorità per una regolazione del fenomeno *FinTech* capace di limitarne i rischi senza tuttavia ostacolarne il naturale sviluppo, ma anzi promuovendolo con l'obbiettivo di dare forma al Mercato unico tecnologico dei servizi finanziari a livello europeo. Il cammino potrà essere agevolato dalla conoscenza e dalla fiducia nelle nuove tecnologie, nonché da processi di educazione finanziaria e soprattutto digitale.

Le innovazioni *FinTech* hanno aperto nuove opportunità di business e ridotto significativamente il costo di nuove iniziative, motivo che ha determinato la nascita di nuove *start-up* innovative che, per loro natura, fanno convergere competenze finanziarie e competenze tecnologiche e che, superata la fase iniziale di sperimentazione, stanno muovendosi sempre più verso obiettivi di business tangibili. Nell'analisi specifica delle varie innovazioni del campo *FinTech*, ho voluto dare luce alle principali *start-up* italiane che hanno mostrato caratteristiche di eccellenza, riuscendo ad emergere nel panorama finanziario nazionale ed europeo. Tali *start-up* innovative, attraverso l'uso di nuove tecnologie, propongono un ripensamento dell'esperienza del cliente nella fruizione dei prodotti e servizi finanziari, soddisfacendo le esigenze proprie delle nuove generazioni (in un mercato dalle fattezze sempre più digitali) e favorendo l'inclusione finanziaria. La diffusione delle *start-up FinTech* è stata favorita anche dal progressivo deteriorarsi del rapporto tra banca e cliente, dal venire meno della fiducia nel sistema finanziario tradizionale (soprattutto dopo la recente crisi economica) e dalla stretta creditizia messa in atto dalle banche per fronteggiare tale crisi.

L'esplosione in questi ultimi anni del fenomeno *FinTech* ha fatto gridare a molti l'imminente *distruption* dell'attuale mercato bancario e finanziario. In realtà mettere in contrapposizione il *FinTech* con le banche è sbagliato e nasce solo da una visione di breve periodo, focalizzata su questa prima fase di sviluppo dirompente di nuovi attori e nuove soluzioni alternative al *banking*. Le enormi potenzialità insite nelle *start-up* del ramo *FinTech*, dovute all'implementazione di nuove potenti tecnologie, dovrebbero essere considerate non una minaccia ma al contrario un'opportunità per le banche tradizionali di rinnovarsi e modernizzarsi attraverso forme di collaborazione e *partnership* (c.d. *Fintegration*) con esse. In un futuro prossimo il progredire della digitalizzazione porterà ad una forte convergenza tra le aziende *FinTech* e le banche tradizionali. La *Fintegration* difatti si presenta come un processo *win-win* in cui le *FinTech* porteranno innovazione, agilità, *customer experience* e le banche forniranno la dimensione, il *brand* e il *know how* su aspetti di *compliance*.

# BIBLIOGRAFIA


Accenture, “Building Confidence - Facing Cybersecurity Conundrum”, 2016

Armstrong P., “The Adoption of Regteh”,2017

Arner D.W., Barberis J.N., Buckley R.P., “The Evolution of FinTech: A New Post-Crisis Paradigm?”, 2016

Azzalini, Adelchi, Scarpa, “Analisi dei Dati e Data Mining”, 2009

Banca d’Italia, “Avvertenza sull’utilizzo delle cosiddette valute virtuali”, 2015

Banca d’Italia, “FINTECH IN ITALIA Indagine conoscitiva sull’adozione delle innovazioni tecnologiche applicate ai servizi finanziari”, 2017

Bank of England, “The Economics of digital currencies”, 2014

Bank of International Settlements (BIS), “Payment aspects of financial inclusion”, 2016

BCE, “Virtual currency schemes”, 2012

Birch D., “Identity is the new money”, 2014

Bofondi M., “Il lending-based crowdfunding: opportunità e rischi”, 2017

Bruckenstein J., “Robo advisers, digital advice and the future of the advisory business”, 2017

Bulgarelli D., Malverti E., Villa G., “FinTech. La finanza digitale. Strategie di investimento con i roboadvisor”, 2018

Cacciamani C., Fiorelli A. (a cura di), “Il crowdfunding”, 2017

Cano A., “Problemi evolutivi e nuove prospettive in tema di riciclaggio di denaro, beni o altre utilità”, 2014

Cascinelli F., Pistoni V., Zanetti G., “La Direttiva (UE) 2015/2566 relativa ai servizi di pagamento nel mercato interno”, 2016

Castaldi G., Conforti G., “Manuale antiriciclaggio”, 2013

Cencetti C., “Cybersecurity: Unione europea a Italia. Prospettive a confronto”, 2014

Chiaramonti N., “L'affermazione delle financial technologies: l'influenza dei cambiamenti normativi e tecnologici sull'operatività degli istituti di credito”, 2017

Chisti S., Barberis J., “The FinTech book. The financial technology handbook for investors, entrepreneurs and visionaries”, 2016

Ciraolo F., “Pagamento fraudolento con carta di credito e ripartizione delle responsabilità. Dagli orientamenti attuali alla revisione della PSD”, 2017

Clarke S., “Reducing the impact of cyberthreats with robust data governance”, 2016

Commissione europea, “Consumer financial services action plan: better products, more choice, greater opportunities”, 2017

Commissione europea, “Crowdfunding in EU Capital Market Union”, 2016

Commissione europea, “Feedback Statement for the public Consultation on the Capital Market Union”, 2017

Commissione europea, “FinTech: a more competitive and innovative European financial Sector”, 2017

Commissione europea, “Il crowdfunding cos’è? Una guida per le piccole e medie imprese”, 2015

Committee on the Global Financial System, Financial Stability Board, “FinTech: Credit – Market Structure, Business Models and Financial Stability Implications”, 2017

Condemi M., De Pasquale F., “Lineamenti della disciplina internazionale di prevenzione e contrasto del riciclaggio e del finanziamento del terrorismo”, 2008

D’Acquisto G., Di Nardo M., “Big Data e privacy by design”, 2017

De Collibus F., Mauro R., “Hacking finance. La rivoluzione del bitcoin e della blockchain”, 2016

De Luca R., “Il crowdfunding: quadro normativo, aspetti operativi e opportunità”, 2015

Deloitte, “10 disruptive trends in wealth management”, 2015

Densham B., “Three cyber-security strategies to mitigate the impact of a data breach”, 2015

Di Mascio A., “Wealth Management e FinTech: Le nuove sfide tra Private Banker e Robo Advisor”, 2018

Di Porto F. (a cura di), “Big Data e concorrenza”, 2016

Domingos P., “A Useful Things to Know about Machine Learning”, 2012

EBA, “Discussion paper on the EBA’s approach to financial technology (FinTech)”, 2017

EBA, “Opinion on virtual currency”, 2014

EBA, “Report on Innovative use of Personal data by Finantial Institute”, 2017

ENISA, “An evaluation Framework for Natural Cyber Security Strategy”, 2014

ENISA, “Nation Cyber Security Strategies. Practical Guide on Development and Execution”, 2012

ENISA, “National Cyber Security Strategies. Practical Guide on Development and Execution”, 2012

ENISA, “Setting the course for national efforts to strenghten security in cyerspace”, 2012

Enria A., “FinTech: regulatory challenges and open questions”, 2017

Ernst and Young, “EY FinTech Adoption Index 2017 – The rapid emergence of FinTech”, 2017

ESMA, “Avvertenza per gli investitori relativa alle insidie degli investimenti online”, 2012

ESMA, “Investment using virtual currency or distributed ledger technology”, 2015

ESMA, “Report. The Distributed Ledger Technology Applied to Securities MArkets”, 2017

European Banking Authority, “Avvertenza per i consumatori sulle monete virtuali”, 2013

European Payments Council, “White Paper Mobile Payments”, 2017

Fayyad U., “The Digital Physics of Data mining”, 2001

Ferrari R., “L’era del FinTech. La rivoluzione digitale nei servizi finanziari”, FrancoAngeli, 2016

Financial Industry Regulatory Authority, “Report on digital investment advice”, 2016

Financial Stability Board, “Financial Stability Implications from FinTech. Supervisory and Regulatory Issues that Merit Authorities’ Attention”, 2017

Financial Stability Board, “Financial Stability Integration from FinTech”, 2017

Financial Stability Board, “FinTech credit. Market structure, business models and financial stability implications”, 2017

FSUG, “Paper on Assessment of current and future impact of Big Data on Financial Services”, 2016

GAFI/FATF, “Valute Virtuali, definizioni chiave e potenziali rischi in ambito antiriciclaggio e finanziamento del terrorismo”, 2014

Gerber E. M., Pei-Yi Kuo J. S., “Crowdfunding: Why People Are Motivated to Post and Fund Projects on Crowdfunding Platforms”, 2012

Global Agenda, “The Future of FinTech: A Paradigm Shift in Small Business Finance”, 2015

Greco G.L., Abate D.D., “Riserve di attività versus piattaforme di gestione delle valute virtuali: il caso Sardex”, 2016

Hayen R., “FinTech: The Impact and Influence of Financial Technology on Banking and Financial Industry”, 2016

ING International Survey “Mobile Banking 2017 – Newer Technologies”, 2017

Institute for International Finance, “RegTech in Financial Services: Technology Solutions for Compliance and Reporting”, 2016

IOSCO, “Research Report on Financial Technologies (FinTech)”, 2017

King B., “Banks 3.0”,2012

KPMG, “The Pulse of FinTech Q117”, 2017

Lemme G., Peluso S., “Criptomoneta e distacco della moneta legale: caso Bitcoin”, 2016

Maggiolino M., “Big Data e prezzi personalizzati”, 2016

Malinova K., Park A., “Market Design with Blockchain Technology Market”, 2016

Mancini N., “Bitcoin: rischi e difficoltà normative”, 2016

Martinelli F., “Rivoluzione FinTech: come la digitalizzazione sta cambiando il settore bancario. Il caso Banca di Pisa e Fornacette Credito Cooperativo”, 2017

Mayer-Schönberger V., Cukier K. N., “Big data. Una rivoluzione che trasformerà il nostro modo di vivere e già minaccia la nostra libertà”, 2013

McKinsey “Cutting through the FinTech noise: Markers of Success, Imperatives For Banks”, 2015

McKinsey, “The Virtual financial advisor: delivering personalized advice in the digital age”, 2015

Milne A., Parboteeah P., “The Business Model and Economics of Peer-to-Peer Lending, European Credit Research Institute”, 2016

Mirra V., “Equity crowdfunding: la guida pratica”, 2014

Motta M., “Competition Policy. Theory and Practice”, 2004

Osservatorio Crowdfunding, “Secondo Report Italiano sul Crowdfundinvesting”, 2017

Paracampo M.T. (a cura di), “FINTECH Introduzione ai profili giuridici di un mercato unico tecnologico dei sistemi finanziari”, 2017

Paracampo M.T., “Nuove tecnologie e sfide regolamentari. LA tutela dell’investitore nella consulenza digitale”, 2015

Parlamento europeo, “Relazione sulle implicazioni dei Big data per i diritti fondamentali: privacy, protezione dei dati, non discriminazione, sicurezza e attività di contrasto”, 2017

Parlamento Europeo, “Tecnologia finanziaria: influenza della tecnologia sul futuro del settore finanziario”, 2017

Passerelli N., “Bitcoin e antiriciclaggio”, 2016

Pezzuto A., “Profili evolutivi della legislazione in materia di antiriciclaggio e contrasto al finanziamento del terrorismo”, 2017

Philippon T., “The FinTech opportunity”, 2016

Piattelli U., “Il crowdfunding in Italia. Una regolamentazione all'avanguardia o un'occasione mancata?”, 2013

Politecnico di Milano, “2$^{o}$ Report italiano sul Crowdinvesting”, 2017

Pwc, “Asset Management 2020: A brave new world”, 2015

Pwc, “Blurred lines: how FinTech is shaping financial services”, 2016

PWC, “Il colloquio tra Third Party Provider e le Banche. Quale sarà l’impatto tecnologico?”, 2016

Pwc, “Le aziende del FinTech in Italia 2017”, 2017

Razzante R., “Il riciclaggio come fenomeno transnazionale. Normative a confronto”, 2014

Reed J., “Blockchain: Blockchain, Smart Contracts, Investing in Ethereum, FinTech”, 2016

Reznor E. P., “FinTech: Hacking, Blockchain, Big data, Cryptocurrency (Financial Technology, Smart Contracts, Digital Banking, Internet Technology)”, 2017

Rizzi M., “FinTech revolution: start-up tecnologie e rivoluzione digitale cambiano il settore più sicuro del mondo: le banche si evolvono, il nostro denaro viaggia tra social media e player dell'e-commerce”, 2016

Rizzi M., “FinTech revolution”, Egea, 2016

Santander Innoventures, “The FinTech 2.0 Paper: rebotting the financial servicies”, 2015

SDA Bocconi, “CRIF, Peer to peer lending, mito o realtà?”, 2015

Sica S., Stanzione P., Zeno Zencovich V., “La moneta elettronica: profili giuridici e problematiche applicative”, 2006

Sironi P., “FinTech Innovation. From robo advisors to goal based investing and gamification”, 2016

Skinner C., “Value Web: How FinTech Firms are Using Bitcoin Blockchain and Mobile Technologies to Create the Internet of Value”, 2016

Swan M., “Blockchain. Blueprint for a new economy”, 2015

The Economist Intelligence Unit, “The disruption of banking”, 2015

Troisi A., “Crowdfunding e mercato creditizio: profili regolamentari”, 2014

Vangone G., “Il terrorismo islamico nell’era di Internet, fra bitcoin e dark web”, 2015

Vinay Gupta, “The Promise of Blockchain Is a World Without Middlemen”, 2017

World Economic Forum, “The Future of FinTech – A Paradigm Shift in Small Business Finance”, 2015

# SITOGRAFIA

www.ansa.it

www.bancaditalia.it

www.bandbackers.com

www.blockchain4innovation.it

www.consob.it

www.crowd-funding.cloud

www.darwinsurance.auxledger.com

www.economyup.it

www.eppela.com

www.infodata.ilsole24ore.com

www.insuranceup.it

www.insurzine.com

www.investopedia.com

www.italiancrowdfunding.it

www.moneyfarm.com

www.pwc.com

www.repubblica.it

www.sardex.net

www.satispay.com

www.smartika.it

www.starsup.it

www.start-upbusiness.it

www.starteed.com

www.unfraud.com

www.wikipedia.org

www.workinvoice.it

# RIASSUNTO

## 1. *Fintech*

La "rivoluzione digitale", intesa come la diffusione su ampia scala delle tecnologie digitali, ha modificato radicalmente lo stile di vita e il modo di comunicare e di agire delle persone, con impatti significativi su tutti i comparti produttivi. Tra questi anche il settore dei servizi finanziari si trova attualmente al centro di una rivoluzione di vasta portata e senza precedenti, nota come *FinTech*. Con il termine *FinTech*, abbreviazione di tecnologia finanziaria, si indentifica un ecosistema, in continua evoluzione, di innovazioni tecnologiche applicate al settore finanziario, che si concretizzano in nuovi modelli di business, processi e prodotti e i cui effetti sono dirompenti e di carattere rivoluzionario sia per i mercati finanziari che per le istituzioni. *FinTech* comprende alcune tra le principali innovazioni degli ultimi anni che investono tutti i settori dell'intermediazione bancaria e finanziaria: il *crowdfunding*, la *robo advice*, il P2P, le valute virtuali, *lending platforms*, la *blockchain* ecc.

*FinTech* ha segnato l'accesso nel mercato dei servizi finanziari di *start-up* tecnologiche e dei colossi della tecnologia informatica la cui affermazione in questo settore scaturisce dalla loro connaturata capacità di creare innovazione tecnologica e utilizzarla per l'offerta di servizi finanziari ad alto contenuto tecnologico e a prezzi contenuti. Altrettanto importanti per lo sviluppo delle imprese *FinTech* sono i fattori legati alla crescita della domanda di servizi finanziari digitalizzati, contestuale all'aumento della porzione di popolazione familiare con i servizi digitali, in particolare i più giovani. La diffusione delle *start-up FinTech* è stata favorita inoltre anche dal progressivo deteriorarsi del rapporto tra banca e cliente, dal venire meno della fiducia nel sistema finanziario tradizionale (soprattutto dopo la recente crisi economica) e dalla stretta creditizia messa in atto dalle banche per fronteggiare tale crisi. L'ingresso di nuovi operatori stimola enormemente la competitività nel settore finanziario e può rappresentare un forte stimolo all'innovazione ma al tempo stesso può delinearsi come un fattore disruptive per l'industria finanziaria tradizionale se questa non si dimostri in grado di adattare la propria attività di intermediazione alle nuove tecnologie. Le banche tradizionali hanno quindi risposto alla sfida digitale ripensando il proprio modello di business e intraprendendo un percorso di *restyling* tecnologico con l'introduzione di nuovi canali digitali. La via più efficace da seguire è quella del passaggio da una competizione tra banche e *FinTech* ad una più proficua *co-opetition* attraverso opportune forme di partnership che favoriscano una sorta di simbiosi, o *fintegration*. I vantaggi competitivi della *fintegration* investirebbero infatti sia le banche che i nuovi operatori digitali: da un lato gli intermediari tradizionali potrebbero digitalizzarsi e compiere quel salto tecnologico altrimenti troppo lungo e costoso da praticare, dall'altro le imprese *FinTech* potrebbero avere accesso alla vastissima platea di clienti bancari cui offrire i propri servizi, accelerando così il proprio business e abbattendo i costi di marketing.

Le innovazioni *FinTech* si mostrano in grado di apportare diversi benefici sia ai consumatori che alle imprese in quanto permettono di offrire servizi finanziari migliori, più rapidi, meno costosi, più personalizzati, inclusivi, resilienti e trasparenti permettendo così a tutti i cittadini condizioni di accesso al mercato più ottimali e favorendo l'inclusione finanziaria. Oltre ai numerosi benefici però FinTech ingloba in sé anche rilevanti rischi che possono mettere a repentaglio la stabilità finanziaria

tra cui: assetti di *governance* e di sistemi di controllo inadeguati dei nuovi operatori FinTech , spesso non soggetti ad alcuna regolamentazione o comunque assoggettati a controlli meno stringenti rispetto agli *incumbents*; rischio di sicurezza informatica legato al furto di informazioni personali, identità digitale o risorse economiche; l'accresciuta interconnessione tra i mercati che incrementa le esposizione a fenomeni di contagio e la portata sistemica di attacchi informatici.

In uno scenario di questo tipo sono scese in campo tutte le Autorità e le Istituzioni a livello internazionale, europeo e nazionale, che si sono impegnate a studiare ed analizzare, in diversa misura il fenomeno che interessa una sempre più ampia gamma di servizi finanziari. Nella consapevolezza che ogni innovazione tecnologica reca con sé una sfida regolamentare, le Autorità si stanno interrogando sul tipo di azione e di intervento da intraprendere per una regolamentazione del fenomeno *FinTech* al fine di gestire eventuali rischi e tutelare i diritti dei consumatori e la stabilità del sistema finanziario. Tale intervento regolatorio non deve tuttavia ostacolare il naturale sviluppo dell'innovazione tecnologico-finanziaria ma anzi supportarlo con l'obbiettivo di favorire l'operatività *cross-border* e dare forma al Mercato unico tecnologico dei servizi finanziari a livello europeo. Il cammino potrà essere agevolato dalla conoscenza e dalla fiducia nelle nuove tecnologie, nonché da processi di educazione finanziaria e soprattutto digitale.

Anche l'Italia, come gran parte dei Paesi nel mondo, sta attraversando un periodo di fermento legato alla diffusione del *FinTech* anche se rimane relativamente indietro rispetto ad altre realtà. Gli investimenti in *FinTech* però stanno accelerando e si stima che potrebbero portare ad un aumento di valore fino al 30% nei prossimi cinque anni. In più si registra un aumento delle *start-up* innovative italiane che si stanno affermando all'interno del territorio nazionale e non solo.

## 2. *Big Data*

Tra le principali innovazioni *FinTech* abbiamo i cosiddetti *Big data*, ossia quel nuovo settore dell'informatica dedicato alla gestione di database di grandi dimensioni. In particolare, la Commissione europea ha definito i *Big data* come quelle situazioni caratterizzate da un notevole volume di differenti tipologie di dati prodotti, da diversi tipi di fonti, ad altissima velocità, spesso in tempo reale grazie all'utilizzo delle tecnologie IT. Il concetto di *Big data* non si riferisce solo ai dati in sé ma anche e soprattutto alla loro rielaborazione tramite tecniche sofisticate e i risultati della loro analisi. In particolare, il fattore più importante che caratterizza i *Big data* è quello predittivo, ossia la possibilità, attraverso una serie numerosissima di dati diversi, di catalogare e profilare gli utenti secondo una differenziazione tipologica quasi illimitata.

Nella *digital economy* il vantaggio competitivo tra le imprese è largamente basato sulla capacità, attraverso l'uso di sofisticati algoritmi, di raccogliere e analizzare i dati dei propri clienti e dei potenziali tali per meglio comprenderne i gusti e le esigenze, offrendo loro servizi nuovi, personalizzati, qualitativamente migliori e a prezzi più contenuti rispetto a quelli dei mercati tradizionali. L'uso dei dati è funzionale anche alla formulazione di strategie di produzione e commerciali al fine di conquistare nuovi segmenti di mercato e clientela.

Tra i principali benefici apportati dalla tecnologia dei *Big data* nel settore finanziario è da considerare il contributo al miglioramento della qualità dei servizi, maggiormente personalizzati e adattati alle esigenze dei consumatori e la possibilità di ottemperare agli obblighi di tutela imposti con MiFID 2. Per il settore creditizio, l'utilizzo dei *Big data* consente di rendere più efficace il

processo decisionale e di estendere l'accesso al credito di soggetti fino ad oggi esclusi perché considerati *unbanked* secondo i tradizionali modelli di stima. I *Big data* possono poi contribuire anche alla prevenzione di fenomeni di *cybercrime*, frodi e attività illecite come il riciclaggio e il finanziamento del terrorismo tramite l'uso di algoritmi sofisticati che permettono di rilevare comportamenti sospetti grazie al controllo delle operazioni di pagamento.

Tra i principali rischi legati alla tecnologia dei *Big data* vi è quello della tutela della *privacy* e dei dati personali. Il Parlamento europeo ha affermato che nell'utilizzo di tali dati sia le autorità pubbliche che i soggetti privati devono rispettare rigorosamente la normativa a tutela dei diritti fondamentali e della protezione dei dati e in particolare, il regolamento europeo 2016/679, entrato in vigore il 25 maggio 2018. Attraverso tale regolamento il Parlamento europeo ha consentito ai singoli di mantenere un controllo sul trattamento dei propri dati da parte di soggetti terzi (soprattutto nel processo di profilazione) e il diritto alla portabilità dei dati.

Di notevole importanza è anche il problema dell'impatto dei *Big data* sulla concorrenza che pone nuove sfide regolamentari nel settore del diritto della concorrenza e della legislazione antitrust. Tra gli effetti più preoccupanti dell'economia digitale fondata sui dati si annovera la tendenza alla concentrazione del potere di mercato nelle mani di pochi operatori e la conseguente creazione di barriere all'ingresso da parte di questi ultimi a danno degli aspiranti concorrenti (*foreclosure effect*).

Pericolose sotto il profilo della concorrenza e dell'antitrust sono inoltre le intese e le pratiche collusive tra imprese volte a rafforzare la loro posizione di dominanza nel mercato. Tali condotte potrebbero causare un allineamento dei prezzi e la fissazione di una soglia di prezzo più alta, in modo da garantire una rendita costante alle imprese stesse e il mantenimento nel tempo degli equilibri preesistenti.

Altra grande preoccupazione per il diritto antitrust legata alla *digital economy* è lo sfruttamento abusivo della posizione dominante, acquisita sul mercato grazie ai *Big data* e i *data-set*. Il problema riguarda perlopiù le imprese che non sono in grado di raccogliere da sé i dati degli utenti e debbano quindi necessariamente, per competere su mercato, acquistarli da altre imprese in maniera grezza o già sotto forma di metadati.

Particolare attenzione da parte della Autorità antitrust viene posta anche ai casi di concentrazioni tra imprese nel settore della *digital economy*, legate alla detenzione dei *Big data*. La Commissione europea ha tuttavia deciso finora di autorizzare le operazioni concentrative poste sotto la sua attenzione non riscontando rischi di abusi legati alla creazione o al rafforzamento di posizioni dominanti.

Problemi di carattere commerciale e concorrenziale, legati all'uso dei *Big data*, sono causati anche dalla tendenza nella *digital market economy* alla personalizzazione delle offerte da parte degli operatori, in quanto porta alla cosiddetta discriminazione dei prezzi. Tale condotta, derivante da offerte personalizzate, viene considerata come pratica commerciale scorretta se operata all'insaputa del cliente poiché carente di trasparenza e contraria alla correttezza professionale. Questa pratica infatti è capace di incidere in modo rilevante sulle scelte di consumo del singolo, inducendolo all'acquisto inconsapevole o non sufficientemente informato di un determinato prodotto o servizio.

L'uso dei *Big data* è in continua crescita, per cui sarà necessario un futuro intervento del regolatore volto a disciplinare tale fenomeno, in ragione delle numerose problematiche che esso comporta e dei rischi per la tutela dei consumatori.

## 3. Robo advice

Tra le maggiori innovazioni dell'ecosistema *FinTech* annoveriamo la *robo advice*, ossia la prestazione di servizi finanziari attraverso strumenti automatizzati. Tale definizione comprende diverse fattispecie accomunate dal fatto di utilizzare delle piattaforme online che, sulla base di sofisticati algoritmi, permettono di offrire ai risparmiatori soluzioni di investimento precostituite e di creare, gestire, monitorare e, se necessario, ribilanciare portafogli di investimento da raccomandare ai clienti in base a un processo di consulenza. Quest'ultimo si ottiene dall'analisi dei dati inseriti dal cliente in un questionario volto a valutare il suo profilo di rischio e individuare la combinazione rischio-rendimento che meglio gli si adatta. Si tratta di un vero e proprio consulente finanziario virtuale che, sfruttando la tecnologia, offre servizi di consulenza al pubblico in modo efficiente e a costi contenuti rispetto a quelli connessi alla prestazione del servizio *face-to-face* puntando sulla semplicità e sulla qualità dell'esperienza online per il consumatore. Il principale punto di forza della *robo advice* è la capacità di colmare un gap nel mercato dei servizi di consulenza consentendone l'accesso ai segmenti della clientela mass market grazie ai costi più contenuti e l'assenza di limiti di portafoglio. I *robo advisor* rispondono quindi ad un tentativo di democratizzazione dei servizi di consulenza (riservati dai canali tradizionali per lo più alla sola clientela private) al fine di favorire l'inclusione finanziaria di soggetti considerati *unbanked*. Nonostante ciò vi sono però nell'ambiente finanziario numerosi oppositori preoccupati soprattutto dell'impatto disruptive del *robo advice* sul settore dell'intermediazione finanziaria. I maggiori timori riguardano: l'ingresso nel mercato di *start-up FinTech* non soggette a nessun controllo o regolamentazione che rappresentano pericolosi competitor per gli operatori tradizionali; il rischio di disintermediazione umana a favore di un'intermediazione digitale; la molteplicità delle fattispecie che possono essere ricollegate al settore della *robo advice*, tali da creare problematiche normative diverse da un caso all'altro. Esistono inoltre rilevanti rischi legati al funzionamento degli algoritmi, alla loro mancanza di trasparenza e affidabilità, alla difficoltà di comprensione da parte dei consumatori e ai non chiari profili di responsabilità relativi alla formulazione di raccomandazioni errate da parte degli algoritmi.

A livello europeo è stata l'ESMA a tentare di fornire le prime risposte alle problematiche legate alla *robo advice*, contribuendo alla formazione di un vero e proprio statuto dei *robo advice*, costituito da misure di 3 livello o di *soft law*. I *robo advice* divengono soggetti ad un regime più severo dovendo sottostare sia alle norme relative ai servizi di consulenza in generale sia a specifiche *guidelines* aggiuntive di carattere informativo e organizzativo che tengono conto delle criticità legate all'uso degli algoritmi alla base dei *robo advice*. La strada intrapresa dall'ESMA sembra andare in direzione di una *robo advice governance* che, utilizzando *guidelines*, raccomandazioni e misure di *soft law*, fornisce chiarimenti e indicazioni agli intermediari finanziari a partire dalla stessa ideazione e progettazione degli algoritmi fino al loro utilizzo finale per la prestazione del servizio al cliente.

Tra le principali *start-up* italiane attive nel settore della *robo advice* ricordiamo *Moneyfarm*, una Società di intermediazione mobiliare (SIM), fondata nel 2011, che offre servizi di consulenza finanziaria automatizzata a livello europeo. I costi di *Moneyfarm* risultano essere circa la metà dei costi richiesti per l'investimento in un fondo standard. Si può affermare quindi che *Moneyfarm* ha

reso di fatto accessibile a tutti il servizio di gestione patrimoniale e, a conferma della sua eccellenza tra le realtà *FinTech*, sono i numerosi premi ricevuti tra i quali lo Uk-Italy Business Award 2017 riservato alle aziende italiane che più si sono distinte come esempio di eccellenza nel Regno Unito.

## 4. Crowdfunding

Un'altra rilevante innovazione in ambito *FinTech* è il *crowdfunding*, una particolare tecnica che permette il finanziamento (*funding*) di iniziative di vario genere (umanitarie, politiche, culturali, scientifiche, sociali, imprenditoriali ecc.) attraverso la raccolta di capitali tra la folla (*crowd*), effettuata tramite l'utilizzo di una piattaforma online.

Il *crowdfunding* si presenta quindi come un moderno strumento per finanziamenti sostenibili, grazie alla sua capacità di unire esigenze e interessi di natura diversa, sia di carattere individuale/privatistico sia collettivo/pubblicistico. Esso rientra nell'ambito della *sharing economy* e ribalta il tradizionale rapporto tra produttore e consumatore; quest'ultimo infatti non si limita al semplice acquisto di un bene o servizio prodotto da altri ma partecipa attivamente alla sua produzione, assumendosi il rischio connesso al finanziamento.

Esistono diverse tipologie di *crowdfunding*: *donation based, reward-based, lending-based, invoice trading, royalty-based, investment-based*, modelli ibridi di *crowdfunding*, *Do-It-Yourself* (DIY) o *crowdfunding* indipendente.

Nell'*investment-based crowdfunding* particolari tipi di imprese emettono azioni o obbligazioni e li offrono al pubblico tramite una piattaforma online. Rientra in questa categoria l'*equity crowdfunding*, in cui i finanziatori acquistano sulla piattaforma azioni dell'impresa diventandone soci a tutti gli effetti e quindi esposti all'andamento della stessa e al rischio di impresa. L'*equity crowdfunding* rappresenta un'efficace fonte di finanziamento alternativa che assume particolare rilevanza soprattutto per le imprese che tipicamente sono escluse dal mercato del credito per l'assenza di *asset* tangibili da porre a garanzia oppure semplicemente perché troppo piccole e rischiose. Per quanto riguarda gli investitori, tra le opportunità principali che l'*equity crowdfunding* offre loro, abbiamo sicuramente l'elevato potenziale di rendimento e vantaggi fiscali. A fronte di tali benefici vi sono però anche diversi rischi da tenere in considerazione, come la perdita di capitale nel caso in cui il progetto della *start-up* non vada a buon fine e il divieto di distribuzione di utili per tutto il periodo in cui la società mantiene i requisiti di *start-up* innovativa. Ulteriore rischio riguarda il fatto che questi strumenti finanziari risultano molto illiquidi non potendo essere negoziati su mercati secondari.

Gli interventi delle Autorità europee fino ad ora risultano per lo più di carattere esplorativo e conoscitivo del fenomeno, per cui, in assenza di una regolamentazione uniforme a livello europeo, gli Stati membri si sono dotati di regimi domestici che, seppure somiglianti nell'approccio generale, presentano notevoli differenze nella progettazione e attuazione delle regole, determinando una forte frammentazione del mercato europeo. In generale, i regimi adottati dagli Stati membri presentano il duplice obbiettivo di promuovere il *crowdfunding*, come nuova fonte di finanziamento per le piccole imprese, garantendo al contempo la difesa degli investitori dai possibili rischi che esso comporta. L'Italia è stata il primo paese europeo a dotarsi di una displica specifica in materia di *equity crowdfunding* con l'emanazione nel 2013 da parte della Consob del Regolamento

N.18592/2013 che prevede particolari obblighi di comportamento e di trasparenza per gli offerenti, i gestori e i risparmiatori.

*Startsup,* fondata nel 2013, è stata la prima piattaforma di *equity crowdfunding* in Italia ad aver ottenuto dalla Consob l'iscrizione al registro dei portali online per la raccolta di capitale di rischio da parte di *start-up* e PMI innovative. La mission di *Startsup* è quella di promuovere e valorizzare l'innovazione italiana, proporre progetti di "*new economy*", soprattutto se in grado di fornire un servizio utile per la collettività, e sostenere le aziende più meritevoli e innovative, capaci di conquistare i mercati. La società ad oggi ha finanziato progetti per un volume superiore ai 2,9 milioni di euro, posizionandosi come prima piattaforma in Italia con 347 investitori attivi.

Per *invoice financing* (o *invoice trading*) si intende l'insieme delle modalità attraverso cui le piattaforme specializzate consentono alle imprese di monetizzare le fatture emesse e non ancora scadute attraverso la cessione ad investitori online, senza così dover attendere il pagamento da parte del cliente. Questo permette alle imprese (soprattutto PMI) di ottimizzare la gestione del capitale circolante, di proteggere il portafoglio crediti dai mancati pagamenti e migliorare così la propria solidità finanziaria. L'istituto giuridico italiano alla base dell'*invoice trading* è la cessione dei crediti, la cui disciplina si trova negli artt. 1260 ss. del Codice Civile.

Tra i portali di *invoice trading* attivi in Italia ricordiamo *Workinvoice*, *start-up* innovativa fondata nel dicembre del 2014 a Milano. Si tratta di un portale su cui le aziende, soprattutto di piccola e media dimensione, possono vendere all'asta le proprie fatture *pro-soluto* ricevendo liquidità immediata e gli investitori possono acquisirle, mirando a rendimenti potenzialmente più vantaggiosi rispetto a quelli ottenibili da altri asset di breve termine.

Il *royalty-based*, o semplicemente *royalty*, è un tipo di *crowdfunding* in cui si finanzia una determinata iniziativa, ricevendo in cambio una parte dei profitti. In pratica, chi lancia una campagna di *crowdfunding* di questo tipo, offre delle quote dei guadagni futuri del progetto per il quale richiede il finanziamento. Gli investitori possono, quindi, ottenere un reddito regolare garantito dalle vendite ed al contempo i proprietari del business, restandone i soli titolari, mantengono interamente il controllo sull'andamento dell'attività. La disciplina del modello, in genere, è riferibile alle norme sull'associazione in partecipazione (artt. 2549 ss. c.c.3), nella quale chi finanzia partecipa in quota agli utili generati.

Una famosa piattaforma italiana di *royalty crowdfunding* è *BandBackers* (attiva dalla fine del 2015) che opera come *Social Music Label*, ovvero un'etichetta discografica che viene finanziata dai fan dei vari progetti e dagli appassionati attraverso il *crowdfunding*. Si presenta quindi come uno strumento di *sharing economy*, che opera sul mercato discografico e consente di rendere sostenibili le carriere degli artisti, fornendo fondi per produrre e promuovere la loro musica. Il finanziatore (o *backer*) del progetto riceve in cambio un corrispettivo sulla base dell'importo che ha finanziato, in sostanza parteciperà agli utili generati dall'artista/dalla band.

La prima forma originaria di *crowdfunding*, che ha dato il via al fenomeno, è quella del *donation-based*, ossia un modello tipico di donazione, in cui si devolve altruisticamente il proprio denaro a sostegno di una causa specifica non ricevendo in cambio alcuna ricompensa o, al massimo, ricompense simboliche, spesso intangibili.

Il *reward crowdfunding*, invece, consiste nella raccolta di finanziamenti via internet a fronte di una ricompensa, non finanziaria, proporzionale all'importo investito dal sostenitore. Questa tipologia di *crowdfunding* presenta due varianti: la "*all or nothing*", in cui il denaro raccolto andrà a finanziare il progetto solo se raggiungerà la cifra inizialmente determinata; la "*keep it all*", in cui le somme raccolte finanzieranno il progetto a prescindere dal raggiungimento o meno dell'ammontare fissato.

*Eppela* è una tra le principali piattaforme di *reward crowdfunding* in Italia ed è specializzata in progetti di arte, tecnologia, cinema, musica, fumetto, innovazione sociale, scrittura, moda, no-profit. È stata fondata nel 2011 e ad oggi ha finanziato più di 3000 progetti e gli utenti registrati hanno superato la soglia dei 200.000.

Il *Do-It-Yourself* (DIY) è una nuova forma di *crowdfunding* che consente di realizzare una campagna all'interno del sito stesso dell'organizzazione, senza dover passare su di una piattaforma specifica di *crowdfunding*: si crea quindi una propria campagna personale su un proprio sito web e lo si promuove al pubblico. Detto anche *crowdfunding* indipendente, sta diventando abbastanza di moda ultimamente, a causa del fatto che molti siti di *crowdfunding* stanno restringendo il numero di progetti approvati, modificando le regole e le norme delle loro piattaforme, rendendo di conseguenza non idonei progetti che magari in precedenza avevano le giuste qualifiche. Il *crowdfunding* indipendente presenta diversi benefici tra cui: la possibilità di personalizzare al 100% e amministrare senza restrizioni; l'assenza di categorie proibite; si evita la commissione da dare al portale intermediario; si possono effettuare campagne più lunghe. Vi sono però anche diversi difetti e problemi legati a questa forma di *crowdfunding* ossia: meno esposizione (il marketing è tutto sulle proprie spalle); investitori meno accessibili e credibili; eventuali difficoltà nella creazione di *lending page* e nella gestione dei pagamenti; problemi tecnici da dover risolvere da sé.

*Starteed* è una *crowd-company* italiana, attiva dal 2012, che sviluppa soluzioni nel mercato del *crowdfunding* e della co-creazione con l'obiettivo di fornire infrastrutture tecnologiche personalizzate e servizi specializzati per chi vuole creare campagne *Do-It-Yourself* totalmente personalizzate e di ogni genere, dalle donazioni alla partecipazione in *equity* nelle *start-up*. Ad oggi *Starteed* conta più di 90 progetti sviluppati e più di 4.500.000€ transati.

## 5. *Peer-to-Peer Lending*

Il *Peer-to-Peer Lending* (P2P *Lending*) o *Social lending* è una forma di *crowdfunding* basata sul prestito tra pari svolto senza l'intervento di un intermediario finanziario, poiché l'incontro tra domanda e offerta di finanziamenti, avviene esclusivamente attraverso la piattaforma virtuale a condizioni particolarmente vantaggiose, in quanto i costi di struttura e di intermediazione sono fortemente ridotti se non addirittura azzerati. Il taglio dei costi di intermediazione è stato uno dei punti di forza per la diffusione del P2P *Lending*, poiché da un lato consente a chi presta denaro di percepire un tasso di interesse superiore sia a quello proposto dagli intermediari finanziari tradizionali sia a quello ottenibile dall'investimento in obbligazioni o depositi a risparmio; dall'altro lato consente a chi richiede il prestito di pagare un tasso di interesse notevolmente più basso rispetto ai tassi del tradizionale credito al consumo. La caratteristica che differenzia nettamente il P2P *Lending* dalle altre forme di *crowdfunding* è che i prestiti erogati attraverso le piattaforme di *social lending* non costituiscono finanziamenti finalizzati poiché l'interesse del prestatore è esclusivamente legato all'ottenimento di una remunerazione a fronte del denaro prestato a prescindere dal fine per il quale il finanziamento è stato richiesto. Per le altre forme di *crowdfunding*

invece, come visto nel capitolo precedente, i prestatori di fondi sono mossi principalmente dall'interesse alla realizzazione del progetto finanziato a volte anche prescindendo da un ritorno economico.

A livello europeo manca una disciplina specifica in materia di *lending based crowdfunding*. Nei documenti ufficiali europei viene però messa in luce la necessità di un intervento degli Stati membri, volto a favorire la convergenza della prassi di vigilanza del fenomeno, al fine di evitare arbitraggi regolamentari e per creare un sistema normativo omogeneo a livello europeo.

In Italia i primi interventi normativi in materia di P2P *lending* si sono avuti con l'ultimo aggiornamento delle disposizioni generali della Banca d'Italia sulla raccolta del risparmio da parte di soggetti diversi dalle banche, pubblicate nel novembre del 2016 e ed entrate in vigore nel gennaio 2017. Si tratta di una normativa ancora allo stato embrionale e di carattere ricognitivo, ma rappresenta un primo riconoscimento nell'ordinamento interno del *social lending*. L'attività viene così legittimata a patto che venga svolto nel rispetto delle norme che stabiliscono riserve di attività a particolari tipi di soggetti.

La piattaforma di P2P *Lending* attualmente leader in Italia è *Smartika* fondata nel 2011. *Smartika* opera come istituto di pagamento ed è quindi un operatore finanziario autorizzato a prestare servizi di pagamento su richiesta dei prestatori e richiedenti di finanziamenti.

## 6. Servizi di pagamento digitali

Tra le attività finanziare sottoposte maggiormente ai cambiamenti generati dall'evoluzione tecnologica, si annoverano i servizi di pagamento. Negli ultimi anni il progresso tecnologico dell'era digitale e il continuo sviluppo delle telecomunicazioni, hanno portato alla nascita di servizi e prodotti innovativi e sofisticati come: la moneta elettronica, metodi di pagamento utilizzabili per l'acquisto di beni e servizi online, l'utilizzo di carte di credito in modalità *contactless*, la possibilità di effettuare pagamenti tramite cellulare e altri dispositivi mobili. È proprio quella dei *mobile payments,* probabilmente, la maggior innovazione degli ultimi tempi nel campo dei servizi di pagamento, considerato il loro elevatissimo tasso di crescita dovuto per lo più alla massiccia diffusione degli *smartphone*s e altri dispositivi mobili. Tra le più importanti applicazioni in ambito di *m-payments* annoveriamo i cosiddetti portafogli elettronici (*digital wallets*), che sostituiscono i portafogli veri e propri e le carte fisiche.

Nonostante le diversità operative delle varie fattispecie eterogenee rientranti nel settore dei servizi di pagamento elettronici e digitali, vi sono alcune problematiche di carattere regolamentare che investono l'intero settore di riferimento come: la necessità di garantire la protezione dei dati personali e finanziari degli utenti, l'esigenza di assicurare un adeguato livello di sicurezza delle operazioni e il bisogno di porre chiarezza sui profili di responsabilità in capo ai fornitori del servizio. La necessità di disciplinare in maniere completa e organica le diverse fattispecie di servizi di pagamento, raggruppandole in un unico quadro normativo, ha trovato risposta con l'adozione della direttiva 2007/64/CE (*Payment Service Directive* PSD) recepita in Italia col d.l. n. 11/2010. L'obbiettivo di tale direttiva è quello di armonizzare le regole in materia di servizi di pagamento elettronici al fine di agevolare il buon funzionamento del mercato unico dei servizi di pagamento al dettaglio. La PSD costituisce infatti le fondamenta giuridiche della SEPA (*Single Euro Payment Area*), ossia un'area perfettamente integrata e concorrenziale in cui non vi siano differenze di trattamento

tra pagamenti nazionali e transfrontalieri in euro. La PSD ha permesso di definire all'interno di una cornice giuridica unitaria, gli aspetti fondamentali dei servizi di pagamento come i requisiti di accesso al mercato per i fornitori, la trasparenza delle condizioni relative all'erogazione dei servizi stessi e i diritti, gli obblighi e le responsabilità di prestatori e utenti.

La PSD ha rappresentato senza dubbio un significativo traguardo nella regolamentazione del settore dei servizi di pagamento, ma dalla sua entrata in vigore ad oggi si sono registrate notevoli innovazioni tecniche che l'hanno resa inadeguata e obsoleta. È stato quindi necessario un ammodernamento del quadro regolamentare tracciato dalla PSD, operato con la recente direttiva UE 2015/2366 definita PSD2. L'obbiettivo di tale nuova direttiva è quello di garantire un mercato dei pagamenti maggiormente integrato, basato su regole chiare, moderne e uniformi che possa stimolare la crescita economica in tutta l'UE. Più nello specifico la nuova normativa dovrebbe costituire il presupposto giuridico per una più ampia diffusione di nuovi strumenti e servizi di pagamento innovati fermo restando la garanzia di un elevato livello di protezione dei consumatori, a sua volta necessaria per rafforzare la fiducia nel mercato dei pagamenti.

Tra le principali novità apportate dalla PSD2 si annovera l'apertura del mercato dei servizi di pagamento a due nuove categorie di operatori cosiddetti *third party providers* (TPPs): i prestatori di servizi di disposizione di ordini di pagamento (*Payment Initiation Service Providers*, PISPs) e i prestatori di servizi di informazione sui conti (*Account Information Service Providers*, AISPs). I primi servizi consentono al prestatore (PISP) di disporre per conto dell'utente un pagamento a valore su un conto trattenuto dall'utente stesso presso un altro intermediario, il cosiddetto prestatore di servizi di radicamento del conto o Account *Servicing Payment Service Provider* (ASPSP) di solito rappresentato da una banca. Gli AISPs offrono invece, tramite una piattaforma online, un servizio di consolidamento delle informazioni riguardanti i diversi conti intestati al cliente consentendo al cliente stesso di avere una visione chiara e complessiva della propria situazione finanziaria e delle proprie abitudini di spesa.

Tra le problematiche più spinose legate all'utilizzo delle nuove tecnologie nel settore dei servizi di pagamento vi è senza dubbio quella della sicurezza. La crescente complessità tecnica dei pagamenti digitali espone gli utenti a notevoli rischi di frode che minano la fiducia del pubblico nella sicurezza dei servizi di pagamento e incidono pesantemente sul buon funzionamento del relativo mercato. Occupa quindi, una posizione centrale nella PSD2 il profilo della sicurezza con un *focus* particolare sul tema delle frodi e degli abusi nella prestazione dei servizi di pagamento. Per prevenire eventuali operazioni di pagamento non autorizzate la PSD2 impone specifici obblighi di condotta sia a carico del prestatore di servizi di pagamento che dell'utente.

Il settore dei servizi di pagamento è in continua evoluzione e numerose sono le tecnologie innovative che si stanno sperimentando in questi anni. In particolare, è possibile individuare alcune fondamentali direzioni di innovazione che potranno nei prossimi anni rivoluzionare ulteriormente il mercato dei servizi di pagamento, soprattutto quello del *Mobile Payment*: geolocalizzazione, biometrica e *Internet-of-Things* (IoT).

Tra le principali *start-up* italiane attive nel settore dei pagamenti digitali ricordiamo *Satispay*, operativa dal 2015). La sua app permette di effettuare micropagamenti con il proprio *smartphone* senza alcun costo per l'utente, mentre per l'esercente l'unica spesa è rappresentata da una commissione di 20 centesimi quando la somma della singola transazione supera i 10 €. L'azienda,

per incoraggiare l'adozione del servizio da parte di utenti ed esercenti, fa leva su offerte speciali come quella di *cashback*. A fine 2017 l'app contava oltre 330.000 *download*, 175.000 utenti privati attivi, circa 3 milioni di euro di transato mensile ed oltre 16.000 esercenti aderenti.

## 7. Valute virtuali e monete complementari

Le monete virtuali, tra le quali *Bitcoin* è la più nota e diffusa, si distinguono dalla moneta bancaria in quanto non costituiscono un semplice strumento di pagamento alternativo regolato in moneta legale ma si presentano come una vera e propria moneta a sé stante, non statale, che può essere trasferita, archiviata, negoziata elettronicamente e accettata in via convenzionale dagli operatori per eseguire pagamenti o per finalità speculative. La creazione della valuta virtuale così come la sua adoperabilità come strumento di pagamento non prevede il coinvolgimento delle autorità pubblica in funzione di garanzia; gli emittenti sono infatti soggetti privati e anonimi, per cui l'affidabilità della valuta fa leva esclusivamente sulla tecnologia alla base del funzionamento del *network*. La valuta virtuale non ha efficacia solutoria legale, ma solo su base convenzionale e volontaria, laddove cioè il beneficiario accetti tale valuta come mezzo di estinzione dell'obbligazione pecuniaria.

Nel 2015 la Banca d'Italia in un'apposita Avvertenza ha messo i luce i seguenti rischi legati alle monete virtuali: assenza di tutele legali e contrattuali; carenza di informazioni; assenza di forme di controllo e vigilanza; assenza di forme di garanzia a tutela delle somme depositate; rischio di perdita permanente della moneta a causa di attacchi informatici o malfunzionamenti; accettazione su base volontaria; elevata volatilità del valore con annesso rischio di elevate perdite; rischio di utilizzo per finalità illecite come il riciclaggio di denaro e il finanziamento del terrorismo. Riguardo quest'ultimo aspetto la Commissione Europea ha adottato in bozza una direttiva con l'obbiettivo di estendere parti della disciplina comunitaria in materia di antiriciclaggio alle transazioni eseguite tramite valute virtuali e di includere le piattaforme di cambio delle valute virtuali nell'ambito di applicazione della direttiva antiriciclaggio, al fine di eliminare l'anonimato associato a tali piattaforme.

L'innovazione tecnologica degli ultimi anni ha permesso la nascita e lo sviluppo delle cosiddette valute complementari o locali. Nella Proposta di legge n.2582 del 20 luglio 2014 queste vengono definite come «strumenti di pagamento esclusivamente elettronici volti a facilitare gli scambi di beni e servizi, compreso il lavoro, all'interno di una comunità socio-economica definita utilizzando, anche congiuntamente, criteri di carattere territoriale o funzionale». Seppur accomunate dall'assenza di materialità, le monete complementari non possono essere annoverate tra le monete virtuali, in quanto le prime sono destinate ad essere usate come mezzo di scambio in un mercato locale e circoscritto, le seconde invece sono aperte al mercato globale. Le monete complementari non vanno confuse neanche con la moneta elettronica in quanto, a differenza di quest'ultima, non costituiscono una mera rappresentazione digitale delle comuni valute legali. Le monete complementari rappresentano quindi strumenti di scambio che si affiancano alle valute legali senza tuttavia sostituirle. Oltre che per l'acquisto di beni e servizi in ristretti ambiti territoriali, le monete complementari vengono utilizzate anche all'interno di circuiti come moneta scritturale di credito cooperativo, al fine di permettere la compensazione tra crediti e debiti derivanti dalle transazioni commerciali tra i partecipanti del circuito stesso.

Una rilevante questione è quella riguardante la possibilità o meno di considerare la moneta complementare come uno strumento di pagamento avente funzione solutoria; in questo senso è necessario verificare in primo luogo la dimensione del circuito al cui interno la specifica moneta

complementare è accettata. Tale dato consente infatti di cogliere il grado di spendibilità e affidabilità di tale valuta alternativa.

In Italia tra i più importanti circuiti di moneta complementare ricordiamo il *Circuito di Credito Commerciale Sardex* nato nel 2010 e consistente in una piattaforma integrata di pagamenti tra gli aderenti progettata per facilitare le relazioni tra soggetti economici operanti inizialmente solo in Sardegna e poi estesa anche in altre regioni italiane. Lo scopo dichiarato del circuito gestito dalla *Sardex* S.p.a. è quello di facilitare la collaborazione e la nascita di nuove relazioni tra gli operatori economici del territorio, di valorizzare le produzioni locali e di riattivare i consumi, attraverso l'erogazione di strumenti di pagamento e di credito paralleli e complementari a quelli tradizionali. Ad oggi il circuito *Sardex* è attivo in 12 regioni italiane e nel 2017 i crediti transati raggiungono 100 milioni, in questo stesso anno è entrata a far parte del *FinTech* District di Milano ed è stata inserita nell'FT1000 del *Financial Times*, *ranking* delle mille aziende a maggior crescita in Europa.

## 8. Blockchain

La *Blockchain* è la tecnologia ideata da Satoshi Nakamoto (pseudonimo di un individuo o di un gruppo di sviluppatori), che regola il funzionamento della valuta virtuale più diffusa e celebre, ovvero il *Bitcoin*. Il fine della *Blockchain* è quello di consentire lo scambio, sicuro e in tempo reale, di moneta virtuale tra più soggetti, senza la necessità che la transazione sia validata da un'autorità centrale. Il principio dominante alla base della *Blockchain* è difatti quello dell'eliminazione del cosiddetto *middleman*, ossia di quei soggetti che a livello centrale validano determinate transazioni, scambi e registri. La *Blockchain* permette di sostituire tali soggetti con un meccanismo di consenso basato sulla crittografia, che consente a tutti i partecipanti alla rete di poter porre fiducia sulla legittimità di una transazione senza la necessità di una sua validazione da parte di un soggetto centrale di natura pubblicistica o para-pubblicistica. Nella pratica, la *Blockchain* consiste in un database distribuito, condiviso e basato sulla crittografia che serve quale irreversibile e incorruttibile registro di informazioni e dati memorizzati, non su un singolo computer, ma su più macchine collegate tra loro, chiamate nodi. Le unità fondamentali della *Blockchain* sono i cosiddetti blocchi, ciascuno dei quali contiene: una serie di informazioni riferite ad un numero determinato di transazioni; un collegamento con il blocco precedente nella catena dei blocchi; la risposta ad un complesso quesito matematico utilizzato per validare e confermare i dati contenuti nel blocco stesso. Una copia di tutta la catena dei blocchi viene conservata in tutti i computer della rete, i quali vengono periodicamente sincronizzati in modo che ognuno di essi disponga del medesimo registro distribuito.

La *Blockchain* di *Bitcoin* è una *blockchain* pubblica e *permissionless* in quanto tutti gli utenti di internet possono accedervi e operarvi in maniera incondizionate, ma esistono anche *blockchain* private o modelli ibridi di *blockchain* che si stanno sempre più affermando negli ultimi anni. Per *blockchain* privata si intende un registro che, seppur fondato sulla stessa tecnologia della *Blockchain* di *Bitcoin*, differisce da questa in quanto prevede un'autorità centrale (che validi l'aggiunta di blocchi alla catena e le relative transazioni) e un accesso alle informazioni contenute nei blocchi che può essere sia pubblico che ristretto (*permission based*). Queste ultime ossia le *blockchain* private e *permission based* vengono più correttamente chiamate *Distributed Ledger Technology* (DLT). I modelli ibridi di *blockchain* i cosiddetti *consortium blockchain* permettono di superare la dicotomia pubblico/privato e sfruttare al meglio le potenzialità di entrambi i modelli. I *consortium blockchain*

basano il meccanismo di consenso sull'adesione di specifici soggetti partecipanti alla rete di computer e possono essere definiti come modelli parzialmente decentralizzati.

Un recente studio, realizzato dall'ufficio studi del Parlamento europeo, ha evidenziato come i possibili ambiti di applicazione delle *blockchain* sono pressoché illimitati: dalle valute virtuali, alla distribuzione di contenuti digitali, alla protezione dei diritti di proprietà intellettuale fino ad arrivare agli *smart contracts* e alle *Decentralized Autonomous Organizations* o DAOs.

L'eliminazione del *middleman* (di fatto la premessa fondamentale della *Blockchain*) dal punto di vista giuridico, rappresenta il principale punto critico di tale fattispecie, in quanto pone una rilevante questione, ossia se possa essere sufficiente affidarsi alla tecnologia, escludendo l'intervento di un autorità centrale di controllo, per assicurare che i dati immessi nel registro distribuito siano veritieri e corretti e che, in quanto tali, possano avere riconoscimento giuridico ed essere vincolanti per i partecipanti al registro e non solo. A questo interrogativo è possibile dare una risposta affermativa sulla base delle caratteristiche stesse della *Blockchain* (l'affidabilità, la piena trasparenza degli scambi, la solidità e l'irrevocabilità delle transazioni, il carattere integralmente digitale e dematerializzato) che la rendono a tutti gli effetti una tecnologia sicura.

nell'Unione europea la legislazione su tale innovativa tecnologia risulta ancora alle prime armi e limitata essenzialmente all'applicazione della stessa nell'ambito dei soli servizi finanziari. È auspicabile un futuro intervento regolatorio delle Autorità europee volto a facilitare lo sviluppo e la penetrazione della *Blockchain*, assicurando al contempo un'adeguata tutela dei soggetti convolti, in particolare consumatori e investitori.

Oltre che comprando e vendendo su una piattaforma criptovalute già esistenti, oppure creandole attraverso il processo di *mining*, esiste un altro modo per investire nel mondo dei nuovi strumenti finanziari digitali ossia quello di partecipare alle cosiddette ICO (*Initial Coin Offering).* queste sono un nuovo strumento di finanziamento attraverso il quale delle *start-up* raccolgono il capitale necessario per sviluppare i propri progetti legati alla *Blockchain*, creando nel frattempo una nuova criptovaluta con la quale ricompensano i finanziatori. Quanto ai vantaggi legati alle ICO, essi riguardano sia chi lancia la nuova offerta, in quanto permette a chiunque di sviluppare un progetto senza ricorrere alle tradizionali forme di finanziamento bancario; sia gli investitori, capaci di identificare i progetti più promettenti e ottenere significativi ritorni dagli investimenti effettuati. D'altra parte, però la promessa di profitti facili non deve far dimenticare che si tratta di un mercato ad alto rischio. Per definizione, infatti, le ICO si riferiscono a progetti non ancora realizzati, e di cui nessuno garantisce il successo, con l'aggravante che a differenza di quanto accade sui mercati regolati, qui l'investitore non ha alcuna forma di protezione nel caso i cui i promotori dell'ICO si dovessero rivelare dei truffatori, o anche se, più semplicemente, nonostante le buone intenzioni, questi non riuscissero a far avanzare il progetto con i finanziamenti ricevuti.

## 9. *RegTech* e *InsurTech*

*RegTech* viene considerato da molti un sottoinsieme del *FinTech*, al pari dell'*InsurTech* che cavalca l'innovazione nel modo delle assicurazioni. Il termine *RegTech*, contrazione di *regulation* e *technology*, indica l'impiego di strumenti tecnologici per facilitare l'implementazione delle nuove regolamentazioni e della *compliance* nell'ambito dei servizi finanziari, per supportare le procedure di adeguamento, conformità, rispetto di norme e regolamenti e per l'automatizzazione dei processi

di reportistica alle autorità di vigilanza. Il *RegTech* mira ad aiutare le imprese e le organizzazioni non solo a essere sempre in regola con le diverse normative e regolamentazioni, aspetto non da poco, soprattutto in sistemi altamente burocratici e soggetti a frequenti cambiamenti come quello italiano, ma anche a comprendere meglio come le regolamentazioni possono essere utilizzate per migliorare le prestazioni della stessa organizzazione. L'obiettivo è quello di creare processi standardizzati in modo da accelerare tempi e ridurre costi. Oltre che dalle imprese e dalle istituzioni finanziarie, le innovazioni tecnologiche del ramo *RegTech* vengono ampliamente utilizzate anche dai supervisori e dalle Autorità di vigilanza per la gestione dei dati e delle informazioni, ricevute dai soggetti vigilati, al fine di potenziare l'efficienza e la velocità dei controlli.

*InsurTech* identifica praticamente tutto ciò che è innovazione tecnologica in ambito assicurativo: *software*, applicazioni, *start-up*, prodotti, servizi. Mutuato dal termine *FinTech*, che afferisce al mondo più propriamente bancario, l'*InsurTech* è considerato anche un figlio di questo ed è pertanto molto simile, sia per l'impatto che sta producendo sulle imprese tradizionali del settore, sia per i fondamenti e le specifiche tecnologie (*Blockchain*, roboadvice, P2P, ecc.) su cui si basa, sia per la velocità con la quale si sta affermando.

Tra le *start-up* italiane attive nel settore dell'*InsurTech*, ricordiamo *Darwinsurance* fondata nel 2016. *Darwinsurance* è una piattaforma web finalizzata a rendere l'assicurazione *social*, conveniente e trasparente. Il progetto è legato all'insurance *peer to peer* (primo caso in Italia) e intende distribuire alle persone polizze assicurative costruendo piccoli gruppi mutualistici di amici e di persone di fiducia con cui condividere e controllare i propri rischi. Con una parte dei premi pagati dai membri del gruppo *Darwinsurance* crea una sorta di salvadanaio. Se il gruppo di assicurati mantiene basso il livello dei sinistri il denaro nel salvadanaio non verrà speso del tutto e la somma rimasta sarà rimessa a disposizione degli assicurati sotto forma di un bonus. Al momento è attiva solo nel mercato delle polizze viaggi ma a breve l'offerta verrà ampliata.

## 10. *Cybersecurity*

La sicurezza informatica rappresenta oggigiorno un elemento essenziale per l'efficace funzionamento di quei mercati che si fondano sempre di più sulle tecnologie digitali, come appunto quello del *FinTech*, in cui tra l'altro si presentano preoccupazioni ancora più rilevanti rispetto ad altri mercati, alla luce della specifica tipologia di servizi offerti. La corruzione di una rete o di un sistema informatico utilizzato per offerta di servizi finanziari difatti, può avere effetti nefasti sull'intero sistema finanziario e corrodere la fiducia dei consumatori in quest'ultimo. Alla luce di queste considerazioni, il quadro normativo relativo alla sicurezza informatica rappresenta un segmento fondamentale del complesso sistema di norme applicabili, direttamente o indirettamente, ai servizi *FinTech*.

La disciplina di riferimento a livello europeo è contenuta nella direttiva 2016/1148 o direttiva NIS che ha introdotto stringenti requisiti per diversi attori privati tra cui banche e fornitori di servizi internet, al fine di responsabilizzarli nella valutazione dei rischi in materia di cibersicurezza e di imporre meccanismi adeguati di gestione del rischio, capaci di garantire la resilienza delle reti e dei sistemi informativi. Nello specifico, la direttiva ha come obbiettivo principale quello di raggiungere la ciberresilienza per contrastare i rischi e le minacce cibernetiche con dimensione transfrontaliera e facilitare l'elaborazione di risposte coordinate a livello europeo da adottare in situazioni di emergenza. L'ambito di applicazione della direttiva NIS si estende a due diverse categorie di soggetti

gli operatori di servizi essenziali e i fornitori di servizi digitali. La direttiva inoltre, per garantire un adeguato livello di tutela della sicurezza delle reti e dei sistemi informativi, richiede agli Stati membri di individuare: una o più autorità competenti in materia di sicurezza delle reti e dei sistemi; un punto di contatto unico con il compito di garantire la cooperazione transfrontaliera tra le diverse autorità competenti degli Stati membri; uno o più gruppi di intervento per la sicurezza informatica in caso di incidente (CSIRT) con il compito di trattare incidenti e rischi secondo una procedura predefinita.

Le problematiche inerenti alla sicurezza cibernetica, assumono particolare rilievo in riferimento allo specifico settore dei servizi finanziari che, presentando una particolare esposizione nei confronti del pubblico, risultano maggiormente vulnerabili ad attacchi cibernetici. Sebbene la direttiva NIS appaia già presentare le potenzialità per garantire la tutela della sicurezza cibernetica in un campo assai vasto di servizi, rimane l'interrogativo se la tutela da attacchi cibernetici nel settore dei servizi finanziari richieda l'adozione di un approccio specialistico, con un intervento regolatorio *ad hoc*, in ragione delle peculiarità dei rischi in ambito *FinTech*.

In Italia è nel 2013 che matura il primo provvedimento in materia di cibersicurezza, ossia il D.P.C.M. rubricato "*Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale*". A questo primo importante passo si è arrivati per effetto di una crescente percezione di minaccia cibernetica come fonte di rischio per la sicurezza nazionale, rendendo improcrastinabile l'elaborazione di un piano strategico nazionale. Quest'ultimo avrebbe dovuto definire un'architettura istituzionale, in cui fossero chiaramente individuati i soggetti competenti a intervenire e i rispettivi ruoli e responsabilità in materia di cibersicurezza e definiti meccanismi e procedure rilevanti.

L'unica italiana, su 137 aziende di tutto il mondo che si occupano di *cybersecurity* in ambito finanziario, si chiama *Unfraud*, ha sede a Roma ed è una *start-up* fondata nel 2014. L'obbiettivo di *Unfraud* è quello di migliorare sensibilmente l'affidabilità delle transazioni online attraverso un sistema di intelligenza artificiale in grado di scovare e prevenire le frodi che minacciano le transazioni, con un costante monitoraggio delle attività di business online. Ad oggi *Unfraud*, che ha meno di dieci dipendenti, ha raccolto in tutto più di 130 mila dollari Il valore di mercato della *fraud prevention* è oggi di 10 miliardi di euro (circa 20 miliardi entro il 2019).

## 11. *Fintech* e antiriciclaggio

Il riciclaggio, qualificato come reato nella maggior parte degli ordinamenti penali nazionali, consiste nella riutilizzazione per attività legali, di denaro frutto di attività illecite. È un fenomeno economico-finanziario di natura transnazionale e incide notevolmente sulle dinamiche della ricchezza di una nazione. I criminali occultano l'origine illecita del denaro, in modo che non possa essere ricondotta ad una azione criminale, mediante la divisione della somma di denaro in piccole quote di importo esiguo, inserite in molteplici conti stabiliti in più Paesi e intestati ad individui o aziende diverse; spesso viene conferita un'origine legale apparente al denaro per poterlo immettere nel mercato creando finti contratti, prestiti, vincite o fatture.

Il finanziamento del terrorismo invece, può avere come fonti di denaro attività sia lecite che criminose; ed è proprio l'origine non necessariamente illecita delle disponibilità finanziarie, insieme all'utilizzo di somme spesso di importo esiguo, che rendono particolarmente complessa l'individuazione preventiva delle condotte finalizzate appunto al finanziamento del terrorismo. Le

organizzazioni terroristiche sfruttano abilmente le opportunità offerte dall'integrazione a livello globale dei mercati e le nuove tecnologie in campo finanziario, al fine di veicolare, da un Paese all'altro, in modo occulto, i fondi essenziali per le proprie attività. Gli attentati terroristici statunitensi degli anni 2000 hanno messo in luce la permeabilità dei sistemi finanziari internazionali all'attività terroristiche e l'esistenza di serie lacune regolamentari.

Il riciclaggio di denaro e il finanziamento del terrorismo dunque, rappresentano una grave minaccia per l'integrità e la stabilità del sistema finanziario, con conseguenze potenzialmente devastanti sia per la società che per l'economia. In questo contesto *FinTech* si mostra come un'arma a doppio taglio: da un lato, può essere utilizzato per promuovere e finanziare il terrorismo; dall'altro però può costituire un potente strumento per fortificare le difese contro quest'ultimo, grazie al suo utilizzo per l'individuazione di somme, anche di importo esiguo, destinate ad organizzazioni criminali.

Tra le innovazioni fintech più utilizzate per fini illeciti annoveriamo il *crowdfunding* e le valute virtuali. Con riferimento al *crowdfunding* i rischi di riciclaggio e finanziamento del terrorismo possono essere attenuati qualora le piattaforme siano obbligate dalla normativa vigente al compimento di controlli minimi che prevedano un'adeguata verifica del titolare del progetto, del progetto stesso e degli investitori, per individuare le situazioni che presentano maggiori rischi e anomalie. Per quanto riguarda le monete virtuali, gli elevati rischi di riciclaggio e di finanziamento del terrorismo sono legati al maggior grado di anonimato di cui le operazioni in valute virtuali beneficiano rispetto ai classici trasferimenti di fondi, caratteristica che le rende più appetibili alle organizzazioni terroristiche. Altri rischi sono legati inoltre all'irreversibilità delle operazioni, alla natura opaca e tecnologicamente complessa su cui si basa il loro funzionamento e alla mancanza di garanzie regolamentari.

A livello europeo la normativa di riferimento in materia di contrasto al riciclaggio di denaro e al finanziamento del terrorismo è la direttiva (UE) 2015/849 o Quarta Direttiva Antiriciclaggio (applicabile del 26 giugno 2017). Essa persegue i seguenti obbiettivi: tutelare gli interessi della società dalla criminalità e dagli attacchi terroristici; salvaguardare la prosperità economica dell'Unione assicurando un efficiente contesto imprenditoriale; contribuire alla stabilità, alla solidità, al regolare funzionamento e all'integrità del sistema finanziario mediante la prevenzione, l'individuazione e il contrasto del riciclaggio e del finanziamento del terrorismo.