Quaderni FinTech

Il FinTech e l'economia dei dati

Considerazioni su alcuni profili civilistici e penalistici

Le soluzioni del diritto vigente ai rischi per la clientela e gli operatori

E. Palmerini, G. Aiello, V. Cappelli

G. Morgante, N. Amore, G. Di Vetta, G. Fiorinelli, M. Galli

2

dicembre 2018

CONSOB

COMMISSIONE NAZIONALE PER LE SOCIETÀ E LA BORSA

Nella collana dei Quaderni FinTech
sono raccolti lavori di ricerca relativi
al fenomeno «FinTech» nei suoi molteplici aspetti
al fine di promuovere la riflessione e
stimolare il dibattito su temi attinenti
all'economia e alla regolamentazione
del sistema finanziario.

Consob

00198 Roma - Via G.B. Martini, 3
t +39.06.84771 centralino
f +39.06.8477612

20121 Milano - Via Broletto, 7
t +39.02.724201 centralino
f +39.02.89010696

h www.consob.it
e studi_analisi@consob.it

ISBN 9788894369717

Il FinTech e l'economia dei dati

Considerazioni su alcuni profili civilistici e penalistici

Le soluzioni del diritto vigente ai rischi per la clientela e gli operatori

E. Palmerini[(i)], G. Aiello[(ii)], V. Cappelli[(iii)]

G. Morgante[(iv)], N. Amore[(v)], G. Di Vetta[(vi)], G. Fiorinelli[(vii)], M. Galli[(viii)]

Sintesi del lavoro

Lo Studio analizza il contesto giuridico entro il quale collocare il fenomeno FinTech in relazione all'economia dei dati, e in particolare nell'utilizzo di dati personali: traendo spunto dalla 'tassonomia dei rischi' delineata nel primo *Volume* della *Collana*, si individuano i rischi per la clientela e per gli operatori del settore. Si procede secondo un duplice approccio, che convoglia le problematiche di inquadramento civilistico e quelle di carattere penalistico. La *Sezione* civilistica si occupa in particolare di leggere il fenomeno alla luce delle tendenze, apparentemente antitetiche, del *free flow of data* e della protezione della *privacy*, e di rilevare i profili di possibile contrasto tra uso e controllo dei *big data* e diritto antitrust. La *Sezione* penalistica mira a individuare contenuti e limiti degli strumenti che, nel diritto vigente, possano contribuire a costruire un quadro di tutela per i dati e il patrimonio della clientela dei servizi FinTech, unitamente all'approfondimento di taluni profili di *compliance* rispetto alla disciplina di settore. Lo Studio si conclude con alcune tabelle riassuntive della legislazione in materia e con una riflessione che coinvolge l'identità digitale e le future prospettive di ricerca.

(i) Erica Palmerini. Professoressa Associata di Diritto privato, Scuola Superiore Sant'Anna di Pisa, erica.palmerini@santannapisa.it

(ii) Giuseppe Aiello. Sostituto Procuratore presso la Procura della Repubblica di Trani.

(iii) Viola Cappelli. Dottoranda di ricerca in Diritto privato, Scuola Superiore Sant'Anna di Pisa, viola.cappelli@santannapisa.it

(iv) Gaetana Morgante. Professoressa Associata di Diritto penale, Scuola Superiore Sant'Anna di Pisa, gaetana.morgante@santannapisa.it

(v) Nicolò Amore. Dottorando di ricerca in Diritto penale dell'economia, Università degli Studi della Tuscia. nicolo.amore@unitus.it

(vi) Giuseppe di Vetta. Dottore di ricerca in Diritto penale, Scuola Superiore Sant'Anna di Pisa, giuseppe.divetta@santannapisa.it

(vii) Gaia Fiorinelli. Dottoranda di ricerca in Diritto penale, Scuola Superiore Sant'Anna di Pisa, gaia.fiorinelli@santannapisa.it

(viii) Martina Galli. Dottoranda di ricerca in Diritto penale, Università degli Studi della Tuscia. martina.galli@unitus.it

Si ringraziano Giuseppe D'Agostino e Pasquale Munafò per gli utili commenti a questo lavoro e per l'opera di coordinamento del progetto Fintech. Si ringraziano, inoltre, gli operatori del settore per le interviste svolte presso la Consob nel corso del primo semestre del 2017. Errori e imprecisioni sono imputabili esclusivamente agli Autori. Le opinioni espresse nel lavoro sono attribuibili esclusivamente agli autori e non impegnano in alcun modo la responsabilità dell'Istituto. Nel citare il presente lavoro, non è, pertanto, corretto attribuire le argomentazioni ivi espresse alla Consob o ai suoi Vertici.

FinTech and the data-driven economy

Some civil and criminal law issues

Finding legal solutions to the risks involving customers and operators

Working group Scuola Superiore Sant'Anna di Pisa

Abstract

This paper analyzes the legal framework applicable to FinTech services with regard to the data-driven economy: the analysis draws on the 'risk taxonomy' described in the first *Volume* of the *Series* and is focused on the risks involving customers and operators in this sector. The study connects civil law issues with criminal law questions, trying to adopt an interdisciplinary approach to the subject. The first part frames the FinTech phenomenon in the light of the tendencies towards the free flow of data, on the one hand, and the protection of personal data, on the other hand, and it identifies possible clashes between the use and control over *big data* sets and competition law. The second part adopts a criminal law perspective and it aims to identify contents and limits of the legal tools that can play a role in the construction of a solid criminal framework, in order to protect data and assets of the clients involved in FinTech services; it deals also with compliance questions raised by some sectoral legislations. Each part of the paper contains tables that summarize the main conclusions of the previous section. Some final considerations are laid out, that outline the most relevant notions examined, such as digital identity, and suggest future research topics.

JEL Classification: K24: Cyber Law; K14: Criminal Law; K15: Civil Law • Common Law; K21: Antitrust Law.

Keywords: FinTech; Big Data; Data Protection; Privacy; Data-driven economy; Personal Data.

Sommario

Obiettivi e struttura del lavoro

Il presente Volume si pone l'obiettivo di razionalizzare alcune delle principali questioni di carattere giuridico che sorgono intorno all'applicazione di tecnologie digitali con particolare riguardo all'utilizzo di dati personali nel settore finanziario, adottando una duplice prospettiva civilistica e penalistica. L'esigenza di sviluppare questa riflessione deriva dalla diffusione di prodotti e servizi finanziari innovativi, accanto all'elaborazione di nuove modalità di prestazione dei servizi più tradizionali. Questa *disruptive digitalization* ha comportato sostanziali modifiche di contesto, dalla configurazione del mercato all'evoluzione delle relazioni commerciali e sociali. Se, dunque, nel primo Volume della Collana sono stati messi in evidenza i principali rischi di carattere economico ed operativo che la digitalizzazione dei servizi finanziari comporta – al fine di ripensare i tradizionali business model propri dei vari settori – in questa sede si cercherà di fornire un quadro d'insieme degli stessi problemi in chiave di analisi giuridica. Nella maggior parte delle ipotesi, si tratta non già di trovare soluzioni de iure condito alle questioni messe in luce, ma ancor prima di comprendere in che modo gli istituti giuridici tradizionali possano intercettare le nuove istanze di tutela imposte dallo sviluppo tecnologico.

Per impostare la riflessione si è deciso di fare specifico riferimento alla 'tassonomia dei rischi' delineata nel primo Volume della Collana[1]: tale classificazione risulta particolarmente utile per la presente analisi in quanto focalizzata sull'individuazione dei soggetti sui quali tali rischi ricadono. In tal modo, il rischio sarà pietra angolare per valutare le problematiche giuridiche inerenti non soltanto alla questione primaria e fondamentale della tutela della clientela, ma anche alla particolare posizione ricoperta dagli operatori.

Il lavoro è suddiviso in due Sezioni principali, dedicate l'una all'inquadramento civilistico delle questioni trattate, l'altra alla rilettura penalistica delle medesime questioni. Tale scelta deriva dalla volontà di coordinare le soluzioni che la prospettiva giuridica può dare a questioni di carattere inevitabilmente complesso, in un'unità funzionale che una rigida bipartizione tra discipline impedirebbe di cogliere.

Con riferimento ai rischi per la clientela (utenti di servizi finanziari in ambito digitale), ci si concentrerà sul particolare ambito dei rischi operativi connessi alla raccolta, gestione e utilizzo di dati personali, poiché terreno fertile per il proliferare di comportamenti inquadrabili nelle coordinate del diritto vigente (dunque, al di là delle discipline speciali dell'intermediazione finanziaria applicabili). Più nello specifico, si prenderanno in considerazione le istanze di tutela e le soluzioni – in termini rimediali, repressivi e preventivi – identificate schematicamente nella tabella seguente:

1 Schena C., Tanda A., Arlotta C., Potenza G., "*Lo sviluppo del FinTech. Opportunità e rischi per l'industria finanziaria nell'era digitale*", CONSOB - Quaderno FinTech n. 1 (marzo 2017).

Rischio	Prospettiva civilistica	Prospettiva penalistica
Rischi di tutela dei dati e *privacy*	Problemi legati al trattamento dei dati, alla luce dei principi del GDPR, protezione della *privacy* e *free flow of data*	Inquadramento delle problematiche relative, in senso ampio, alla tutela penale dell'identità digitale, tra *privacy*, *cybersecurity*, reati informatici
Frodi o comportamenti scorretti delle imprese FinTech	Pratiche commerciali scorrette	Problematica della tutela penale della libertà contrattuale

Con riferimento, invece, ai rischi per gli operatori FinTech, ci si soffermerà in particolare sui rischi di *compliance*, aspetto quest'ultimo particolarmente controverso per un fenomeno di carattere innovativo e, dunque, tendenzialmente sfuggente alle maglie della regolazione.

Rischio	Prospettiva civilistica	Prospettiva penalistica
Trasparenza e correttezza	Problemi di concorrenza e discriminazione dei prezzi Problematiche connesse al procedimento automatico di profilazione dei clienti	
Rischio di riciclaggio del denaro e utilizzo ai fini di finanziamento del terrorismo		Ricognizione del fenomeno alla luce della disciplina in materia di *anti money laundering*
Rischio di condurre un'attività non autorizzata		Problematiche connesse alle riserve di attività previste dal TUB e dal TUF

Da un punto di vista metodologico, entrambe le *Sezioni* sono state sviluppate anche mediante il confronto diretto con gli operatori del settore, al fine di avere una visione del fenomeno quanto più possibile aderente alla realtà entro la quale si muovono prestatori di servizi e consumatori. Inoltre, tale confronto ha consentito di comprendere quali siano i settori nei quali è più urgente un intervento chiarificatore da parte delle Autorità di regolazione o, addirittura, legislativo e, invece, in quali aree risposte efficaci si trovino già nel sistema attuale.

La prima *Sezione* del *Volume*, elaborata dal gruppo di ricerca coordinato dalla Prof.ssa Erica Palmerini, è dedicata in particolare ad analizzare il FinTech nel contesto della *data-driven economy*. Seguendo lo schema della classificazione bipartita tra rischi per la clientela e rischi per gli operatori, il contributo si propone di approfondire alcune delle questioni più rilevanti sorte attorno all'uso massiccio di informazioni, che assume importanza cruciale per lo stesso sviluppo del settore FinTech nel contesto della *digital economy*. Il settore finanziario rappresenta un campo di indagine privilegiato del fenomeno dei *big data*, perché permette di mettere in luce il complesso bilanciamento tra opportunità e rischi, tra benefici e svantaggi, proponendo una vera e propria sfida regolamentare.

L'indagine si è concentrata anzitutto sulla normativa applicabile alla raccolta e al trattamento delle informazioni nel settore FinTech nel contesto dominato dall'entrata in vigore del GDPR.

L'analisi è condotta sulla falsariga di un bilanciamento continuo tra le tendenze del *free flow of data* e della protezione della *privacy*: lungi dall'essere due esigenze antitetiche, lo stretto legame che intercorre tra queste, e che si ripropone nel binomio *competition policy|privacy policy,* va valorizzato al fine di creare un clima di fiducia sia per gli operatori sia per la clientela. La prima parte della Sezione fornisce una visione d'insieme sullo strumentario di principi e regole che orientano il trattamento dei dati personali nel mercato dei servizi finanziari digitali, per poi mettere in luce alcune delle questioni più discusse in un'ottica ricostruttiva e propositiva. Tra di esse spiccano il tema della portabilità dei dati, emblematico del complesso e precario equilibrio tra *privacy* e concorrenza, e quello del controllo sui propri dati personali da parte dell'utilizzatore di servizi digitali, cui le istanze di "contrattualizzazione della *privacy*" e in particolare il modello del *services for data,* cercano di dare una prima risposta.

La seconda parte della Sezione, si occupa, invece, di approfondire i principali rischi cui potrebbe incorrere il prestatore dei servizi finanziari che si avvale dell'utilizzo di *big data*. A questo riguardo, la riflessione sul rapporto tra concorrenza e mercato dei *big data* sembra suscettibile di estensione al settore FinTech. Da un primo punto di vista, è necessario evidenziare che, nell'ambito della *digital economy*, il vantaggio competitivo tra imprese si fonda sull'offerta di servizi sempre più complessi, derivanti da una sofisticata capacità di analisi di dati: la domanda che domina la riflessione coinvolge, dunque, le modalità tramite le quali le figure tradizionali del diritto *antitrust*, ed in particolare l'abuso di posizione dominante, possono avere applicazione in questo ambito. In secondo luogo, la tematica della discriminazione dei prezzi e delle offerte personalizzate ai clienti, derivanti da procedimenti di profilazione fondati anche sull'analisi di *big data,* pone rilevanti problemi di qualificazione: se è difficile ricondurre la fattispecie ad uno specifico illecito, il compenetrarsi tra esigenze di tutela della *privacy* e promozione della concorrenza fornisce soluzioni più soddisfacenti, garantendo che il consumatore sia consapevole della natura personalizzata dell'offerta a lui rivolta.

Muovendosi nel prisma dei rischi che gravano sui soggetti attivi nel mercato digitale dei servizi finanziari, la prima Sezione propone dunque una mappatura dei

temi rilevanti in chiave civilistica: da una parte, l'analisi del sistema vigente permette di distillare le criticità legate al dinamismo della prassi di un settore in continua evoluzione; da un'altra parte, le grandi potenzialità dell'uso dei *big data n*ella digitalizzazione dei servizi finanziari richiedono uno sforzo ermeneutico volto a conciliare tali prassi con le tutele esistenti.

La seconda *Sezione* del *Volume*, elaborata dal gruppo di ricerca coordinato dalla Prof.ssa Gaetana Morgante, è dedicata all'inquadramento in termini penalistici del fenomeno FinTech. Anche in questa sezione si riprende con funzione classificatoria la distinzione tra i rischi per la clientela e i rischi per gli operatori, sia pur con la consapevolezza della stretta interconnessione che sussiste tra questi due profili: infatti, ad ogni rischio di carattere operativo per la clientela – rispetto a dati, identità digitale e patrimonio – corrisponde simmetricamente un 'rischio penale' per gli operatori, da intendersi quale obbligo – penalmente sanzionato, anche indirettamente – di valutare e gestire la fonte di rischio; parallelamente, il rischio per gli operatori di compiere attività illecite – riciclaggio, finanziamento del terrorismo, abusivismo – è penalmente sanzionato con lo scopo di proteggere la legalità e l'integrità del mercato, ma anche, in forma collettiva, gli interessi della clientela. Ad ogni modo si è deciso di seguire tale schema classificatorio per l'indubbia chiarezza espositiva che ne consegue, anche in considerazione dell'esigenza di rendere possibile il confronto con il segmento civilistico dell'analisi.

Quanto al metodo seguito, si è deciso di muovere dai singoli rischi concreti, per individuare la disciplina applicabile ed eventualmente, soprattutto in caso di evidenti vuoti normativi, formulare proposte *de iure condendo*. Si è voluto, inoltre, non limitare l'analisi alla sola legislazione nazionale, dedicando attenzione altresì alle fonti internazionali e sovranazionali, nonché alle indicazioni di *soft law* elaborate dalle autorità di vigilanza.

Quanto ai contenuti della *Sezione* dedicata ad *Enforcement e regimi sanzionatori*, una prima sotto-sezione è finalizzata alla ricerca degli strumenti giuridici di carattere penale per tutelare la clientela dai rischi operativi, connessi ora alla natura digitale delle transazioni, ora alla natura finanziaria delle stesse. Con riferimento al primo profilo, si tenta di fornire un inquadramento giuridico ai rischi per la *privacy* e per la tutela dei dati dei clienti di servizi FinTech, sia rispetto a un utilizzo improprio degli stessi da parte delle piattaforme, sia nel caso di appropriazione e indebito utilizzo da parte di terzi. Lo strumentario cui fare ricorso consiste, come si vedrà, nelle disposizioni sanzionatorie – penali o amministrative – contenute nel Codice della *privacy* nonché nelle fattispecie contenute nel codice penale riconducibili al *corpus* dei reati informatici. Con riferimento al secondo profilo, invece, la natura finanziaria delle transazioni porta con sé peculiari rischi di carattere operativo, determinati dall'assenza di un'apposita disciplina finalizzata – come invece accade nel settore della finanza 'istituzionale' – a individuare il profilo di rischio del cliente e modularne di conseguenza le scelte di investimento. In conseguenza di ciò si tratta, dunque, di effettuare una ricognizione della disciplina applicabile a tale tipologia di relazione contrattuale, con specifico riferimento ai profili della *compliance* e dell'*enforcement* delle regole di condotta; tale trattazione dovrà,

tuttavia, svolgersi con meri cenni, dato che un approfondimento più ampio del problema sarà contenuto in altro e successivo *Volume* della Collana, dedicato al tema dell'inclusione finanziaria.

La seconda sotto-sezione è, invece, dedicata a rischi per gli operatori, segnatamente ai rischi di *compliance* rispetto alla normativa penale in materia di riciclaggio, finanziamento del terrorismo e abusivismo nello svolgimento di operazioni sottoposte a riserva di attività. Le peculiarità dei servizi FinTech, in particolare del *crowdfunding* e del *social lending*, espongono, infatti, i prestatori di servizi a considerevoli rischi di illegalità: non soltanto, come si è anticipato, rispetto al potenziale utilizzo di tali strumenti per il compimento o l'agevolazione di attività criminali, ma anche perché la stessa prestazione di servizi di natura finanziaria in forma 'atipica' può entrare in collisione con la disciplina delle attività bancarie e finanziarie, soggette a poteri di autorizzazione e vigilanza da parte delle autorità del settore.

L'analisi si conclude con la schematizzazione della normativa applicabile e la risoluzione di alcune questioni molto dibattute in dottrina. Infine, tale approfondimento è anche occasione per formulare proposte di *policy* e per evidenziare le prospettive di ricerca ancora lasciate aperte nell'ambito di un settore in continua evoluzione.

SEZIONE I

Il FinTech nel contesto della *data-driven economy*: profili civilistici tra rischi per la clientela e rischi per gli operatori

E. Palmerini, G. Aiello, V. Cappelli

La disponibilità di informazioni di tipo sia generico sia specifico - sugli *assets* patrimoniali, sulla propensione al rischio degli investitori, sulle abitudini di consumo, sulla pregressa storia finanziaria – rappresenta un elemento cruciale per lo sviluppo di molte applicazioni del settore FinTech[2]. Come si evidenzia nei numerosi studi di primo approccio al fenomeno, dati di quantità e qualità elevate non sono un mero fattore di facilitazione dei processi di digitalizzazione della prestazione dei servizi finanziari, ma un vero e proprio requisito di operatività.

Le condizioni che hanno favorito lo sviluppo del settore FinTech sono infatti costituite, oltre che dalle ben note contingenze economiche legate alla crisi finanziaria e al ridursi dei margini di profitto delle attività di prestito e di investimento, da un particolare *background* tecnologico, dove si intersecano l'aumento del potere computazionale, la grande accessibilità e disponibilità di dati a livello macro e a livello individuale, e la moltiplicazione delle piattaforme in cui avvengono la raccolta e lo scambio di informazioni.

L'uso massiccio di informazioni per lo svolgimento di attività finanziarie si inserisce a pieno titolo nel fenomeno, di rilievo soprattutto socio-economico, della c.d. *data-driven economy*[3]. Quest'espressione designa un ecosistema composto da molteplici attori che generano e raccolgono grandi quantità di dati, li processano attraverso tecniche di *big data analytics* e offrono, anche sulla base dei risultati di questa attività, servizi di varia natura, tra cui quelli di interesse per l'ambito del prestito e del finanziamento, dei sistemi di pagamento e degli investimenti finanziari[4].

Più in particolare, attraverso queste tecniche numerose tipologie di attività come la profilazione dei clienti, la determinazione del merito creditizio, i test di

2 Joint Committee of European Supervisory Authorithies (ESAs) (2016), p. 8.

3 Commissione europea, *Building a European Data Economy*, COM(2017) 9 final, Bruxelles, 10.1.2017.

4 Commissione europea, *Towards a data-driven economy*, COM(2014) 442 final, Bruxelles, 2.7.2014.

adeguatezza, la fidelizzazione, le campagne di marketing, lo sviluppo di nuovi prodotti, la fissazione dei prezzi, l'identificazione dei rischi e la prevenzione delle frodi sono suscettibili di essere eseguite, rese più efficienti e raffinate rispetto ai sistemi tradizionali.

Dal punto di vista dei regolatori, il settore finanziario costituisce uno, se non il principale, terreno di implementazione della strategia per un mercato digitale da parte dell'Unione europea[5]. La profonda relazione che sussiste tra l'innovazione nel settore della finanza e la digitalizzazione dell'economia è puntualmente messa in luce dal recente documento che lancia il Piano d'azione europeo per il FinTech, in cui quest'ultimo è collocato proprio all'intersezione tra i due ambiti[6].

Esso costituisce in effetti un campo privilegiato di osservazione e, in prospettiva, di intervento per quanto concerne l'uso di grandi quantità di dati per la messa a punto di forme non convenzionali di prestazione dei servizi ovvero di prodotti innovativi. I benefici derivanti dall'analisi dei *big data* sono identificati in una migliore conoscenza e segmentazione, a livello granulare, della clientela, con il duplice vantaggio di soddisfare le esigenze dei singoli individui attraverso servizi personalizzati anziché di tipo standardizzato ed, eventualmente, persino di raggiungere soggetti finora esclusi dal mercato del credito, a causa della minore precisione dei metodi tradizionali di stima del merito creditizio. Questa più fine conoscenza della clientela ha ricadute anche sul piano della *compliance*, perché risponde in modo avanzato al precetto della *know your customer rule*. Servizi aggiuntivi rispetto a quelli tradizionali, talvolta offerti in forma gratuita, possono essere sviluppati per effetto della maggiore efficienza ed economicità complessiva del sistema, così come sconti, offerte speciali o pubblicità mirate sono proposti combinando i dati già in possesso di istituzioni bancarie con le informazioni sulle abitudini di consumo o su particolari eventi della vita (ad esempio, la nascita di un bambino)[7]. Una analisi costante e un monitoraggio delle informazioni generate in questa catena possono servire anche ad anticipare problemi o la inadeguatezza sopravvenuta del prodotto ai bisogni dell'investitore e, dunque, a introdurre azioni correttive.

La grande disponibilità di dati e lo sfruttamento intensivo cui questi sono sottoposti – spesso ad opera di poche imprese di grandi dimensioni –costituiscono un

5 Commissione europea, Comunicazione Strategia per il mercato unico digitale in Europa, COM(2015) 192 final, Bruxelles, 6.5.2015; Comunicazione sulla revisione intermedia dell'attuazione della strategia per il mercato unico digitale. Un mercato unico digitale connesso per tutti, COM(2017) 228 final, 10.5.2017. Altre aree di intervento sono quelle del diritto dei contratti e, in particolare, della vendita on line e a distanza di beni tangibili e della vendita di beni digitali, oggetto di due proposte di direttiva: rispettivamente *Proposal for a Directive concerning contracts for the online and other distance sales of goods*, COM(2015) 635 final; *Proposal for a Directive on certain aspects concerning contracts for the supply of digital content*, COM(2015) 634 final, 9.12.2015. Su quest'ultima v. Schulze, Staudenmayer e Lohsse (eds) (2017); in termini più generali, Basedow (2016).

6 "*Fintech sits at the crossroads of financial services and the digital single market*": Commissione europea, *FinTech Action plan: For a more competitive and innovative European financial sector*, COM(2018) 109 final Brussels, 8.3.2018, p. 2.

7 Per un quadro di sintesi sui pregi dell'uso di big data in relazione ai servizi finanziari v. F. Mattasoglio (2017), p. 72 s.; European Banking Authority (EBA) (2016), p. 19 ss.

fenomeno tenuto sotto osservazione da parte dei regolatori poiché presenta, accanto ai benefici appena enumerati, elementi di rischio aggiuntivi rispetto alle attività realizzate in forma tradizionale. Il moltiplicarsi delle fonti di raccolta dei dati può causare una scarsa qualità o incongruenze dei medesimi, che finiranno per ridondare, anziché in una conoscenza più approfondita del cliente, in una profilazione inaccurata, fino all'estremo dell'esclusione di soggetti erroneamente ritenuti inaffidabili da alcune tipologie di servizi. Il grande valore economico dei dati implica rischi maggiori per la sicurezza e richiede l'adozione di misure di tutela corrispondenti, ad evitare usi illeciti. Vi è una necessità accentuata di tutela della *privacy* delle persone cui i dati si riferiscono, ma alcuni elementi di vischiosità, legati alla complessità delle informazioni da fornire ai clienti, per un verso, e intrinseci all'ambiente digitale in cui spesso avviene la raccolta dei dati, creano difficoltà pratiche di attuazione[8].

1 *Free flow of data* e protezione della *privacy* tra rischi per la clientela e per gli operatori: due tendenze antitetiche?

Tra le tendenze che ispirano l'opera di regolazione con riguardo a questo fenomeno vi sono, da un lato, il forte risalto dato alla necessità della circolazione dei dati (c.d. *free flow of data*)[9], talvolta prospettata come la quinta libertà economica fondamentale da aggiungere a quelle già operanti nel mercato unico[10], da un altro lato, la protezione accentuata di cui godono la *privacy* e i dati personali a livello europeo, in contrapposizione, ad esempio, al modello statunitense[11].

Secondo una prima prospettiva, relativa ai rischi per la clientela, si può affermare che le due linee che dovranno informare il quadro giuridico di riferimento sono tra di loro in apparenza dicotomiche. Esse tuttavia trovano un componimento per due ordini di ragioni: anzitutto, sul piano tecnico, nella distinzione tra categorie di dati, che risulteranno inclusi ovvero estranei al campo di applicazione della disciplina sul trattamento dei dati personali in ragione della loro attinenza a una persona determinata. Occorre infatti precisare che mentre la tutela della *privacy* si estende unicamente alle informazioni personali, per come definite dalla stessa normativa, le tecniche di *data mining* e *analytics* interessano in buona parte dati (ad esempio, *machine-generated data* oppure dati statistici su fenomeni demografici, climatici o macroeconomici) non riferibili a un soggetto individuato, e ciò esclude in radice un problema di *privacy*. Per vero, i dati maggiormente appetibili per il mercato,

8 EBA (2016), p. 22 ss.

9 European Parliament, *Resolution on FinTech: the influence of technology on the future of the financial sector*, 2016/2243(INI), 17.5.2017, punto 22.

10 Secondo la proposta del Governo estone, di cui riferisce il Commission Staff Working Document on *the free flow of data and emerging issues of the European data economy accompanying the document Communication Building a European data economy*, SWD(2017) 2 final, Bruxelles, 10.1.2017, p. 23. In tal senso anche il documento dello European Political Strategy Center (EPSC) (2017), p. 10.

11 Tale divario nelle impostazioni di tutela della privacy di Europa e US è stato all'origine dell'invalidazione del c.d. *Safe Harbour Agreement* da parte della Corte di Giustizia nel caso Schrems: Schrems v. Data Protection Commissioner, ECR 1 (2015).

e più in particolare per il mercato dei servizi finanziari, sono proprio quelli riferibili a uno specifico individuo, e dunque personali[12]. Tale constatazione è però controbilanciata da altri elementi: l'elevata capacità nel trattamento dei dati e l'intensa protezione assicurata alle informazioni sono infatti in grado di generare fiducia nei consumatori e, dunque, appaiono strategici rispetto all'obiettivo della loro circolazione. Un alto livello di tutela dei dati personali, in quanto strumentale alla tutela della persona e della sua dignità, rappresenta in definitiva non una barriera, bensì un fattore di facilitazione per lo sviluppo di un mercato digitale.

A corroborare questo circuito virtuoso tra forte tutela e circolazione delle informazioni è anche la recente applicazione (dal 25 maggio 2018) del Regolamento 2016/679 (GDPR)[13]. Fin dalle premesse, esso mette in stretta connessione la protezione dei dati con l'aspetto prettamente economico, là dove reputa la prima necessaria a creare quel "clima di fiducia" che può consentire lo sviluppo del mercato digitale (considerando 7)[14]. Ma vi è di più: con il passaggio dalla direttiva al regolamento si rafforza l'obiettivo del legislatore europeo di creare le condizioni più favorevoli per la circolazione dei dati, smorzando l'accento sulla disciplina come architettura rivolta principalmente alla protezione della persona. Lo evidenzia la norma di apertura, là dove si precisa che "*la libera circolazione dei dati personali nell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali*" (art. 1, comma 3); lo sottende la scomparsa, nello stesso articolo, del riferimento ampio e comprensivo al diritto alla vita privata come oggetto di tutela (art. 1, comma 1, Dir. 95/46), sostituito dal diritto, di natura strumentale, al trattamento dei dati personali (art. 1, comma 2, GDPR)[15].

Lo stesso mutamento dello strumento giuridico – da direttiva a regolamento – amplifica l'effetto di favorire la circolazione dei dati, poiché garantisce l'applicazione della medesima disciplina a ogni trattamento di dati personali realizzato all'interno dell'Unione europea. In base all'art. 3, è sufficiente, infatti, che l'elaborazione sia effettuata nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione, essendo irrilevante il fatto che il trattamento stesso sia effettuato all'estero. (art. 3, co. 1). Qualora titolare e responsabile non siano stabiliti nell'UE, il Regolamento è applicabile al trattamento di dati di interessati che si trovano nell'Unione se nel territorio di quest'ultima è effettuata l'offerta di beni e servizi cui il trattamento è relativo ovvero il monitoraggio del comportamento delle persone (art. 3, co. 2). L'applicazione di questo modello di regolazione avanzato è in grado di attribuire agli utenti dei servizi finanziari un elevato controllo sui propri dati e di creare, al tempo

12 Lo osserva Mattasoglio (2017), p. 66.

13 Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati).

14 Sottolinea, tra gli altri, questa relazione reciproca Thiene (2017), p. 414. Da tempo rileva l'essenzialità di privacy e cybersicurezza rispetto all'implementazione del mercato unico digitale Weber (2015).

15 Piraino (2017), p. 375, qualifica la scelta non "neutrale" e rivolta a valorizzare il "momento circolatorio dei dati personali" rispetto alle implicazioni personalistiche.

stesso, un ambiente competitivo per diversi tipi di operatori, *incumbent* e FinTech *start-ups*, e per soggetti che sono stabiliti in Europa o al di fuori del territorio comunitario.[16]

Questo identico livello di protezione della *privacy* renderà ingiustificate, ad esempio, quelle restrizioni alla circolazione dei dati dipendenti da specifiche previsioni normative, finora accettate in funzione di una maggiore sicurezza o di una più agevole possibilità di controllo da parte del singolo Stato. Tra di esse si annoverano le regole che impongono l'elaborazione e la conservazione dei dati su un server situato nel territorio del singolo Stato, comuni proprio nel settore in esame, allorché i prestatori di servizi finanziari sono tenuti alla localizzazione domestica dei dati sottoposti al controllo delle autorità di supervisione. Con l'armonizzazione massima della disciplina applicabile diviene infondato l'assunto per cui un sistema giuridico garantirebbe un livello di protezione o di accessibilità dei dati superiore rispetto ad un altro[17]. A ciò deve aggiungersi che requisiti di localizzazione potrebbero essere addirittura controproducenti rispetto agli obblighi di sorveglianza, e che questi potrebbero essere garantiti da una migliore cooperazione tra autorità a livello europeo, nonché creando le condizioni per accedere ai dati ovunque essi siano conservati sul territorio comunitario senza la necessità di assolvere onerose procedure amministrative[18].

Poiché tutte le imprese che intendano offrire beni o servizi all'interno del mercato europeo saranno soggette al nuovo Regolamento, questo sviluppo normativo è ad un tempo un forte dispositivo di protezione per i cittadini europei ma altresì un volano di crescita per la prestazione di servizi transfrontalieri. Grazie all'uniformità dei requisiti cui le prime devono ottemperare, si eliminano infatti i costi legati alla messa a punto di diversi protocolli e prassi operative che rispettino i diversi regimi operanti nei Paesi verso cui il singolo operatore vuole espandersi.

Deve evitarsi, tuttavia, che la maggiore protezione che l'Unione europea assicura ai suoi cittadini in relazione al trattamento dei loro dati personali si traduca in uno svantaggio competitivo. All'uopo, la necessità di conformarsi ad una disciplina unica ogni qualvolta si svolgano attività che implicano di processare dati personali allinea la posizione delle imprese innovative a quella degli operatori tradizionali, che, almeno a questo riguardo, non sono tenuti ad adempimenti ulteriori o al rispetto di requisiti più stringenti. È peraltro opportuno che si chiarisca il quadro normativo complessivo[19]. al momento composto da norme contenute in discipline diverse che comprendono, oltre al nuovo Regolamento 2016/679, sostituivo della Direttiva 95/46, anche la seconda Direttiva sui servizi di pagamento (PSD2), la quarta Direttiva

16 European Banking Federation (EBF) (2016), p. 15.

17 Commission SWD on the free flow of data and emerging issues of the European data economy, p. 7, dove si nota come la sicurezza dei dati in formato elettronico dipenda dai dispositivi tecnologici e dalle tecniche di crittazione impiegati per proteggerli, più facilmente disponibili nei grandi centri, tecnologicamente avanzati e per questo meno vulnerabili ad attacchi.

18 Commissione europea, Communication Building a European Data Economy, p. 5 e nt. 17.

19 Parlamento europeo, Progetto di relazione sulla tecnologia finanziaria: l'influenza della tecnologia sul futuro del settore finanziario (2016/2243(INI)), 27.1.2017, p. 9.

antiriciclaggio (AMLD4) e la Direttiva sulla cybersicurezza (NIS). Devono, in particolare, essere identificate le regole applicabili a ciascun rapporto e risolte eventuali sovrapposizioni o contraddizioni.

Un secondo punto di vista tramite il quale risulta estremamente rilevante analizzare il rapporto tra *free flow of data* e protezione della *privacy* è quello che giunge a lambire i confini del diritto della concorrenza. In questo caso il terreno su cui condurre la riflessione diventa particolarmente insidioso perché lo sforzo interpretativo coinvolge la stessa individuazione della disciplina applicabile. Indubbiamente il *corpus* normativo *antitrust* e il diritto della *privacy* si occupano di questioni radicalmente diverse, ma nell'ambito del mercato dei *big data* – con effetti particolarmente rilevanti nell'area della prestazione di servizi finanziari – le sfere di interesse di queste due branche possono giungere a sovrapporsi. A tal proposito, appaiono emblematiche le parole del Parlamento Europeo, che, nella Risoluzione sulla tecnologia finanziaria del 17 maggio 2017, tracciano l'indirizzo regolatorio da seguire: in particolare si afferma l'esigenza di finalizzare il quadro normativo relativo al FinTech alla "promozione della concorrenza leale, la neutralizzazione delle eventuali rendite economiche e la creazione di condizioni di parità"[20].

Una delle esigenze più pressanti che si pone in questo contesto è di evitare la concentrazione del potere di mercato nelle mani di pochissimi operatori: il rischio è che alcune imprese assumano una posizione di dominanza tale da permettere loro di realizzare condotte di esclusione, così impendendo l'accesso al mercato dei dati ad altre imprese più piccole.

La ricerca di un equilibrio tra le diverse istanze avanzate dai vari attori in gioco coinvolge in primo luogo le stesse potenzialità innovative del settore dei *big data* nel panorama più ampio della *digital economy*: le informazioni rappresentano infatti una risorsa di strategica importanza, e una legislazione troppo restrittiva in termini di *privacy* potrebbe limitarne l'impatto innovativo.

La stessa applicazione delle categorie del diritto antitrust al sistema dell'economia dei dati può risultare non soddisfacente. Risulta particolarmente ostico prevedere un quadro regolatorio in cui un'impresa che ha acquisito una competenza sull'analisi e sulla raccolta dei dati, costituendosi così uno specifico *know how*, debba poi condividerla con i propri concorrenti sul mercato. Tuttavia, allo stesso tempo, il rischio di concentrazione di potere di mercato nelle mani di pochissimi operatori è reale: le Autorità antitrust di Francia e Germania hanno portato l'attenzione su questo profilo, evidenziando che la raccolta di dati personali da parte delle grandi imprese permette a queste di offrire servizi sempre più sofisticati, incrementando così il divario qualitativo con le imprese emergenti.

L'ambito di applicazione della disciplina sulla concorrenza nel contesto dell'economia dei dati si estende fino alla questione delle intese o delle pratiche collusive tra imprese, operanti anche in mercati diversi: emblematica in tal senso è la

20 Sottolinea questo passaggio, Vessia (2016). Il riferimento è alla Risoluzione del Parlamento europeo del 17 maggio 2017 sulla tecnologia finanziaria, l'influenza della tecnologia sul futuro del settore finanziario, 2016/2243 (INI).

vicenda *Google/Android*. In ogni caso, fino ad ora sono state le operazioni di concentrazione tra imprese ad aver suscitato maggiormente l'attenzione delle Autorità antitrust, sebbene la Commissione europea abbia espresso sempre un giudizio positivo su quelle sottoposte alla sua valutazione[21]. Il sistema di valutazione stesso, tuttavia, è poco incentrato sull'aspetto dinamico della questione, e quindi sugli effetti che una concentrazione, e il connesso aumento della disponibilità di dati in capo ad un'impresa, può avere sulla struttura del mercato. La fusione tra *Facebook* e *Whatsapp* è esemplificativa di ciò che si intende dire: la posizione di dominanza acquisita da *Facebook* nel mercato dei *social network* si è trasferita, tramite la fusione con *Whatsapp*, nel mercato delle comunicazioni[22].

Inoltre un altro elemento problematico da considerare nel contesto dei rapporti tra concorrenza e megadati riguarda l'imposizione di regole di trasparenza, necessarie nell'ottica di *empowerment* del consumatore. La trasparenza potrebbe rivelarsi un'arma a doppio taglio: indubbiamente i consumatori acquisirebbero una maggiore consapevolezza, ma la stessa trasparenza, nell'agevolare un più veloce scambio di informazioni, potrebbe provocare un allineamento dei prezzi e disinnescare una diversificazione delle offerte. Emerge così ancora una volta la complessità dell'intersezione tra tutela dei dati personali e promozione della concorrenza. Anche in relazione a questo aspetto il quadro normativo esistente dovrebbe essere chiarito ed integrato: la Comunicazione della Commissione del 12 gennaio 2011 (2011/C 11/01) "Linee direttrici sull'applicabilità dell'art. 101 del Trattato sul funzionamento dell'Unione europea agli accordi di cooperazione orizzontali" prende in considerazione il problema, ma non lo cala nel contesto dell'economia dei dati, né dei servizi finanziari digitali.

2 I rischi per la clientela: profili di tutela della *privacy* e sicurezza

2.1 Il trattamento di dati personali nella prestazione di servizi finanziari: il quadro dei principi

Al fine di risolvere l'inevitabile tensione tra l'obiettivo del *free flow of data* e le garanzie per la *privacy* degli individui e per comprendere quali siano i principali rischi cui questi ultimi sono esposti nel contesto della *digital economy*, occorre disarticolare il profilo della gestione dei dati nel rapporto tra impresa FinTech e utente dal tema, più vasto, della *big data analytics*. Il primo segmento è retto inevitabilmente dalla normativa rilevante sul trattamento dei dati personali. Al riguardo, il Regolamento 2016/679, entrato in vigore il 25 maggio 2018, è interamente applicabile anche ai trattamenti di dati effettuati per rendere servizi

21 Vassia (2017), p. 98. Il riferimento è ai casi Google/Double Click, Microsoft/Yahoo!SearchBusiness, Microsoft/Skype, Facebook/WhatsApp e Microsoft/LinkedIn

22 Ibidem. L'Autrice, in particolare, cita il provvedimento n. 26597/2017 dell'AGCM, con cui *Whatsapp* è stata sanzionata per pratiche commerciali scorrette (artt. 20 comma 2, 24 e 25 cod. cons.) "per aver indotto i consumatori ad accettare la clausola di condivisione dei propri dati con Facebook nella fase di accettazione dell'aggiornamento dei termini di utilizzo di Whatsapp Messanger".

finanziari per via telematica. Al fine di evitare l'insorgere di gravi rischi di elusione, la protezione delle persone fisiche è infatti neutrale sotto il profilo tecnologico e non dipende dalle tecniche impiegate per il trattamento (considerando 15).

Le tipologie di dati raccolte e usate dagli operatori del settore sono di varia natura e possono includere le informazioni anagrafiche, l'indirizzo mail e i contatti telefonici, la professione svolta, le attività extraprofessionali, i dati di connessione e la cronologia, dati relativi ai sistemi di pagamento utilizzati, le propensioni di consumo ed eventuale contenzioso al riguardo, l'uso dei social network, informazioni raccolte per effettuare valutazioni di adeguatezza o per accertare il merito creditizio[23]; più in generale tutti i microcomportamenti finanziari che lasciano tracce nell'ambiente digitale. I dati trattati possono provenire da fonti sia interne sia esterne alle istituzioni finanziarie: del primo tipo sono quelli raccolti in occasione dell'instaurarsi di una relazione contrattuale (ad esempio, apertura di un conto) e successivamente in rapporto alle operazioni (es. pagamenti, iscrizione a un programma premi a punti, rilascio di carte fedeltà) effettuate nel corso di essa; del secondo tipo sono quelli ottenuti da altri soggetti, pubblici o privati, e dai social media: ad esempio, i dati presenti in pubblici registri, come quelli dello stato civile e catastali, i dati forniti da agenzie per la valutazione del merito creditizio, da società dello stesso gruppo ma operanti in un altro ramo, dalle imprese del settore digitale che aggregano e combinano dati variamente immessi on line dallo stesso consumatore[24].

Al trattamento di dati personali da parte delle FinTech sono applicabili i principi già posti dalla Direttiva 95/46 e oggi elencati all'art. 5 del GDPR: liceità, correttezza e trasparenza (art. 5, comma 1, lett. a). Ad essi si aggiunge il principio di finalità, ricavabile dalla regola secondo cui ogni raccolta deve essere effettuata per finalità "determinate, esplicite e legittime" e, quanto al successivo trattamento, dispone che esso sia realizzato in modo "non incompatibile con tali finalità" (art. 5, comma 1, lett. b).

Tra i principi generali che delineano la cornice giuridica entro cui può avvenire il trattamento di dati, più critica può risultare l'attuazione dell'obiettivo di «minimizzazione dei dati» da parte delle imprese del settore FinTech (art. 5, comma 1, lett. c). Esso richiede che i dati raccolti e trattati siano adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità. Si tratta di un principio che fa da complemento alla regola del consenso, compensando le debolezze intrinseche a tale strumento; benché sia un adempimento oneroso, rimane essenziale per il rispetto

23 Joint Committee ESA (2016), p. 12. Un elenco più dettagliato e granulare delle tipologie di dati personali trattati nella prestazione di servizi finanziari on line è presente nel documento di EBA (2016), p. 9: a) dati anagrafici (nome e cognome, cittadinanza, luogo e data di nascita, età, sesso, stato civile, numero di familiari a carico; *b)* dati di contatto (indirizzo, numero di telefono, e-mail, geolocalizzazione; *c)* dati sul domicilio informatico (cronologia di navigazione, indirizzo IP, dati di log, attività di chiamata e dati dei messaggi); d) proprietà e locazione dell'abitazione; e) formazione e condizione professionale (titolo di studio, lavoratore autonomo o dipendente, settore e datore di lavoro, reddito, inizio e fine dei rapporti di lavoro); *f)* altri tipi di dati sensibili; *g)* hobby e sport praticati; altri interessi personali; *h)* informazioni da *Social Network* (collegamenti sociali, informazioni fornite negli aggiornamenti di stato).

24 EBA (2016), p. 15 s.

della normativa, fermo restando quanto si dirà sulle tecniche di analisi dei *big data* che si avvalgono della anonimizzazione. Le imprese dovranno quindi sempre giustificare la selezione delle categorie di dati adoperati e specificare in modo comprensibile nei contratti gli usi ultronei rispetto all'esecuzione delle obbligazioni principali derivanti dall'accordo[25]. Nondimeno, in un contesto così favorevole allo sfruttamento della più grande mole di dati disponibili, in funzione di una diminuzione dei costi e di un incremento complessivo dell'efficienza del sistema, l'imperativo in questione, funzionale alla tutela della *privacy*, rischia effetti controproducenti sul piano della qualità e della completezza dei risultati[26].

La Direttiva sui servizi di pagamento nel mercato interno (cd. PSD2)[27], entrata in vigore il 13 gennaio 2016 e applicabile dal 13 gennaio 2018, riprende questi principi e li adatta allo specifico contesto di riferimento, dedicando il Capo 4 alla "*Protezione dei dati*" personali[28]. La Direttiva muove dall'elementare constatazione per cui "la prestazione di servizi di pagamento [..] può comportare il trattamento di dati personali"; in aggiunta, essi appartengono al novero dei dati dai quali è possibile "estrarre" il maggior valore: ogni volta che un consumatore effettua un pagamento, disvela infatti abitudini di acquisto e preferenze, che costituiscono informazioni interessanti non soltanto per gli operatori finanziari, ma per qualsiasi impresa presente sul mercato di prodotti e servizi[29]. Ne consegue che debba essere specificato lo scopo preciso del trattamento dei dati, siano citate le basi giuridiche pertinenti, e siano rispettati i requisiti di sicurezza nonché i principi di necessità, proporzionalità, limitazione delle finalità e proporzionalità del periodo di conservazione dei dati. Inoltre, la protezione dei dati fin dalla progettazione ("*by design*") e la protezione dei dati di *default* dovrebbero essere integrate in tutti i sistemi di trattamento dei dati sviluppati e utilizzati nell'ambito delle attività coperte dalla direttiva (considerando 89).

Alcuni principi ulteriori, tra quelli che definiscono il perimetro di liceità delle operazioni di trattamento, sembrano particolarmente rilevanti per quanto concerne la prestazione di servizi finanziari per via telematica.

25 Joint Committee ESA (2016), p. 14 menziona l'utilizzo di dati bancari per valutare l'allocazione dei rischi a fini assicurativi.

26 Un cenno alla ambiguità del principio in European Commission, Summary of contributions to the "Public Consultation on FinTech: a more competitive and innovative European financial sector", p. 5.

27 Direttiva 2015/2366 del Parlamento europeo e del Consiglio del 25 novembre 2015 relativa ai servizi di pagamento nel mercato interno, che modifica le direttive 2002/65/CE, 2009/110/CE e 2013/36/UE e il Regolamento (UE) n. 1093/2010, e abroga la direttiva 2007/64/CE.

28 La Direttiva riconosce l'applicabilità della normativa rilevante in materia e, in particolare, della direttiva 95/46/CE, delle relative norme nazionali di attuazione (il rinvio deve oggi intendersi riferito al Regolamento 2016/679) e del Regolamento (CE) n. 45/2001 concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati (art. 94, comma 1).

29 EBA (2016), p. 4.

Sicurezza dei dati

Il GDPR include la sicurezza tra i principi generali che presiedono all'attività di trattamento dei dati (art. 5, comma 1, lett. f); riceve poi un inquadramento generale con la Direttiva sulla cybersicurezza (NIS); emerge infine, in maniera più specifica, nell'ambito delle direttive che regolano il mercato finanziario. Ad esempio, è posto dall'art. 16, comma 5, della MiFiD II, mentre l'art. 17 richiede esplicitamente per le imprese che svolgono "negoziazione algoritmica" di garantire che i sistemi siano testati e monitorati in maniera adeguata e che siano in grado di assicurare la regolarità e la continuità del servizio e una contrattazione ordinata. L'Art. 95 della PSD2, a sua volta, richiede ai prestatori di servizi di pagamento di mettere a punto un sistema di gestione dei rischi operativi e di sicurezza, nonché degli eventuali incidenti. Il tema, infine, è al centro del Piano d'azione sul FinTech promosso dalla Commissione europea, che lo indica tra quelli prioritari di intervento: gli allarmi sui cyber-attacchi minano, infatti, la fiducia dei consumatori, e rappresentano una minaccia per la stabilità del sistema finanziario. A questo riguardo è considerato essenziale un approccio integrato, che prevede l'adozione da parte dei fornitori di servizi digitali di un principio di "*security by design*" e la verifica tramite un meccanismo di certificazione all'interno di un quadro di disciplina uniforme[30], allo scopo sia di migliorare la qualità delle misure di sicurezza in generale sia di favorire le attività transfrontaliere soggette a requisiti e standard omogenei[31].

Oltre alle misure preventive rivolte a rafforzare la resilienza dei sistemi, il contrasto alle intrusioni illecite nei database delle imprese passa anche per la segnalazione tempestiva degli accessi non autorizzati. In particolare, in caso di violazioni dei dati personali sono previsti obblighi di notifica. Gli artt. 33 e 34 del GDPR prevedono, rispettivamente, l'onere di comunicare tali eventi tanto all'autorità nazionale di controllo quanto all'interessato. Tuttavia, lo stesso legislatore europeo si avvede del concreto rischio che un'applicazione eccessivamente scrupolosa della prescrizione metta ingiustificatamente in allarme i clienti ed esclude, pertanto, l'obbligo di notifica al Garante quando "*sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche*". Sono previste altresì esclusioni dell'obbligo di notifica agli interessati, che non devono essere allarmati qualora i dati «sotto attacco» siano cifrati e, dunque, incomprensibili a soggetti non autorizzati ad accedervi (art. 34, comma 3, lett. a); nel caso in cui il titolare del trattamento abbia adottato misure atte a scongiurare il sopraggiungere di un rischio elevato (lett. b), ovvero quando la comunicazione individuale richiederebbe sforzi sproporzionati (lett c). Il titolare del trattamento può chiedere ai garanti nazionali di filtrare la necessità di effettuare queste notifiche e di verificare la sussistenza delle condizioni per l'esenzione, sollevandosi così dal gravoso onere di valutare autonomamente l'importanza e la pericolosità della violazione.

30 Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act").

31 Commissione europea, *FinTech Action plan*, cit., p. 15 ss.

Per altro verso, la protezione elevata dei dati personali non può costituire impedimento o motivo di esonero dall'obbligo di condividere le informazioni sulle violazioni o gli accessi non autorizzati, poiché il GDPR individua come interesse legittimo tale da giustificare il trattamento dei dati, in misura necessaria e proporzionata, quello di garantire la sicurezza delle reti, dell'informazione e dei servizi offerti (considerando 49).

Il trattamento di dati automatizzato

La prestazione di servizi finanziari per via telematica comporta un frequente utilizzo di processi decisionali automatizzati. Nel P2P *lending*, ad esempio, possono essere automatizzate tramite algoritmi l'assegnazione del merito creditizio e la selezione e la scelta degli investimenti da parte di chi presta denaro. "Il rifiuto automatico di una domanda di credito online" è una delle esemplificazioni usata dal GDPR per illustrare la decisione basata su un processo automatizzato che produce effetti giuridici o incide significativamente sulla persona (considerando 71).

Questo tipo di trattamenti include altresì la "profilazione"[32], definita come "qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica" (art. 4, n. 4).

Il trattamento automatizzato di dati non è vietato ma presuppone l'adozione di cautele aggiuntive a tutela di coloro che vi sono sottoposti. Già disciplinato dall'art. 15 della Direttiva 95/46, è ora contemplato dall'art. 22 del GDPR, che riconosce alla persona a cui i dati si riferiscono il diritto "di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato". La natura di questa situazione attribuita all'interessato è di per sé ambigua: significa che questi ha una sorta di diritto di opposizione o di blocco, ma ha l'onere di attivarsi in tal senso, oppure che questa tipologia di trattamenti è vietata? Il comma 2 ammette inoltre tre eccezioni: la necessità per la conclusione o l'esecuzione di un contratto; una previsione legale (nazionale o europea); il consenso dell'interessato.

Una tutela rafforzata opera in ogni caso sul piano informativo: il Regolamento obbliga il titolare del trattamento a fornire all'interessato – al momento della raccolta – informazioni ulteriori rispetto a quelle previste per ogni tipo di trattamento sulla logica utilizzata, sull'importanza e sulle conseguenze previste (art. 13, comma 2, lett. f; art. 14, comma 2, lett. g). Quanto al diritto di accesso dell'interessato, esso include la conoscenza dell'esistenza del trattamento e, almeno nei casi in cui esso consista nella profilazione, anche la logica di funzionamento del processo e l'incidenza potenziale che avrà su di lui (art. 15, comma 1, lett. h). Rispetto

32 In generale, sul rapporto tra disciplina della privacy e profilazione del cliente nel contesto finanziario, v. Mattasoglio (2016).

all'informazione preventiva, che presenta necessariamente aspetti di genericità, questa seconda previsione, che è destinata al applicarsi al trattamento in corso, offre alla valutazione dell'interessato elementi specifici che lo riguardano, il cui impatto in concreto può essere più facilmente misurato.

Il quadro si completa con la norma di chiusura dell'art. 22, comma 4, che riconosce al soggetto sottoposto a una decisione sulla base di un processo interamente automatizzato, necessario per eseguire il contratto di cui è parte o da lui consentito, "il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione". La contestazione, in particolare, sembra poter riguardare la decisione finale, raggiunta a seguito della valutazione degli argomenti portati dall'interessato secondo quando esplicitato dal considerando 71.

Tutte queste previsioni, distribuite in disposizioni diverse di natura sia definitoria sia prescrittiva, sono dirette a rimediare alle condizioni di asimmetria informativa che, di regola presenti nel rapporto tra interessati e titolare del trattamenti, potrebbero aggravarsi in relazione a decisioni che i consumatori non sono in grado di influenzare ovvero neppure di comprendere proprio a causa del fatto che si basano su un processo di calcolo algoritmico, alimentato da una quantità importante di informazioni. L'uso, anche non esclusivo, di algoritmi incrementa infatti l'opacità dei processi di decisione; la disponibilità di grandi quantità di dati, sui quali l'analisi algoritmica si basa, e che provengono da fonti diverse incrementa il rischio che siano di bassa qualità, non accurati o non aggiornati e, dunque, incide negativamente sulle inferenze sviluppate; la stessa logica di funzionamento del processo può determinare che non siano considerate informazioni ulteriori, viceversa pertinenti.

Occorre tuttavia evidenziare che le garanzie previste dalla disciplina a contrastare i rischi intrinseci ai trattamenti automatizzati presentano qualche limite, che la dottrina ha puntualmente evidenziato: gli obblighi aggiuntivi di informazione, specialmente quelli preventivi, sono difficilmente attuabili oltre una soglia minima, a causa della complessità dei procedimenti di analisi, a maggior ragione se impiegano tecniche di *machine learning*[33], gli elementi sui quali dovrebbe cadere l'informazione possono essere coperti da diritti di proprietà intellettuale o costituire *trade secrets*[34], prima ancora, alcune garanzie, e segnatamente le informazioni sulla logica di funzionamento e sull'importanza delle conseguenze per l'interessato, sembrano applicarsi solo alle decisioni completamente automatizzate[35], cosicché un intervento umano, anche minimo, potrebbe valere a depotenziare l'effetto protettivo. L'ulteriore requisito della decisione automatizzata, ossia "che produca effetti giuridici" che

33 Financial Services User Group (FSUG), Assessment of current and future impact of Big Data in Financial Services, giugno 2016, p. 6 s.

34 "Il segreto industriale e aziendale e la proprietà intellettuale, segnatamente i diritti d'autore che tutelano il software" sono indicati nel Regolamento 216/679 quali possibili limiti all'accesso ai propri dati da parte dell'interessato (cfr. il considerando 63).

35 L'art. 22, comma 1, si riferisce infatti alla "decisione basata unicamente sul trattamento automatizzato, inclusa la profilazione" e solo a questo tipo di decisioni ("almeno in tali casi") si riferiscono gli obblighi di informazione previsti dagli artt. 13, 14 e 15, nonché la possibilità di contestazione di cui allo stesso art. 22, comma 3.

riguardano l'interessato "o che incida in modo analogo significativamente sulla sua persona" potrebbe, se inteso restrittivamente, escludere certe pratiche (ad esempio, la mera pubblicità personalizzata) dal proprio campo applicativo[36].

Il diritto alla portabilità dei dati

Particolarmente significativo per le attività del settore FinTech è il diritto alla portabilità dei dati riconosciuto e regolato dall'art. 20 GDPR. Questa disposizione tutela tanto l'interesse generale ad un mercato competitivo quanto quello particolare della persona fisica: da un lato, previene il rischio che si formino monopoli nella detenzione di informazioni utili alla prestazione di servizi finanziari, da un altro lato, garantisce all'individuo il diritto di scegliere il migliore fornitore di servizi e consente la migrazione da una piattaforma ad un'altra, contrastando il caratteristico effetto di *lock in*[37].

Nel dettaglio, l'interessato ha il diritto di ricevere i dati personali che lo riguardano dal titolare del trattamento al quale li abbia forniti e il diritto di trasmetterli ad un altro soggetto. Così potrà, ad esempio, trasferire la propria «carriera» di investitore dall'operatore tradizionale al quale si è rivolto nel corso degli anni ad un'impresa innovativa.

Il regolamento cerca di garantire l'effettività del diritto alla portabilità precisando che l'originario detentore dei dati non può opporre "*impedimenti*"; che deve rilasciarli "in un formato strutturato, di uso comune e leggibile da dispositivo automatico" (art. 20, comma 1); che deve trasmetterli in via diretta al nuovo titolare del trattamento se tecnicamente fattibile (art. 20, comma 2).

Il diritto alla portabilità non comprende qualsiasi dato personale comunicato a un soggetto terzo. È necessario, innanzitutto, che il trattamento sia effettuato con mezzi automatizzati (art. 20, comma 1, lett. b), ma nel settore FinTech la stragrande maggioranza (ove non la totalità) dei dati è acquisita e gestita automaticamente. Altrettanto frequente, nella materia di cui ci si occupa, è la ricorrenza della seconda condizione per la portabilità: il trattamento deve basarsi sul consenso o su un contratto (art. 20, comma 1, lett. a).

Un problema interpretativo e applicativo legato alla disposizione concerne l'esatta individuazione dei dati «portabili»: il riferimento testuale ai dati "*forniti*" all'originario titolare del trattamento dovrebbe limitarne il novero ai c.d. «dati grezzi» (*raw data*), escludendo la possibilità di trasferire «dati elaborati» dall'impresa (*managed data*) mediante un'organizzazione che aggiunga valore agli stessi. La questione è particolarmente interessante nel settore bancario: gli istituti bancari raffinano e migliorano, talvolta perché vi sono tenuti *ex lege* (ad esempio, in relazione alle disposizioni sull'antiriciclaggio o sui prestiti agevolati), la qualità dei dati. La portabilità di dati raffinati di questo tipo comporterebbe un ingiustificato

36 Discutono i problemi interpretativi generati da queste disposizioni e si esprimono in favore di una lettura non riduttiva delle garanzie per l'interessato Malgieri e Comandé (2017).

37 EBF (2016), p. 16. Sulla funzione proconcorrenziale anche Joint Committee ESA (2016), p. 15.

arricchimento (ovvero un esproprio di valore) a danno delle banche europee, magari a beneficio dei giganti della *internet economy*.[38]

Un prerequisito della portabilità dei dati è l'interoperabilità sulla base di standard (ad esempio per la formattazione), tale da consentire la lettura degli stessi *set* di dati da parte di diverse piattaforme o *provider* di servizi. Essa è importante, invero, non solo quale dispositivo di *empowerment* del consumatore, ma anche, specialmente rispetto ai dati non personali, per facilitare l'accesso di nuove imprese al mercato digitale, ferma restando la necessità di tutelare gli investimenti in innovazione già fatti dagli *incumbent*. Non a caso la definizione di processi di standardizzazione a livello regionale costituisce una delle misure, delineate dal Piano di azione della Commissione sul FinTech, dirette a consentire ai modelli di *business* innovativi di raggiungere una dimensione europea. [39] L'esigenza di un'armonizzazione degli standard di protezione dei dati personali emerge con forza nell'intersecarsi delle istanze alla base del diritto alla portabilità dei dati con le ragioni della concorrenza. Più nello specifico, analizzare il diritto alla portabilità dei dati nella prospettiva del diritto della concorrenza pone delle questioni di non agevole soluzione: se è vero che il diritto alla portabilità garantisce un maggiore dinamismo all'interno del mercato per il consumatore, evitando il cosiddetto effetto di *lock in*, per altro verso la libertà di trasferire i dati presso un'altra piattaforma può risultare pregiudizievole in termini di tutela dei dati personali. Il secondo operatore presso il quale i dati vengono trasferiti potrebbe infatti non garantire un adeguato livello di protezione della *privacy*. Poiché i dati rappresentano una *essential facility*, il diritto alla portabilità è virtuoso in termini di promozione della concorrenza, allorché riduce le barriere all'ingresso nel mercato: occorre tuttavia, per completare il circolo, un movimento complementare in termini di tutela della *privacy*[40]. In questo senso sembra muoversi la già citata strategia per un mercato unico digitale adottata dalla Commissione europea, che identifica nella standardizzazione una delle tematiche principali legate all'evoluzione delle nuove tecnologie: in particolare, nella Comunicazione del 19 aprile 2016 della Commissione al Parlamento europeo sulle Priorità per la normazione delle TIC per il mercato unico digitale, il settore della tecnologia dei *big data* è indicato tra i cinque prioritari in cui è necessario un intervento, proprio al fine di incrementare l'interoperabilità dei dati. Inoltre lo stesso GDPR rappresenta il primo passo verso una progressiva armonizzazione dei *data protection standards* e il diritto alla portabilità dei dati in esso contenuto un primo tentativo efficace finalizzato di incrementare il controllo dei consumatori sui propri dati personali.

2.2 *Big data analytics* nel settore finanziario e tutele giuridiche

Le potenzialità delle tecniche di analisi dei *big data* sono enormi e riguardano ambiti molteplici, dalla sanità all'agricoltura, dalla produzione industriale al settore dei trasporti, dalla tutela ambientale alla sicurezza e alla prevenzione dei

38 EBF (2016), p. 16.

39 Commissione europea, FinTech Action plan, cit., p. 7 s.

40 Weber R. H. (2016)

crimini[41]. Nel settore finanziario, gli scopi perseguiti attraverso queste tecniche sono legati principalmente alla ottimizzazione dei servizi offerti, nel senso di una migliore qualità per l'investitore e di una più efficiente gestione dei rischi da parte dell'impresa FinTech. A loro volta, questi sono raggiungibili, tipicamente, per mezzo di una micro-segmentazione in fasce di rischio e, dunque, di valutazioni più raffinate del merito creditizio o della adeguatezza di un investimento. Per proporre un'offerta sempre più sofisticata, le istituzioni finanziarie devono integrare nei processi di analisi e di decisione sia dati personali, spesso generati o ottenuti per scopi diversi, sia altri tipi di informazioni, come quelle relative all'andamento dei mercato finanziari, alle notizie economiche e politiche, al sistema dei prezzi[42], ai dati generati da sensori di cui sono dotati dispositivi intelligenti o che sono il prodotto di calcoli computazionali. Contro una certa rappresentazione negativa degli effetti sui consumatori dell'uso di *big data* da parte delle istituzioni finanziarie, si fa notare come ciò potrebbe anzi produrre benefici, per i singoli e per il sistema in generale, ad esempio in termini di servizi o prodotti personalizzati e ritagliati sulle esigenze individuali. Investimenti finanziari e gestione del portafoglio potrebbero essere orientati ai bisogni dei singoli sia al momento della scelta di un prodotto sia successivamente, monitorando le variazioni della situazione economico-finanziaria dell'investitore e le tendenze del mercato. Si fa l'esempio, nel settore assicurativo, del calcolo estremamente personalizzato delle polizze di vario tipo (sanitario, vita, viaggio, oltre che dell'assicurazione dei crediti), con la possibilità di ridurre il premio e abbattere i costi per titolari a basso rischio. Si stanno inoltre diffondendo le polizze *pay per use* la cui accuratezza e rispondenza al rischio può essere migliorata grazie a soluzioni telematiche che aggiornano le informazioni in tempo reale. In ambito bancario, la possibilità di determinare più precisamente il rischio creditizio può valere a garantire condizioni migliori a determinati creditori. Dal lato degli intermediari, queste stesse informazioni potrebbero servire ad identificare *patterns* anomali di comportamento del cliente e prevenire l'innescarsi di una spirale di sovraindebitamento.

La disponibilità di analisi dettagliate e di una segmentazione granulare delle informazioni potrebbe persino avere l'effetto di espandere il mercato, arrivando a includere nella prestazione di servizi consumatori che ne sarebbero stati altrimenti esclusi. La prevenzione delle frodi, legata alle capacità di individuazione tempestiva di comportamenti sospetti dei consumatori, è un altro dei vantaggi derivanti dall'analisi dei *big data* applicata al contesto finanziario.

Allo stesso tempo, l'uso dei *big data*, specialmente con finalità predittiva, può generare effetti sfavorevoli per gli utenti di servizi finanziari, anche in assenza di condizioni di monopolio, allorché individui interessati ad uno stesso prodotto oppure appartenenti a classi di rischio simili vengano trattati diversamente sulla base della

41 In termini generali e di alta divulgazione sul fenomeno dei Big Data e le sue possibili applicazioni, nonché su rischi e benefici, si veda Mayer-Schönberger e Cukier (2013). Inoltre, J. Manyika et al. (2011); World Economic Forum (2012); Federal Trade Commission (2016); Organisation for economic cooperation and development (OECD) (2014). Indaga il tema nel suo rapporto con la privacy il volume del Garante per la protezione dei dati personali (2017).

42 Joint Committee ESA (2016), p. 12.

disponibilità individuale, predetta attraverso queste analisi, a spendere di più o a cambiare operatore. La fedeltà ad un certo marchio, la scarsa propensione a rivolgersi a diversi prestatori di servizi o la capacità di pagare prezzi più alti possono così essere sfruttate a fini discriminatori[43]. Il c.d. *dynamic pricing* può in effetti ridondare a vantaggio dei consumatori, cui sono proposte offerte corrispondenti alla loro capacità economiche, ma anche, viceversa, dare luogo a effetti avversi, consentendo, ad esempio, alle imprese di erodere tutto il potenziale di spesa di individui o gruppi determinati. Più in generale, gli effetti positivi dell'innovazione digitale in termini di risparmio di costi possono essere rivolti ad ottimizzare i profitti e non ad abbattere i costi per i consumatori[44].

L'impiego di massicce quantità di dati, personali e non, per finalità descrittive, prognostiche o prescrittive non può essere dissociato dalla questione della protezione dei dati personali nel rapporto tra utente e impresa FinTech. In linea teorica, le pratiche dirette ad un uso abusivo delle informazioni granulari raccolte sui consumatori possono essere contrastate, anzitutto, sulla scorta dei principi che informano il quadro europeo sulla tutela dei dati e attraverso i rimedi specifici contro il trattamento illecito o scorretto di dati personali[45], ma anche ricorrendo alla disciplina più generale di tutela dei consumatori e, in particolare, a quella relativa alle pratiche commerciali scorrette.

Il modello basato sull'autodeterminazione e i suoi limiti

I complessi insiemi di informazioni, spesso di diversa natura, che sono la base per l'analisi algoritmica si compongono di dati personali; di dati in origine personali ma resi anonimi, e quindi non più soggetti alla disciplina sulla *privacy*; di dati non personali come ad esempio, tipicamente, *machine generated data*. La proporzione tra i diversi tipi di informazioni è difficile da stimare, anche perché essa dipende dalla mancanza di nozioni di partenza certe e, dunque, di confini netti tra gli elementi da delimitare[46].

Quando le tecniche di analisi coinvolgono dati personali, si dovrà senz'altro applicare la relativa disciplina. Essa prevede, tra i presupposti di liceità del trattamento, il consenso dell'interessato ovvero l'esecuzione di un contratto di cui questi è parte o, ancora, una previsione legale (art. 6, GDPR). Il consenso dell'interessato regge anche la comunicazione dei dati a terzi quale forma di

43 Joint Committee ESA (2016), p. 21 s. Anche la Risoluzione del Parlamento europeo *on FinTech*, cit., punto 28, segnala precisamente che l'uso crescente di dati della clientela e di big data può dapprima avvantaggiare i consumatori ma anche finire per nuocere all'obiettivo di un mercato competitivo. In termini più generali sui possibili effetti discriminatori delle tecniche algoritmiche di *data mining* e di *machine learning* cfr. Barocas e Selbst (2016).

44 Sottolinea in modo particolare i possibili danni per i consumatori il rapporto del Financial Services User Group, un organismo di carattere consultivo stabilito presso la Commissione europea: cfr. FSUG (2016); nonché ESA (2016), p. 17. In tema anche Di Porto (2017), p. 120 s.

45 Ma rilievi critici sulla adeguatezza del nuovo Regolamento UE 679/2016 rispetto alle prassi di trattamenti automatizzati e basati sull'analisi dei Big Data sono espresse da Mantelero (2017).

46 EPSC (2017), p. 2 e nt. 3.

trattamento dei dati, che può avvenire comunque solo se rientra nelle finalità per le quali i dati sono stati raccolti, oggetto di specifica informativa, oppure soddisfa una finalità compatibile con le prime (art. 6, co. 4).

Il modello che affida in via esclusiva il controllo sui propri dati al consenso dell'interessato è in verità oggetto di valutazioni controverse. Da tempo è stato evidenziato come sia puramente illusoria l'immagine di un individuo che, informato delle implicazioni della propria manifestazione di volontà al trattamento dei dati, la esprime consapevolmente magari selezionando tra le alternative possibili quelle che ritiene compatibili con i propri scopi. Per la mole di informazioni che sono fatte oggetto di comunicazione, per il tecnicismo e la complessità che le connota, per i *bias* cognitivi che affliggono il consumatore e, infine, per la frequente presenza di dispositivi di semplificazione della scelta (ad esempio, la spunta di una casella che equivale ad accettazione), è stato dimostrato come il consenso rappresenti uno strumento altamente inefficiente per una protezione dei dati e, soprattutto, per un reale *empowerment* dell'individuo a questo riguardo[47]. Se anche un ipotetico individuo, preoccupato della propria *privacy*, leggesse le lunghe, complicate e talvolta opache informative al riguardo, non avrebbe verosimilmente nessun potere di negoziare condizioni differenti.

Occorre altresì considerare che nel contesto dell'economia digitale le piattaforme operano spesso su un doppio versante, coinvolgendo i c.d. *two sided-markets*, ossia offrono servizi e prodotti, tendenzialmente gratuiti, e acquisiscono in cambio dati dai consumatori che poi serviranno per un *marketing* personalizzato, sostenendo in pratica la raccolta pubblicitaria delle medesime imprese. Questo è, tipicamente, il modello di *business* dei grandi motori di ricerca, dei *social networks* e delle piattaforme che ospitano le recensioni su operatori turistici, alberghieri o di altra natura[48]. Pratiche di questo tipo sono normalmente governate dal consenso dell'utente espresso attraverso l'adesione alle condizioni del servizio e confermano la sostanziale debolezza di tale strumento di controllo. Oltretutto il consumatore medio è spesso disponibile a condividere i propri dati in cambio dell'accesso gratuito ad un servizio o per ottenere un vantaggio in termini di riduzione della complessità delle possibilità che il mercato offre e, quindi, ad esempio per identificare più facilmente le opzioni più confacenti ai propri bisogni individuali.

Regolare a livello contrattuale il regime del trattamento dei dati è piuttosto comune; forme avanzate di trattamento e la condivisione delle informazioni con terzi rispondono, entro certi limiti, all'interesse del consumatore stesso poiché possono, come detto, semplificare gli scenari sempre più complessi dell'offerta di beni e di servizi. Allo scopo di facilitare un controllo reale, e non formalistico, del consumatore sulla selezione delle opzioni che preferisce in termini di *privacy* occorrerebbe,

47 Cfr. European Data Protection Supervisor (EDPS) (2014), p. 34 s. La letteratura al riguardo è molto vasta: basti qui richiamare Solove (2013). Con riguardo al nuovo Regolamento privacy ne discutono, tra gli altri, Koops (2015); Mantelero (2017), p. 148 ss., che invita ad abbandonare la "retorica della centralità del soggetto". Tra gli studi che attingono ad evidenze anche empiriche, si segnala di recente Gatt, Montanari e Caggiano (2017), p. 57 ss.

48 In tema Geslevich Packin e Lev-Aretz (2016); cenni anche in Vessia (2017), p. 85; Bellomo (2016), p. 2 ss. Con specifica attenzione al problema della privacy, si veda EDPS (2016a).

tuttavia, un affinamento delle clausole che prevedono la possibilità di trattamenti ulteriori rispetto a quello necessario per eseguire il contratto. Ciò dovrebbe avvenire attraverso una migliore specificazione degli scopi che giustificano la trasmissione dei dati dalla controparte contrattuale a terzi, nonché evitando di impostare modalità di acquisizione del consenso che incentivino automatismi nella manifestazione di volontà. A quest'ultimo riguardo, dispositivi presenti nello stesso nuovo Regolamento come il concetto di *privacy by default* (art. 25) possono neutralizzare le pratiche di acquisizione dei dati in assenza di una minima consapevolezza dell'utente.

Rilievi critici ha sollevato viceversa la strategia prescelta in sede di revisione della c.d. Direttiva e-*privacy*, che vede il consenso ancora come l'architettura centrale sulla quale i fornitori di servizi di comunicazione digitale dovrebbero basare la propria attività[49]. Il nuovo regolamento si applicherebbe non solo ai servizi di comunicazione tradizionale, ma anche ai servizi di messaggistica istantanea, alle telefonate tramite internet, al calendario elettronico, agli assistenti personali digitali, alle comunicazioni *machine to machine*; in quanto disciplina speciale, in questi ambiti sarebbe destinata a prevalere sul GDPR. La disposizione dell'art. 6, comma 3, lett. b) richiede un consenso esplicito di tutti gli utenti finali per il trattamento del contenuto delle comunicazioni elettroniche per uno o più fini specificati (diverse le condizioni per il trattamento dei c.d. metadati), e non ammette quindi che possa operare un altro dei requisiti di legittimità del trattamento tra quelli individuati dall'art. 6 del GDPR. Ciò sottoporrebbe gli utenti a continue richieste di consenso, un vero e proprio "*consent bombing*" che, oltre ad essere inutile o controproducente dal punto di vista dell'autodeterminazione dell'interessato, potrebbe anche causare l'abbandono del servizio[50].

La contrattualizzazione della privacy

L'intrinseca debolezza dello strumento del consenso, unita alla pluralità di giustificazioni alternative del trattamento che la disciplina continua a contemplare, inducono a rivolgersi anche a strumenti alternativi per assicurare un maggiore controllo sui propri dati. La concettualizzazione dei dati come oggetto di un diritto di proprietà individuale[51] o come possibile oggetto di scambio oneroso[52], secondo una ricostruzione dogmaticamente più solida, sono tra le proposte recenti che perseguono tale obiettivo. Esse avrebbero il vantaggio di rendere trasparente la dinamica degli scambi che attualmente si consumano nell'economia digitale, là dove l'accesso a svariati servizi avviene senza una controprestazione monetaria, ma consentendo al trattamento, inclusa la comunicazione a terzi, dei propri dati. Questa realtà per cui i dati finiscono per rappresentare una forma di pagamento è colta molto bene a livello

49 Cfr. la Proposta di Regolamento del Parlamento europeo e del Consiglio relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche e che abroga la direttiva 2002/758/CE (regolamento sulla vita privata e le comunicazioni elettroniche), COM(2017) 10 final, 10.1.2017.

50 Bolognini, Bistolfi e Crea (2018), p. 15 s.

51 Digital privacy rights require data ownership, Financial Times, 22.3.2018, 8.

52 Langhanke e Schmidt-Kessel (2015); Zech (2017); De Franceschi e Lehmann (2015); Purtova (2015).

politico e di analisi economica, al punto da avere originato alcune note metafore circa i dati come le nuove forme di ricchezza[53], ma era finora mancata una problematizzazione in chiave giuridica[54]. Allo stesso tempo, la consapevolezza del valore economico delle informazioni personali non è una percezione diffusa da parte del pubblico di utenti dei servizi digitali.

Una delle risposte avanzate dalla dottrina per garantire un controllo sui propri dati è quello di addivenire alla loro commercializzazione, che apre alla alternativa, sul piano tecnico-giuridico, tra due paradigmi: il primo costruisce i dati come *commodity*, sulla quale insiste un diritto di proprietà cedibile oppure, senza specificare la situazione vantata al riguardo dal disponente, li assume comunque come possibile oggetto di un contratto di scambio. Il secondo paradigma del "*services for data*" prospetta la creazione di una sorta di nuovo tipo contrattuale, in cui si scambiano informazioni personali per ottenere l'accesso a un servizio. Il primo paradigma presenta alcune debolezze, quali l'incompatibilità della ricostruzione in termini dominicali del diritto sui dati rispetto al quadro europeo e l'impossibilità pratica di trasmettere il potere di uso esclusivo della cosa come nella vendita: garantire l'accesso ai dati non esclude che lo stesso titolare o altri possano avervi ugualmente accesso o trarne utilità economica. Tuttavia, potrebbe trovare un termine di riferimento nei negozi di disposizione dei diritti della personalità[55]. La revocabilità del consenso (art. 7, comma 3, GDPR) potrebbe avere inoltre l'effetto di rendere strutturalmente precari gli accordi al riguardo e, dal punto di vista strutturale, opporsi alla configurazione dei medesimi come accordi traslativi. Il secondo modello varrebbe a fornire una base concettuale alla prassi attuale, con il vantaggio di esplicitare la dimensione dello scambio e renderne consapevole l'utente. Una volta concettualizzato l'accordo in questi termini, la disciplina dell'oggetto del contratto – in particolare, il requisito della determinatezza o determinabilità – richiederebbe una chiara delimitazione del perimetro dei dati trattati e delle finalità del trattamento, aggiungendosi alle previsioni in materia di tutela dei dati. L'interessato dovrebbe cioè essere messo in condizione di comprendere la portata esatta e l'incidenza sulla sua sfera dell'atto che compie, per ragioni che attengono strettamente alla validità, e dunque all'efficacia, dello stesso negozio dispositivo[56].

Questo inquadramento dovrebbe inoltre lasciare inoltre aperta agli utenti l'alternativa dell'accesso al servizio dietro prestazione monetaria[57]. La disponibilità a fornire informazioni su se stessi e sulle proprie abitudini di vita e di consumo non dovrebbe infatti costituire *a priori* motivo di esclusione del consumatore da certi

53 Quali quelle dei dati come "new currency", "new air" (cfr., ad esempio, <https://thefinanser.com/2017/11/data-new-currency.html/>) o "new oil" (https://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource). M v. già P. Schwartz (2004), p. 2056.

54 Cfr. il volume di Lohsse, Schulze e Staudenmayer (eds) (2017), che raccoglie gli Atti del III Convegno nella serie dei *Münster Colloquia on EU Law and the Digital Economy*.

55 In termini generali, cfr. Resta (2005); con riguardo al tema specifico del diritto sui dati v. Thobani (2016).

56 Sulla lettura in questa chiave della "specificità" del consenso al trattamento dei dati, cfr. Resta (2005), p. 284 ss.

57 Sulla relazione commerciale implicita che si instaura tra utenti e fornitori di servizi cfr. Autorità per le garanzie nelle comunicazioni (giugno 2018), Interim report nell'ambito dell'indagine conoscitiva di cui alla delibera n. 217/17/CONS.

settori di mercato[58]. Ciò richiede per l'appunto che a fronte del diniego alla raccolta, alla diffusione o alla conservazione di dati oltre il tempo necessario a garantire il servizio, il consumatore debba versare un corrispettivo per il medesimo, che sarebbe altrimenti gratuito[59].

Modelli di tutela oggettiva

La consapevolezza dei limiti in termini di tutela della persona e della scarsa efficienza allocativa degli (attuali) modelli basati sulla autodeterminazione inducono a rivolgersi a forme alternative di controllo, che innalzano il livello degli obblighi gravanti sui titolari del trattamento oppure propongono l'introduzione di schemi di aggregazione degli interessi quali quelli già esistenti nel diritto dei consumatori. Alla prima tipologia appartengono gli strumenti della valutazione d'impatto e della consultazione preventiva[60], diretti essenzialmente a ottimizzare la qualità dei trattamenti; mentre sembrano ancora funzionali a garantire un controllo più efficace dell'individuo sui propri dati i c.d. *Personal Information Management Systems* (PIMS), una sorta di console digitale personale dove archiviare le proprie informazioni, che restano suscettibili in ogni momento di verifica e di sfruttamento da parte dell'interessato[61].

La seconda categoria di meccanismi di controllo risponde invece alla rilevanza non più individuale ma collettiva della *privacy* e struttura di conseguenza i rimedi rispetto ai rischi di discriminazione che coinvolgono i gruppi più che i singoli individui. Sul modello di quanto già accade in altri settori come il diritto del lavoro e dei consumatori, prospetta analoghe forme di rappresentazione collettiva degli interessi che possano operare contro le pratiche commerciali scorrette e un ruolo accresciuto delle autorità indipendenti per la protezione dei dati[62].

Anonimizzazione e pseudonimizzazione

Un dispositivo che permette di trattare dati al di fuori della cornice della disciplina in materia di *privacy* è il processo di anonimizzazione di dati in origine personali. Esso rimuove la riferibilità del dato ad un individuo specifico e dunque esclude in radice l'applicabilità della relativa disciplina. La frequente rilevanza della natura personale del dato ai fini del suo trattamento limita tuttavia l'utilità del ricorso a tale approccio, di cui, peraltro, si contesta talvolta anche la reale efficacia[63].

58 FSUG (2016), p. 5 s., segnala come l'anomalia del profilo di un consumatore rispetto a dei modelli ovvero l'assenza di dati riguardo a uno specifico individuo possano implicare il diniego di accesso a certi servizi.

59 Sulla disponibilità degli utenti a pagare o, in alternativa, a cedere i propri dati come forma di corrispettivo per i servizi *online* cfr. Autorità garante della concorrenza e del mercato (giugno 2018), Indagine conoscitiva sui Big Data. Analisi della propensione degli utenti online a consentire l'uso dei propri dati a fronte dell'erogazione di servizi. Primi risultati.

60 Sui quali v. Mantelero (2017), p. 156 ss.; Mantelero (2012).

61 EDPS (2016b).

62 Mantelero (2016).

63 V., ad esempio, EDPS (2014), p. 9; in termini più generali, Ohm (2010).

Un'alternativa espressamente regolata dal GDPR è la pseudonimizzazione dei dati, operazione che rende impossibili attribuirli all'interessato "senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire" il ripristino della riferibilità ad un individuo specifico (art. 4, n. 5). Mentre la disciplina sul trattamento dei dati non si applica alle informazioni anonime, i dati pseudonimizzati non dovrebbero fuoriuscire dal suo raggio di operatività (considerando 21). L'operazione costituisce più semplicemente una misura di sicurezza, incentivata dallo stesso regolamento, ma che non elimina la necessità di adottare altri meccanismi di protezione (considerando 28 e 29).

2.3 Le altre iniziative sulla libera circolazione dei dati nel quadro europeo

Fermo restando quanto detto sulla rilevanza della normativa in materia di trattamento dei dati personali, le ulteriori questioni giuridiche oggetto di studio nel contesto delle azioni sul c.d. *free flow of data* sono essenzialmente legate all'appartenenza delle informazioni, all'accesso e alla responsabilità per danni in caso di cattiva qualità delle informazioni medesime.

L'analisi del quadro regolatorio porta a concludere nel senso che non vi è una disciplina comprensiva al riguardo e, in particolare, non sono chiaramente attribuibili diritti (di accesso e di uso) ai *set* di dati esistenti e, dunque, forme di protezione degli investimenti fatti nella raccolta e nella organizzazione dei dati. Le forme di regolazione più prossime, ciascuna con sue peculiarità, ma comunque non in grado di cogliere con precisione le caratteristiche specifiche del fenomeno, sono date dalla Direttiva sui database[64] e dalla Direttiva sui segreti commerciali[65]. La normativa sulla proprietà intellettuale è anch'essa esclusa dalla natura grezza dei dati e dalla mancanza di un risultato innovativo che possa essere protetto attraverso diritti di privativa.

Si è, dunque, spesso di fronte a una possesso di fatto e di esclusività nell'uso da parte di chi detiene i *cluster* di informazioni, solo in parte giustificata dal valore aggiunto impresso dalle attività di raccolta e di trattamento dei dati[66]. Questa situazione si rivela altamente inefficiente perché immobilizza una risorsa cruciale allo sviluppo dell'economia digitale; attribuisce un potere di fatto ai soggetti che ne sono detentori originari, ma che spesso non hanno le capacità tecniche per estrarne tutto il potenziale, ovvero hanno un interesse contrario alla propagazione dei dati; non permette l'incremento e l'adeguata remunerazione delle attività di aggregazione ed

64 Direttiva 96/9/CE del Parlamento europeo e del Consiglio, dell'11 marzo 1996, relativa alla tutela giuridica delle banche di dati.

65 Direttiva (UE) 2016/943 del Parlamento europeo e del Consiglio, dell'8 giugno 2016, sulla protezione del know-how riservato e delle informazioni commerciali riservate (segreti commerciali) contro l'acquisizione, l'utilizzo e la divulgazione illeciti.

66 Commission SWD on the free flow of data and emerging issues of the European data economy, cit., p. 22.

elaborazione di dati che avrebbero molteplici applicazioni pressoché in ogni settore economico, sociale e scientifico.

Da qui derivano sia l'esigenza di indagare le potenzialità del diritto *antitrust* in materia, come si farà nel paragrafo seguente, sia le azioni intraprese a livello europeo per rimediare, anche con interventi di tipo legislativo, alle lacune del sistema attuale. Tra gli obiettivi vi sono, in modo particolare, l'identificazione di forme di appartenenza e/o di accesso ai dati, non necessariamente alternative ai modelli tradizionali (ad esempio, con licenze obbligatorie), oppure il ricorso a modelli aperti; l'adeguata remunerazione di tutti i soggetti presenti nella catena del valore, che con il loro apporto contribuiscono a un affinamento dei dati migliorandone la qualità; la promozione della regolazione dell'accesso e del trasferimento dei dati su base contrattuale (attraverso contratti o clausole standard)[67].

In questo quadro si inserisce la proposta di Regolamento diretta a stabilire e facilitare la libera circolazione dei dati non personali all'interno dell'Unione[68]. Essa è complementare al GDPR perché attua lo stesso principio di libera circolazione dei dati, ma confina il proprio campo di applicazione alle informazioni di carattere non personale (art. 1). Avendo come obiettivo quello di promuovere la mobilità transfrontaliera dei dati, si articola secondo tre direttrici principali: anzitutto, l'eliminazione o la riduzione degli obblighi di localizzazione dei dati, che costituiscono, anche in base alle risultanze delle consultazioni con gli *stakeholders*, un fattore che condiziona pesantemente le strategie aziendali. Le imprese non possono scegliere i luoghi per l'archiviazione dei dati secondo criteri di economicità o fare pieno uso di servizi di cloud[69]; ciò genera costi e difficoltà a entrare in nuovi mercati o fornire servizi aggiuntivi. Per combattere il principale impedimento alla circolazione dei dati, la proposta ammette l'imposizione di obblighi di localizzazione esclusivamente per motivi di sicurezza pubblica (art. 4, comma 1), richiede la notificazione alla Commissione degli eventuali nuovi obblighi (comma 2) e la revisione di quelli esistenti in vista della loro eliminazione se non conformi alle nuove regole (comma 3). La seconda linea di intervento riguarda la messa a disposizione dei dati alle autorità competenti per controlli regolamentari o di vigilanza. Questa esigenza è spesso addotta per giustificare obblighi di localizzazione dei dati sul territorio nazionale e viene dunque contrastata garantendo l'accesso alle informazioni anche se localizzate in un altro Stato e istituendo all'uopo meccanismi di cooperazione tra Stati (art. 5). Il terzo pilastro della proposta è la rimozione degli ostacoli giuridici, tecnici e contrattuali alla portabilità dei dati, che gli utenti professionali sperimentano al termine di un contratto o quando prevedono di trasferirsi da un fornitore di servizi a un altro. La strategia regolatoria si avvale in questo caso di codici di condotta rivolti per definire buone pratiche del settore, ed essenzialmente a introdurre obblighi informativi in fase precontrattuale nell'ottica di una trasparenza delle condizioni osservate per il trasferimento di dati (art. 6).

67 In chiave di sintesi EPSC (2017), p. 10 s.

68 Proposta di Regolamento del Parlamento europeo e del Consiglio relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea, COM(2017) 495 final, 13.9.2017.

69 Sul problema dell'uso dei servizi cloud da parte delle istituzioni finanziarie v. anche EBA (2017).

3 I rischi per gli operatori FinTech: profili di concorrenza e *dynamic pricing*

3.1 Il possesso di data-set tra rischio di pratiche collusive e abuso di posizione dominante

Se il quadro normativo in materia di tutela della *privacy* risulta soddisfacente, nonostante alcune criticità che non si è mancato di evidenziare, altrettanto non si può dire in relazione al rapporto tra megadati e concorrenza nell'ambito della prestazione di servizi finanziari. Come già accennato, il problema si pone in relazione alla distribuzione del potere di mercato nell'ambito dei servizi relativi all'economia digitale, che tende a concentrarsi nelle mani di pochi operatori. Tale potere si sostanzia nel possesso di *data-set* che permettono alle imprese di guadagnare un vantaggio competitivo sulle concorrenti. La rilevanza del fenomeno è sottolineata dalle metafore impiegate in dottrina, quali "*data is one of the main raw materials of contemporary economics*"[70] o "*data is the oil of the information society*"[71].

Invero, la particolare natura dei dati implica l'esistenza di una molteplicità di mercati rilevanti. Su tutti, un mercato rilevante dei dati si avrà quando questi costituiscano il prodotto finale fornito da un'impresa: esso risulta segmentato in base alle varie fasi del processo di trattamento, che va dalla raccolta (*big data capture*) e dall'immagazzinamento (*big data storage*), fino all'analisi (*big data analytics*) e all'utilizzazione (*big data utilization*). Alcune imprese utilizzano i dati come semplice *input* della produzione, quindi essi rappresentano un bene necessario alla stessa prestazione del servizio: sebbene in tal caso non sia agevole individuare un mercato rilevante, è proprio in relazione a questa particolare situazione che si pongono i problemi più significativi in termini di concorrenza. Essi si articolano lungo due direttrici principali: da una parte la questione delle intese e delle pratiche collusive tra imprese operanti nel settore della *digital economy*, dall'altra l'abuso di posizione dominante sul mercato – legato al possesso di *data-set* – da parte di imprese che abbiano conquistato grandi quote di mercato.

Intese e pratiche collusive nel mercato dei big data

Sulla prima questione, assume rilevanza quello che è stato definito lo *snowball effect* nel mercato dei dati: il riferimento è al circolo vizioso che si crea nelle maglie dei rapporti tra gli utenti e le maggiori imprese detentrici di dati – *Facebook*, *Google*, etc. – per cui i primi cedono alle seconde i loro dati, e queste, in tal modo, sono in grado di fornire servizi gratuiti sempre più sofisticati e innovativi.

Un'altra caratteristica del tutto peculiare della *digital economy*, sostenuta dall'evidenza dei fatti, è legata alla circostanza che spesso le imprese coinvolte in intese appartengono a mercati diversi: il caso *Google/Android* è emblematico, poiché

70 Zeno-Zencovich V., Giannone Codiglione G. (2016), p. 30.

71 Weber R. (2016), p. 60

rappresenta un tentativo di rafforzamento sul rispettivo mercato da parte di due imprese che offrono servizi diversi, sebbene connessi[72]. Sul punto, è stato autorevolmente evidenziato[73] che lo stesso effetto dell'imposizione di regole di trasparenza nei mercati *online* può avere effetti non solo positivi, ma anche negativi: come già accennato, da una parte una maggiore trasparenza incrementa la consapevolezza del consumatore e gli permette di scegliere più agevolmente anche tramite una comparazione; la più libera circolazione di informazioni, tuttavia, può indurre un allineamento dei prezzi, la cui qualificazione come accordi collusivi risulta altamente problematica. Infatti, la pubblicità delle informazioni dalla quale potrebbe trarre origine la mancanza di alternative sul mercato di per sé non rappresenta un indice presuntivo di comportamenti anticoncorrenziali, che andrebbero dunque misurati sulla base di altri parametri. Tra le varie soluzioni prospettate per invertire la tendenza sui potenziali effetti anti concorrenziali causati da un incremento di trasparenza, emerge la proposta di "elaborare regolamenti di esenzione in relazione allo scambio di informazioni bancarie e finanziarie essenziali come *input* nella produzione di servizi nel campo FinTech"[74]. Inoltre la stessa pratica della personalizzazione del prezzo potrebbe rappresentare un rimedio all'allineamento collusivo dei prezzi, sebbene questa soluzione – come si dirà – ponga altri, e non meno significativi, problemi.

L'abuso di posizione dominante per possesso di data set: limiti e prospettive

La questione che desta maggiore preoccupazione e più anima la discussione in dottrina concerne i potenziali effetti restrittivi della concorrenza derivanti dal possesso e dall'uso di *data-set* e dal conseguente sfruttamento abusivo della posizione dominante così acquisita sul mercato. Invero, nel contesto della *digital economy* i dati rappresentano una risorsa chiave, un *input* essenziale allo sviluppo di servizi sempre più sofisticati, talvolta, la stessa infrastruttura fondamentale su cui si costruisce un'impresa. Non è chiaro, però, se sia applicabile la disciplina *antitrust* – e in particolare quella relativa alla figura dell'abuso di posizione dominante – nel caso in cui un'impresa, detentrice di un elaborato sistema di dati personali, raccolti e analizzati nello svolgimento della propria attività, ostacoli l'entrata sul mercato di altre concorrenti.

A tal proposito, sembra difficile che un'impresa che abbia costituito il proprio *know how* sulla base di tecniche di raccolta ed analisi di dati, sia disposta poi a condividerlo con le altre imprese concorrenti. Anzi, questo potrebbe avere rilevanti effetti negativi anche in termini di innovazione, scoraggiando l'investimento nel settore ricerca e sviluppo nell'ambito dei *big data*. Ammesso, dunque, che l'utilizzo

72 Nella fattispecie, è stata avviata un'indagine da parte della Commissione europea sulle due imprese, per il potenziale valore collusivo della impostazione predefinita della stringa di ricerca di *Google* in tutti i sistemi *Android* presenti sugli smartphone.

73 Report congiunto *dell'Autorité de la Concurrence* francese e della tedesca *Bundeskartellamt*, *Competition Law and Data*, 10 May, 2016, in www.autoritedelaconcurrence.fr/doc/reportcompetitionlawdatafinal.pdf.

74 Vessia F. (2017), p. 91.

esclusivo di tecnologie coinvolgenti i megadati da parte delle imprese titolari sia pienamente legittimo, solamente l'applicazione della *Essential Facility Doctrine* potrebbe rappresentare una soluzione finalizzata a rendere maggiormente accessibile la disponibilità di dati per le imprese che vogliano entrare nello stesso mercato della *digital economy*. In questo modo, tramite l'esclusività nell'uso di una risorsa insostituibile si impedirebbe l'accesso ad altre imprese: si configurerebbe in capo al titolare esclusivo del bene, quindi, un dovere di consentire l'accesso alla stessa risorsa.

L'*Essential Facility Doctrine*, sorta nell'ambito delle grandi infrastrutture non replicabili, è stata per la prima volta applicata in riferimento alla società dell'informazione nel caso Mangil TV Guide vs. ITP/BBC/RTE, per poi trovare spazio nel settore dei trasporti e dei *software*. Secondo questa impostazione, il titolare esclusivo dell'*input* deve consentirne l'accesso: 1) se il bene-*input* sia insostituibile, 2) se sia utilizzato dall'impresa concorrente per produrre un bene diverso da quello offerto dal titolare (operando quindi su un mercato diverso), 3) se il rifiuto alla fornitura del bene non sia giustificato e giustificabile. Soddisfatte queste tre condizioni, allora il rifiuto dell'impresa titolare esclusiva del bene può configurare gli estremi di un abuso di posizione dominante.

La domanda, dunque, è: i dati possono essere considerati *essential facility input*? Come notato da più parti, appare difficile non solo elaborare una regola generale tramite la quale ravvisare gli estremi di una posizione di dominanza (e dello sfruttamento abusivo di questa) da parte delle imprese nel mercato dei dati[75], ma, anche tramite una valutazione caso per caso, riscontrare i caratteri dell'essenzialità e della insostituibilità nella risorsa dei dati[76]. La causa di questo va ravvisata nella stessa natura dei dati, in particolare nella loro "ubiquità, non rivalità, facilità di acquisizione (per raccolta diretta o presso i terzi), dinamicità e velocità (di raccolta e aggiornamento come anche di obsolescenza e distruzione del valore dei dati set), non ultimo per effetto della portabilità dei dati personali esercitato dagli utenti"[77]. Dunque, l'estrema mobilità dei dati come risorsa si riflette anche nella struttura del mercato che li riguarda: in altre parole, le modalità di raccolta dei dati sembrano molteplici, così come le fonti a cui accedere. Inoltre spesso risulta assente anche la seconda condizione di operatività della *Essential Facility Doctrine*, perché *l'input* rappresentato dai dati potrebbe essere utilizzato dalle imprese concorrenti anche nell'offerta di beni o servizi dello stesso tipo.

Pertanto, i presupposti di applicazione della *Essential Facility Doctrine* risultano in linea generale assenti: appare estremamente difficile individuare nel rifiuto di fornire l'accesso ai dati da parte delle imprese titolari esclusive del bene i profili dell'abuso di posizione dominante (con le conseguenti sanzioni). Una diversa soluzione approfondisce il ruolo della figura dell'abuso di dipendenza economica *ex* art. 9 della legge 192 del 1998 nell'ambito del mercato dei *big data*. In particolare, la

75 Zeno Zencovich V., Giannone Codiglione G. (2016).

76 Esprime una posizione antitetica, pur sempre condividendo l'approccio caso per caso, Pitruzzella G. (2016).

77 Vessia F. (2017).

natura trans-tipica della fattispecie – affermata dalla Cassazione nella sentenza 24906 del 2011[78] – si presta ad essere adattata allo specifico contesto qui in esame: infatti, il potere di mercato acquisito grazie al possesso di *data-set* creerebbe un rapporto asimmetrico tra piccole e grandi imprese della *digital economy*, che potrebbe integrare quell'"eccessivo squilibrio di diritti e obblighi", caratterizzante la figura dell'abuso di dipendenza economica. In aggiunta, si sostiene che il *refusal to supply* potrebbe risultare abusivo, al di fuori delle strette maglie dell'abuso di posizione dominante e della *Essential Facility Doctrine*, dimostrando che non sia possibile "reperire sul mercato alternative soddisfacenti"[79].

Al di là dell'esigenza pratica di individuare una figura del diritto antitrust risolutiva della questione, occorre provare a cogliere il senso di un quadro di insieme nella prospettiva dei rapporti tra *privacy* e concorrenza. Esclusa la qualificazione, in generale, dei dati quale *input* essenziale, bisogna però rilevare che una situazione in cui le maggiori imprese detengono i dati dei consumatori possa risultare non ottimale per il benessere di questi ultimi[80]. Per questo, il diritto della concorrenza, nell'ambito del mercato dei *big data*, esprime le sue potenzialità solo se integrato in un sistema in cui il livello di *privacy* sia sufficiente: in altre parole "*the competitive relevance of data protection rules demands that companies that compete in the same market are subject to the same rules*"[81]. Infatti, il diritto antitrust appare intrinsecamente limitato nel perseguire obiettivi di tutela dei dati personali e della *privacy*: al di fuori dell'accertamento dell'esistenza di una posizione di dominanza nel mercato, di un'intesa o di una concentrazione, questo non può intervenire a reprimere un comportamento lesivo dei principi in materia di tutela dei dati personali. "*Il diritto antitrust non può essere applicato al di là dei propri confini*"[82]: invero, l'applicazione di strumenti posti a presidio della concorrenza non può essere finalizzata alla protezione dei dati personali dei consumatori o delle loro identità digitali, ma mira a contrastare i fenomeni di concentrazione del potere di mercato. Il giudizio antitrust, secondo la dottrina e la prassi prevalenti[83], non può essere basato sul parametro della violazione della *privacy,* poiché così si istituirebbe una sorta di automatismo per cui qualsiasi violazione in materia di tutela dei dati personali potrebbe essere considerata alla stregua di un abuso concorrenziale, riducendo così la plurioffensività delle condotte ad un elemento puramente formale[84]. La stessa Commissione Europea ha affermato la necessità di non confondere le questioni di concorrenza con quelle di *privacy*, dapprima nel caso Google/DoubleClick[85] e poi nel caso Facebook/Whatsapp,

78 Cass. Sez. Un., 25 novembre 2011, n. 24906, in NGCC, 2012, I, 298 ss.

79 Vessia F. (2017).

80 Maggiolino M. (2018). L'Autrice chiarisce questo punto, sostenendo che "pare corretto affermare che il diritto antitrust tuteli il benessere del consumatore, ma solo in via indiretta e mediata, ossia solo nella misura in cui una riduzione di tale benessere si sia prodotta (o si sarebbe potuta produrre) per effetto di una pratica imprenditoriale che ha modificato il funzionamento del mercato".

81 Pitruzzella G. (2016).

82 Maggiolino M. (2018).

83 Bisogna segnalare l'apertura delle Autorité de la Concurrence & Bundeskartellamt (2016) in materia, come rilevato nella nota 87.

84 IT Media Consulting in collaborazione con l'Univ. Bocconi (2018).

85 CE, 11 marzo 2008, Google/DoubleClick, COMP/M.4731, § 368.

ribadendo che "*any privacy-related concerns flowing from the increased concentration of data within the control of Facebook as a result of the transaction do not fall within the scope of the EU data protection rules*"[86]. Tuttavia, è possibile individuare dei profili di complementarietà tra diritto della *privacy* e diritto antitrust, riconoscendo che un adeguato livello di tutela dei dati personali possa essere virtuoso per il raggiungimento degli obiettivi del diritto antitrust[87].

In definitiva, si può affermare che gli strumenti offerti dal diritto antitrust, pur non essendo i più adatti per risolvere le problematiche inerenti il mercato dei *big data*[88], se integrati in un adeguato contesto di tutela della *privacy*, possono avere un ruolo determinante nel promuovere una concezione armonica tra le ragioni del mercato e le esigenze di protezione dei consumatori[89], soprattutto in un contesto complesso quale quello della finanza digitale. Un tale approccio sembra incontrare le sollecitazioni del Parlamento europeo alla Commissione nella già citata risoluzione del 17 maggio 2017, finalizzate all'individuazione nell'ambito del settore FinTech delle "*misure da adottare per creare un contesto che sostenga lo sviluppo di un tale sistema* [...] *e che interagisca con altre soluzioni di pagamento innovative nell'interesse della concorrenza*".

3.2 La problematica qualificazione illecita della discriminazione dei prezzi

L'altro fenomeno legato all'uso dei *big data* che coinvolge il diritto *antitrust* è quello della discriminazione dei prezzi e dell'offerta di prodotti a prezzi personalizzati. L'enorme sviluppo della tecnologia permette non soltanto di raccogliere e conservare una enorme quantità di dati, ma anche di processarli e analizzarli in modo automatico o semi automatico. Ciò permette di acquisire una conoscenza sulle modalità di comportamento delle persone (profilazione), utile a comprendere come promuovere un certo prodotto, a chi venderlo e a quale prezzo[90].

86 CE, 3 ottobre 2014, Facebook/Whatsapp, caso COMP/M.7217, § 164.

87 E' necessario precisare che in alcuni casi certamente la violazione antitrust può essere integrata da una condotta lesiva della tutela dei dati personali: così Autorité de la Concurrence & Bundeskartellamt (2016), 'Competition Law and Data', "*Privacy policies could be considered from a competition standpoint whenever these policies are liable to affect competition, notably when they are implemented by a dominant undertaking for which data serves as a main input of its products or services. In those cases, there may be a close link between the dominance of the company, its data collection processes and competition on the relevant markets, which could justify the consideration of privacy policies and regulations in competition proceedings*".

Cfr. Maggiolino M. (2018). L'Autrice nota che tramite l'adozione di questo approccio si intende procedere ad una valutazione caso per caso delle condotte plurioffensive, escludendo qualsiasi automatismo tra violazione della privacy e applicazione della disciplina sulle condotte anticompetitive.

88 Maggiolino M. (2018).

89 Pitruzzella G. (2016).

90 Il riferimento è alla cosiddetta behavioural discrimination. Ezrachi A., Stucke M.E. (2016) "A second risk involves behavioural discrimination, which differs from price discrimination in several important respects. The strategy involves firms harvesting our personal data to identify which emotion (or bias) will prompt us to buy a product, and what is the most we are willing to pay. Sellers, in tracking us and collecting data about us, can tailor their advertising and marketing to target us at critical moments with the right price and emotional pitch. So behavioural discrimination increases profits by increasing overall consumption (by shifting the demand curve to the right and price discriminating) and reducing consumer surplus".

La questione si colloca nel più ampio quadro dei rapporti tra *big data* e identità personale nella sfera digitale[91]: le interferenze e le predizioni derivanti dall'uso di tecniche di analisi di megadati[92] possono non solo compromettere il processo decisionale dell'individuo, ma anche restituire un ridisegno dell'identità digitale incompleto e frammentato, che solo in parte trova corrispondenza nell'identità reale[93].

Una premessa è però necessaria in ottica applicativa e in termini concorrenziali: bisogna evidenziare che le offerte personalizzate non comportano necessariamente solo effetti negativi. Mentre nella prospettiva del benessere individuale dei singoli consumatori, l'effetto concorrenziale negativo è legato al fatto che quelli disposti a pagare di più per ottenere un certo bene risultino svantaggiati rispetto a quelli disposti a pagare prezzi più bassi, dall'angolo visuale del benessere generale potrebbe rinversi un effetto positivo secondo la formula per cui la personalizzazione dei prezzi rende "*più poveri i più ricchi e meno poveri i meno ricchi*"[94].

Non esiste, quindi, la possibilità di considerare in maniera uniforme tale fenomeno: sebbene spesso i consumatori siano agevolati dai suggerimenti veicolati dalle piattaforme *online* in seguito ad un processo di profilazione, l'eventualità che le imprese siano a conoscenza della disponibilità a pagare dei singoli consumatori potrebbe apparire ingannevole nell'ottica del diritto della concorrenza, come si evidenzierà di seguito.

Il dynamic pricing *quale pratica commerciale scorretta: limiti e prospettive*

La qualificazione illecita di tale pratica per violazione del principio di parità di trattamento nell'ambito dei rapporti tra imprese e consumatori risulta problematica alla luce del diritto *antitrust*. Posto che la personalizzazione dei prezzi può essere messa in atto anche da coloro che non rivestono alcuna posizione dominante nel mercato, è controversa anche la sua qualificazione come pratica commerciale scorretta. Anzitutto, perché non sembra rientrare nelle ipotesi previste

91 Floridi L. (2014).

92 Si pensi ai processi di clusterizzazione attraverso i quali si possono formare attualmente le identità digitali: in tal caso l'attività di profilazione può avvenire estendendo agli individui profilati le proprietà degli altri individui che appartengono al medesimo cluster, cfr. Mantelero A. (2017).

93 Per un'ampia trattazione del tema dei rapporti tra Big Data e identità digitale, e sulla necessità di garantire agli utenti un controllo su quest'ultima, si rinvia a Richards N.M., King J. H. (2016) (2014). In ottica maggiormente applicativa World Economic Forum (2018), *Digital Identity. On the Threshold of a Digital Identity Revolution*. Cfr. Alpa G. (2017): "*le classificazioni dei dati e soprattutto la loro connessione ricostruisce una identità che in parte combacia con quella reale e in parte la deforma, la ingigantisce o la deprime*".

94 Maggiolino M. (2016). L'Autrice osserva (p. 137) che "i prezzi personalizzati permettano, anche quando praticati da un'impresa in posizione dominante, di soddisfare più consumatori di quelli che si sarebbero accontentati con prezzi uguali per tutti, riducendo il solo surplus di consumatori che vantano una maggiore disponibilità a pagare e un maggiore interesse per quei prodotti. A meno dunque di non eleggere il benessere di questi soggetti a bene giuridico degno di tutela e a meno di non voler pregiudicare l'efficiente allocazione dei prodotti, il diritto antitrust non dovrebbe perseguire i prezzi personalizzati, seppur offerti da un'impresa in posizione dominante".

dagli articoli 23 e 26 cod. cons. (pratiche considerate in ogni caso ingannevoli o aggressive), né tanto meno tra le pratiche aggressive di cui agli art. 24 e 25 cod. cons. In seconda istanza perché, pur risultando il *dynamic pricing* una pratica opaca e sospetta agli occhi dei consumatori – i quali, culturalmente, percepiscono la parità dei prezzi come un valore – non esiste alcun obbligo per le imprese di praticare condizioni paritarie ai consumatori con cui contraggono, quindi la personalizzazione dei prezzi non sarebbe una pratica commerciale scorretta neanche per violazione del principio di parità di trattamento. Emblematiche dell'assenza di un generale obbligo di parità di trattamento nell'ambito dei rapporti contrattuali sono l'imposizione dell'obbligo a contrarre in condizioni di parità solo al monopolista legale *ex* artt. 2597 e 1679 c.c. e la stessa disciplina delle clausole abusive nei contratti dei consumatori *ex* art. 34 cod. cons., che esclude la abusività di una clausola solo sulla base della congruità dei prezzi.

Resta, infine, da valutare, se la pratica in esame possa essere considerata un'omissione ingannevole ai sensi dell'art. 22 cod. cons. o, comunque, un indebito condizionamento *ex* art. 20, comma 2 cod. cons.[95]. La riflessione sul punto è estremamente rilevante, perché permette di dar conto ancora una volta dello stretto legame funzionale tra *privacy* e concorrenza. Certamente la discriminazione dei prezzi può essere considerata nell'ottica della carenza di trasparenza e correttezza: questo non tanto perché, nell'attuare un'omissione ingannevole o un indebito condizionamento, l'impresa ha ridotto al minimo la convenienza dell'offerta per il consumatore, quanto perché il consumatore è stato profilato e gli è stata sottoposta un'offerta personalizzata a sua insaputa[96]. Il sospetto che riguarda le pratiche di *dynamic pricing* sembra fondarsi insomma non tanto nell'eventuale valutazione negativa da parte del consumatore circa la convenienza dell'acquisto derivante da un'offerta personalizzata – convenienza che peraltro non sarebbe garantita nemmeno al di fuori del mercato digitale – quanto nel "*senso di disagio che potrebbe nascere dal sapere di essere stati classificati, eventualmente anche sulla scorta dell'elaborazione dei propri dati personali, allo scopo di ricevere un'offerta commerciale*"[97]. La diffidenza che circonda le pratiche di *dynamic pricing* attiene quindi più che al *quantum* del prezzo personalizzato, al processo automatizzato che ha portato alla sua elaborazione. Se è così, le esigenze dei consumatori sarebbero probabilmente meglio soddisfatte dalla disciplina a tutela della *privacy*, rispetto a quella sulle pratiche commerciali scorrette. A tal proposito, l'art. 22 del GDRP sembra fornire una prima soluzione, nella parte in cui stabilisce che "*l'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona*" salvo che "*la decisione* [...] *c) si basi sul consenso esplicito dell'interessato*". Infatti, la pratica di prezzi personalizzati dovrebbe così essere sottoposta al consenso preventivo, libero ed espresso dei

95 Di questo avviso Vessia F. (2016), p. 102. *Contra* Maggiolino M. (2016), p. 130.

96 Maggiolino M. (2016).

97 Ibidem.

consumatori alla profilazione, tramite la quale ottenere offerte ritagliate su indagini basate sul loro comportamento di consumo[98].

Per concludere, anche con riguardo alla pratica del *dynamic pricing* trovano spazio le considerazioni svolte sui rapporti tra *privacy* e concorrenza nel più ampio contesto della *digital economy*: un tale approccio integrato risulta utilmente applicabile anche allo specifico settore FinTech, che, con velocità sorprendente, si è esteso dalla digitalizzazione dei servizi di pagamento e di quelli bancari, a quella delle negoziazioni finanziarie, della consulenza e delle assicurazioni.

Nel comprendere le implicazioni derivanti dal fenomeno della finanza digitale, ecco che le categorie giuridiche già esistenti, come gli istituti del diritto *antitrust* e della tutela dei dati personali possono rappresentare valide coordinate di inquadramento.

98 Della stessa opinione anche Miller A.A. (2014), p.104: "More generally, redressing the problems of unfair and deceptive pricing requires that consumers become better informed. This can be achieved if government and the media insist that retailers and data brokers come clean about their pricing practices".

4 Sintesi dell'indagine e prospettive

Da una visione d'insieme delle principali questioni trattate in ottica civilistica emergono le seguenti considerazioni di sintesi e alcune indicazioni prospettiche:

1. Positiva valutazione del sistema delineato dal GDPR, che coniuga la protezione dei dati con condizioni più favorevoli per la loro circolazione, al fine di creare un *clima di fiducia* necessario allo sviluppo del mercato digitale.

2. Necessità di adottare un sistema armonizzato di *data protection standards*, in grado di rendere effettivo l'impatto positivo del diritto alla portabilità dei dati, nella sua duplice accezione di strumento utile allo sviluppo di un mercato concorrenziale e indispensabile al consumatore per evitare l'effetto *lock in*.

3. Necessità di approfondire il paradigma del *service for data* e, più in generale, lo scambio dei dati attraverso il contratto in alternativa al mero strumento del consenso, che non riesce a garantire al consumatore un controllo efficiente sui propri dati.

4. Avvio di una riflessione sul rapporto tra figure di illecito *antitrust* e sfruttamento del potere di controllo sui dati da parte delle imprese attive sul mercato dei *big data*. Considerare la figura dell'abuso di dipendenza economica come prospettiva di inquadramento.

5. Studiare il fenomeno del *dynamic pricing* alla luce della disciplina sulle pratiche commerciali scorrette e in coordinamento con la disciplina in materia di *privacy*, in particolare al fine di rendere edotto il consumatore della natura personalizzata del prezzo dell'offerta a lui rivolta nell'ambito delle piattaforme *online*.

6. Avviare una riflessione articolata sulla questione dell'identità digitale[99], la quale si pone sullo sfondo rispetto alle problematiche affrontate. In particolare, occorre tematizzare il concetto di "identità commerciale virtuale"[100], quale *transaction identity* di un soggetto in relazione alla sua più ampia *digital person*[101].

99 Per un'ampia trattazione sui rischi derivanti dal ridisegno dell'identità personale nel contesto dello spazio virtuale, cfr. Floridi L. (2014).

100 Alpa G. (2017).

101 Ibidem, p. 725: "Le carte di debito e di credito, le carte del bancomat, le carte di ingresso alle palestre, ai teatri, i biglietti aerei e ferroviari, le prenotazioni delle auto pubbliche e private, le iscrizioni alla scuola, all'università, a corsi liberi, di lingue, di ricreazione, le affiliazioni a movimenti, partiti, associazioni di ogni tipo, le tessere sanitarie, annonarie, professionali, e poi gli acquisti mediante internet, la partecipazione ai giochi, gli abbonamenti a riviste, a cineteche, alle televisioni, le iscrizioni a Facebook, Instagram, E-bay, PayPal, Catawiki, e cosı` via costituiscono un mondo di informazioni digitali in cui le classificazioni dei dati e soprattutto la loro connessione ricostruisce una identità che in parte combacia con quella reale e in parte la deforma, la ingigantisce o la deprime, a seconda degli angoli visuali o dei frammenti di specchi – per riprendere la metafora iniziale – in cui la persona è stata scomposta".

Rischi per la clientela
Tutela dei dati e *privacy*
Art. 5 GDPR: Principi applicabili al trattamento dei dati. *1. I dati personali sono:* *a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);* *b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità [...] («limitazione della finalità»);* *c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);* *d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);* *e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono [...] («limitazione della conservazione»);* *f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).* *2.Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («responsabilizzazione»).*
Sottoposizione a processo decisionale automatizzato, compresa la profilazione
Art. 22 GDPR: Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione *1.L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.* *2.Il paragrafo 1 non si applica nel caso in cui la decisione:* *a) sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento;* *b) sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato;* *c) si basi sul consenso esplicito dell'interessato.*
Effetto *lock in*
Art. 20 GDPR: Diritto alla portabilità dei dati *1.L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti qualora:* *a) il trattamento si basi sul consenso ai sensi dell'articolo 6, paragrafo 1, lettera a), o dell'articolo 9, paragrafo 2, lettera a), o su un contratto ai sensi dell'articolo 6, paragrafo 1, lettera b); e* *b) il trattamento sia effettuato con mezzi automatizzati.* *2.Nell'esercitare i propri diritti relativamente alla portabilità dei dati a norma del paragrafo 1, l'interessato ha il diritto di ottenere la trasmissione diretta dei dati personali da un titolare del trattamento all'altro, se tecnicamente fattibile.*

Rischi per gli operatori
Intese e pratiche collusive Art. 101 TFUE *1. Sono incompatibili con il mercato interno e vietati tutti gli accordi tra imprese, tutte le decisioni di associazioni di imprese e tutte le pratiche concordate che possano pregiudicare il commercio tra Stati membri e che abbiano per oggetto o per effetto di impedire, restringere o falsare il gioco della concorrenza all'interno del mercato interno ed in particolare quelli consistenti nel:* *a) fissare direttamente o indirettamente i prezzi d'acquisto o di vendita ovvero altre condizioni di transazione;* *b) limitare o controllare la produzione, gli sbocchi, lo sviluppo tecnico o gli investimenti;* *c) ripartire i mercati o le fonti di approvvigionamento [...]*
Sfruttamento abusivo di posizione dominate – sfruttamento abusivo di dipendenza economica Art. 102 TFUE *È incompatibile con il mercato interno e vietato, nella misura in cui possa essere pregiudizievole al commercio tra Stati membri, lo sfruttamento abusivo da parte di una o più imprese di una posizione dominante sul mercato interno o su una parte sostanziale di questo.* *Tali pratiche abusive possono consistere in particolare:* *a) nell'imporre direttamente od indirettamente prezzi d'acquisto, di vendita od altre condizioni di transazione non eque;* *b) nel limitare la produzione, gli sbocchi o lo sviluppo tecnico, a danno dei consumatori [...].* Art. 9, l. 192/1998: Abuso di dipendenza economica *1. È vietato l'abuso da parte di una o più imprese dello stato di dipendenza economica nel quale si trova, nei suoi o nei loro riguardi, una impresa cliente o fornitrice. Si considera dipendenza economica la situazione in cui una 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.* *2. 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.*
Concentrazioni tra imprese Art. 2 Regolamento 139/2004/CE, Valutazione delle concentrazioni *1. Le concentrazioni di cui al presente regolamento sono valutate conformemente agli obiettivi del presente regolamento e alle seguenti disposizioni per stabilire se siano compatibili o meno con il mercato comune.* *In tale valutazione la Commissione tiene conto:* *a) della necessità di preservare e sviluppare una concorrenza effettiva nel mercato comune alla luce, segnatamente, della struttura di tutti i mercati interessati e della concorrenza effettiva o potenziale di imprese situate all'interno o esterno della Comunità;* *b) della posizione sul mercato delle imprese partecipanti, del loro potere economico e finanziario, delle possibilità di scelta dei fornitori e degli utilizzatori, del loro accesso alle fonti di approvvigionamento o agli sbocchi, dell'esistenza di diritto o di fatto di ostacoli all'entrata, dell'andamento dell'offerta e della domanda dei prodotti e dei servizi in questione, degli interessi dei consumatori intermedi e finali nonché dell'evoluzione del progresso tecnico ed economico purché essa sia a vantaggio del consumatore e non costituisca impedimento alla concorrenza.* *2. [...]* *3. Le concentrazioni che ostacolino in modo significativo una concorrenza effettiva nel mercato comune o in una parte sostanziale di esso, in particolare a causa della creazione o del rafforzamento di una posizione dominante, sono dichiarate incompatibili con il mercato comune.*
Discriminazione dei prezzi Ostacoli ad una configurazione quale pratica commerciale scorretta *ex* artt. 23 ss. codice del consumo. Rilevanza del processo automatizzato di profilazione sul quale si basa eventuale discriminazione del prezzo, quindi applicabilità art. 22 GDPR.

Sezione II

Enforcement e regimi sanzionatori tra rischi per la clientela e vincoli per gli operatori: i profili penalistici dell'analisi

G. Morgante, N. Amore, G. di Vetta, G. Fiorinelli, M. Galli

Chiarita la molteplicità di profili civilistici legati al fenomeno FinTech, occorre ora soffermarsi sugli strumenti di *enforcement* e sui regimi sanzionatori amministrativo-penali. I temi che verranno qui trattati attengono, segnatamente, alla tutela dell'identità digitale e alla definizione degli strumenti penali di prevenzione e repressione del suo indebito utilizzo, tra tutela della *privacy* e *cybersecurity*, nonché, sul versante degli operatori, ai rischi di infiltrazioni criminali nelle piattaforme *on line* a scopo di riciclaggio e finanziamento del terrorismo (anche internazionale) e ai profili sanzionatori dell'abusivo esercizio di attività finanziarie su piattaforme digitali.

5 La tutela della clientela e i rischi operativi del FinTech: tra *privacy* e *cybersecurity*

Come si è sottolineato in apertura del presente *Volume*, il progressivo sviluppo delle attività di finanza tecnologica ha comportato la singolare convergenza di due distinti profili di rischio per la clientela: accanto, infatti, ai rischi di natura *finanziaria* cui tali attività sono per natura connesse, la prestazione di servizi mediante strumenti tecnologici introduce inedite istanze di tutela, emergenti direttamente dalla natura *digitale* ed *informatica* dell'attività: ciò non soltanto a causa della 'smaterializzazione' delle relazioni tra clientela ed operatori, ma anche – e soprattutto – in conseguenza dell'assoluta rilevanza ora assunta dalla necessità di tutela dei dati.

I dati posseduti o inseriti dalla clientela meritano, infatti, particolare tutela, non soltanto nei confronti dei terzi, ma anche nei confronti dei gestori delle piattaforme *online*, che potrebbero vantare propri diritti di proprietà – finanche intellettuale – su realtà digitali frutto dell'espressione identitaria dell'utente.

Peraltro, se, da un lato, occorre forse riferirsi ai dati personali non già come "dati identificativi" (e cioè che aiutano a identificare), bensì come "dati identitari" perché espressivi dell'identità personale che si è scelto di costruirsi, in linea con il

concetto di *identity information* coniato dalla tradizione di *common law*, dall'altro, anche ai fini dell'identificazione degli strumenti sanzionatori connessi allo sviluppo del FinTech, deve altresì prendersi atto della progressiva patrimonializzazione o "proprietarizzazione" dei dati personali del soggetto che si registra in una piattaforma di *lending* o *crowdfunding*, con conseguente sempre maggiore interesse commerciale all'acquisizione di quei dati, al punto da spingere la dottrina a parlare di "oro digitale".

Si tratta del "costo della gratuità" dei servizi su Internet, e non solo su Internet se pensiamo a un recente esperimento di *business model* in Danimarca, in cui in un negozio la metà dei beni sono gratuiti a patto che ci si registri con i propri dati e si indichino i propri gusti e interessi[102]. La complessità del concetto di identità digitale oggetto di considerazione nei contesti FinTech rispetto a quello tradizionale di identità personale si apprezza nel frazionamento delle diverse componenti del c.d. "patrimonio umano digitale" in *a)* chiave d'accesso ad un patrimonio materiale (*bancomat*, carte di credito, password per l'accesso a conti *on line*), *b)* strumenti per un guadagno commerciale (corrispondente al valore economico dei dati personali in sé), *c)* domicilio virtuale, *d)* estrinsecazione della proprietà intellettuale: una proiezione complessa, economicamente più appetibile e più facilmente riproducibile dell'identità personale. Ne deriva che né il delitto contro la persona tradizionalmente intesa (nella sua identità e riservatezza), né quello contro il patrimonio (che peraltro già subisce, per opera delle nuove tecnologie, la *disruption* rispetto allo storico dualismo della condotta violenta/fraudolenta), né quello lesivo di beni sovraindividuali (fede pubblica, amministrazione della giustizia) riescono a fotografare fedelmente il fenomeno in esame.

5.1 La tutela penale dei dati e dell'identità digitale nello spettro della legislazione in materia di *privacy*

Tra le principali sfide per il diritto penale nell'era del FinTech si ritrova, dunque, l'esigenza di fornire una tutela rafforzata ai dati e all'identità digitale degli utenti[103]. Anzitutto, la questione può e deve essere inquadrata – come già con riferimento ai profili civilistici – richiamando la disciplina relativa alla tutela della *privacy*. Essa, infatti, rappresenta ormai un diritto fondamentale dell'individuo[104], incontestabilmente riconosciuto sia dalle fonti nazionali[105] che sovranazionali[106].

102 Cfr. l'articolo pubblicato su repubblica.it, a firma di C. Accogli, *In Danimarca c'è un negozio dove si compra senza pagare* (accessibile al link https://www.repubblica.it/tecnologia/2014/09/03/news/freemarket_in_danimarca_compri_gratis_in_cambio_di_pubblicit-94917875/): si fa riferimento a "Freemarket", il negozio aperto a Copenhagen nell'agosto del 2013, che vende prodotti alimentari ai clienti in cambio di pubblicità sui social network. In particolare, si prevede che il cliente, per poter usufruire del servizio, debba registrarsi al sito web, fornendo una serie di dati personali nonché acconsentendo a pubblicare sui social network foto e giudizi dei prodotti 'acquistati' gratuitamente.

103 Sul tema cfr. C. Crescioli (2018), 266, ove si sottolinea come il furto di identità digitale sia un fenomeno criminoso allarmante, e solitamente prodromico alla commissione di ulteriori illeciti.

104 Per un'analisi dell'evoluzione storica di questa situazione giuridico-soggettiva, v. ex multis S. Niger (2006).

105 La base giuridica è individuata solitamente nell'art. 2 Cost. (cfr. Cass. civ., Sez. III, n. 5658 del 1998; in dottrina v. S. Niger (2006), 43; P. Troncone (2011); T. Vitarelli (1999); v. anche G. Finocchiaro (2010); P. Zatti (1981)) oppure nell'art. 21 Cost (A. Cerri (1995)).

Tradizionalmente inteso come *right to be let alone*, a veder preservati gli aspetti intimi della propria esistenza da ingerenze di vario tipo (c.d. diritto alla riservatezza[107]), a seguito dello sviluppo tecnologico e dei sistemi informatici dei quali il FinTech stesso è figlio, se ne è affermata una diversa accezione, come diritto a poter decidere autonomamente i limiti e le modalità con le quali possono essere diffuse le informazioni private, a tutela della propria dignità personale[108].

Anche con riguardo ai profili penalistici della questione occorre, dunque, far riferimento al Regolamento Europeo n. 679/2016, c.d. *GDPR,* e al c.d. *codice della privacy* (d. lgs. n. 196 del 2003) – per come modificato con il d. lgs. di adeguamento al *GDPR*, n. 101/2018[109] – *sedes materiae* delle disposizioni sanzionatorie amministrative e penali.

Tra queste ultime, spicca in particolare l'art. 167, norma a più fattispecie già prevista dalla l. n. 675 del 1996 (art. 35) e dalla previgente versione del d. lgs. 196/2003, incaricata di proteggere la *privacy* della persona attraverso la repressione del c.d «trattamento illecito dei dati»[110].

I suoi due commi si aprono con la clausola di sussidiarietà «salvo che il fatto costituisca più grave reato»[111], e puniscono **i trattamenti di dati personali compiuti in violazione delle norme** espressamente richiamate, quando sono sorretti dal dolo specifico di conseguire un **profitto** per sé o per altri o, altresì, di recare un **danno** a terzi. Per queste condotte è prevista la detenzione se si «arreca nocumento all'interessato» (da 6 a 18 mesi per le violazioni enunciate al comma 1, da 1 a tre anni per quelle enunciate al comma 2). Il soggetto attivo dell'art. 167 è «chiunque». Nondimeno, come osservato da attenta dottrina[112], talune delle violazioni ivi indicate possono essere commesse solo dai destinatari degli obblighi individuati dalla legge, con la conseguenza che in quelle ipotesi il reato dovrà essere considerato proprio[113].

La condotta tipica è descritta mediante la discutibile tecnica del rinvio formale ad altre disposizioni del codice della *privacy*[114], ed è perciò a esse che si deve

106 Artt. 8 CEDU, 8, par. 1 Car. Nizza, 15, par. 1 TFUE.

107 Si richiama sovente la definizione data da una risalente pronuncia della Corte di legittimità, quale interesse «alla tutela di quelle situazioni personali e familiari svoltesi anche al di fuori del domicilio domestico che non hanno per i terzi un interesse socialmente apprezzabile, contro le ingerenze non giustificate da interessi pubblici prevalenti, anche se lecite e tali da non offendere l'onore e il decoro» (cfr. Cass., n. 2129 del 1975).

108 S. Rodotà (1991); S. Rodotà (2004).

109 A riguardo si rinvia per tutti a M. Lamanuzzi (2017); F. Pizzetti (2016).

110 La rubrica è rimasta la stessa, ma tra il 1995 e il 2003 il precetto è stato modificato a fondo, trasformandone la tipologia (da reato di pericolo astratto a reato di danno, v. *Infra*) e ampliandone l'ambito applicativo (il quale, come sottolineato dalla Relazione parlamentare di accompagnamento al d. lgs. 196 del 2003, ricomprende anche le condotte punite antecedentemente, ai sensi dell'abrogato art. 35 D.L. 171 del 1998). Sul punto si veda tra i tanti A. Manna (2003); P. Troncone (2011); P. Zangoni (1982).

111 Si pensi, ad esempio, al delitto di abuso d'ufficio (art. 323 c.p.), laddove chi agisce rivesta anche la qualifica di pubblico ufficiale o incaricato di pubblico servizio (art. 357 e 358 c.p.).

112 A. Manna (2005), 260.

113 Si pensi ad esempio alla violazione dei principi relativi al trattamento di dati giudiziari (art. 21), la quale può essere commessa solo da soggetti pubblici.

114 Si tratta di un chiaro esempio delle tanto vituperate «clausole sanzionatorie finali», che hanno contribuito grandemente a pregiudicare la determinatezza della tutela penale e, in definitiva, «la sua essenziale capacità di

guardare per desumerne i connotati obiettivi. Per quanto qui interessa, l'analisi si può limitare al co. 1, ove si rinvia alla «violazione di quanto disposto dagli articoli 123, 126 e 130 o dal provvedimento di cui all'articolo 129»: si fa riferimento, rispettivamente, alla violazione della disciplina in materia di trattamento dei dati relativi al traffico e all'ubicazione, nonché all'invio di comunicazioni indesiderate e all'inserimento degli utenti nei c.d. elenchi dei contraenti, ai fini delle comunicazioni pubblicitarie[115]. Rilevante è altresì la condotta tipica di cui al co. 3, consistente nel trasferimento dei dati personali verso un paese terzo o un'organizzazione internazionale, al di fuori dei casi consentiti ai sensi degli articoli 45, 46 o 49 del Regolamento. Si tratta con tutta evidenza di disposizioni rilevanti per gli operatori del settore FinTech, data la potenziale natura commerciale dell'attività svolta, nonché la dimensione transnazionale delle comunicazioni e delle operazioni.

È necessario osservare, peraltro, che la norma predispone una fitta rete di meccanismi selettivi, tesi a evitare che la sanzione penale possa essere irrogata in riferimento ad azioni di mera manomissione formale della signoria sul dato personale. Nello specifico, l'art. 167 cod. *privacy* richiede anzitutto l'accertamento di un dolo specifico, consistente nel fine di trarre per sé o per altri profitto o per recare un danno all'interessato[116]. La Cassazione – con riferimento al testo previgente della disposizione – non si è particolarmente spesa sul punto, adagiandosi sulla risalente massima adoperata in una delle prime applicazioni giurisprudenziali della fattispecie, secondo cui «i termini profitto e danno devono essere intesi nella massima estensione, comprendendo tutte le situazioni di pregiudizio e vantaggio anche non patrimoniale»[117]. Questa soluzione interpretativa, non certo imposta da necessità logica[118], trova tuttavia conferma in numerose pronunce di legittimità aventi a oggetto altre tipologie di reato, come ad esempio quelli previsti dagli artt. 171-*bis* e 171-*ter* l. n. 633 del 1941[119]. Oltre al dolo specifico, l'art. 167 subordinava, inoltre, la punibilità del fatto alla produzione di un effettivo «nocumento» ai danni del soggetto passivo: a tal proposito, si ritiene pacificamente che il «nocumento» si realizzi allorquando la condotta illecita determini un pregiudizio a un qualsiasi interesse giuridicamente rilevante, tanto di tipo patrimoniale che

orientare il comportamento dei consociati [e] dunque, la funzione di prevenzione generale» (cfr. A. Pagliaro (2009), 86).

115 Il co. 2, invece, richiama il trattamento dei dati personali «di cui agli articoli 9 e 10 del Regolamento» - categorie particolari di dati personali e dati relativi a condanne penali e reati – in violazione delle disposizioni e dei principi di cui agli articoli 2-*sexies* e 2-*octies*, o delle misure di garanzia di cui all'articolo 2-*septies* ovvero operando in violazione delle misure adottate ai sensi dell'articolo 2-*quinquiesdecies*.

116 Si tratta perciò di un dolo specifico c.d. «di ulteriore offesa», ossia posto in funzione restrittiva della punibilità (cfr. F. Mantovani (2011), 326 ss.).

117 Cass. pen., Sez. III, n. 30134 del 2004. In senso conforme si veda ex multis Cass. pen., Sez. V, n. 28280 del 2013 e Cass. pen., Sez. V, n. 11994 del 2017, le quali estendono la portata del concetto di profitto rilevante «a qualsiasi soddisfazione o godimento che l'agente si ripromette di ritrarre, anche non immediatamente dalla propria azione», di fatto privando il dolo specifico di qualunque capacità selettiva. In tal modo, infatti, potrà ritenersi sussistente la finalità di profitto – richiesta dalla norma incriminatrice – con il solo riferimento al ben più ampio concetto di "qualsiasi soddisfazione o godimento che l'agente si ripromette di ritrarre", estendendo, dunque, la portata applicativa della fattispecie.

118 Per una panoramica delle diverse ricostruzioni del dolo specifico prospettabili e delle relative conseguenze applicative derivanti dalla loro adozione, si veda per tutti S. Del Corso (2007), 2065.

119 Nel precetto di queste due disposizioni si sono infatti alternati a più riprese i termini «profitto» e «lucro», con il fine, secondo la Cassazione, di ampliare la soglia di punibilità con l'espressione «a scopo di profitto», e di restringerla allorché il fatto è stato previsto come reato solo se commesso a «fine di lucro», ossia perseguendo un vantaggio economicamente apprezzabile (v. ex multis Cass. pen., Sez. III, n. 149 del 2007).

non, appartenente al titolare dei dati[120] oppure a un terzo[121]. Previsto come circostanza aggravante nel previgente art. 35 l. n. 675 del 1996, nella disposizione attuale la sua natura giuridica è divenuta alquanto controversa, discutendosi in particolare se esso rappresenti un elemento costitutivo del reato oppure un presupposto influente sulla sua sola punibilità (art. 44 c.p.). Per l'opinione prevalente si tratterebbe di una condizione di punibilità «intrinseca»[122], la quale, in sinergia con il dolo specifico, contribuirebbe a selezionare tra i fatti già «meritevoli di pena», quelli che in concreto risultino anche «bisognosi di pena»[123]. Si sostiene, infatti, che sarebbe incongruo prevedere come elemento costitutivo del reato proprio uno dei fini tipizzati dal dolo specifico, la cui realizzazione come noto non è necessaria per la consumazione dell'illecito[124]. Nondimeno, alcuni autori revocano in dubbio la possibilità di sottrarre al dolo e configurare come condizione di punibilità un elemento causalmente legato alla condotta tipica e del tutto omogeneo alla fattispecie sul piano dell'offesa: non si vede, infatti, come una conseguenza direttamente correlata all'azione del reo e lesiva dello stesso bene giuridico protetto dalla norma incriminatrice possa limitarsi a influire sulla sola punibilità del fatto, piuttosto che sulla sua tipicità[125]. D'altra parte, l'obiezione correlata all'incompatibilità logica tra dolo specifico di «danno» ed evento di «nocumento» risulta fallace, perché trascura da un lato che il dolo specifico dell'art. 167 c.p. può essere integrato anche attraverso il solo perseguimento di un «profitto», dall'altro che il soggetto che il reo intende danneggiare potrebbe anche essere diverso da quello che ha effettivamente subito il pregiudizio. Conseguentemente, secondo quest'orientamento, il «nocumento» menzionato dal delitto d'illecito trattamento dei dati deve essere considerato quale elemento costitutivo del reato, atto a descrivere l'evento materiale causato dal reo e preveduto e voluto come conseguenza

120 Cfr. Cass. pen., Sez. III, n. 30134 del 2004, Cass. pen., Sez. V, n. 44940 del 2011, Cass. pen., Sez. III, n. 23798 del 2012, Cass. pen., Sez. V, n. 51089 del 2014, Cass. pen., Sez. III, n. 40103 del 2015, Cass. pen., Sez. V, n. 11994 del 2017.

121 Cass. pen., Sez. V, n. 44940 del 2011, Cass. pen., Sez. III, n. 7504 del 2013, Cass. pen., Sez. III, n. 40103 del 2015; in dottrina v. P. Troncone, (2011), 158, il quale annovera questa ipotesi criminosa tra quelle c.d. «a vittima diffusa». Restano escluse soltanto quelle inosservanze che determinano una minima lesione dell'identità personale e della privacy del soggetto, e che non provocano apprezzabili pregiudizi patrimoniali (cfr. Cass. pen., Sez. III, n. 30134 del 2004).

122 La distinzione tra condizioni di punibilità «estrinseche» e «intrinseche» è stata proposta per la prima volta da P. Nuvolone (1955), 14, al fine di ricondurre almeno quest'ultime al principio della responsabilità colpevole: dovranno, infatti, essere rimproverabili almeno a titolo di colpa quelle condizioni della punibilità intrinseche al piano dell'offesa, che hanno la funzione di attualizzare o rendere comunque irreversibile il pregiudizio del bene giuridico protetto dalla norma incriminatrice.

123 Si veda a riguardo Corte. Cost., sent. n. 247 del 1989.

124 Cfr. R. Lotierzo (2013), 1589; A. Manna (2003); in giurisprudenza v. da ultimo Cass. pen., Sez. III, n. 40103 del 2015.

125 Invero, le Sezioni Unite hanno puntualizzato a più riprese come le condizioni di punibilità siano sottoposte a un regime giuridico che si giustifica esclusivamente in relazione a situazioni del tutto scorrelate dall'oggetto giuridico del reato e dalla condotta incriminata (cfr. Cass. pen., Sez. Un., n. 13954 del 1990 e n. 2 del 2008). Il tema che si pone è, dunque, il rapporto tra elementi costitutivi del fatto tipico e condizioni obiettive di punibilità, un tema "classico" in diritto penale. Si tratta, com'è noto, di una distinzione con risvolti sia teorici sia pratici, per cui in generale, v. G. Fiandaca-E. Musco (2014b), 813 ss.: nei casi in cui il legislatore subordini la punibilità del fatto alla sussistenza di determinati requisiti, si pone l'esigenza di comprendere se tali elementi siano da ritenersi costitutivi del fatto tipico, in quanto appartenenti al nucleo dell'offesa al bene che si mura a tutelare (e, dunque, debbano essere oggetto di volontà e rappresentazione da parte dell'autore del reato), ovvero se costituiscano elementi aggiuntivi, non essenziali ma inseriti nella norma per rispondere a valutazioni di opportunità politico-criminale. Nel caso dell'art. 167 cod. privacy (nella versione previgente alla modifica di cui al d. lgs. 101/2018) ritenere che il nocumento arrecato all'interessato, in conseguenza di una violazione delle disposizioni del codice, non sia elemento costitutivo ma condizione obiettiva di punibilità confinerebbe la lesione dei diritti dell'interessato a mero elemento *esterno* all'offesa individuata dalla disposizione.

della sua condotta[126]. Dopo le modifiche introdotte con il d. lgs. 101/2018, la disposizione riporta, invece della clausola «se dal fatto deriva nocumento», la formulazione «arreca nocumento all'interessato»: nell'attesa dei primi riscontri giurisprudenziali, sembra non più revocabile in dubbio l'appartenenza del «nocumento» agli elementi costituitivi del reato di cui all'art. 167 cod. *privacy*.

Di notevole rilevanza ai fini della presente analisi è, inoltre, l'art. 167-*bis* cod. *privacy*, ove, al co. 2, salvo che il fatto costituisca più grave reato, si punisce con la reclusione da uno a sei anni «chiunque, al fine trarne profitto per sé o altri ovvero di arrecare danno, comunica o diffonde, senza consenso, un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala», quando il consenso dell'interessato è richiesto per le operazioni di comunicazione e di diffusione. A tutelare la clientela da potenziali acquisizioni illecite di dati personali interviene altresì l'art. 167-*ter* cod. *privacy*, che punisce con la reclusione da uno a quattro anni chiunque, al fine trarne profitto per sé o altri ovvero di arrecare danno, acquisisce con mezzi fraudolenti un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala.

Questo primo segmento dell'analisi consente di formulare talune osservazioni di sintesi: le disposizioni penali contenute nel codice *privacy* risultano principalmente orientate a sanzionare le violazioni più macroscopiche della disciplina in materia di dati personali, soprattutto con riferimento a dati aggregati in archivi o *databases* o a trasferimenti di carattere transfrontaliero (anche con riguardo, dunque, alla crescente valenza commerciale dei dati, cui si è accennato in apertura). Inoltre, taluni tra i più recenti interventi legislativi di fonte europea – segnatamente il richiamato *GDPR* e la direttiva c.d. *NIS* (2016/1148)[127] – dimostrano l'esistenza di un ormai stretto collegamento tra tutela della *privacy* ed esigenze di *cybersecurity*: Nell'era dell'economia dei dati, infatti, la tutela dell'integrità e della sicurezza di un sistema informatico acquisisce un ruolo di primo piano, come dimostrato dalle prescrizioni – contenute nei testi normativi ora richiamati – relative all'obbligo, per i gestori di portali *online*, di adottare peculiari misure tecniche e organizzative finalizzate a evitare violazioni e *data breaches*[128]. In un mercato quale quello del

126 Cfr. Cass. pen., Sez. III, n. 40103 del 2015 (in senso conforme v. Cass. pen., Sez. III, n. 38406 del 2008, Trib. Roma, Sez. II, 30 gennaio 2004); in dottrina v. G. Corrias Lucente (2004), 644 ss. In questo senso, perciò, l'art. 167 c.p. disciplinerebbe indubbiamente un reato di danno e non di pericolo.

127 Cfr. Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.

128 Con riferimento al profilo della sicurezza, v. ad es. l'art. 32 del *GDPR*, rubricato «*Sicurezza del trattamento*», ove si prevede espressamente che «tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di **sicurezza** adeguato al rischio». Così anche il d. lgs. 65/2018, che ha recepito nell'ordinamento italiano la citata direttiva (UE) 2016/1148, prevede all'art. 12 (*Obblighi in materia di sicurezza e notifica degli incidenti*») che gli operatori di servizi essenziali – tra i quali figurano anche servizi di natura bancaria e finanziaria – debbano adottare «misure tecniche e organizzative adeguate e proporzionate alla gestione dei rischi posti alla sicurezza della rete e dei sistemi informativi che utilizzano nelle loro operazioni. Tenuto conto delle conoscenze più aggiornate in materia, dette misure assicurano un livello di sicurezza della rete e dei sistemi informativi adeguato al rischio esistente», nonché «misure adeguate per prevenire e minimizzare l'impatto di incidenti a carico della sicurezza della rete e dei sistemi informativi

FinTech, fondato su infrastrutture digitali, la sicurezza informatica assume così un ruolo centrale, quale presupposto dell'integrità dei dati e dello stesso funzionamento del sistema. Emerge, dunque, l'esigenza di integrare l'analisi con riferimento ad ulteriori testi legislativi per fornire un inquadramento più completo del fenomeno FinTech.

Le interviste condotte con gli operatori del settore hanno, infatti, mostrato come le diverse piattaforme siano dotate di adeguati strumenti di protezione dei dati personali dell'utenza. Ciò nonostante, resta il pericolo che esse siano fatte oggetto di forme di criminalità informatica finalizzate all'apprensione dei dati altrui e permane il rischio che gli utenti stessi divengano, singolarmente, vittima di comportamenti criminosi finalizzati alla sottrazione di dati e credenziali.

5.2 La tutela penale dell'identità digitale tra frode informatica e fattispecie limitrofe

Volendo adottare la prospettiva di una tutela maggiormente incentrata sull'individuo, la smaterializzazione inevitabilmente connessa allo sviluppo delle tecnologie e la progressiva *giuridificazione* della nozione di identità scolpiscono con sempre maggiore forza i nuovi confini dell'identità della persona nella rete, fino ad indurre ad un progressivo passaggio dall'*identità personale* all'*identità digitale*. Se in sociologia e filosofia si è parlato al riguardo di post-umano, la dottrina giuridica già da quasi un decennio si occupa delle ricadute per il diritto della trasformazione del corpo umano in un corpo elettronico[129]. La metafora alla quale si fa riferimento per rendere icasticamente l'idea dell'identità digitale è quella della "maschera" dal momento che è l'individuo che contribuisce in prima persona a creare un suo *profilo* (o i suoi tanti diversi profili a seconda delle esigenze connesse alla registrazione nella piattaforma di volta in volta considerata e dei relativi sistemi di profilatura).

Il presente paragrafo si propone, dunque, l'obiettivo di delineare lo schema che, *de iure condito*, riesca ad intercettare in modo più pertinente il complesso delle condotte offensive dell'identità digitale, dalla sua indebita apprensione al suo indebito utilizzo, e finanche all'indebita "costruzione" dell'identità digitale tramite la manipolazione informatica di dati personali oggetto di elaborazione.

La frode informatica

Per quanto attiene alla tutela penale dell'identità digitale lo strumento che viene primariamente in considerazione è quello della frode informatica (art. 640-*ter* c.p.). È noto come lo sviluppo delle tecnologie informatiche abbia determinato l'emersione di nuove forme di aggressione ad interessi già tutelati nell'ordinamento (ad es. di natura patrimoniale) e, al contempo, l'affermarsi di inedite istanze di tutela,

utilizzati per la fornitura dei servizi essenziali, al fine di assicurare la continuità di tali servizi»; parallelamente, si prevede all'art. 14 che obblighi di natura analoga ricadano anche sui fornitori di servizi digitali».

129 A tal proposito v. le riflessioni di S. Rodotà (2006).

ben oltre l'orizzonte della tradizionale protezione (penalistica) del patrimonio (e dei diritti soggettivi aventi contenuto patrimoniale)[130]. Il consueto sistema dei «reati contro il patrimonio», previsti nel Codice penale, si è subito dimostrato inadeguato a garantire un'efficace ed effettiva prevenzione delle nuove fenomenologie criminali, caratterizzate da un'essenziale e insopprimibile componente tecnologico – informatica che ne costituisce, anche da un punto di vista criminologico, il tratto distintivo e qualificante. Gli strumenti informatici sono così impiegati come originali mezzi di aggressione patrimoniale, i cui risvolti lesivi, tuttavia, non sono affatto limitati ad interessi di natura squisitamente patrimoniale; essi si proiettano, invece, in una pluralità di dimensioni di tutela qualitativamente eterogenee, di consistenza istituzionale, come l'interesse al regolare funzionamento dei sistemi informatici e telematici, o fortemente individuale (o *personale* in senso proprio): in particolare, l'interesse alla riservatezza, che coinvolge informazioni e dati digitalizzati.

Le fattispecie incriminatrici tradizionalmente poste a presidio di interessi di natura patrimoniale si sono rivelate anacronistiche a fronte di modalità offensive tendenzialmente inafferrabili in termini di applicazione giudiziaria. La sostanziale inadeguatezza dei c.d. reati patrimoniali e, più nello specifico, del delitto di truffa di cui all'art. 640 c.p., ha interessato, come intuibile, le *forme modali* della condotta e l'*oggetto materiale del reato*.

Ci si è chiesti, nella prassi applicativa, se potessero rilevare a titolo di truffa (art. 640 c.p.) anche quelle ipotesi concrete in cui la condotta strumentale fraudolenta non aveva come effetto l'induzione in errore della vittima, quale presupposto del successivo atto di disposizione patrimoniale, cui corrisponde la locupletazione ingiusta del soggetto attivo[131]. Si tratta di tutti quei casi in cui la condotta decettiva si risolve in una manipolazione, con alterazione di un sistema informatico, o in un intervento sul processo di elaborazione dei dati informatici, tale da determinare, in modo automatico, un vantaggio patrimoniale ingiusto.

La dottrina ha tendenzialmente negato la riconducibilità di tali fattispecie concrete, tutte caratterizzate dall'uso di strumenti informatici e dal difetto di un'induzione in errore di una vittima determinata, al delitto di truffa di cui all'art. 640 c.p.[132].

I limiti *strutturali* delle fattispecie incriminatrici in materia di tutela del patrimonio a realizzare un concreto effetto deterrente rispetto al crescente fenomeno della criminalità informatica hanno indotto il legislatore a prevedere un'autonoma figura delittuosa – la *frode informatica* di cui all'art. 640-*ter* c.p.[133] - che solo apparentemente ripropone lo schema consolidato della truffa di cui all'art. 640 c.p., in quanto priva proprio di quegli elementi oggettivi – l'induzione in errore del soggetto passivo e gli «artifizi o raggiri» - che sono in realtà incompatibili con le effettive

130 In generale, sul tema della criminalità informatica, A. Alessandri (1990).; C. Pecorella (2000); F. Mucciarelli (1988); L. Picotti (2004); C. Parodi (1997).

131 Sul punto, A. Fanelli (2009), 446.

132 Così, tra gli altri, G. Fiandaca-E. Musco (2014), 209.

133 Introdotta dalla Legge 23 dicembre 1993, n. 547.

dinamiche di aggressione tecnologico-informatica ad interessi di natura patrimoniale, istituzionale o individuale[134]. Viene così colmata un'eclatante lacuna di tutela del sistema penale nazionale.

Il nuovo paradigma punitivo se, da un lato, risulta sensibilmente svincolato dall'originaria fattispecie di truffa (art. 640 c.p.), dall'altro ne riproduce alcuni tratti strutturali di fondo: il duplice evento dell'ingiusto profitto con l'altrui danno (c.d. evento plurimo), la connotazione decettiva della condotta *strumentale,* consistente nell'alterazione, in qualsiasi modo compiuta, del funzionamento di un sistema informatico ovvero l'intervento, senza diritto, con qualsiasi modalità realizzato, su dati o informazioni contenuti in un sistema informatico o telematico e, infine, il trattamento sanzionatorio e il regime di procedibilità a querela, salvo che ricorra taluna delle circostanze di cui ai co. 2 e 3 dello stesso art. 640-*ter* c.p. o taluna delle circostanze previste dall'art. 61, co. 1 n. 5 – limitatamente all'aver approfittato di circostanze di persona, anche in riferimento all'età – e n. 7 c.p.

La configurazione strutturale della condotta tipica esprime in modo significativo il profilo qualificante (o *specializzante*) del delitto di frode informatica: essa può estrinsecarsi, infatti, in una duplice forma, l'alterazione di un sistema informatico o telematico ovvero l'abusivo intervento, con ogni mezzo effettuato, su dati, informazioni o programmi contenuti in detti sistemi[135]. La connotazione decettiva (artifizi o raggiri) che è propria della truffa di cui all'art. 640 c.p. è qui sostituita dall'attività materiale di manipolazione del sistema informatico, da cui deriva la *distorsione del processo di elaborazione dei dati*.

Il danno patrimoniale, cui corrisponde il profitto ingiusto, è conseguenza automatica del distorto processo di elaborazione dei dati informatici, realizzato dall'attività di manipolazione del sistema. Ai fini della configurabilità del delitto, pertanto, l'operazione di elaborazione dei dati deve presentare un oggettivo contenuto patrimoniale[136], che si riverbera in un pregiudizio nella sfera patrimoniale del soggetto passivo e nella simmetrica locupletazione ingiusta dell'agente.

La *specificità* del modello di tutela delineato dall'art. 640-*ter* c.p. è per vero costituita, come si è già accennato, dalla circostanza che la sua configurabilità prescinde dalla *cooperazione artificiosa* del soggetto passivo, indotto in errore attraverso la condotta decettiva dell'agente, nella produzione del pregiudizio di natura patrimoniale[137].

134 Così, tra gli altri, F. Antolisei (2008), 384; F. Mantovani (2014), 217.

135 Per questo rilievo, C. Pecorella (2000), 93; D. Pulitanò (2013), 277.

136 G.I.P. Trib. Milano, 29 marzo 2008.

137 In questi termini, G. Fiandaca-E. Musco (2014), 209; in giurisprudenza, sui profili strutturali che differenziano il "tradizionale" delitto di truffa (ex art. 640 c.p.) e la frode informatica, si consideri, tra le altre, Cass., sez. II, 9 giugno 2016, n. 41435, in Dejure, che individua l'elemento discretivo nel fatto che l'«attività fraudolenta dell'agente investe», nell'ipotesi di cui all'art. 640-ter c.p., «non la persona (soggetto passivo), di cui difetta l'induzione in errore, bensì il sistema informativo di pertinenza della medesima, attraverso la manipolazione di detto sistema»; in particolare, il caso concreto, affrontato dalla Corte di cassazione, concerneva

La frode informatica descrive una modalità di *aggressione unilaterale ad un sistema informatico*[138], senza che il danno patrimoniale, cui si giustappone dinamicamente l'ingiusto profitto, sia il risultato di un'attività compartecipativa della vittima[139].

La descrizione alquanto ampia delle due modalità realizzative della condotta tipica corrisponde ad una precisa opzione politico-criminale: garantire la possibilità di applicazione della previsione incriminatrice a forme di aggressione a contenuto tecnologico sempre nuove e inedite.

Paiono opportune alcune precisazioni preliminari in ordine alla nozione di «sistema informatico o telematico», con riferimento alla condotta di alterazione, e di «dati, informazioni o programmi», con riguardo, invece, all'attività di abusivo intervento. Quanto alla prima, essa indica ogni sistema di trattamento automatico della informazione attraverso mezzi elettronici, ivi compresi anche i sistemi che utilizzano carte e bande magnetiche e che forniscono beni o servizi, microchip, lettori ottici, CD-Rom e simili, nonché memorie complementari di massa, apparecchiature di input (tastiere, scanner, lettori ottici) e quelle di output (video, stampanti e via dicendo)[140]. Sono naturalmente esclusi i mezzi elettronici che svolgono un'esclusiva funzione di protezione: la loro manipolazione, a ben vedere, non può implicare il raggiungimento del profitto ingiusto da parte dell'agente, in quanto funzionale solo ad una successiva e diversa aggressione del patrimonio altrui. È sistema telematico, rilevante ai fini dell'integrazione della fattispecie, qualunque sistema costituito da reti di telecomunicazione o connessione a distanza, con mezzi elettronici, fibre ottiche, cavi, che sia gestito con tecnologie informatiche, ovvero sia servente rispetto ad autonome tecnologie informatiche. Tra i sistemi telematici si annovera certamente la rete Internet.

I dati, che invece formano oggetto della condotta di abusivo intervento, sono registrazioni elementari, effettuate attraverso simboli (numeri, lettere, ecc.) che, solo qualora interpretati, divengono informazioni, cioè notizie che devono essere poste ad oggetto di elaborazione tramite computer e organizzate secondo una logica che consenta l'attribuzione alle stesse di un particolare significato, estrapolabile dall'utente del sistema informatico. I programmi, a loro volta, costituiscono gruppi di istruzioni che permettono all'elaboratore di lavorare e compiere specifiche operazioni[141].

L'esame delle due forme tipiche di realizzazione della condotta penalmente rilevante deve essere svolto alla luce della complessa casistica giudiziaria sinora formatasi in tema.

L'alterazione consiste in qualsiasi operazione di manipolazione di un sistema informatico o telematico, come sopra definito, che incida sulla componente fisica (c.d. *hardware*) o logica (c.d. *software*) del sistema. Solo manomettendo tali

138 Espressamente, M. Belli (2015), 704.

139 Il profitto ingiusto dell'agente deve costituire il risultato diretto del distorto processo di elaborazione, attuato automaticamente dal sistema a seguito dell'intervento manipolativo dell'autore: così, per tutti, F. Mucciarelli (1996), 138.

140 L'esaustiva definizione è proposta da M. Belli (2015), 707.

141 Per questa nozione, G. Pica (1999), 526.

componenti basilari del sistema è possibile realizzare una deviazione funzionale del sistema, con conseguente esito irregolare, strumentale al raggiungimento di un profitto ingiusto, richiesto ai fini della rilevanza penale del fatto[142].

La deviazione funzionale è da intendersi come «distrazione» del sistema (*rectius,* del processo di elaborazione dei dati) dagli schemi predefiniti: essa è strumentale al conseguimento del profitto, con altrui danno[143]. La giurisprudenza ha così escluso che l'operazione di duplicazione dei dati informatici, acquisiti nell'accesso abusivo ad un sistema informatico o telematico, possa costituire condotta rilevante ai sensi dell'art. 640-*ter* c.p., in quanto carente dell'ineliminabile componente decettiva, identificata nella manomissione dell'*hardware* o del *software,* con conseguente deviazione funzionale del processo di elaborazione dei dati.

Nelle alterazioni che investono la c.d. componente logica del sistema informatico o telematico rientrano anche le ipotesi di manipolazione dei c.d. programmi, cioè dei passaggi logici previsti in un programma originale o nell'utilizzo di un programma diverso o ulteriore rispetto a quello normalmente in uso in un determinato sistema informatico. Un caso paradigmatico di manipolazione di programma è ravvisabile nel settore bancario e consiste nell'utilizzo di un *software* predisposto per il calcolo degli interessi dovuti alla banca sugli accrediti dei clienti per defraudare arrotondamenti minimi confluenti, invece che sui legittimi conti, sul conto dell'agente o di chi, per lui, ne trae un ingiusto vantaggio[144].

La giurisprudenza riconduce all'art. 640-ter c.p., nella forma dell'alterazione di un sistema informatico o telematico, la seguente casistica:

a. illeciti prelievi compiuti dall'estero con carte bancomat clonate: la rete Bancomat costituisce, infatti, un sistema informatico, e la clonazione delle tessere è rilevante come attività materiale di alterazione[145];

b. utilizzo di schede elettroniche clonate, con numero identificativo corrispondente a quello delle schede originariamente inserite in apparecchi da gioco, in modo tale che gli stessi apparecchi potessero restare scollegati dalla rete dell'amministrazione dei Monopoli di Stato, così da impedire la percezione dell'effettivo importo delle somme giocate[146];

c. introduzione in apparecchi elettronici per il gioco di intrattenimento senza vincite di una seconda scheda, attivabile a distanza, che li abilita all'esercizio del gioco d'azzardo[147];

142 Si è così ritenuta sussistente la condotta tipica di alterazione di un sistema informatico con riguardo all'introduzione, in apparecchi elettronici per il gioco di intrattenimento senza vincite, di una seconda scheda, attivabile a distanza, tale da abilitarli all'esercizio del gioco d'azzardo (c.d. slot machines): in tal senso, cfr. Cass., sez. V, 19 marzo 2010, n. 27135, in C.E.D. Cass., rv. 248306.

143 Sul punto, L. Bisori (2013), 607.

144 Il caso è tratto da E. Dolcini - G. Marinucci (2011), 4639.

145 Trib. Rovereto, 11 dicembre 2007.

146 Trib. Trapani, G.U.P., 17 marzo 2008.

147 Cass. pen., sez. V, 19 marzo 2010, n. 27135.

d. manipolazione dei dati di un sistema informatico, consistente nella predisposizione di false attestazioni di risarcimento dei danni, resa possibile grazie alla sottrazione della password rilasciata al responsabile di zona di una compagnia assicurativa[148];

e. abusiva penetrazione nel sistema informatico dell'Agenzia delle Entrate, seguita dall'inserimento di provvedimenti di sgravio fiscale illegittimi, perché mai adottati, in relazione a tributi già iscritti a ruolo per la riscossione coattiva, in tal modo alterando i dati contenuti nel sistema, facendo apparire come insussistente il credito tributario vantato dall'Erario nei confronti di molti contribuenti[149].

La frode informatica, come già rilevato, può anche realizzarsi nella forma di un intervento abusivo («senza diritto»), con qualsiasi mezzo realizzato, su dati, informazioni o programmi, da cui consegua un danno patrimoniale per il soggetto passivo e un corrispondente vantaggio economico – patrimoniale per l'autore del reato. L'intervento è abusivo quando l'operazione in cui esso consiste è stata compiuta in assenza di autorizzazione o di altro titolo che sia idoneo a legittimare il soggetto alla sua realizzazione (ad es., quando l'intervento su dati, informazioni o programmi è compiuto in esecuzione di un provvedimento del giudice).

Con la locuzione «intervento» si allude ad una pluralità di operazioni a contenuto tecnico – informatico che implicano un'interazione, diretta o indiretta, con il sistema operativo. Costituisce *intervento* rilevante ai sensi dell'art. 640-*ter* c.p. l'azione manipolativa che produca sui dati, informazioni o programmi una *modificazione del loro contenuto o della loro destinazione.* L'intervento abusivo può investire tutte le fasi specifiche del procedimento informatico, dall'*input* all'*output*.

La manipolazione di *input* si realizza con l'alterazione o la soppressione di dati che costituiscono oggetto di elaborazione in un determinato procedimento informatico ovvero nell'introduzione nel sistema di *dati non autorizzati* o di *dati falsi*, comunque idonei ad incidere sull'esito regolare e predefinito del processo telematico di elaborazione. Così, ad es., nel caso in cui l'intervento abusivo avvenga sfruttando l'identità digitale di altro soggetto, solitamente individuata da una chiave di accesso e relativo *user-id*, per compiere a suo vantaggio operazioni dal contenuto economico, appunto non autorizzate dal legittimo titolare (sfruttamento dell'identità digitale altrui per accedere abusivamente al servizio *home banking,* disponendo *sine titulo* bonifici bancari a proprio vantaggio)[150].

148 Cass. pen., sez. II, 11 novembre 2009, n. 44720.

149 Cass. pen., sez. V, 30 settembre 2008, n. 242938.

150 La Corte di cassazione (cfr. Cass., sez. I, 15 aprile 2011, n. 17748, in Dir. & Giust., 2011) ha altresì riconosciuto la sussistenza della condotta di «intervento senza diritto» su dati, informazioni o programmi nell'utilizzazione di carte di debito falsificate e nella previa artificiosa captazione dei codici segreti di accesso (c.d. PIN): il soggetto agente, infatti, mediante la condotta di utilizzazione e captazione, penetra abusivamente («intervento senza diritto») nei vari sistemi bancari telematici, alterando i relativi dati contabili, mediante la disposizione, naturalmente sine titulo, di operazioni di trasferimento di fondi (ad es. prelevamento abusivo di contanti mediante i servizi di cassa continua). Più di recente, la stessa Suprema Corte (sez. VI, 4 novembre 2015, n. 1333, in C.E.D. Cass., rv. 266233) ritiene, invece, che il reiterato prelievo di denaro contante da uno sportello bancomat, mediante l'utilizzo di un supporto magnetico clonato, integri il reato di cui all'art. 55, co. 9, D.lgs. n. 21 novembre 2007, n. 231 (Indebita utilizzazione di carte di credito) e non già il delitto di frode informatica. Conferma la prima soluzione applicativa,

Si registrano, nella prassi giudiziaria, ipotesi di intervento abusivo, per manipolazione di *input,* nel caso del dipendente di un istituto di credito che, per favorire alcuni clienti, aveva accreditato sui loro conti somme di denaro proveniente dal versamento di assegni, facendo risultare l'avvenuto pagamento in contanti; ovvero il caso di alcune aziende che evadono gli obblighi contributivi, dovuti all'INPS, interferendo con l'elaboratore centrale dell'istituto previdenziale, facendo risultare che i versamenti dovuti erano stati regolarmente eseguitici[151].

La manipolazione può avere anche ad oggetto le informazioni che derivano da un processo informatico: la condotta, più precisamente, consiste nella modifica di alcuni dati utili al procedimento di elaborazione (ad es., per un caso tratto dalla giurisprudenza svizzera, la falsificazione di formulari elettronici, recanti gli estremi delle fatture mandate in pagamento, così determinando l'emissione, ad opera dell'elaboratore, di assegni intestati a persona diversa rispetto al creditore effettivo[152]).

A sua volta, l'interferenza abusiva sui *programmi* è ravvisabile allorquando l'intervento incida sull'esito di un processo di elaborazione di dati; la dottrina trae dalla giurisprudenza americana un caso paradigmatico di manipolazione di programma, individuabile nell'intervento abusivo sul *software* di gestione della contabilità di un istituto di credito, operato da un dipendente che aveva inserito sullo stesso un'istruzione supplementare, grazie al quale il suo conto corrente bancario «scoperto» non veniva sottoposto a verifica[153].

Il trattamento sanzionatorio è aggravato quando ricorrono le circostanze rispettivamente indicate dal secondo e dal terzo comma dell'art. 640-*ter* c.p. Il secondo comma della disposizione incriminatrice rinvia, in particolare, alle circostanze di cui al n. 1 del comma 2 dell'art. 640 c.p., ossia che il fatto sia stato commesso in danno dello Stato, o di altro ente pubblico o col pretesto di far esonerare taluno dal servizio militare. É *specifica* del delitto di frode informatica, invece, la circostanza aggravante che il fatto sia stato commesso con abuso della qualità di operatore del sistema. La ragione dell'aggravamento del trattamento sanzionatorio è rintracciabile nel maggior disvalore che assume il fatto quando l'alterazione del sistema informatico o telematico ovvero l'intervento *abusivo* sia stato commesso da un soggetto che, in funzione della sua qualifica (ad es. professionale), è tenuto ad un oggettivo dovere di lealtà nei confronti del titolare del sistema informatico compromesso dalla sua attività penalmente rilevante.

La qualifica di *operatore del sistema* va intesa in senso a-tecnico: si allude, infatti, ad ogni soggetto che sia incaricato di svolgere qualsiasi mansione finalizzata all'utilizzazione del sistema informatico o telematico (ad es. in colui che esercita, a titolo occasionale, la funzione di manutenzione, controllo o attivazione del

nel senso della configurabilità della fattispecie di cui all'art. 640-ter c.p., Cass., sez. II, 9 maggio 2017, n. 26229, in Dejure.

151 Casistica tratta da E. Dolcini - G. Marinucci (2011), 4642.

152 In tema, C. Pecorella (2000), 91.

153 Sul punto, E. Dolcini - G. Marinucci (2011), 4642.

medesimo)[154]. Si ritiene, dunque, che nella nozione possano rientrare tutti i soggetti che partecipano a titolo diverso alle varie fasi dei processi d'intermediazione finanziaria basati su ICT (ancorché realizzati online e/od offline) nonché gli operatori delle piattaforme digitali di servizi finanziari.

Il furto e l'indebito utilizzo di identità digitale

Il terzo comma dell'art. 640-*ter* c.p., introdotto dall'art. 9 della Legge 15 ottobre 2013, n. 119, descrive una circostanza aggravante con pena indipendente per il caso in cui il fatto sia stato commesso mediante il *furto o l'indebito utilizzo dell'identità digitale* in danno di uno o più soggetti. Si tratta di due specificazioni *modali* (o strumentali) della condotta tipica descritta al primo comma, tra loro reciprocamente alternative[155]. L'indebito utilizzo dell'identità digitale consiste nell'uso *non autorizzato* o comunque *distorto* (deviato) di dati personali identificativi *illecitamente acquisiti,* ad esempio perché liberamente noti o perché raccolti consensualmente dall'effettivo titolare per determinati scopi, invero traditi dal soggetto agente che li ha per l'appunto impiegati per finalità aliene da quelle predefinite.

Il furto d'identità, diversamente dall'indebito utilizzo, implica l'illecita apprensione dei dati c.d. identitari (ad es. chiavi d'accesso a sistemi informatici o a reti che richiedono l'identificazione digitale del soggetto passivo, spogliato della sua identità). L'effetto delle due condotte è sempre la sostituzione di persona, strumentale al conseguimento, nel caso della frode informatica, di un vantaggio economico – patrimoniale. La soluzione, però, non sgombra il campo da dubbi: in questo caso, infatti, per quanto si abbia un "intervento senza diritto" all'interno di un sistema informatico, vi è una indubbia componente di frode e di inganno perpetrata a danno della vittima, indotta a fornire le proprie informazioni, il cui disvalore non sembra pienamente espresso dal semplice ricorso alla frode informatica aggravata. Peraltro, il ricorso all'art. 640-*ter* c.p. fa emergere l'offesa soltanto nel momento in cui si realizza il danno patrimoniale e il fatto dell'indebita acquisizione dell'altrui identità resta tuttora un'ipotesi non del tutto inquadrabile all'interno di una precisa fattispecie.

Ad esempio, di particolare rilievo criminologico è la c.d. pratica del *phishing*, intendendo per tale, secondo la letteratura più sensibile al tema[156], una tecnica di *social engineering,* cioè una metodologia di comportamento sociale, indirizzata a carpire informazioni personali oppure abitudini e stili di vita. La dinamica dei *phishing attacks* è sostanzialmente bifasica e può essere così descritta:

a) la prima fase consiste nell'induzione del soggetto passivo a fornire al *phisher* dati sensibili o informazioni personali, come ad es. le chiavi di autenticazione per

154 Amplius, M. Belli (2015), 713.

155 Per tutti, G. Malgieri (2015), 143 ss.

156 Per tutti, in argomento, R. Flor (2007).

accedere ad aree informatiche esclusive o a servizi finanziari o bancari *online,* numeri di carte di credito o di pagamento, identificativi per le abilitazioni all'accesso a siti di vario genere, *user –id* e *passwords* di accesso diretto alle piattaforme *banca via internet,* numeri di conto corrente, estremi di documenti identificativi;

b) la seconda fase, invece, si identifica nell'utilizzazione dei dati ottenuti per conseguire l'abilitazione all'accesso (abusivo) ai servizi *online*, assumendo virtualmente l'identità del legittimo titolare o utente[157].

Le modalità operative del *phishing* sono in continua evoluzione ed è pertanto difficile fornirne una selezione aggiornata. Di regola, nel *phishing attack,* si ricorre all'invio di *e-mail* apparentemente provenienti da enti o istituzioni reali (ad es. istituti di credito), contenenti messaggi, immagini e informazioni formulate appositamente per indurre la vittima a connettersi ad una pagina *web* che simula la veste grafica ed operativa della pagina autentica, e ad inserire i dati relativi all'accesso ad aree informatiche riservate o a servizi *on line*. Una seconda variante consiste, invece, nell'intervenire direttamente sul sistema informatico dell'utente, ricorrendo, in tal caso, all'impiego di *software* c.d. autoinstallanti, quali ad es. *trojan, malware* o *keylogger*, idonei a reperire o registrare i dati dell'utente, sì da trasmetterli, in automatico, al *phisher*[158].

La giurisprudenza è tendenzialmente orientata a negare la configurabilità del delitto di frode informatica (art. 640-*ter* c.p.) in relazione al fenomeno del *phishing*, ravvisandovi, invece, l'alternativa fattispecie di truffa semplice, di cui all'art. 640 c.p.: l'invio di *e-mails* attraverso le quali, per il loro contenuto decettivo, l'utente è indotto a fornire dati e informazioni utili (ad es. chiavi di accesso a *banca via internet*) costituisce un «artifizio e raggiro» rilevante ai fini dell'integrazione del delitto di truffa semplice. Sussiste, in tali casi, anche il requisito strutturale della truffa *ex* art. 640 c.p., individuato nell'induzione in errore del soggetto passivo: è l'utente, vittima del *phishing,* a comunicare direttamente al *phisher* i dati o le informazioni che poi saranno impiegate per il conseguimento di un ingiusto profitto (ad es. tramite la disposizione di operazioni bancarie illecite).

Diverso è il caso in cui, invece, il *phishing attack* si realizzi mediante l'impiego di un *software* c.d. autoinstallante, capace di decifrare i dati sensibili e trasmetterli in automatico al *phisher*. Si tratta di una condotta che assume la consistenza tipica dell'alterazione di un sistema informatico o telematico ovvero dell'intervento abusivo su dati, informazioni o programmi riferibili all'utente. L'elemento dirimente è tuttavia rappresentato dal consenso prestato dalla vittima all'installazione del *software* di captazione di dati sensibili: quando è il soggetto passivo, indotto in errore, a prestare il consenso, non vi sarebbero margini per

157 In questi termini, L. Bisori (2013), 612 ss.

158 Così, R. Flor (2007), 893.

configurare il delitto di frode informatica, bensì quello di truffa semplice *ex* art. 640 c.p.[159].

Un'altra ipotesi problematica è il *pharming*, o frode *man in the browser*, che descrive una peculiare truffa, attuata mediante un'interposizione fittizia nelle interazioni tra l'utente e, ad esempio, un sito istituzionale: in questo caso, il soggetto attivo del reato altera il funzionamento della rete, modificando la corrispondenza numerica dei server DNS, in modo che l'utente, dopo aver inserito l'indirizzo *web* corretto, venga reindirizzato su una pagina diversa, anche se identica a quella ufficiale. In questo caso il reato di cui all'art. 640-*ter* c.p. è, almeno apparentemente, integrato, poiché si ha l'alterazione di un sistema informatico; nuovamente, però, sembra che tale condotta trascenda quanto previsto dalla norma stessa, poiché vi è un'indubbia induzione in errore a danno della persona fisica, che non può semplicemente trovare un precipitato nella compromissione del funzionamento del sistema.

Infine, il *man in the middle attack* è un'ulteriore tipologia di frode, che presenta notevoli difficoltà di inquadramento, e, al tempo stesso, una peculiare pericolosità, poiché è una condotta spesso diretta non soltanto a danno di privati, ma anche di imprese. Le modalità operative possono essere delineate schematicamente: un *hacker* viola la casella di posta della vittima designata e ne monitora tutti i movimenti, nell'attesa di intercettare una comunicazione relativa a un'operazione commerciale o finanziaria. Dopo aver individuato un affare potenzialmente profittevole, il soggetto ne segue attentamente lo sviluppo e, soltanto quando l'accordo è quasi perfezionato, "esce dall'ombra": inviando una comunicazione dall'indirizzo *mail* violato alla controparte, comunica una fittizia variazione delle coordinate bancarie di riferimento e riesce a deviare a proprio vantaggio il pagamento dell'operazione. Questo schema truffaldino di nuova invenzione non può rientrare in nessuna delle varianti di cui all'art. 640 *ter* c.p. e richiede un ritorno a figure di reato "tradizionali": si tratta, infatti, di una condotta articolata, che aggrava la truffa mediante la violazione della corrispondenza.

Questi esempi permettono di delineare le numerose criticità delle cd. *input frauds*, che potrebbero realizzarsi nei portali digitali di servizi finanziari.

Si tratta di condotte che ledono una pluralità di beni diversi ed eterogenei, poiché realizzano un ingiusto profitto mediante la violazione della "sfera privata" della vittima, anche se in forma dematerializzata. Se, quindi, l'intervento senza diritto su un sistema informatico aggravato dall'abuso dell'identità digitale altrui, che realizzi un ingiusto profitto e un corrispondente danno patrimoniale, risulta ad oggi pienamente tipizzato dalla norma di cui all'art. 640-*ter* co. 3 c.p., nel diritto penale vigente non si rinviene una fattispecie tipica che punisca *ex professo* l'"apprensione" abusiva dell'altrui identità digitale, a prescindere dalla realizzazione di una frode o di un danno patrimoniale. Pur trattandosi di una fattispecie a forma libera ("alterare in

159 É la soluzione prospettata da R. Flor (2007), 899.

qualsiasi modo", "intervenire con qualsiasi modalità"; "dati, informazioni o programmi"), essa pone dei forti limiti ad una tutela piena all'identità digitale. Un primo limite potrebbe ravvisarsi già nella descrizione della condotta sanzionata nella fattispecie di frode informatica. Infatti, si è ritenuto che l'indebito utilizzo di dati non possa integrare da solo il reato di frode informatica, necessitando questo di un "intervento" modificativo sulla struttura dei dati e dunque, almeno, di un trasferimento illecito di denaro da un patrimonio all'altro (dato che solo così si avrebbe un "intervento senza diritto sui dati"). Seguendo tale impostazione dovremmo concludere che il "furto o indebito utilizzo di identità digitale" (in quanto uso illecito di dati) possa costituire soltanto un insieme di condotte strumentali alla realizzazione del fatto tipico. In realtà, la norma così formulata tutela l'identità digitale almeno nei casi (per nulla rari) in cui essa sia "rubata" o indebitamente utilizzata tramite un'azione di *hackeraggio,* rientrando quest'ultimo nella "alterazione del funzionamento di un sistema telematico" o comunque in un "intervento senza diritto su dati, informazioni, programmi". Tuttavia, per valorizzare pienamente il richiamo all'identità digitale compiuto dal più recente legislatore, e considerando che la vaghezza del dato linguistico non richiede una lettura univoca in senso di "modificazione", sembra preferibile sposare l'opposta lettura in dottrina, per cui anche il mero utilizzo di dati (tra cui *password* e *account* e quindi una "sostituzione d'identità digitale") costituisca una condotta rientrante nell'"intervento senza diritto sui dati", purché a ciò consegua un *danno* ed un *profitto*. L'indebito utilizzo di dati personali viene prevalentemente considerata in giurisprudenza alla stregua di una condotta strumentale al furto d'identità e non come condotta alternativa come sembrerebbe dalla formulazione dell'attuale art. 9 del d.l. 119/2013 così come modificato in sede di conversione. A suffragare tale punto di vista, occorre menzionare la definizione del furto d'identità proposta dall'OCSE, secondo cui esso consiste, tra l'altro, in un "uso di informazioni personali in modo non autorizzato". Anche tale definizione, infatti, sembra considerare l'"indebito utilizzo" come una sottocategoria del furto d'identità. Spunti opposti, invece, ci sono forniti dalle definizioni della dottrina di *common law* e del centro studi delle Nazioni Unite: per entrambe le definizioni, infatti, il furto d'identità digitale è visto come mera apprensione di dati, mentre l'"utilizzo" illecito di tali dati rientra tra gli elementi strutturali della "frode d'identità" (peraltro molto più affine al ruolo che il nuovo furto d'identità digitale assume nel nostro ordinamento).

Le altre fattispecie applicabili

Analoghe difficoltà applicative presenta la riconduzione dell'indebito utilizzo di identità digitale ad altre fattispecie diverse da quella di cui all'art.640 ter c.p. Nel *phishing*, ad esempio, la prima fase di realizzazione della frode, consistente nella captazione delle credenziali inducendo in errore la vittima, non può essere facilmente ricondotta né all'art. 640 c.p., né all'art. 494 c.p. (delitto di sostituzione di persona frequentemente applicato ai casi di fittizia creazione di profili personali nell'ambito di piattaforme digitali e social network), poiché nel primo caso manca quell'atto di disposizione patrimoniale da parte della vittima che si è visto essere il perno centrale

della fattispecie di truffa; quanto alla sostituzione di persona, invece, si è opportunamente obiettato che il semplice invio di una *mail* non possa costituire una effettiva "sostituzione" di "persona fisica". Controverso sarebbe altresì il tentativo di riconduzione al "furto" ex art.624 c.p., poiché mancherebbe l'effettiva "sottrazione" di una "cosa mobile altrui". Anche nell'ipotesi del *pharming*, il tentativo di riconduzione a rilevanza penale, nel pieno rispetto del principio di legalità, può essere piuttosto controverso, poiché vi è indubbiamente l'alterazione di un sistema informatico, al fine del "furto" delle credenziali, però il danno patrimoniale si realizza soltanto mediatamente: il re-indirizzamento dell'utente, infatti, non realizza *in sé*, il profitto, ma è soltanto funzionale alla captazione dei codici di accesso, e soltanto in seguito si avrà un intervento "senza diritto" aggravato dal furto dell'identità digitale altrui. L'ipotesi del *man in the middle attack*, infine, può risultare la più complessa, poiché nella prima fase esecutiva viene in rilievo la violazione della casella di posta elettronica di un soggetto, che potrebbe risultare rilevante ai sensi dell'art. 615-*ter* c.p., oppure dell'art. 616 c.p.; nella seconda fase, invece, si ha una truffa in senso tecnico, poiché mediante la creazione di una falsa apparenza si induce in errore la vittima, per il compimento di un atto patrimoniale. L'atto della captazione delle altrui credenziali potrebbe, invero, acquisire autonoma rilevanza ai sensi dell'art. 615-*quater* c.p., che espressamente sanziona la condotta di chi «al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura [...] codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza», anche se la norma contiene nuovamente un riferimento al "profitto" ed equipara nel disvalore le diverse modalità di acquisizione di tali credenziali.

A conclusione dell'analisi sulle virtualità applicative dell'art.640 ter c.p. alla tutela dell'identità digitale nel mondo FinTech emergono, dunque, non poche criticità derivanti dal fatto che la commissione in ambiente digitale delle condotte variamente collegate all'abusivo utilizzo di dati digitali non coincide sempre e comunque con la fattispecie di frode informatica di cui all'art. 640-ter co. 3 c.p. L'autonoma responsabilità amministrativa dell'ente, quando il reato-presupposto è costituito dal delitto di frode informatica, è, poi, limitato alle sole ipotesi in cui quest'ultimo sia commesso in danno dello Stato o di altro ente pubblico, ai sensi dell'art. 24-bis, comma 1, D.lgs. n. 231/2001.

5.3 La tutela penale della clientela dal rischio di frodi. Cenni e rinvio

Questa sezione dedicata alla tutela penale della clientela deve concludersi con un cenno al rischio di frodi, perpetrate ai danni degli utenti da parte di altri utenti, delle piattaforme o di terzi. Oltre alle molteplici istanze di protezione dei dati, infatti, anche la natura *finanziaria* delle operazioni richiede peculiari cautele. Invero, al tema sarà dedicato un approfondimento in un apposito volume della Collana FinTech della Consob, dedicato all'argomento dell'inclusione finanziaria. Tuttavia, a completamento di quanto osservato finora, è possibile anticipare taluni profili della questione.

Da un lato, infatti, la clientela è esposta al rischio di vere e proprie frodi, ad es. da parte di piattaforme fittizie o illegali, miranti non già a sottrarre dati, bensì direttamente denaro e investimenti: in queste ipotesi non potrà che applicarsi la fattispecie di truffa di cui all'art. 640 c.p., dato che la frode informatica, come si è anticipato, può riguardare soltanto le ipotesi in cui la condotta manipolativa abbia ad oggetto direttamente un sistema informatico. La natura *informatica* della truffa semplice potrà, allora, emergere con riferimento alla circostanza aggravante di cui all'art. 61 c.p. co. 1 n. 5: è la Corte di Cassazione a riconoscere, infatti, la specifica applicabilità - nel caso di frodi *online* – della circostanza aggravante dell'*avere l'autore del reato profittato di circostanze di luogo tali da ostacolare la pubblica o privata difesa*[160].

Dall'altro lato, poi, deve considerarsi il rischio che la clientela di servizi digitali (FinTech in senso lato) possa essere indotta – mediante condotte dissimulative o decettive – a sottoscrivere investimenti non diversificati, non adatti rispetto al profilo di rischio e di competenza finanziaria, con l'inadempimento, da parte dei gestori dei portali, dei doveri connessi alla profilatura e alla trasparenza e chiarezza delle informazioni fornite. Anche in tali casi la giurisprudenza è solita far ricorso alla fattispecie di cui all'art. 640 c.p., intercettando le caratteristiche tipologiche della situazione descritta mediante il richiamo – in funzione di integrazione della fattispecie – alle regole di condotta previste in capo agli intermediari finanziari "tradizionali"[161].

6 Il «rischio penale» per gli operatori FinTech: repressione e prevenzione

È necessario concludere l'analisi dedicando questo ultimo segmento al tema del «rischio penale» che si presenta per qualunque soggetto che si avvalga di tecnologia digitale per prestare servizi finanziari riservati: come si è anticipato in apertura, anche i profili analizzati in precedenza possono tradursi in un concreto rischio di sanzioni penali per i prestatori di servizi FinTech che pongano in essere comportamenti illeciti, con riferimento ai dati o al patrimonio della clientela. Questa sotto-sezione ha, invece, il preciso scopo di inquadrare in termini giuridici il c.d. rischio *'compliance'*, derivante dallo svolgimento di attività in settori sottoposti a

160 Cass. Pen., sez. II, sent. 29 settembre 2016, n. 43705, in Riv. pen. 2016, 12, 1104: non del *web*, che, come ripetutamente ribadito dalla stessa giurisprudenza di legittimità è un "non luogo", ma per la distanza tra il luogo in cui si è commesso il reato, dove si trovava l'agente al momento in cui ha conseguito il profitto, e il luogo in cui si trovava l'acquirente: rileva la Corte che si tratti di una caratteristica oggettiva, del tutto assimilabile ad altre contingenze pacificamente rientranti all'interno di questa circostanza aggravante. Si legge nella pronuncia, infatti che «proprio la distanza tra il luogo di commissione del reato, ove l'agente si trova ed il luogo ove si trova l'acquirente del prodotto on line [...] è l'elemento che consente all'autore della truffa di porsi in una posizione di maggior favore rispetto alla vittima, di schermare la sua identità, di fuggire comodamente, di non sottoporre il prodotto venduto ad alcun efficace controllo preventivo da parte dell'acquirente; tutti vantaggi che non potrebbe sfruttare a suo favore, con altrettanta comodità, se la vendita avvenisse *de visu*».

161 Così, *ex multis*, Cass. Pen., sez. II, sent. 23 giugno 2016, n. 29853, su dejure.it; Cass. Pen., sez. II, sent. 7 novembre 2013, n. 49446, su Dir. e Giust., 10 dicembre 2013; Cass. Pen., sez. II, 16 dicembre 2011, n. 47421, su Riv. It. Dir. Proc. Pen., 2012, 1, 363 ss.

rigida regolamentazione. Per quanto 'innovativa' e *disruptive*, infatti, la finanza tecnologica irrompe in un mercato caratterizzato da precise barriere all'ingresso – autorizzazioni, vigilanza *on-going* prudenziale nonché sul mantenimento dei requisiti organizzativi e degli standard normativi di comportamento – e da consistenti obblighi finalizzati al controllo dei flussi finanziari, con la finalità di prevenire riciclaggio e finanziamento di attività illecite. Questa ricognizione è, dunque, finalizzata a ricostruire una cornice giuridica che possa assicurare l'integrità del mercato dei servizi FinTech anche sotto il profilo anti-riciclaggio, senza contare che una maggiore chiarezza in ordine alla regolamentazione giuridica consente anche agli stessi operatori una maggiore libertà e certezza.

6.1 FinTech e correlati rischi di indebito utilizzo delle piattaforme on line a scopi di riciclaggio e finanziamento del terrorismo

Un ulteriore profilo che merita di essere sviluppato in questa sezione (ed altresì già emerso durante alcune interviste agli operatori di settore) riguarda le possibili ricadute dello sviluppo del FinTech sul tema della prevenzione dell'indebito utilizzo delle piattaforme finanziarie *on line* (le c.d. *digital financial marketplaces,* e ogni altra forma di gestione digitale di asset finanziari) a scopi di riciclaggio e finanziamento (anche internazionale) del terrorismo.

Al fine di offrire una più chiara rappresentazione dell'ambientamento tipico di questi fenomeni, è possibile collocare l'utilizzo delle piattaforme *on line* a scopo di riciclaggio[162] e finanziamento del terrorismo[163] tra i meccanismi di infiltrazione delle organizzazioni criminali nell'economia lecita. In particolare, essi costituiscono un tipico esempio dell'estrema abilità e rapidità di adeguamento della criminalità organizzata agli sviluppi della tecnologia e degli strumenti informatici; capacità, queste, che ne accrescono ulteriormente la pericolosità.

Le organizzazioni criminali sembrano infatti oggi mostrare grande interesse per i nuovi canali di finanziamento[164], alternativi a quello bancario tradizionale, di

162 Il riciclaggio di denaro può essere descritto come l'attività di riutilizzo del denaro "sporco" in attività legali, al fine di mascherarne la provenienza illecita. Il processo di riciclaggio si lascia descrivere in tre fasi. La prima fase di "piazzamento" (placement) dei proventi illeciti nel mercato interno o internazionale serve a collocare provvisoriamente i beni lontano dal locus commissi delicti, in modo da ostacolare eventuali attività d'indagine. Segue la seconda fase di "stratificazione" (layering), finalizzata a predisporre plurimi strati documentali idonei ad ostacolare il paper-trail, in particolare mediante operazioni finanziarie (es. trasferimenti internazionali di fondi, operazioni societarie in paesi off-shore etc.). Infine, per mezzo della c.d. "integrazione" (integration), i proventi ormai puliti vengono immessi in bacini di giacenza di capitali di origine lecita o in circuiti economico-finanziari legali. Cfr. F. Brizzi – G. Capecchi – A. Rinaudo, (2014), 3 ss. Si veda inoltre: D. Masciandaro (2007).

163 Il finanziamento del terrorismo, al contrario, può avere come fonte anche attività lecite. L'origine non necessariamente illecita delle disponibilità nonché l'utilizzo di somme spesso di importo esiguo rendono particolarmente complessa l'individuazione preventive delle condotte finalizzate a finanziare il terrorismo. Inoltre, il network terrorista sfrutta abilmente le potenzialità offerte dall'integrazione a livello globale dei mercati al fine di veicolare, da un Paese all'altro, i fondi essenziali per la propria attività. V. in tema B. Bandiera (2017) e M. Condemi, F. De Pasquale (2008).

164 Con la Comunicazione "Prevenzione del finanziamento del terrorismo internazionale" del 18 aprile 2016, l'Unità di Informazione Finanziaria per l'Italia (UIF) ha sottolineato che le opportunità offerte dall'innovazione tecnologica, in particolare dal web, possono essere utilizzate per finalità di finanziamento del terrorismo e riciclaggio di denaro.

recente emersi per rispondere alla difficoltà – particolarmente grave nell'ambito di una complessa congiuntura economica – delle imprese di piccole e medie dimensioni nel soddisfare il proprio fabbisogno finanziario (c.d. *funding gap*). Tra i canali di approvvigionamento emergenti si collocano le piattaforme digitali di intermediazione creditizia/finanziaria sia di tipo *peer-to-peer* sia basate su modelli di *crowdfunding,*[165]. Queste piattaforme - ove non assoggettate a regole e controlli amministrativi dedicati e grazie alla straordinaria facilità negli scambi e all'operatività a distanza possono prestarsi ad attività illegali, quali appunto il riciclaggio e il finanziamento del terrorismo[166]. Lo dimostra ad esempio il *case study,* riportato all'interno del *Report* GAFI del 2015 *"Emerging Terrorist Financing Risks"*[167], relativo ad una raccolta fondi mediante lo schema di *crowdfunding* in cui il denaro raccolto, apparentemente destinato al sostentamento e alle cure mediche per i rifugiati siriani, nonché alla costruzione di moschee, scuole ed asili, era in realtà rivolto al finanziamento dei terroristi.

Emerge dunque l'urgenza di prevenire e contrastare simili fenomeni con idonei strumenti. Eppure, il confronto diretto con i soggetti interessati restituisce un quadro poco rassicurante: dalle interviste agli operatori del settore condotte nel corso della presente ricerca, è emerso infatti come soltanto una piccola parte dei soggetti auditi abbiano predisposto opportune misure di contrasto. In questo paragrafo ci si propone, dunque, di delineare sinteticamente i rischi di riciclaggio e finanziamento del terrorismo connessi all'utilizzo abusivo delle piattaforme on-line dedicate, per procedere, poi, a tratteggiare un quadro degli strumenti che, ad oggi, si pongono in un'ottica di prevenzione di tali fenomeni.

Pur nascendo con la finalità principale di finanziare progetti imprenditoriali creativi, le piattaforme *on-line* di *crowdinvesting* sembrano prestare il fianco ad utilizzi abusivi da parte di organizzazioni criminali interessate a sfruttare i canali dell'economia legale a scopi di riciclaggio e finanziamento del terrorismo. Simili rischi sono evidenziati all'interno di una pluralità di documenti elaborati dalle Autorità nazionali e sovranazionali. Tra questi, in ambito europeo, si segnala l'*"Opinion"* in materia di *Lending based crowdfunding* emessa dall'*European Banking Authority* (EBA)[168], il documento *Questions&Answers* prodotto dall'*European Securities and Markets Authority* (ESMA) in tema di prevenzione delle attività di *money laundering* e

La Comunicazione è reperibile al link: http://uif.bancaditalia.it/pubblicazioni/comunicati/documenti/comunicazione-uif-180416.pdf .

165 Tale espressione è impiegata per indicare il finanziamento di iniziative, progetti o *start-up* da parte della folla (*crowd*) dei *web surfers* per mezzo di piattaforme *on-line*. Il concetto di crowdfunding e la sua connessione con il crowdsourcing è approfondito in A. Fregonara (2014), 4 ss. In proposito inoltre, A. Laudonio (2016), 113 ss. Deve inoltre considerarsi la recente e sempre più rilevante emersione di vere e proprie *exchange platforms* che supportano le operazioni di emissione di cripto asset.

166 Sul punto v. lo studio condotto la L. Bonucci (2017), reperibile su https://www.cssii.unifi.it/upload/sub/bonucci_finanziamento-del-terrorismo-e-money-transfer.pdf.

167 Il documento è reperibile al sito: www.fatf-gafi.org/publications/methodsandtrends/documents/emerging-terrorist-financing-risks.html .

168 Cfr. EBA/Op/2015/03, reperibile su www.eba.europa.eu, 26 febbraio 2015, par. 85, 23: «The risks of money laundering, terrorist financing and financial crime are primarily related to the borderless nature and potential anonymity of borrower/lenders carrying out transactions on a peer-to-peer basis that do not require personal identification».

terrorist financing nell'ambito dell'*investment-based crowdfunding*[169], nonché, da ultimo, la *Relazione* SRNA (*Supra National Risk-Assessment*) sull'antiriciclaggio pubblicata dalla Commissione europea allo scopo di orientare le autorità degli Stati membri verso una migliore gestione del c.d. *ML* (*Money Laundering*) *and FT* (*Financing Terrorism*) *risk*[170], secondo quanto previsto dall'art. 6 della *IV Direttiva Antiriciclaggio* (Dir. 2015/849/UE)[171]. In ambito internazionale, particolarmente degno di nota è il documento prodotto nell'ottobre 2015 da parte del *Gruppo di azione finanziaria internazionale* (GAFI-FAFT)[172], in cui, anche attraverso casi studio, sono enucleate particolari modalità di utilizzo di piattaforme *on-line* di *crowdfunding* a scopi di finanziamento del terrorismo; le indicazioni ivi contenute, oltre ad aver ispirato la più recente normativa europea in materia di contrasto al finanziamento del terrorismo e al riciclaggio di proventi da reato[173], sono state fatte proprie, in ambito nazionale, dalla Comunicazione del 18 aprile 2016 dell'Ufficio di Informazione Finanziaria per l'Italia (UIF).

Questi documenti mettono in luce come siano le stesse caratteristiche alle quali il *crowdinvesting* deve il proprio successo a renderlo anche particolarmente attrattivo per le organizzazioni criminali: a) operatività a distanza, anche *cross-border*; b) limitata o inesistente *due diligence* sugli ideatori dei progetti ovvero sui progetti stessi[174]; c) breve durata degli investimenti; d) possibilità di fenomeni di *early redemption* degli investimenti.

In proposito appare inoltre opportuno segnalare come la nascita di accordi collusivi tra ideatori del progetto e investitori, oppure tra gestori della piattaforma e investitori, finalizzati a pulire fondi di provenienza illecita, possa risultare connessa all'utilizzo di piattaforme improntate al c.d. *principio all-or-nothing*. Questo modello di piattaforma, in sé perfettamente lecito, potrebbe prestarsi a schemi criminali finalizzati all'occultamento e al lavaggio di capitali illeciti: così nel caso in cui fondi di origine criminosa vengano prestati in misura tale da non raggiungere

169 Si veda ESMA/2015/1005, Questions and Answers. Investment-based crowdfunding: money laundering/terrorist financing, reperibile su https://www.esma.europa.eu , 1 luglio 2015, 4 ss.

170 COM/2017/340, Report from the Commission to the European Parliament and the Council on the assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border activities, Brussels, 26 giugno 2017, 55 ss., su http://eur-lex.europa.eu/legal-content/en/txt/?uri=com:2017:340:fin.

171 L'art. 6 della IV Direttiva Antiriciclaggio prevedeva che la Commissione, entro il 26 giugno 2017, elaborasse una relazione tesa ad identificare e valutare i rischi di riciclaggio e finanziamento del terrorismo a livello dell'Unione. Lo scopo era di formulare raccomandazioni agli Stati membri riguardo alle misure idonee ad affrontare i rischi individuati. Al comma 5 dello stesso articolo è stabilito che «qualora gli Stati membri decidano di non applicare alcuna delle raccomandazioni nei rispettivi sistemi nazionali di AML/CFT lo notificano alla Commissione fornendone una motivazione».

172 Si tratta del già citato Report "Emerging Terrorist Financing Risks" del 2015.

173 In proposito L. Borlini (2017), 356 ss.

174 Motivi economici di fattibilità sembrano non consentire di impostare, a carico dei gestori dei portali, pratiche di regolare due diligence, come invece accade nelle operazioni di finanza internazionale. Cfr. in proposito D. Isenberg (2012) reperibile al sito https://hbr.org/2012/04/the-road-to-crowdfunding-hell.

(volutamente) il *target* di raccolta predefinito, in modo tale da dare avvio ad una loro pronta restituzione[175].

Il sistema di prevenzione del finanziamento del terrorismo e di riciclaggio dei capitali illeciti appare ad oggi caratterizzato da un profondo disallineamento tra raccomandazioni internazionali del FAFT-GAFI, normativa europea e discipline vigenti nell'ambito dei singoli Stati membri[176]. Considerata la transnazionalità dei fenomeni di cui ci si occupa, pare infatti che solo la migliore armonizzazione possa frapporsi in modo efficace ed efficiente, in termini preventivi e repressivi, alle condotte illecite.

La V Direttiva Antiriciclaggio (Dir. 2018/843/UE) mostra la consapevolezza del problema: emerge, al *Considerando* n. 2, la necessità di fronteggiare nuove tendenze, dato che «*taluni servizi basati sulle moderne tecnologie stanno diventando sempre più popolari come sistemi finanziari alternativi*». Modificando la precedente direttiva 2015/849/UE, si è dunque deciso di aggiungere all'elenco dei soggetti obbligati ai presidi antiriciclaggio anche i prestatori di servizi la cui attività consiste nella fornitura di servizi di cambio tra valute virtuali e valute aventi corso forzoso (lett. g) e i prestatori di servizi di portafoglio digitale (lett. h), sia pur con la consapevolezza che ciò non risolva completamente il problema dell'anonimato e della non tracciabilità delle operazioni. Ad esempio, la direttiva tuttora non contiene un obbligo di estensione dei presidi antiriciclaggio ai gestori di piattaforme *crowdfunding* e *crowdinvesting.* Rimane intatta, nella direttiva 2015/849/UE, la previsione di cui all'art. 4: «*gli Stati membri provvedono a estendere, secondo un approccio basato sul rischio, in tutto o in parte, l'ambito di applicazione della presente direttiva ad attività professionali e categorie di imprese diverse dai soggetti obbligati di cui all'articolo 2, paragrafo 1, le quali svolgono attività particolarmente suscettibili di essere utilizzate a fini di riciclaggio di denaro o di finanziamento del terrorismo*». A tal proposito la Commissione Europea, all'interno del *Report* sul *risk-assessment* (SNRA) in materia di AML (*Anti-money laundering*) e CFT (*Combating the Financing of Terrorism*), avendo rintracciato livelli *significant* di *vulnerability* delle piattaforme *crowdfunding*, ha previsto che gli Stati membri «*when applying article 4 of the 4AML Directive for extending the scope of obliged entities*» dovrebbero considerare «*the need to define crowdfunding platforms as obliged entities to be subject to AML/CFT requirements*».

Il nostro Paese può invero già considerarsi allineato alle indicazioni della Commissione. Richiamando il quadro normativo dell'*equity based crowdfunding*, l'operatività dei presidi antiriciclaggio e antiterrorismo di cui al D.Lgs. n. 231/2007 (tra cui identificazione degli investitori, registrazione dei dati e segnalazione delle

175 Cfr. in proposito la ricostruzione offerta in www.compliancejournal.it/governance-e-rischio-di-riciclaggio-connesso-a-piattaforme-di-crowdfunding/ (31 gennaio 2017).

176 Questo disallineamento emerge con particolare evidenza all'interno del "Discussion Paper on the EBA's approach to financial technology (FinTech)" del 4 agosto 2017, in particolare al punto 61 (https://www.eba.europa.eu/documents/10180/1919160/EBA+Discussion+Paper+on+Fintech+%28EBA-DP-2017-02%29.pdf). Dal documento emerge peraltro che l'EBA, insieme all'ESMA e all'EIOPA, sta predisponendo un'opinion sull'uso di FinTech per contrastare il riciclaggio e il finanziamento del terrorismo.

operazioni sospette alla UIF[177], in presenza di indicatori di anomalia[178]) vorrebbe essere garantita dal mantenimento dell'onere di attivazione dei tradizionali presidi antiriciclaggio e antiterrorismo in capo agli intermediari bancari e finanziari di cui i gestori dei portali sono obbligati ad avvalersi. In materia di *social lending,* gli obblighi di cui al D.Lgs. 231/2007 ricadono invece direttamente in capo ai gestori delle piattaforme: questi ultimi, potendo operare solamente in qualità di Istituti di Pagamento, Istituti di Moneta Elettronica oppure come Intermediari Finanziari *ex* art. 106 TUB, autorizzati a prestare servizi di pagamento, ricadono infatti tra i soggetti sottoposti, ai sensi dell'art. 3 d.lgs. 231/2007, agli obblighi antiriciclaggio.

In estrema sintesi, il *framework* legale di contrasto[179] all'indebito utilizzo di piattaforme di *crowdinvesting* per scopi di riciclaggio e finanziamento del terrorismo nel nostro ordinamento è così composto:

1. Obblighi antiriciclaggio – in particolare obblighi di identificazione[180] – di cui al D.Lgs. 231/2007[181], come modificato dal D.Lgs. 90/2017, posti a carico dei gestori delle piattaforme di *social lending* e degli intermediari autorizzati incaricati della raccolta di fondi nell'ambito *dell'equity crowdfunding,* e relative

177 Come noto, la UIF è la struttura nazionale incaricata di richiedere e ricevere rapporti ed informazioni dai soggetti obbligati (art. 6 D.Lgs. 231/2007). Essa effettua l'analisi finanziaria delle segnalazioni ricevute (artt. 6, comma 6, lett. b e 47, comma 1, lett. a) al fine di comprendere, sulla base dell'insieme degli elementi acquisiti, il contesto all'origine della segnalazione, individuare i collegamenti soggettivi e operativi, ricostruire il percorso dei flussi finanziari segnalati come sospetti e identificare le possibili finalità sottostanti; a tali fini può acquisire ulteriori informazioni presso i soggetti obbligati, avvalersi degli archivi ai quali ha accesso, scambiare informazioni con omologhe autorità estere (FIU). Al termine dell'analisi finanziaria, la UIF trasmette le segnalazioni, corredate di una relazione tecnica, al Nucleo Speciale di Polizia Valutaria della Guardia di Finanzia (NSPV) e alla Direzione Investigativa Antimafia (DIA) per gli eventuali approfondimenti investigativi; comunica all'Autorità Giudiziaria i fatti di possibile rilevanza penale; archivia le segnalazioni che reputa infondate, dandone comunicazione al segnalante mediante un flusso di ritorno (art. 9, comma 9 e 10; art. 47, comma 1, lett. c) e d); art. 48, comma 1).

178 La UIF, con la Comunicazione del 18 aprile 2016 già richiamata, ha indicato le nuove modalità di finanziamento del terrorismo: oltre ai canali tradizionali, costituiti dalle organizzazioni nonlucrative e dai money transfer, sono state messe in luce tecniche innovative quali la raccolta di fondi on line attraverso piattaforme di crowdfunding e il ricorso alle valute virtuali. In proposito v. anche il documento prodotto nell'ottobre 2016 dalla Commissione di studi "Antiriciclaggio" del CNDCEC (reperibile sul sito del CNDCEC, www.cndcec.it), in cui si dice espressamente che «la presenza congiunta di operatività finanziarie in cui gli strumenti del money transfer, delle valute virtuali e delle piattaforme di crowdfunding siano presenti è già di per sé una indicazione di anomalia da valutare con grande attenzione sia ai fini dell'obbligo di adeguata verifica che dell'obbligo di segnalazione di operazioni sospette».

179 Si segnala peraltro che, nel suo complesso, il sistema italiano di contrasto al riciclaggio nell'ultimo Rapporto FATF-GAFI (10 febbraio 2016) è definito «maturo, sofisticato e assistito da un robusto assetto normativo e istituzionale» e, dunque, pienamente conforme agli standard internazionali). Il Rapporto e la sua sintesi sono pubblicati sul sito del GAFI (http://www.fatf-gafi.org/countries/d-i/italy/documents/mer-italy-2016.html). Una traduzione (non ufficiale) in lingua italiana è stata predisposta dalla V Direzione del Dipartimento del Tesoro (http://www.dt.tesoro.it/export/sites/sitodt/modules/documenti_it/prevenzione_reati_finanziari/prevenzione_reati_finanziari/rapporto_di_valutazione_aml-cft_-_versione_in_italiano.pdf).

180 V. art. 19 D.Lsg. n. 231/2007.

181 Si ricorda che le disposizioni previste dal D.Lgs. 231/2007 mettono sullo stesso piano normativo la prevenzione e il contrasto del riciclaggio e del finanziamento al terrorismo, senza operare specifiche distinzioni sotto il profilo giuridico. Ne consegue che l'esperienza in materia di prevenzione e contrasto al riciclaggio trova piena e completa applicazione con riferimento ai presidi per il contrasto del finanziamento al terrorismo. Per un quadro completo del sistema antiriciclaggio in Italia v. S. Capolupo - M. Carbone - G. Sturzo (2015); S. De Flemmitis (2017).

disposizioni sanzionatorie di ordine penale (art. 55) e amministrativo (art. 56-69) previste per il caso di contravvenzione agli stessi obblighi[182].

2. Misure di congelamento dei fondi e delle risorse economiche[183], predisposte, ai sensi del D.Lgs. 109/2007, come modificato dal D.Lgs. 90/2017, dal Ministro dell'Economia e delle Finanze (di concerto con il Ministro degli Affari Esteri, e su proposta del Comitato di Sicurezza Finanziaria), nei confronti di persone fisiche, giuridiche, gruppi o entità, designati dal Consiglio di sicurezza dell'ONU o da un suo Comitato, secondo i criteri e le procedure stabiliti dalle risoluzioni adottate ai sensi del Capitolo VII della Carta delle Nazioni Unite.

3. Misure di prevenzione personali e patrimoniali contenute nel c.d. *Codice Antimafia* (D.Lgs. n. 159/2011), disposte dall'autorità giudiziaria nei confronti delle categorie di soggetti indicate agli artt. 4 e 16[184].

4. Normativa penale applicabile alle persone fisiche, contenuta all'interno del codice penale e nella legislazione speciale (v. ad esempio il reato di trasferimento fraudolento di valori, di cui all'art. 12-*quinquies,* L. 356/1992),

182 Secondo i criteri dettati della legge delega 170/2016 (art. 15, lett. h, no. 1), la riforma delle disposizioni penali del d.lgs. 231/2007 aveva l'obiettivo di selezione e riduzione dell'area di rilevanza penalistica, anche in considerazione del principio del ne bis in idem in relazione all'articolato apparato sanzionatorio amministrativo. Il legislatore delegato, infatti, aveva il compito di «limitare la previsione di fattispecie incriminatrici alle sole condotte di grave violazione degli obblighi di adeguata verifica e di conservazione dei documenti, perpetrate attraverso frode o falsificazione, e di violazione del divieto di comunicazione dell'avvenuta segnalazione, prevedendo sanzioni penali adeguate alla gravità della condotta e non eccedenti, nel massimo, tre anni di reclusione e 30.000 euro di multa». Dal confronto tra il nuovo art. 55 d.lgs. 231/2007 e il precedente, emerge in primo luogo la semplificazione e la riduzione delle fattispecie con l'abbandono (quasi) totale della tecnica del rinvio che caratterizzava il sistema previgente. La semplificazione è stata ottenuta non solo con l'opportuno cambiamento della tecnica di redazione delle norme, ma anche limitando l'area di rilevanza penale a condotte caratterizzate da un maggiore disvalore, con la costruzione di nuove fattispecie delittuose, per quanto riguarda i reati più strettamente legati agli obblighi gravanti sugli operatori. In particolare, con il D.Lgs. 90/2017 è stata prevista la sanzione penale (reclusione da 6 mesi a 3 anni e multa da euro 10.000 a euro 30.000) anche nei confronti di chi, essendo tenuto all'osservanza degli obblighi di adeguata verifica, in occasione dell'adempimento degli stessi, "utilizza" dati e informazioni falsi relativi al cliente, al titolare effettivo, all'esecutore, allo scopo e alla natura del rapporto continuativo o della prestazione professionale e all'operazione (art. 55, comma 1). Lo stesso D. Lgs. ha importato una generale riduzione dell'importo delle sanzioni amministrative. Sul punto v. A. Alessandri (2016), 374 ss., nonché F. Antonacchio - G. Miccoli (2016) e T. Giacometti – O. Formenti (2017).

183 Il congelamento di fondi consiste nel divieto di movimentazione, trasferimento, modifica, utilizzo o gestione o accesso ad essi, così da modificarne il volume, l'importo, la collocazione, la proprietà, il possesso, la natura, la destinazione o qualsiasi altro cambiamento che consente l'uso degli stessi, compresa la gestione di portafoglio. Il congelamento di risorse economiche si traduce nel divieto di trasferimento, disposizione o utilizzo, compresi, a titolo esemplificativo, la vendita, la locazione, l'affitto o la costituzione di diritti reali di garanzia, pena la nullità dei relativi atti. I soggetti che devono attuare le misure di congelamento disposte dalle autorità sono alcuni dei destinatari della normativa antiriciclaggio, principalmente intermediari finanziari e professionisti giuridico-economici.

184 In particolare, il D.L 7/2015, c.d. "decreto antiterrorismo" ha modificato la fattispecie di pericolosità prevista dall'art. 4, c. 1, lett. d) del D.Lgs. 159/2011 (c.d. "Codice antimafia"), inserendo una nuova categoria di destinatari delle misure di prevenzione: «coloro che, operanti in gruppi o isolatamente, pongano in essere atti preparatori, obiettivamente rilevanti, diretti a ... a prendere parte ad un conflitto in territorio estero a sostegno di un'organizzazione che persegue le finalità terroristiche di cui all'articolo 270-sexies del codice penale». L'art. 16 estende poi l'ambito di applicazione delle misure di prevenzione patrimoniale non solo ai soggetti indicati nell'art. 4, che richiama anche l'art. 1 (soggetti a pericolosità generica), ma anche alle persone fisiche e giuridiche segnalate al Comitato per le sanzioni delle Nazioni Unite, o ad altro organismo internazionale competente per disporre il congelamento di fondi o di risorse economiche, quando vi sono fondati elementi per ritenere che i fondi o le risorse possano essere dispersi, occultati o utilizzati per il finanziamento di organizzazioni o attività terroristiche, anche internazionali (lett. b).

comprensiva di una nutrita schiera di fattispecie di reato in materia di terrorismo (da ultimo è stato aggiunto il delitto di *finanziamento di condotte con finalità di terrorismo*, di cui all'art. 270-*quinquies*.1 c.p.) [185], riciclaggio (art. 648-*bis* c.p.), reimpiego (art. 648-*ter* c.p.) e autoriciclaggio (art. 648-*ter.1* c.p.).

5. Misure in tema di sequestro e confisca, contenute sia nel codice penale (in particolare, art. 270-*septies* c.p. e art. 648-*quater* c.p.)[186], sia all'interno della legislazione speciale. Con riferimento a quest'ultima, il D.Lgs. 202/2016, di attuazione della Direttiva europea 2014/42/UE in materia di congelamento e confisca dei beni strumentali e dei proventi da reato[187], ha esteso l'applicazione della confisca c.d. *allargata* o *per sproporzione*, prevista all'interno dell'art. 12-*sexies*, L. 356/1992, – già applicabile in caso di ricettazione, riciclaggio e reimpiego – al reato di autoriciclaggio; con lo stesso D.Lgs. il legislatore ha precisato, così da fugare ogni dubbio interpretativo, che l'istituto della confisca allargata trova applicazione anche con riguardo ai delitti commessi per finalità di terrorismo "internazionale"[188].

6. Normativa in materia di responsabilità da reato degli enti (D.Lgs. 231/2001), che prevede l'applicazione di sanzioni pecuniarie e interdittive, nonché la confisca obbligatoria del prezzo o del profitto del reato, agli enti nel cui ambito siano

185 La L. 153/2016 (intervenuta a brevissima distanza dal D.L. 7/2015, conv. L. 43/2015) adegua il nostro ordinamento agli impegni internazionali in materia di contrasto al terrorismo, aggiungendo alla già copiosa costellazione di fattispecie incriminatrici il delitto di finanziamento di condotte con finalità di terrorismo (art. 270-quinquies.1 c.p.), che punisce «chiunque raccolga, eroghi o metta a disposizione beni o denaro, in qualunque modo realizzati, destinati a essere in tutto o in parte utilizzati per il compimento di condotte con finalità di terrorismo» e «chiunque depositi o custodisca i medesimi beni o il denaro», nonché il delitto di sottrazione di beni o denaro sottoposti a sequestro (art. 270-quinquies.2, c.p.), che invece punisce «chiunque sottrae, distrugge, disperde, sopprime o deteriora beni o denaro, sottoposti a sequestro per prevenire il finanziamento delle condotte con finalità di terrorismo». In tema v. V. Aragona (2017).

186 La L. 153/2016 ha introdotto una nuova ipotesi di confisca obbligatoria, diretta e per equivalente, per tutti i reati commessi con finalità di terrorismo (art. 270-septies c.p.). L'art. 648-quater c.p. a sua volta prevede che, nel caso di condanna o di applicazione della pena su richiesta delle parti per i reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, autoriciclaggio, sia sempre ordinata la confisca dei beni che ne costituiscono il prodotto o il profitto (anche per equivalente), salvo che appartengano a persone estranee al reato. L'art. 5 D.Lgs. 90/2017, all'art. 5, "ribadisce" l'operatività dell'art. 648-quater c.p., nonché dell'art. 25-octies del d.lgs. 231/2001 sulla responsabilità degli enti per lo stesso ordine di reati. Nella prima versione del decreto pubblicata in Gazzetta Ufficiale, probabilmente per un errore nella redazione della norma, questi articoli erano "ribaditi" omettendo ogni riferimento all'autoriciclaggio (art. 648-ter.1 c.p.). Da ciò sarebbero, inevitabilmente, derivate due rilevanti conseguenze: l'eliminazione dell'autoriciclaggio dal catalogo dei reati presupposto della responsabilità dell'ente e l'eliminazione della possibilità di disporre l'ipotesi di confisca speciale, anche per equivalente, in relazione a tale reato. All'esito di tale intervento normativo poteva persino ipotizzarsi l'abrogazione (tacita) dell'art. 648-ter.1 c.p., in ragione della tecnica redazionale adoperata nel "nuovo" testo dell'art. 72 d.lgs. 231/2007, che prevedeva testualmente l'inserimento nel codice penale dell'art. 648-quater «dopo l'art. 648-ter», facendo così "rivivere" la disciplina penalistica della materia anteriore alla l. 186/2014 (che ha introdotto il delitto di autoriciclaggio). Nei giorni di vacatio legis tale imprevista quanto dirompente conseguenza è stata prontamente segnalata da attenta dottrina; il legislatore ha posto rimedio tempestivo alla propria vistosa distrazione, pubblicando, nella Gazzetta Ufficiale del 28 giugno 2017, una rettifica al testo del d.lgs. 90/2017, con la ri-collocazione dell'autoriciclaggio tra gli articoli richiamati dalle due norme in questione. Ciò consente di fugare in radice ogni dubbio sulla persistente vigenza dell'art. 648-ter.1 c.p., sia come autonoma fattispecie delittuosa (i cui proventi sono passibili di confisca a mente dell'art. 648-quater c.p.), sia quale illecito rientrante nel catalogo dei reati-presupposto della responsabilità da reato degli enti ex d.lgs. 231/2001.

187 Per un quadro completo v. A. Marandola (2016); N. Selvaggi (2015); A. Maugeri (2014).

188 V. T. Trinchera (2016).

commessi delitti con finalità di terrorismo (art. 25-*quater*)[189] e delitti di riciclaggio, reimpiego e autoriciclaggio (art. 25-*octies*)[190].

6.2 Il rischio di svolgimento di attività non autorizzata: profili sanzionatori dell'abusivismo nella finanza digitalizzata

Coerentemente con i temi affrontati nei precedenti sotto-paragrafi, si tratta ora di calare il fenomeno FinTech all'interno della disciplina del TUB e del TUF per cogliere eventuali profili di *abusivismo* nell'esercizio dell'attività finanziaria "digitalizzata"[191]. L'adozione di una prospettiva penalistica nell'indagine del fenomeno FinTech, infatti, impone anche di valutarne l'effettiva liceità sulla base della normativa vigente, nel tentativo di mediare tra le istanze di sviluppo tecnologico e l'essenziale tutela (anche penale) del risparmio. Occorre, dunque, verificare la compatibilità di tali operazioni con le riserve di attività nel settore dei servizi bancari e finanziari, considerando che una più compiuta delimitazione del rischio penale consentirebbe anche agli stessi operatori una maggiore libertà[192].

Com'è noto, infatti, il diritto delle attività bancarie, finanziarie e di intermediazione nel mercato dei valori mobiliari, prevede una regolamentazione molto stringente: la rilevanza degli interessi coinvolti ha reso necessario porre una riserva, per lo svolgimento di tali attività, a favore di soggetti opportunamente organizzati, autorizzati e vigilati[193], e ha reso necessario altresì porre a presidio di tale riserva (anche) la sanzione penale. Il bene giuridico tutelato mediante la repressione delle condotte abusive è stato variamente ricostruito, ma è chiara la convergenza indiretta della tutela sul bene del patrimonio dei risparmiatori, in una dimensione superindividuale: si tratta di un bene di rilevanza tale da legittimare il ricorso allo strumento penale, in funzione di tutela preventiva.

La disciplina del controllo all'accesso sul mercato è, pertanto, «omogeneamente estesa a tutte le forme di movimentazione del denaro in ambito finanziario: sia la raccolta del risparmio, sia l'erogazione del credito, sia l'intermediazione finanziaria, sia la gestione dei servizi di investimento del risparmio, sono sottoposte a uno statuto penale che rafforza i meccanismi di selezione, volti a consentire l'ingresso nel mercato ai soli soggetti i cui requisiti di professionalità ed onorabilità sono stati previamente vagliati dagli organi di vigilanza, per poter poi

189 Da ultimo sull'argomento v. R. Sabia (2017).

190 Sul tema sia consentito di rinviare a M. Galli (2016) e N. Amore (2016).

191 Sul tema dell'abusivismo in generale cfr. da ultimo E. Basile (2017).

192 Cfr. R. M. Lacasse, B.A. Lambert, E. Osmani, C. Couture, N. Roy, J. Sylvain, F. Nadeau (2016), 2: un sondaggio realizzato dal Wall Street Journal nel 2015 tra gli operatori di servizi finanziari digitalizzati ha identificato nell'assente o confusa regolazione uno tra i principali ostacoli per la crescita e l'affermazione del FinTech.

193 Si rinvia, tra tutti, a F. Giorgianni, C.M Tardivo (2009), 240 ss.: per l'esercizio delle attività bancarie e finanziarie occorre un'apposita autorizzazione, fondata sul rispetto di una pluralità di condizioni, tra cui l'adozione di determinati tipi societari, l'ammontare minimo del capitale versato, requisiti di onorabilità, professionalità e indipendenza dei soggetti con funzioni di amministrazione e direzione, l'adesione a sistemi di garanzia dei depositi, che, in sostanza, assicurino una sana e prudente gestione.

procedere a controlli e verifiche sulla regolarità della gestione»[194]. È evidente come le attività prestate nel contesto del FinTech siano pericolosamente limitrofe rispetto alle diverse aree presidiate dalla sanzione penale: si rende, pertanto, necessaria una ricostruzione sistematica, per individuare i profili di rischio cui si espongano gli operatori con la prestazione di tali servizi al di fuori del perimetro degli intermediari autorizzati.

Le varie fattispecie di abusivismo che occorre prendere in considerazione si ritrovano disseminate in una pluralità di *corpora* normativi, in particolare TUB (d. lgs. 385/1993) e TUF (d. lgs. 58/1998), in parte adottati in attuazione di direttive europee: la varietà delle attività di finanza tecnologica ne richiede un'elencazione completa.

Quanto alla gestione di servizi di natura *lato sensu* finanziaria, l'art. 166 TUF, nella sua formulazione più recente[195], al co. 1 punisce con la reclusione da uno a otto anni e con la multa da euro quattromila a euro diecimila chiunque, senza esservi abilitato ai sensi di tale decreto, (a) svolga servizi o attività di investimento o di gestione collettiva del risparmio, (b) offra in Italia quote o azioni di OICR, (c) offra fuori sede, ovvero promuova o collochi mediante tecniche di comunicazione a distanza, prodotti finanziari o strumenti o servizi o attività di investimento, (c bis) svolga servizi di comunicazione dati; inoltre, il co. 2 prevede la stessa pena per chiunque eserciti l'attività di consulente finanziario, abilitato all'offerta fuori sede, senza essere iscritto nell'albo indicato dall'art. 31 TUF. Un'altra ipotesi che non può essere trascurata, nell'ambito del TUF, pur se configurata come mero illecito amministrativo, consiste nella c.d. sollecitazione abusiva all'investimento, di cui all'art. 191, ove si sanziona l'inosservanza delle norme che disciplinano l'offerta al pubblico di strumenti o prodotti finanziari. Si tratta di due disposizioni particolarmente rilevanti, poiché sono entrambe riferite genericamente al "prodotto finanziario", categoria non tipizzata[196], che rende tali norme potenzialmente applicabili anche alle operazioni finanziarie atipiche, quali possono essere considerate alcune attività FinTech. Per far riferimento a un caso concreto[197], l'art. 191 TUF è stato applicato per sanzionare la condotta di alcuni soggetti che, tramite una serie di siti *internet*, offrivano al pubblico una moneta digitale di nuovo conio: la Corte di Cassazione ha escluso la possibilità di ricomprendere tale "valuta" nel concetto di "moneta" (essendo la potestà di emissione e gestione del valore monetario esclusiva espressione di una funzione pubblica) e l'ha qualificata, invece, come "prodotto finanziario", ovvero "investimento a titolo oneroso", con la conseguente irrogazione della sanzione per l'abusiva sollecitazione all'investimento, tramite siti internet. Inoltre, occorre richiamare un'ulteriore disposizione recentemente introdotta[198]: l'art. 7-*octies* TUF, infatti, attribuisce alla Consob penetranti poteri di contrasto

194 Così P. Severino di Benedetto (1988), 1526. V. anche T. Padovani (1995), 634 ss.

195 L'art. 166 TUF, infatti, è stato oggetto di recentissima riforma da parte del d. lgs. 129/2017, in attuazione della direttiva 2014/65/UE del Parlamento europeo e del Consiglio, del 15 maggio 2014, relativa ai mercati degli strumenti finanziari; sul tema v., ad es., M. De Poli (2017).

196 Ai sensi dell'art. 1 co. 1 lett. u) TUF sono "prodotti finanziari" gli strumenti finanziari e ogni altra forma di investimento di natura finanziaria.

197 Cfr. Cass. civ., sez. II, sent. 02 dicembre 2011, n. 25837, in Giust. civ., 2012, 1, I, 29, con nota di L. Ciafardini.

198 L'art. 7-octies TUF è stato anch'esso introdotto con il già ricordato d. lgs. 129/2017.

all'abusivismo, dal momento che essa può, nei confronti di chiunque offre o svolge servizi o attività di investimento tramite la rete internet senza esservi abilitato, (a) rendere pubblica tale circostanza, anche in via cautelare, e soprattutto (b) ordinare di porre termine alla violazione.

Nell'ambito della raccolta di capitale di debito, invece, una prima norma da prendere in considerazione è l'art. 130 TUB, che sanziona in via contravvenzionale lo svolgimento non autorizzato di "attività di raccolta del risparmio tra il pubblico", intendendosi, con un richiamo all'art. 11 TUB, "l'acquisizione di fondi con obbligo di rimborso, sia sotto forma di depositi sia sotto altra forma". Un'altra fattispecie rilevante si ritrova nel successivo art. 131 TUB: si tratta di un'ipotesi di delitto che punisce chi svolge attività bancaria senza autorizzazione, intendendosi per "attività bancaria" il contestuale svolgimento di attività di raccolta del risparmio e di erogazione del credito. Le disposizioni successive, gli artt. 131-*bis* e 131-*ter* TUB sanzionano penalmente l'abusiva emissione di moneta elettronica e l'abusiva attività di prestazione di servizi di pagamento, in violazione delle specifiche riserve e delle necessarie autorizzazioni. Infine, l'art. 132 TUB punisce il reato di abusiva attività finanziaria, con essa intendendosi l'intermediazione nello scambio di strumenti del mercato monetario; a necessaria integrazione della norma occorre, infatti, richiamare l'art. 106 TUB, che ricomprende nella nozione di attività finanziaria la "concessione di finanziamenti sotto qualsiasi forma".

Già a un primo sguardo si può facilmente notare come le attività della *financial technology* si intersechino con il mercato regolamentato, pur non facendo uso di strumenti direttamente riconducibili ai modelli tipici tradizionali: è opportuno, quindi, evidenziare le potenziali criticità derivanti dalla prestazione di servizi che si sovrappongano con le attività riservate. L'assenza di una specifica regolamentazione generale, infatti, e la conseguente necessità di far riferimento alla normativa vigente, non consentono, allo stato attuale, di ritenere con certezza lecite le diverse prestazioni di finanza digitale. In relazione ad alcuni settori specifici, tuttavia, in particolare il *social lending* e l'*equity-based crowdfunding*, è possibile pronunciarsi con maggiore precisione, grazie ad alcuni interventi puntiformi delle autorità di vigilanza, finalizzati a risolvere questa pericolosa intersezione tra la stringente regolazione e i servizi di FinTech.

Un primo intervento normativo che è necessario integrare con la ricognizione della regolazione generale è il *Provvedimento recante disposizioni per la raccolta del risparmio dei soggetti diversi dalle banche* adottato da Banca d'Italia l'8 novembre 2016, con particolare riferimento alla sezione IX, dedicata al *social lending*. Per la prima volta è possibile rinvenire un interessante riferimento espresso ai profili di tali "nuove" forme di abusivismo. In un'ottica di progressiva "emersione" dei fenomeni oggetto della presente ricerca dal vuoto normativo nel quale ad oggi prevalentemente si trovano, la ricordata Sezione del documento fa espressamente riferimento al *social lending* (o *lending based crowdfunding*) definendolo alla stregua dello "*strumento attraverso il quale una pluralità di soggetti può richiedere a una pluralità di potenziali finanziatori, tramite piattaforme on-line, fondi rimborsabili per uso personale o per finanziare un progetto*". L'operatività dei gestori dei portali *on-*

line che svolgono attività di intermediazione creditizia e di coloro che prestano o raccolgono fondi tramite i suddetti portali viene consentita nel rispetto delle norme che regolano le attività riservate dalla legge a particolari categorie di soggetti (ad esempio, attività bancaria, raccolta del risparmio presso il pubblico, concessione di credito nei confronti del pubblico, mediazione creditizia, prestazione dei servizi di pagamento). Con specifico riferimento alla raccolta del risparmio tra il pubblico, il documento citato della Banca d'Italia rammenta che tale attività è vietata, in linea di principio e salve le eccezioni di seguito richiamate, sia ai gestori sia ai prenditori. Peraltro, valgono anche per detti soggetti le deroghe al divieto di raccolta di risparmio tra il pubblico previste dall'art. 11 del TUB, nel rispetto di modalità e limiti che vengono puntualmente esemplificati.

Per ritagliare con maggiore determinatezza le aree di liceità dell'attività svolta, si fa palese che, per quanto riguarda i gestori, non costituisce raccolta di risparmio tra il pubblico:

- la ricezione di fondi da inserire in conti di pagamento utilizzati esclusivamente per la prestazione dei servizi di pagamento dai gestori medesimi, se autorizzati a operare come istituti di pagamento, istituti di moneta elettronica o intermediari finanziari di cui all'art. 106 del TUB autorizzati a prestare servizi di pagamento ai sensi dell'art. 114-novies, comma 4, del TUB;
- la ricezione di fondi connessa all'emissione di moneta elettronica effettuata dai gestori a tal fine autorizzati.

Per quanto riguarda, invece, i prenditori, non costituisce raccolta di risparmio tra il pubblico:

- l'acquisizione di fondi effettuata sulla base di trattative personalizzate con i singoli finanziatori. Al riguardo, avute presenti le modalità operative tipiche delle piattaforme on-line di *intermediazione creditizia*, le trattative possono essere considerate personalizzate allorché i prenditori e i finanziatori sono in grado di incidere con la propria volontà sulla determinazione delle clausole del contratto tra loro stipulato e il gestore del portale si limita a svolgere un'attività di supporto allo svolgimento delle trattative precedenti alla formazione del contratto.
  Per non incorrere, dunque, nell'esercizio abusivo della raccolta del risparmio la Banca d'Italia richiede che i prenditori si avvalgano esclusivamente di piattaforme che assicurano il carattere personalizzato delle trattative e sono in grado di dimostrare il rispetto di tale condizione anche attraverso un'adeguata informativa pubblica.
- l'acquisizione di fondi presso soggetti sottoposti a vigilanza prudenziale, operanti nei settori bancario, finanziario, mobiliare, assicurativo e previdenziale.

Tale condizione si considera rispettata, ad esempio, allorché il gestore predisponga un regolamento contrattuale standard che costituisce solo una base di partenza delle trattative, che devono essere in ogni caso svolte autonomamente dai contraenti, eventualmente avvalendosi di strumenti informatici forniti dal gestore.

La definizione di un limite massimo, di contenuto importo, all'acquisizione di fondi tramite portale *on line* di *social lending* da parte dei prenditori è coerente con la *ratio* sottesa alle disposizioni della Banca d'Italia, in quanto volta ad impedire ai soggetti non bancari di raccogliere fondi per ammontare rilevante presso un numero indeterminato di risparmiatori.

Sono comunque precluse ai gestori e ai prenditori la raccolta di fondi a vista e ogni altra forma di raccolta collegata all'emissione o alla gestione di mezzi di pagamento a spendibilità generalizzata. Restano ferme le possibilità di raccolta senza limiti da parte di banche che esercitano attività di *social lending* attraverso portali *on-line*.

Il Provvedimento, che in realtà conferma la tralatizia ricostruzione giuridica dell'abusivismo bancario, è finalizzato a precisare che «*l'operatività dei gestori dei portali on-line che svolgono attività di social lending ("gestori") e di coloro che prestano o raccolgono fondi tramite i suddetti portali ("finanziatori" e "prenditori") è consentita nel rispetto delle norme che regolano le attività riservate dalla legge a particolari categorie di soggetti*».

Per non incorrere nell'esercizio abusivo della raccolta del risparmio, quindi, i prenditori devono avvalersi «*esclusivamente di piattaforme che assicurano il carattere personalizzato delle trattative*» e devono dimostrare il rispetto di tale condizione anche attraverso un'adeguata informativa pubblica. Lo svolgimento di attività di *social lending*, quindi, incontra una precisa regolazione, e, a ulteriore riconferma della potenziale applicabilità delle sanzioni di cui agli artt. 130 TUB ss., è necessario che il portale si limiti a una funzione di intermediazione neutrale in una relazione privatistica assimilabile allo schema del mutuo. Peraltro, è necessario precisare che per individuare la particolare natura di tali rapporti giuridici occorrerà di volta in volta «vedere la sostanza delle concrete clausole contrattuali, indipendentemente dalla formale qualificazione giuridica prospettata dalle parti»: in giurisprudenza, ad esempio, si è ritenuto che la gestione di una piattaforma *web*, formalmente strutturata per mettere in relazione persone fisiche interessate a prestare modeste quantità di denaro (cd. prestatori o *lenders*) con altri soggetti aventi necessità di finanziamento (cd. richiedenti o *borrowers*), configurasse una forma di raccolta di risparmio tra il pubblico in palese violazione della riserva di attività di cui all'art.11 TUB, dal momento che in concreto il funzionamento del portale comportava in capo al gestore il trasferimento della proprietà dei fondi versati dai prestatori, in attesa dell'abbinamento con le richieste dei *borrowers*, andando così a configurare a carico del gestore stesso un obbligo di rimborso nei confronti dei singoli *lenders*[199].

Parzialmente diversa è, invece, la normativa di riferimento dell'*equity-based crowdfunding*, dato che soltanto in questo specifico settore, e a differenza di altri paesi europei[200], si è preferito intervenire con una disciplina apposita, con la finalità

199 Così T.A.R. Lazio Roma, Sez. III, Sent. 12 dicembre 2009, n. 12848, su Giur. comm., 2011, 2, 428 ss., con nota di M. Prestipino.

200 Cfr. E. Macchiavello (2016), 320 ss.: le scelte degli Stati membri circa la regolazione del crowdfunding sono molteplici, nonostante siano le direttive europee MiFiD e MiFiD II a prevedere il rilascio di autorizzazioni per lo svolgimento di servizi di investimento. In diversi ordinamenti, tuttavia, come in Austria, in Belgio e recentemente

di sottrarre taluni profili dell'attività alla normativa generale. La regolazione dell'*equity-based crowdfunding*, introdotta con d.l. 179/2012 (conv. l. 221/2012), ripetutamente modificata e integrata dal Regolamento Consob n. 18592/2013 (*Regolamento sulla raccolta di capitali di rischio tramite portali on-line*)[201], fornisce una sorta di *sostrato normativo liceizzante* rispetto allo svolgimento di tale attività, ma a determinate condizioni: l'art. 50-*quinquies* TUF, infatti, prevede che la gestione di portali per la raccolta di capitali per le piccole e medie imprese e per le imprese sociali sia consentita, ma soltanto alle SIM, alle imprese di investimento UE, alle imprese di paesi terzi autorizzate in Italia, alle imprese di investimento e alle banche autorizzate ai relativi servizi di investimento nonché ai soggetti iscritti in un apposito registro tenuto dalla Consob, a condizione che questi ultimi trasmettano gli ordini riguardanti la sottoscrizione e la compravendita di strumenti finanziari rappresentativi di capitale esclusivamente a banche e imprese di investimento. Se, quindi, la prestazione di tale servizio specifico, in conformità alle modalità prescritte, non incorre nella potenziale applicazione delle relative sanzioni per abusivismo, la stessa cornice normativa di nuova introduzione confina nell'illiceità le condotte difformi rispetto alle specifiche prescrizioni. La gestione di un portale per l'*equity-based crowdfunding*, infatti, è correlata al rilascio di un'autorizzazione per l'iscrizione nell'apposito registro (art. 7 Reg.) e al mantenimento di tutti i requisiti patrimoniali (art. 7-*bis* Reg.) e di onorabilità e professionalità, da parte dei soggetti che ne detengono il controllo (art. 8 Reg.). Peraltro, gli stessi artt. 22 e 23 del Regolamento, attribuiscono alla Consob il potere di disporre in via cautelare o definitiva, la sospensione dell'attività del gestore qualora sussistano *gravi violazioni di legge ovvero di disposizioni generali o particolari impartite dalla Consob*, nonché la radiazione dal registro in caso di specifiche violazioni. Tale disciplina deve essere integrata con quanto previsto dall'art. 50 *quinquies* co. 7 TUF: i gestori di portali che violino le norme relative all'autorizzazione o le disposizioni emanate dalla Consob, sono puniti, in base alla gravità della violazione e tenuto conto dell'eventuale recidiva, con una sanzione amministrativa pecuniaria, applicata ai sensi dell'art 196 co. 2 e 3 TUF. In questo specifico settore, quindi, l'apposito intervento normativo consente di delimitare un'area di sicura liceità, ma tale regolazione ripropone, tuttavia, un'impostazione prudenziale e la scelta di ricorrere alla sanzione penale-amministrativa nel caso di uno svolgimento non autorizzato di attività sostanzialmente riservate.

Considerata la conformazione delle diverse fattispecie a presidio delle riserve di attività, dunque, per valutare l'abusivismo di un determinato servizio, è necessario osservarne in concreto le modalità di prestazione, per verificare che non integrino quei caratteri della professionalità e della continuità idonei a tracimare nell'area di

anche in Germania e Spagna, si è ritenuto che le attività di crowdfunding non siano del tutto sovrapponibile con le aree soggette a riserva. Al contrario, altri Stati membri come Olanda o Regno Unito e la stessa ESMA propendono per una riconduzione di tali servizi all'interno della disciplina dei servizi di investimento di derivazione europea.

201 Il Regolamento sulla raccolta di capitali di rischio tramite portali on-line, adottato dalla Consob con delibera n. 18592 del 26 giugno 2013, è stato da ultimo modificato con la delibera n. 20264 del 17 gennaio 2018, in vigore dal 31 gennaio 2018).

rilevanza penale[202]. Per un giudizio di sostanziale liceità, quindi, è necessario che i diversi portali si limitino allo svolgimento di una funzione non istituzionale di gestione, o di intermediazione nei contatti tra privati: è essenziale che la fonte del rapporto tra gli utenti sia una relazione diretta e privatistica (riconducibile, ad esempio, allo schema della donazione, semplice e remuneratoria o, più frequentemente, del mutuo).

7 Sintesi dell'indagine e prospettive

A conclusione dell'analisi dei profili sanzionatori (penali e non) dello sviluppo del fenomeno FinTech, i temi di riflessione che si impongono in un'ottica di ampia revisione dello strumentario giuridico tradizionale possono essere sintetizzati come segue:

1. Opportunità di una profonda ristrutturazione della fattispecie di furto d'identità digitale come attualmente formulata dall'art. 640 *ter* c.p. in nome di un più pertinente *crime framework* di *abusivo utilizzo di identità digitale* "emancipato" dallo schema, per molti aspetti ormai anacronistico, del delitto contro il patrimonio. Una rivisitazione siffattamente concepita consentirebbe, peraltro, di razionalizzare i rapporti tra codice penale e legislazione complementare (prima tra tutte quella in materia di *privacy*) attualmente oggetto in giurisprudenza di controverse questioni legate alla risoluzione del problema del concorso/conflitto di norme tra esigenza di costruire un sistema sanzionatorio proporzionato e sufficientemente dissuasivo e divieto di *bis in idem* sostanziale;

2. Necessità di procedere ad una regolamentazione sistematica dell'abusivismo nell'attività delle piattaforme di *social lending*;

3. Costruzione di un sistema integrato di sanzioni amministrative e penali, potenziando le prime (sicuramente più agili, tempestive ed efficaci anche perché legate all'intervento di *Law Enforcement Agencies* diverse dall'Autorità giudiziaria) e mantenendo un ruolo residuale alle seconde nel più pieno rispetto del principio di *extrema ratio* del diritto criminale.

4. Proposta *de iure condendo* di semplificazione delle truffe digitali, passando dallo schema tradizionale, e per molti versi ormai inadeguato, del raggiro con induzione in errore con altrui danno/profitto a quello dell'inadempimento dei doveri connessi alla profilatura e alla chiarezza delle informazioni fornite dai portali, in sinergia con le considerazioni relative ai profili di etica finanziaria e di finanza comportamentale in vista dell'impegno comune all'avvio di un percorso di medio/lungo periodo di alfabetizzazione digitale ed educazione finanziaria, unico vero e stabile presidio contro le truffe finanziarie.

202 Così E. Girino (2014), 75: ad esempio, il crowdfunding extra-Regolamento può, quindi, definirsi come «l'incontro di domanda e offerta di denaro che ha luogo fra privati, dunque con esclusione degli attributi della continuità e professionalità dei finanziatori».

Rischi per la clientela	
Trattamento illecito dei dati	Art. 167 cod. privacy: Trattamento illecito di dati *1.* [...] *chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, operando in violazione di quanto disposto dagli articoli 123, 126 e 130 o dal provvedimento di cui all'articolo 129 arreca nocumento all'interessato,* [...] *3.* [...] *chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, procedendo al trasferimento dei dati personali verso un paese terzo o un'organizzazione internazionale al di fuori dei casi consentiti ai sensi degli articoli 45, 46 o 49 del Regolamento, arreca nocumento all'interessato.* [...] Art. 167-*bis* cod. privacy: Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala *2. [...] chiunque, al fine trarne profitto per sé o altri ovvero di arrecare danno, comunica o diffonde, senza consenso, un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala, è punito con la reclusione da uno a sei anni, quando il consenso dell'interessato è richiesto per le operazioni di comunicazione e di diffusione* [...] Art. 167-*ter* cod. privacy: Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala [...] *chiunque, al fine trarne profitto per sé o altri ovvero di arrecare danno, acquisisce con mezzi fraudolenti un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala* [...]
Data breaches	Art. 32 *GDPR*: Sicurezza del trattamento [...] *tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio.* Art. 12 d. lgs. 65/2018: Obblighi in materia di sicurezza e notifica degli incidenti 1. *Gli operatori di servizi essenziali adottano misure tecniche e organizzative adeguate e proporzionate alla gestione dei rischi posti alla sicurezza della rete e dei sistemi informativi che utilizzano nelle loro operazioni. Tenuto conto delle conoscenze più aggiornate in materia, dette misure assicurano un livello di sicurezza della rete e dei sistemi informativi adeguato al rischio esistente.* *2. Gli operatori di servizi essenziali adottano misure adeguate per prevenire e minimizzare l'impatto di incidenti a carico della sicurezza della rete e dei sistemi informativi utilizzati per la fornitura dei servizi essenziali, al fine di assicurare la continuità di tali servizi.* Art. 12 d. lgs. 65/2018: Obblighi in materia di sicurezza e notifica degli incidenti *1. I fornitori di servizi digitali identificano e adottano misure tecniche e organizzative adeguate e proporzionate alla gestione dei rischi relativi alla sicurezza della rete e dei sistemi informativi che utilizzano nel contesto dell'offerta di servizi di cui all'allegato III all'interno dell'Unione europea.*

Appropriazione o indebito utilizzo dell'identità digitale

Art. 640-ter. Frode informatica

Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 51 a euro 1.032.

La pena è della reclusione da uno a cinque anni e della multa da 309 euro a 1.549 euro se ricorre una delle circostanze previste dal numero 1) del secondo comma dell'articolo 640, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema.

La pena è della reclusione da due a sei anni e della multa da euro 600 a euro 3.000 se il fatto è commesso con furto o indebito utilizzo dell'identità digitale in danno di uno o più soggetti.

Art. 615-*ter* c.p.: Accesso abusivo ad un sistema informatico o telematico

Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni.

La pena è della reclusione da uno a cinque anni:

1) se il fatto è commesso [...] con abuso della qualità di operatore del sistema;

[...] 3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti. [...]

Art. 615-*quater* c.p.: Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici

Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino ad un anno e con la multa sino a euro 5.164. [...]

Frodi finanziarie

Art. 640 c.p.: Truffa

Chiunque, con artifizi o raggiri, inducendo taluno in errore, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da cinquantuno euro a milletrentadue euro.

La pena è della reclusione da uno a cinque anni e della multa da euro 309 a euro 1.549:

[...] 2 bis) se il fatto è commesso in presenza della circostanza di cui all'articolo 61, numero 5).

Art. 61: Circostanze aggravanti comuni

[...]5) l'avere profittato di circostanze di tempo, di luogo o di persona, anche in riferimento all'età, tali da ostacolare la pubblica o privata difesa.

Rischi per gli operatori

Riciclaggio e finanziamento del terrorismo

1. **Obblighi antiriciclaggio** – in particolare obblighi di identificazione – di cui al D.Lgs. 231/2007, come modificato dal D.Lgs. 90/2017, posti a carico dei gestori delle piattaforme di social lending e degli intermediari autorizzati incaricati della raccolta di fondi nell'ambito dell'equity crowdfunding, e relative disposizioni sanzionatorie di ordine penale (art. 55) e amministrativo (art. 56-69) previste per il caso di contravvenzione agli stessi obblighi.

2. **Misure di congelamento dei fondi e delle risorse economiche,** predisposte, ai sensi del D.Lgs. 109/2007, come modificato dal D.Lgs. 90/2017.

3. **Misure di prevenzione personali e patrimoniali** contenute nel c.d. Codice Antimafia (D.Lgs. n. 159/2011), disposte dall'autorità giudiziaria nei confronti delle categorie di soggetti indicate agli artt. 4 e 16.

4. **Normativa penale applicabile alle persone fisiche,** contenuta all'interno del codice penale e nella legislazione speciale [v. ad esempio il reato di trasferimento fraudolento di valori, di cui all'art. 12-*quinquies*, L. 356/1992, ma anche il delitto di finanziamento di condotte con finalità di terrorismo, di cui all'art. 270-quinquies.1 c.p., riciclaggio (art. 648-bis c.p.), reimpiego (art. 648-ter c.p.) e autoriciclaggio (art. 648-ter.1 c.p.)].

5. **Misure in tema di sequestro e confisca**, contenute sia nel codice penale sia all'interno della legislazione speciale.

6. **Normativa in materia di responsabilità da reato degli enti** (D. Lgs. 231/2001).

Abusivismo

Art. 166 TUF: Abusivismo

1. È punito con la reclusione da uno a otto anni e con la multa da euro quattromila a euro diecimila chiunque, senza esservi abilitato ai sensi del presente decreto:

a) svolge servizi o attività di investimento o di gestione collettiva del risparmio;

b) offre in Italia quote o azioni di OICR;

c) offre fuori sede, ovvero promuove o colloca mediante tecniche di comunicazione a distanza, prodotti finanziari o strumenti finanziari o servizi o attività di investimento.

c-bis) svolge servizi di comunicazione dati.

[...]

Art. 191 TUF: Offerta al pubblico di sottoscrizione e di vendita

1. Chiunque effettua un'offerta al pubblico in violazione dell'articolo 94, comma 1, [Prospetto d'offerta] è punito con la sanzione amministrativa pecuniaria da euro venticinquemila fino a euro cinque milioni.

[...]

Art. 7-*octies* TUF: Poteri di contrasto all'abusivismo

1. La Consob può, nei confronti di chiunque offre o svolge servizi o attività di investimento tramite la rete internet senza esservi abilitato ai sensi del presente decreto:

a) rendere pubblica, anche in via cautelare, la circostanza che il soggetto non è autorizzato allo svolgimento delle attività indicate dall'articolo 1, comma 5; b) ordinare di porre termine alla violazione.

Art. 130 TUB - Abusiva attività di raccolta del risparmio

1. *Chiunque svolge l'attività di raccolta del risparmio tra il pubblico in violazione dell'articolo 11 è punito con l'arresto da sei mesi a tre anni e con l'ammenda da euro 12.911 a euro 51.645.*

Art.131: Abusiva attività bancaria

1. Chiunque svolge l'attività di raccolta del risparmio tra il pubblico in violazione dell'articolo 11 ed esercita il credito è punito con la reclusione da sei mesi a quattro anni e con la multa da euro 2.065 a euro 10.329.

Art. 131-bis TUB: Abusiva emissione di moneta elettronica

1. Chiunque emette moneta elettronica in violazione della riserva prevista dall'articolo 114-bis senza essere iscritto nell'albo previsto dall'articolo 13 o in quello previsto dall'articolo 114-bis, comma 2, è punito con la reclusione da sei mesi a quattro anni e con la multa da 2.066 euro a 10.329 euro.

Art. 131-ter TUB: Abusiva attività di prestazione di servizi di pagamento

1. *Chiunque presta servizi di pagamento in violazione della riserva prevista dall'articolo 114-sexies senza essere autorizzato ai sensi dell'articolo 114-novies è punito con la reclusione da sei mesi a quattro anni e con la multa da 2.066 euro a 10.329 euro.*

Art. 132 TUB: Abusiva attività finanziaria

1. Chiunque svolge, nei confronti del pubblico una o più attività finanziarie previste dall'articolo 106, comma 1, in assenza dell'autorizzazione di cui all'articolo 107 o dell'iscrizione di cui all'articolo 111 ovvero dell'articolo 112, è punito con la reclusione da sei mesi a quattro anni e con la multa da euro 2.065 ad euro 10.329.

Conclusioni e prospettive di ricerca

In questo lavoro sono stati analizzati i profili giuridici maggiormente rilevanti nell'ottica dello sviluppo delle attività della finanza digitale, da un punto di vista civilistico e penalistico. È stato evidenziato l'impatto che il ricorso a tecnologie digitali sta avendo sui servizi offerti e quindi sugli stessi istituti giuridici; a partire da ciò, si è tentato di riflettere sulle nuove problematiche, cercando di comprendere se i riferimenti normativi esistenti siano sufficienti per regolare questo nuovo fenomeno e in che senso debba muoversi lo sforzo interpretativo.

Dall'analisi svolta è emersa, tanto con riguardo ai profili civilistici, quanto alle categorie penalistiche, la duplice esigenza di utilizzare il diritto per promuovere lo sviluppo tecnologico nell'ambito dei servizi finanziari e, al tempo stesso, di costruire una cornice giuridica che, pur se solida nel tutelare la clientela, non si riveli un ostacolo all'innovazione.

Infatti, da un lato – con particolare riguardo agli interessi della clientela e alla stessa funzionalità ed integrità del mercato – si è ricostruito il ruolo essenziale che il diritto vigente può svolgere nel rispondere alla molteplicità di istanze che sono emerse nella riflessione, indirizzando l'evoluzione tecnologica entro coordinate di tutela e di *empowerment* dei consumatori, nonché di legalità e correttezza dei servizi offerti e delle procedure operative e contrattuali. In tal senso, il GDPR rappresenta una nuova spinta propulsiva nella tutela dei dati personali, conciliando le esigenze dei consumatori con quelle dello sviluppo del mercato dei *big data*, come dimostra l'introduzione del diritto alla portabilità dei dati; parallelamente – e insieme alle indicazioni contenute nel d.lgs. 65/2018, di recepimento della direttiva c.d. NIS – fornisce un quadro di poteri e responsabilità per la prevenzione di comportamenti (anche penalmente illeciti) di apprensione di dati o di violazione della sicurezza di sistemi informatici. Inoltre, la presenza di presidi civilistici – dal consenso alle proposte di contrattualizzazione della *privacy* – e penalistici a tutela della correttezza del comportamento degli operatori può senz'altro costituire uno strumento di salvaguardia nello specifico settore della finanza digitale, contribuendo a disciplinare le relazioni tra gli attori del mercato. Infine, il richiamo alla disciplina antitrust, in coordinamento con quella in materia di *privacy*, e la previsione di obblighi finalizzati alla prevenzione di riciclaggio, terrorismo e abusivismo completano il quadro, costituendo un *framework* di portata più generale, finalizzato alla definizione delle essenziali regole del mercato.

Dall'altro lato, si è cercato anche di delineare soluzioni che non si rivelassero eccessivamente invasive e restrittive rispetto a un settore altamente innovativo e in continua evoluzione: ciò emerge, da un punto di vista civilistico, sia in relazione alla questione della pratica del *dynamic pricing* e alla sua problematica qualificazione illecita sia con riguardo alla difficoltà di rintracciare gli estremi dell'abuso di posizione dominante nell'ambito del possesso di data set. In una prospettiva penalistica, poi, ciò si traduce nell'esigenza di evitare forzature interpretative della

disciplina esistente, invocando, al contrario, interventi legislativi di riforma che siano meglio in grado di intercettare le questioni poste in tema di FinTech: in particolare, sarà fondamentale valutare altresì se la disciplina in materia di riciclaggio, terrorismo e abusivismo possa dirsi proporzionata – quanto alla repressione, ma anche sul versante degli obblighi di carattere preventivo – rispetto alla concreta realtà dei servizi di finanza tecnologica offerti da operatori non istituzionali.

Questo approfondimento costituisce, dunque, soltanto un primo sguardo alla molteplicità di questioni che coinvolgono da un punto di vista giuridico il fenomeno FinTech, non già con l'obiettivo di esaurirne l'analisi, ma, soprattutto, al fine di fornire spunti di riflessione e di provare a stimolare un dibattito giuridico sul tema, che si accompagni alle più consolidate riflessioni di carattere tecnico ed economico. Su tutti, un nodo essenziale è allora quello del rispetto dei diritti fondamentali degli individui all'interno di un mercato altamente innovativo e complesso. In tal senso, dovrà avere un ruolo centrale un nuovo concetto di identità digitale, con il connesso diritto alla "*rappresentazione integrale della persona*"[203], probabilmente incompatibile con la qualificazione in termini proprietari dei dati personali, da intendere piuttosto quale attributo dell'identità del singolo, quasi un "*prolungamento della dimensione umana*"[204]. Da un punto di vista civilistico, le ragioni della *privacy* e quelle della tutela dell'identità si sfiorano, ma non sono perfettamente coincidenti: si afferma cioè l'esigenza, sempre più pressante da parte dei consumatori, di esercitare un controllo sulle proprie identità digitali quali output di un certo processo automatizzato di elaborazione dei dati. Quanto espresso dall'identità digitale potrebbe infatti non solo influire sulle scelte di consumo individuali, ma anche avere ricadute sul piano economico sociale, nel determinare, ad esempio, la stessa possibilità di accesso ad un servizio. Anche da un punto di vista penalistico, poi, il tema merita ulteriori riflessioni, per delineare un quadro di tutela che non sia confinato al settore, ormai anacronistico, dei delitti contro il patrimonio, ma che riesca a comprendere, in chiave repressiva e preventiva, una tutela forte dell'identità del singolo, quale estrinsecazione della sua persona. Inoltre, anche il diritto penale dovrà confrontarsi con il sempre più ampio ricorso a elaborazioni automatizzate dei dati personali e con le proiezioni offensive di questo fenomeno, con riguardo a profili discriminatori e/o di abusivo condizionamento delle scelte di acquisto, in connessione con il ricorso a tecniche di profilazione e di (eventuale) indebito sfruttamento di tale patrimonio conoscitivo nelle relazioni con la clientela.

Il tema è oggetto di un ampio dibattito in dottrina: ciò che in definitiva si intende mettere in luce in questa sede è che la rivoluzione dei *big data* in un contesto particolarmente delicato come quello dei servizi finanziari digitali coinvolge in primo luogo proprio la persona, e la sua – ormai liquida – identità.

203 Rodotà S. (1997), p. 605.

204 Alpa G. (2017), p. 727.

Bibliografia

Accettella, F. e N. Ciocca (2017), Emittente e portale nell'equity-based crowdfunding, in Giur. Comm., 2, 237 ss.

Alessandri, A. (1990), Criminalità informatica, in Riv. trim. dir. pen. econ., 653 ss.

Alessandri, A. (2016), Reati in materia economica, in Trattato teorico-pratico di diritto penale, diretto da F. Palazzo - C. E. Paliero, Giappichelli, Torino

Alpa G. (2017), L'identità digitale e la tutela della persona. Spunti di riflessione, Contratto e Impresa, 723 ss.

Amore, N. (2016), L'autoriciclaggio tra responsabilità individuale e collettiva, in http://www.lalegislazionepenale.eu/.

Antolisei, F. (2008), Manuale di diritto penale. Parte speciale, I, Giuffré, Milano

Antonacchio, F. e G. Miccoli (2016), Restyling delle sanzioni per violazioni degli obblighi antiriciclaggio, in Il Fisco, 7, 651 ss.

Aragona, V. (2017), Il contrasto al finanziamento del terrorismo, in Riv. trim. dir. pen. cont.,1, 96 ss.

Autorità garante della concorrenza e del mercato (giugno 2018), Indagine conoscitiva sui Big Data. Analisi della propensione degli utenti online a consentire l'uso dei propri dati a fronte dell'erogazione di servizi. Primi risultati.

Autorità per le garanzie nelle comunicazioni (giugno 2018), Interim report nell'ambito dell'indagine conoscitiva di cui alla delibera n. 217/17/CONS.

Autorité de la Concurrence francese e della tedesca Bundeskartel-lamt, Report congiunto, Competition Law and Data, 10 May, 2016, in www.autoritedelaconcurrence.fr/doc/reportcompetitionlawdatafinal.pdf.

Bandiera, B. (2017), FinTech e antiriciclaggio, in M. T. Paracampo (a cura di), FinTech. Introduzione ai profili giuridici in un mercato unico tecnologico dei servizi finanziari, Giappichelli, Torino

Barocas S. e Selbst A.D. (2016), Big Data's Disparate Impact, 104 California Law Review 671.

Basedow J. (2016), European Contract Law and the Digital Agenda, in Contratto e Impresa/Europa, 423 ss.

Basile, E. (2017), Chiaroscuri della Cassazione in tema di abusivismo bancario e finanziario, in Dir. Pen. Contemporaneo, 5.

Belli, M. (2015) La frode informatica, in F. Viganò - C. Piergallini (a cura di), Reati contro la persona e contro il patrimonio, in Trattato teorico-pratico di diritto penale, diretto da F. Palazzo - C. E. Paliero, Giappichelli, Torino

Bellomo G.A. (2016), "There aint't no such thing as a free lunch". Una riflessione sui meccanismi di mercato dell'economia digitale e sull'effettività delle tutele esistenti, Concorrenza e mercato, p. 2 ss.

Bisori, L. (2013), Delitti di frode, in A. Cadoppi - S. Canestrari - A. Manna - M. Papa (diretto da), Trattato di diritto penale, Parte speciale, vol. X, I delitti contro il patrimonio, Giappichelli, Torino

Bolognini L., Bistolfi C., Crea G. (2018), Il Regolamento e-Privacy tra principi giuridici e impatti sull'economia digitale, Istituto Italiano per la privacy e la valorizzazione dei dati, https://www.istitutoitalianoprivacy.it/wpcontent/uploads/2018/03/Paper-IIP_ePrivacy_2018_ITA.pdf.

Bonucci, L. (2017), Le vulnerabilità del sistema finanziario come minacce alla sicurezza nazionale: studio sulle tipologie di finanziamento al terrorismo e analisi del sistema Money Transfer, https://www.cssii.unifi.it/upload/sub/bonucci_finanziamento-del-terrorismo-e-money-transfer.pdf

Borgesius F. Z., Poort J. (2017), Online Price Discrimination and EU Data Privacy Law, Journal of Consumer Policy, 347.

Borlini, L. (2017), Soft law, soft organizations e regolamentazione «tecnica» di problemi di sicurezza pubblica e integrità finanziaria, in Riv. di Diritto Internazionale, 2, 356 ss.

Bradford, S. (2012), Crowdfunding and the Federal Securities Laws, in Colum. Bus. L. Rev., 1,14 ss.

Brizzi, F. e G. Capecchi, A. Rinaudo (2014), La reimmissione della liquidità illecita nel circuito economico ed il delitto di reimpiego tra prevenzione patrimoniale e giustizia penale: prospettive di futura armonizzazione, in Arch. Pen., 2, 3 ss.

Bundesanstalt für Finanzdienstleistungsaufsicht, Big data meets artificial intelligence. Challenges and implications for the supervision and regulation of financial services.

Buzzacchi C. (2016), La politica europea per i Big Data e la logica del single market: prospettive di maggiore concorrenza?, in Concorrenza e mercato, 1, 153 ss.

Capolupo, S. e M. Carbone, G. Sturzo (2015), Antiriciclaggio, Ipsoa, Milano

Castrataro D. e I. Pais, Analisi delle piattaforme di crowdfunding italiane, su www.crowdfundingitalia.com

Celi, L. (2010), Il ruolo del limite espresso dall'art. 5, comma 3 del d.lg. n. 196/2003 nella struttura del delitto di trattamento illecito dei dati personali, in Cass. Pen., 1, 311 ss.

Cerri, A. (1995), voce Identità personale, in Enc. giur., Treccani, Roma, 6 ss.

Colangelo G., Falce V. (2017), Concorrenza e comportamenti escludenti nei mercati dell'innovazione, Il Mulino.

Condemi, M. e F. De Pasquale (2008), Lineamenti della disiciplina internazionale di prevenzione e contrasto del riciclaggio e del finanziamento del terrorismo, in Quaderno di Ricerca Giuridica della Consulenza Legale n. 60 della Banca d'Italia, Roma

Corrias Lucente, G. (2004), La nuova normativa penale a tutela dei dati personali, in Aa.Vv., Il codice dei dati personali. Temi e problemi, Giuffré, Milano

Crescioli, C. (2018), La tutela penale dell'identità digitale, in Dir. pen. cont., 2018, 5, 265 ss.

De Flemmitis S. (2017), Gli strumenti di prevenzione del riciclaggio. L'esperienza italiana nel quadro della quarta direttiva europea e prime osservazioni sullo schema di decreto attuativo, in www.penalecontemporaneo.it.

De Franceschi A. e Lehmann M. (2015), Data as Tradeable Commodity and New Measures for Their Protection, The Italian Law Journal, 51 ss.

De Poli, M. (2017), MiFID II e decreto legislativo di recepimento n. 129/2017. L'apparato sanzionatorio e la reazione a condotte antigiuridiche., in Riv. dir. banc., dirittobancario.it

Del Corso, S. (2007), sub art. 167, in La Protezione dei dati personali. Commentario sistematico al d.lgs. 30 giugno 2003, n. 196, vol. I, Cedam, Padova.

Di Porto F., Big Data e scienze cognitive: ripensare la disclosure regulation nel settore finanziario, in FinTech. Introduzione ai profili giuridici di un mercato unico tecnologico dei servizi finanziari, a cura di Maria-Teresa Paracampo, Giappichelli, Torino, p. 104 ss.

Dolcini, E. G. Marinucci (2011), Codice penale commentato, Ipsoa, Milano

EBA (2017), Final Report on Recommendations on outsourcing to cloud service providers, 20.12.2017.

EDPS (2016b), Opinion n. 9/2016 on Personal Information Management Systems. Towards more user empowerment in managing and processing personal data, 20 October 2016.

European Banking Authority (EBA) (2016), Discussion Paper on innovative uses of consumer data by financial institutions, 4.5.2016, DP/2016/01.

European Banking Federation (EBF) (2016), The EBF vision for banking in the Digital Single Market.

European Data Protection Supervisor (EDPS) (2014), Privacy and Competitiveness in the Age of Big Data: The Interplay Between Data Protection, Competition Law and Consumer Protection in the Digital Economy (Preliminary Opinion), March 2014.

European Data Protection Supervisor (EDPS) (2016a), Opinion 18/2016 on coherent enforcement of fundamental rights in the age of big data, 23 September 2016.

European Political Strategy Center (EPSC) (2017), Enter the Data Economy. EU Policies for a Thriving Data Ecosystem, 11.1.2017.

Ezrachi A., Stucke M.E. (2016), Virtual Competition. The Promise and Perils of the Algorithm-Driven Economy, Harvard University Press

Fanelli, A. (2006), La truffa, Giuffré, Milano

Federal Trade Commission (2016), Big data: A Tool for Inclusion or Exclusion? Understanding the Issues, January 2016.

Fiandaca, G. ed E. Musco (2014), Diritto penale. Parte speciale, vol. II, t. II, Zanichelli, Bologna, 6° ed.

Fiandaca, G. ed E. Musco (2014b), Diritto penale. Parte generale, Zanichelli, Bologna, 7° ed.

Financial Services User Group (FSUG), Assessment of current and future impact of Big Data in Financial Services, June 2016.

Finocchiaro, G. (2010), Identità personale (diritto alla), in Dig. Disc. Priv., UTET, Torino, 721 ss.

Flor, R. (2007), Phishing, Identity Theft e Identity Abuse. Le prospettive applicative del diritto penale vigente, in Riv. it. dir. proc. pen., 899 ss.

Floridi L. (2014), The Fourth Revolution. How the infosphere is reshaping human reality, Oxford University Press.

Fregonara, A. (2014), Il crowdfunding: un nuovo strumento di finanziamento per le start up innovative, in Orizzonti del diritto commerciale, 1

Galli, M. (2016), Dentro il castello dei destini incrociati: la responsabilità dell'ente da autoriciclaggio, in Riv. trim. dir. pen. econ., 1-2, 100 ss.

Garante per la protezione dei dati personali, Big data e Privacy. La nuova geografia dei poteri, Atti del Convegno Roma, 30 gennaio 2017.

Gatt L., Montanari R. e Caggiano I.A. (2017), Consenso al trattamento dei dati personali e analisi giuridico-comportamentale, in Nodi virtuali, legami informali: internet alla ricerca di regole, a cura di P. Passaglia e D. Poletti, Pisa University Press, Pisa, p. 57 ss.

Geslevich Packin N. e Lev-Aretz Y. (2016), Big Data and Social Netbanks: Are You Ready to Replace Your Bank?, 53 Houston Law Rev. 1211.

Giacometti, T. e O. Formenti (2017), La nuova disciplina in materia di prevenzione del riciclaggio e di finanziamento del terrorismo (d.lgs. 25 maggio 2017, n. 90), in www.penalecontemporaneo.it

Giorgianni, F. e C. M Tardivo (2009), Manuale di diritto bancario e degli operatori finanziari, Giuffré, Milano.

Girino, E. (2014), Le regole del crowdfunding, in Amministrazione e Finanza, 1, 75 ss.

Gorgoni, M. (2007), sub art. 5, in La Protezione dei dati personali. Commentario sistematico al D.Lgs. 30 giugno 2003, n. 196, vol. I, Cedam, Padova

Grunes A.P., Stucke M.E. (2015), The Important Role of Antitrust in the Era of Big Data, www.antitrustsource.com

Isenberg, D. (2012), The Road to Crowdfunding Hell, in HBR Blog Network

IT Media Consulting in collaborazione con l'Univ. Bocconi (2018), L'economia dei dati. Tendenze di mercato e prospettive di policy.

Joint Committee of European Supervisory Authorithies (ESAs) (2016), Discussion Paper on the Use of Big Data by Financial Institutions.

Joint Committee of European Supervisory Authorithies (ESAs) (2018), Final Report on Big Data

Koops B.-J. (2015), The Trouble with European data Protection Law, Tilburg Law School Legal Studies Research Paper Series, 4/2015, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2505692.

Lamanuzzi, M., (2017), Diritto penale e trattamento dei dati personali. Codice della privacy, novità introdotte dal regolamento 2016/679/UE e nuove responsabilità per gli enti, in Jus, 244 ss.

Langhanke C. e Schmidt-Kessel M. (2015), Consumer Data as consideration, Journal of European Consumer and Market Law, 218 ss.

Laudonio, A. (2016), Le altre facce del crowdfunding, in M. Colurcio-A. Laudonio, La folla e l'impresa, Cacucci, Bari

Lohsse S., Schulze R. e Staudenmayer D. (eds) (2017), Trading Data in the Digital Economy: Legal Concepts and Tools, Hart Publishing – Nomos, Baden-Baden.

Lotierzo, R. (2013), Del nocumento nell'illecito trattamento dei dati personali ovvero dell'esigenza di ascendere alle origini di una incriminazione, in Cass. Pen., 4, 1589

Macchiavello, E. (2016), La modifica al regolamento Consob in materia di equity crowdfunding alla luce dell'evoluzione del diritto finanziario europeo e delle tendenze di regolazione dell'investment-based crowdfunding in Europa, in Banca Impresa Società, 2, 283 ss.

Maggiolino M. (2016), Big Data e prezzi personalizzati, Concorrenza e Mercato, 95 ss.

Maggiolino M. (2018), I Big Data e il diritto anti-trust, EGEA.

Malgieri G. e Comandé G. (2017), Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation, International Data Privacy Law, vol. 7, n. 4, 243 ss.

Malgieri, G. (2015), La nuova fattispecie di indebito utilizzo di identità digitale, in Riv. trim. dir. pen. cont., 2, 143 ss.

Manna, A. (2003), Il quadro sanzionatorio penale ed amministrativo del codice sul trattamento dei dati personali, in Dir. inf., 727 ss.

Manna, A. (2003), Prime osservazioni sul Testo Unico in materia di protezione dei dati personali: profili penalistici, in www.privacy.it

Manna, A. (2005), Privacy on line: quali spazi per la tutela penale?, in Dir. internet, 259 ss.

Mantelero A. (2012), Riforma della direttiva comunitaria sulla data protection e privacy impact assessment, verso una maggiore responsabilità dell'autore del trattamento?, Diritto dell'informazione e dell'informatica, p. 145 ss.

Mantelero A. (2016), Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection, Computer Law & Security Review, 32, p. 238 ss.

Mantelero A. (2017), From group privacy to collective privacy: towards a new dimension of privacy and data protection in the Big Data era 139, Taylor L., Floridi L., van der Sloot B. (a cura di), Group privacy. New challenges of Data technologies.

Mantelero A. (2017), Responsabilità e rischio nel Reg. UE 2016/679, Nuove leggi civili commentate, p. 144 ss.

Mantovani, F. (2011), Diritto penale. Parte generale, Cedam, Padova

Mantovani, F. (2014), Diritto penale. Delitti contro il patrimonio, Cedam, Padova

Manyika J. et al. (2011), Big Data: The Next Frontier for Innovation, Competition, and Productivity, McKinsey Global Institute.

Manzi, V. (2013), Il fenomeno del crowdfunding e del social lending: caratteristiche operative e profili contrattuali, in F. Capriglione (a cura di), I contratti dei risparmiatori, Giuffré, Milano

Marandola, A. (2016), Congelamento e confisca dei beni strumentali e dei proventi da reato nell'Unione Europea: la "nuova" direttiva 2014/42/UE, in Arch. pen., 1

Masciandaro, D. (2007), Il riciclaggio dei capitali illeciti profili di analisi economica, in Gnosis, 13 (3), 51 ss.

Mattasoglio F. (2016), La profilazione dell'investitore nell'era dei big data. I rischi della estremizzazione della regola del "know your customer", Rivista trimestrale di diritto dell'economia, Suppl. n. 1, p. 233 ss.

Mattasoglio F. (2017), Big Data: impatto sui servizi finanziari e sulla tutela dei dati personali, in FinTech. Introduzione ai profili giuridici di un mercato unico tecnologico dei servizi finanziari, a cura di Maria-Teresa Paracampo, Giappichelli, Torino, p. 65 ss.

Maugeri, A. (2014), La direttiva 2014/42/UE relativa alla confisca degli strumenti e dei proventi da reato nell'unione europea tra garanzie ed efficienza: un "work in progress", in www.penalecontemporano.it

Mayer-Schönberger V. e Cukier K. (2013), Big Data. The essential guide to work, life and learning in the age of insight, John Murray Publishers, London.

Mehera S. K. (2016), Antitrust and the Robo-Seller: Competition in the Time of Algorithms, Minnesota Law Review, 1322

Miller A. A. (2014), What do we worry about when we worry about price discrimination? The law and ethics of using personal information for pricing, 19 Journal of Technology Law and Policy, 44 ss.

Mucciarelli, F. (1988), voce Computer (disciplina giuridica del) nel diritto penale, in Dig. disc. Pen., II, UTET, Torino, 373 ss.

Mucciarelli, F. (1996), Commento all'art. 10 della l. n. 547 del 1993, in Leg. pen., 136 ss.

Niger, S. (2006), Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali, Cedam, Padova

Nuvolone, P. (1955), Il diritto penale del fallimento e delle altre procedure concorsuali, Giuffré, Milano

Ohm P. (2010), Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, 57 UCLA Law Review 1701.

Organisation for economic cooperation and development (OECD) (2014), Data-Driven Innovation for Growth and Well-Being: Interim Synthesis Report 19.

Ottolia, A. (2014), L'equity crowdfunding tra incentivi al reperimento di capitale di rischio per start up innovative e responsabilità, in Diritto della Banca e del Mercato finanziario, 43 ss.

Padovani, T. (1995), Diritto penale della prevenzione e mercato finanziario, in Riv. it. dir. proc. pen., 634 ss.

Pagliaro, A. (2009), Il diritto penale fra norme e società. Scritti 1956-2008, Vol. II, Giuffré, Milano.

Parodi, C. (1997), La frode informatica: presente e futuro delle applicazioni criminali nell'uso del software, in Dir. pen. e proc.,1538 ss.

Pecorella, C. (2000), Il diritto penale dell'informatica, Cedam, Padova

Piantivigna, P. (2014), Start-up innovative e nuove fonti di finanziamento, in Riv. Dir. Fin., 2, 272 ss.

Piattelli, U. (2013), Il crowdfunding in Italia, Giappichelli, Torino

Picotti, L. (2004), Il diritto penale dell'informatica nell'epoca di Internet, Cedam, Padova

Piraino F. (2017), Il Regolamento generale sulla protezione dei dati personali e i diritti dell'interessato, Nuove leggi civili commentate, p. 369 ss.

Pitruzzella G. (2016), Big Data, competition and privacy: a look from the antitrust perspective, Concorrenza e Mercato, 15 ss.

Pizzetti, F. (2016), Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo, Giappichelli, Torino

Podszun R., The More Technological Approach - Competition Law in the Digital Economy. Competition on the Internet, 101 ss.

Pulitanò, D. (2013), Diritto penale. Parte speciale, vol. II, Tutela penale del patrimonio, Giappichelli, Torino

Purtova N. (2015), Illusion of Personal Data as No One's Property, Law, Innovation, and Technology, 7(1), p. 83 ss.

Resta G. (2005), Autonomia privata e diritti della personalità, Jovene, Napoli.

Richards N.M., King J.H. (2014), Big Data Ethics, 49, Wake Forest Law Review, 392.

Richards N.M., King J.H. (2016), Big Data and the Future For Privacy, Handbook of Research on Digital Transformations.

Rodotà S. (1997), Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali, in Rivista critica del diritto privato, 583 ss.

Rodotà, S. (1991), Privacy e costruzione della sfera privata. Ipotesi e prospettive, in Politica del diritto, 22, 525 ss.

Rodotà, S. (2004), Privacy, libertà, dignità, 26a Conferenza Internazionale sulla Privacy e sulla Protezione dei dati Personali, Wroclaw, in www.garanteprivacy.it.

Rodotà, S. (2006), Trasformazioni del corpo, in Politica del diritto, 2006, 1.

Sabia, R. (2017), Delitti di terrorismo e responsabilità da reato degli enti tra legalità e esigenze di effettività, in Riv. trim. dir. pen. cont., 1, 208 ss.

Schulze R., Staudenmayer D. e Lohsse S. (eds) (2017), Contracts for the Supply of Digital Contents: Regulatory Challenges and Gaps, Hart Publishing - Nomos, Baden-Baden.

Schwartz P. (2004), Property, Privacy, and Personal Data, 11 Harvard Law Review 2056.

Selvaggi, N. (2015), On instruments adopted in the area of freezing and confiscation, in www.penalecontemporaneo.it

Severino di Benedetto, P. (1988), Sub. Art. 166, in G. Alpa, F. Capriglione (a cura di), Commentario al testo unico delle disposizioni in materia di intermediazione finanziaria, Cedam, Padova, 1988.

Solove D. (2013), Introduction: Privacy Self-management and The Consent Dilemma, 126 Harvard Law Review 1880 ss.

Thiene A. (2017), Segretezza e riappropriazione di informazioni di carattere personale: riserbo e oblio nel nuovo Regolamento europeo, Nuove leggi civili commentate, p. 410 ss.

Thobani S. (2016), La libertà del consenso al trattamento dei dati personali e lo sfruttamento economico dei diritti della personalità, in Europa e diritto privato, p. 513 ss.

Trinchera, T. (2016), Introdotte nuove ipotesi speciali di confisca per dare attuazione alla direttiva 2014/42/UE (D.lgs. 29 ottobre 2016, n. 202), in www.penalecontemporaneo.it

Troncone, P. (2011), Il delitto di trattamento illecito dei dati personali, Giappichelli, Torino

Troyer, L. e M. Zancan (2017), Verso una nuova direttiva in materia di prevenzione del riciclaggio e del finanziamento del terrorismo, in www.penalecontemporaneo.it.

Vessia F., Big Data e profili di concorrenza, in FinTech. Introduzione ai profili giuridici di un mercato unico tecnologico dei servizi finanziari, a cura di Maria-Teresa Paracampo, Giappichelli, Torino, p. 81 ss.

Vitali, M. L. (2014), Equity crowdfunding: la nuova frontiera della raccolta del capitale di rischio, in Riv. Soc., 2/3, 371 ss.

Vitarelli, T. (1999), voce Vita privata nel diritto penale, in Dig. disc. Pen., XV, UTET, Torino, 302 ss.

Weber R. (2015), The digital future. A challenge for privacy?, 31 Computer and Security Law Review, p. 234 ss.

Weber R. (2016), Data Portability and Big Data analytics. New competition policy challenges, Concorrenza e mercato, 59 ss.

World Economic Forum (2012), Big Data, Big Impact: New Possibilities for International Development.

World Economic Forum (2018), Digital Identity. On the Threshold of a Digital Identity Revolution.

Zangoni, P. (1982) Sulla tutela penale del diritto alla riservatezza, in Riv. it. dir. proc. pen., 971 ss.

Zatti, P. (1981), Il diritto all'identità personale e l'applicazione «diretta» dell'art. 2 Cost., in Il diritto all'identità personale (a cura di G. Alpa – M. Bessone – M. Boneschi), Cedam, Padova 1981, 55 ss.

Zech U. (2017), Data as a Tradeable Commodity - Implications for Contract Law, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3063153.

Zencovich, Z. (1998), Una lettura comparatistica della l. n. 675/96 sul trattamento dei dati personali, in Riv. trim. dir. proc. civ., 734 ss.

Zeno-Zencovich V., Giannone Codiglione G. (2016), Ten legal perspectives on the "Big Data Revolution", Concorrenza e mercato, 29 ss.

Quaderni FinTech

1 – marzo 2018 **Lo sviluppo del FinTech**
Opportunità e rischi per l'industria finanziaria nell'era digitale
C. Schena, A. Tanda, C. Arlotta, G. Potenza

2 – dicembre 2018 **Il FinTech e l'economia dei dati**
Considerazioni su alcuni profili civilistici e penalistici
Le soluzioni del diritto vigente ai rischi per la clientela e gli operatori
E. Palmerini, G. Aiello, V. Cappelli
G. Morgante, N. Amore, G. Di Vetta, G. Fiorinelli, M. Galli