Quaderni FinTech

La portabilità dei dati in ambito finanziario

A cura di A. Genovese e V. Falce

8

aprile 2021

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.

Coordinamento della collana
Nadia Linciano

Segreteria di Redazione
Eugenia Della Libera, Paola Maione

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 9788894369755

La portabilità dei dati in ambito finanziario

A cura di A. Genovese e V. Falce [*]

Abstract

Le interferenze e reciproche intersezioni fra regolazione, innovazione finanziaria e innovazione tecnologica si inquadrano a pieno titolo nella quarta rivoluzione digitale. La *disruption* a cui si assiste è di tipo intersettoriale, si caratterizza per processi di "contaminazione" tra soggetti e mercati, modelli e categorie, architetture e geometrie.

Nella nuova era disintermediata e decentralizzata, operatori, banche, intermediari e soggetti terzi elaborano, definiscono, personalizzano e offrono prodotti e servizi, ricorrendo a tecniche predittive ed intelligenti che usano e riusano dati personali, anonimizzati e commerciali, abbinando quelli "esterni", estratti dal magma della rete, con quelli propri del patrimonio aziendale, e come tali "interni" all'impresa, in un ciclo continuo.

Muovendo da queste premesse, il Quaderno si propone di analizzare il *Data space* sotto il profilo dell'oggetto (i dati), dei soggetti (vecchi e nuovi), delle responsabilità e dei diritti, ma solo dopo aver messo a fuoco la cornice regolamentare rilevante, che costituisce il perno essenziale e imprescindibile per mappare e di qui esprimere linee di policy anche in tema di *portabilità di dati*.

(*) Anna Genovese, Ordinario di Diritto commerciale, Università di Verona (anna.genovese@univr.it), Commissaria Consob (a.genovese@consob.it);

Valeria Falce, Jean Monnet Professor in EU Innovation Policy e Ordinario di Diritto dell'economia (Università Europea di Roma); Direttore dell'Innovation, Regulation and Competition Policy Centre – ICPC (valeria.falce@unier.it).

Si ringrazia Lucia Marzialetti per gli utili commenti a precedenti versioni del lavoro. Si ringraziano la Cattedra Jean Monnet in EU Innovation Policy dell'Università Europea di Roma e l'Erasmus + Programme dell'Unione Europea per il sostegno alle attività di ricerca. Eventuali 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.

La normativa nazionale ed europea, nonché i riferimenti dottrinali e giurisprudenziali, sono aggiornati alla data del 5 aprile 2021.

Seguendo la predetta linea, nella Prima Parte, il Quaderno si concentra sul quadro normativo. Dall'assunto secondo cui la rapidità della diffusione delle nuove tecnologie, oltre i confini territoriali ed economici, impone un ripensamento delle tradizionali tecniche di regolamentazione, si affrontano i limiti della matrice regolatoria disegnata negli anni' 90 e i profili di tecnologia regolatoria necessari per cogliere i cambiamenti e ripensare il quadro normativo in un'ottica di cooperazione tra Autorità nazionali e coordinamento fra i diversi ordinamenti nazionali, e con l'obiettivo chiaro di contemperare gli interessi in gioco e tutelare i diritti fondamentali.

Nella Seconda Parte, invece, le questioni della portabilità e della condivisione dei dati sono analizzate con riferimento ai flussi informativi e ai soggetti coinvolti, sotto il duplice aspetto degli ambiti di responsabilità degli attori e delle ricadute in punto di tutela dei clienti e degli investitori. L'emersione di *Third Party Providers* insieme al rafforzamento di costitutori di banche dati e titolari dei software getta le basi per una rinnovata competizione incentrata sull'uso delle *Smart Technologies* nello scenario dell'*Open Banking* e impone una attenta riflessione su ruoli e funzioni, nonché sulla catena delle eventuali responsabilità.

Attraverso i predetti snodi, il Quaderno propone un solido approccio ricostruttivo e sistematico per inquadrare le nuove sfide e intercettare i rischi associati alla trasformazione digitale con particolare riferimento alla disciplina inerente ai flussi di dati. In tal ambito, infatti, la migrazione dei servizi finanziari verso ambienti sempre più digitali e caratterizzati da una normativa frammentaria e settoriale, rischia di sfociare in vuoti di tutela che a loro volta rischiano di minare la fiducia nel sistema finanziario e nella sua stabilità. Il Quaderno fornisce gli strumenti per scongiurare tali eventualità all'insegna della chiarezza ricostruttiva, della certezza giuridica e dei principi generali, così salvaguardando la protezione degli investitori e l'integrità del mercato.

Sommario

II La disintermediazione finanziaria
Flussi informativi e soggetti coinvolti

(con il coordinamento di Simone Alvaro)

5. Evoluzione digitale e nuove misure a tutela dei "consumatori" ... di servizi finanziari

Financial revolution: impatto e prospettive

A. Genovese e V. Falce[*]

L'innovazione tecnologica incentrata sulla digitalizzazione di prodotti e processi avanza essendo anche, secondo i principi del diritto dell'Unione Europea, promossa e positivamente considerata.

Nel settore finanziario, l'innovazione veicolata dalle nuove tecnologie ("Fintech") si esprime in un ampio ventaglio di modalità. Le opportunità del cambiamento, per gli operatori come per la clientela, sono enormi, favorendo la definizione di prodotti e servizi nuovi e personalizzati, consentendo rapporti decentrati, scambi e rapporti disintermediati, agevolando l'emersione di nuovi modelli di *business*, di geometrie variabili sul mercato e di architetture di sviluppo sempre nuove.

Nella formula disintermediata e decentralizzata di relazioni economiche a "matrice digitale", gli operatori del mercato elaborano, definiscono, personalizzano e offrono prodotti e servizi, ricorrendo a tecniche predittive ed intelligenti che usano e riusano i dati personali della clientela, anonimizzati e commerciali, abbinando quelli "esterni", estratti dal magma della rete, con quelli propri del patrimonio aziendali, e come tali "interni" all'impresa, in un ciclo continuo.

L'accrescimento della componente tecnologica della produzione e della erogazione dei prodotti e dei servizi finanziari facilita e velocizza i processi, con possibilità di implicazioni positive e negative che richiedono una attenta riflessione sugli spazi da rimettere al mercato e gli ambiti da assoggettare ad una nuova regolazione. Mentre l'innovazione incalza e il mercato si adatta alle molteplici sollecitazioni del c.d. *Data Space*, ci si interroga sui soggetti che intervengono nella gestione del flusso dei dati e sulle relative responsabilità, nonché sulle tutele che il diritto riserva ad investitori e clientela in generale.

In questo scenario, i diritti fondamentali e i principi generali che li inverano devono restare al timone per promuovere una regolazione del mercato finanziario in grado di mitigare i possibili rischi del *Fintech* senza imbrigliarne lo sviluppo. Tuttavia la laboriosità della ricerca di una soluzione di regolamentazione, entro una

(*) Anna Genovese, Ordinario di Diritto commerciale, Università di Verona (anna.genovese@univr.it); Commissaria Consob (a.genovese@consob.it).

Valeria Falce, Jean Monnet Professor in EU Innovation Policy e Ordinario di Diritto dell'economia (Università Europea di Roma); Direttore dell'Innovation, Regulation and Competition Policy Centre – ICPC (valeria.falce@unier.it).

cornice di cooperazione globale o almeno regionale, sta ritardando l'intervento. Il tempo a diposizione per evitare che la digitalizzazione dei prodotti e dei processi finanziari ponga le istituzioni politiche e di regolazione davanti a "fatti compiuti" - economici e di mercato – irreversibili, e resi ingovernabili *by construction,* si riduce.

Solo alla fine del 2020 la Commissione europea ha impresso una accelerazione ai lavori di regolazione della materia, varando il progetto *Digital Finance Package*. C'è la volontà della massima istituzione dell'UE di tracciare un percorso che spinga e che faccia correre l'innovazione in campo finanziario in sicurezza e verso destinazioni che vale la pena raggiungere. Si spera che vi saranno anche energie e condizioni complessive per recuperare i ritardi e per concludere al meglio il complesso negoziato europeo che è stato aperto dalle proposte della Commissione.

L'innovazione che fa perno sulla digitalizzazione è una risorsa se lo sviluppo della *data economy* e della *token economy* è parte di una strategia più ampia. Una strategia è essenziale per cogliere le opportunità e per mitigare i rischi di una trasformazione che non è certo possibile, ammesso che possa essere desiderabile, frenare. Questa trasformazione – specie in combinazione con la ripresa post pandemia – ha il potenziale per disegnare un nuovo modello di società in Europa. Il pacchetto di proposte avanzato dalla Commissione può, nel frangente in atto, incrociare altre strategie di risposta alla crisi, consentendo di orientare lo sviluppo della finanza digitale verso obiettivi utili per tutti gli *stakeholders*.

Nella costruzione della regolazione andrebbero individuati e perseguiti alcuni obiettivi fondamentali, saldamenti ancorati ai principi dei Trattati UE. La giustificazione di scopo può permettere di varare la regolazione che serve e che fa progredire, insieme con la digitalizzazione (che è innovazione ed è strumento di iniziativa economica), l'utilità sociale di essa, ossia la partecipazione di vasti strati di popolazione ai benefici di questo importante progresso. Per questo piano occorre mettere la dimensione sociale della persona al centro e l'economia al suo servizio, evitando l'acuirsi dei paradossi dello sviluppo economico contemporaneo che fa crescere la ricchezza senza migliorare la vita delle persone.

La regolazione ha anche il compito di presidiare la transizione e fronteggiare scenari in cui il *Fintech* non sostituisce ma affianca modelli tradizionali di produzione di beni e servizi finanziari. Il *Fintech* del resto è già ora una realtà per una fetta di industria finanziaria e per una fascia di clienti e operatori che se ne avvalgono in vario modo. Quando non è tracciata appieno, la penetrazione della digitalizzazione nell'offerta e nella domanda di prodotti e servizi finanziari può cortocircuitare i modelli tradizionali di regolazione e vigilanza.

C'è bisogno di inquadrare il *robo advice e* la negoziazione algoritmica (al momento presidiata solo in punto di resilienza del sistema) nella regolazione dell'offerta di servizi finanziari, avuto riguardo all'insieme di principi di tutela degli investitori che ispirano questa regolazione. Vi è anche da presidiare l'espansione dei canali e dei mercati finanziari innovativi. L'offerta di prodotti e servizi che si collocano su un

mercato distinto, ma contiguo a quello finanziario tradizionale, è in crescita. In questa area si collocano fenomeni vari. Si tratta sovente di attività che per definizione si svolgono in contrasto con la regolazione finanziaria e che possono integrare abusivismo finanziario al ricorrere dei presupposti. C'è dell'altro però, e non si può più ignorare. Ci sono le potenzialità che l'economia e la finanza digitale possono veicolare nell'innovazione e nella crescita. Questo potenziale va incoraggiato ad esprimersi e attratto nel perimetro della regolazione, come si può evincere dagli assunti del *Digital Finance Package* della Commissione europea del 2020 e come si poteva desumere, in precedenza e nel contesto nazionale, dalla pubblica consultazione indetta dalla Consob nel 2019 su una ipotesi di regolazione delle ICOs e dall'iter che - a breve – potrà dotare l'Italia di una normativa (*regulatory sandbox)* di sperimentazione delle applicazioni *Fintech* in ambiente controllato.

Fino a che una cornice regolamentare non sarà delineata e completata, lo sviluppo di *data economy* e di *token economy* riferito a operazioni finanziarie costituirà un terreno in cui le migliori opportunità sono colte da pochi e i rischi si scaricano sul sistema e sui risparmiatori più fragili. Gli *alert* delle autorità sul punto si sono fatti numerosi e insistenti. Mettere in guardia è doveroso ma, al cospetto di fenomeni come questi, insufficiente rispetto al mandato che le autorità di regolazione assolvono per conto delle istituzioni politiche. L'urgenza è il varo di una regolazione appropriata, per garantire adeguati livelli di trasparenza, *accountability* e resilienza a processi, prodotti e servizi. Nello specifico, la regolazione riferita alla produzione, protezione e portabilità dei dati finanziari è cruciale perché afferisce alla materia prima che alimenta l'affermazione della *data economy* in ambito finanziario.

Per altro verso c'è da considerare come la trasformazione digitale sta investendo l'esercizio della vigilanza. Esperimenti pilota di uso dell'IA per finalità di vigilanza sui mercati finanziari (*RegTech* o *Regulatory Technology*, *SupTech* o *Supervisory Technology*) sono praticati in diverse giurisdizioni. Per migliorare la protezione del risparmio e la sua finalizzazione alla crescita dell'economia italiana si può ricorrere alle tecniche di analisi dati basate sull'intelligenza artificiale messe a disposizione dall'innovazione tecnologica. Importantissimo può essere anche il contributo dell'IA per lavorare dati e pervenire a una attendibile valorizzazione dell'effettivo impatto ESG di quelli che vengono definiti investimenti responsabili.

Del resto, la crescita della *data economy* in ambito finanziario ha già fatto crescere la rilevanza dei dati nella regolazione e nella vigilanza del settore. Le iniziative UE in materia sono molteplici, basti ricordare quella già varata sulla digitalizzazione dei bilanci delle società quotate europee, e quella nuova e ancora in costruzione sull'ESAP, ossia sulla costituzione in un *European Single Access Point for Financial and Non Financial Information Publicly Disclosed by Company* integrato e nativo digitale. Siamo all'inizio di un cambiamento di paradigma epocale. Per tenere il passo, le Autorità di mercato dovranno attrezzarsi, rinnovarsi nell'organizzazione e dotarsi di una strategia strutturata per obiettivi e strumenti, per curare integrità e buon funzionamento del mercato e per alimentare fiducia nel nuovo modello di rapporti fra professionisti della finanza e pubblico di risparmiatori.

In questa cornice evolutiva, il Quaderno si prefigge un solido approccio ricostruttivo e sistematico per riconoscere e inquadrare le nuove sfide e per intercettare i rischi associati alla trasformazione digitale, con particolare riferimento alla disciplina inerente ai flussi di dati finanziari. I diversi contributi evidenziano come la migrazione dei servizi finanziari verso ambienti sempre più digitali e caratterizzati da una normativa frammentaria e settoriale, rischi di sfociare in vuoti di tutela che a loro volta possono minare la fiducia nel sistema finanziario, e come si possa usare il ragionamento giuridico per scongiurare tali eventualità, all'insegna della chiarezza ricostruttiva, della certezza del diritto e dei principi generali.

La cornice regolamentare

PRIMA PARTE

(con il coordinamento di S. Alvaro)

EVOLUZIONI NORMATIVE TRA *POLICY* E DIRITTO

S. Alvaro, L. Marzialetti, D. Tuzzolino(*)

1 Gli ambiti della Regulatory technology tra regulation e innovation

1.1 Fintech: *revelation or revolution*?

Una comoda poltrona di velluto avvolge lo spettatore, gli artisti sono in posizione, il maestro, con un rapido e sicuro gesto della mano, dà vita all'insieme orchestrale. Ci si aspetterebbe a questo punto, un crescendo armonico che accompagna l'uditorio lungo le note del brano, con quella rassicurante prevedibilità che contraddistingue l'ascolto di un'opera ben nota. Ed invece, un improvviso colpo di tromba, percussioni e piatti frastornano e disorientano l'ascoltatore.

Questo è quello che è accaduto nel teatro dei mercati finanziari negli ultimi anni.

Si credeva che le novità si sarebbero susseguite con regolare cadenza, dando il tempo ad operatori e regolatori di preparare l'orecchio, di predisporre l'animo. Così non è stato.

La *disruption* originata dalla *financial revolution* ha rapidamente permeato la società nel suo complesso, modificando tanti e vari settori al punto da mettere in discussione i tradizionali schemi giuridici, economici e sociali che erano soliti contenerne e disciplinarne le sonorità. Tale rivoluzione ha interessato e ancora oggi interessa, infatti, tutti i segmenti dell'intermediazione finanziaria, sia sotto il profilo giuridico, determinando un ripensamento del diritto vigente e dei meccanismi di *enforcement*, sia sotto il profilo economico[1]. Velocità, immediatezza e subitaneità sono i concetti da cui

(*) Simone Alvaro, Responsabile Ufficio Sanzioni Amministrative CONSOB (s.alvaro@consob.it);

Lucia Marzialetti, Divisione Informazione Emittenti CONSOB; dottoranda Università Europea e Innovation and Competition Policy Centre-ICPC (l.marzialetti@consob.it);

Davide Tuzzolino, avvocato, dottorando Università Europea e Innovation and Competition Policy Centre-ICPC (davide.tuzzolino@unier.it).

1 Arner, D.W., J. Barberis e R.P. Buckley, *FinTech, RegTech, and the Reconceptualization of Financial Regulation*, 2016; BIS – FSB (2017), FinTech credit. *Market structure, business models and financial stability implications*, Report prepared by a Working Group established by the Committee on the Global Financial System (CGFS - Bank of International

partire per comprendere le sfaccettature, il modo d'essere e di operare di questo fenomeno in atto e, allo stesso tempo, prevederne le mosse future.

La rivoluzione digitale o "*quarta rivoluzione industriale*"[2] è senza dubbio partita con l'avvento di internet ed è arrivata fino al secolo corrente attraverso tre diverse ondate: dapprima, infatti, internet ha reso possibile la diffusione di prodotti e servizi in formato digitale e attraverso il ricorso a sedi di negoziazione *online*; successivamente, il ruolo di intermediario svolto dalle piattaforme *online*, ha permesso di collegare fra loro utenti, venditori e set di prodotti/servizi, fino a giungere al trasferimento diretto non solo di beni, ma anche di valore, sotto forma di prodotti e servizi digitali.

L'impatto della velocità è evidente soprattutto nel settore della finanza. Il mondo dei mercati e dei servizi finanziari, principale laboratorio e banco di prova delle innovazioni tecnologiche, è stato, infatti, forse più di ogni altro, interessato da importanti cambiamenti originati dallo sviluppo del *Fintech*.

La rivoluzione ha investito (e continua ad investire) tutti i settori *latu sensu* finanziari, dal credito (*lending based crowdfunding* o *peer-to-peer lending*) ai servizi di pagamento (*instant payment*), dalle valute virtuali ai servizi di consulenza (*robo-advisor*) e alle tecnologie di validazione decentrata delle transazioni (*blockchain*, DLT e altri sistemi di validazione a doppia chiave crittografata).

Le innovazioni hanno permeato i tradizionali campi dell'azione della finanza, modificando le strutture di mercato, il ruolo ricoperto dagli intermediari, dagli investitori e dai consulenti.

Sofisticate piattaforme di **robo advisory** permettono oggi di elaborare e/o gestire il portafoglio del cliente in forma completamente automatizzata, grazie al ricorso ad algoritmi, che rendono il servizio estremamente personalizzato ed usufruibile da qualsiasi dispositivo h24, in qualsiasi luogo, purché si disponga di una connessione internet[3]. Il ricorso alle piattaforme di *crowdfunding* consente ai *fundraiser* di incontrare un ampio pubblico di potenziali finanziatori e raccogliere in tal modo i finanziamenti necessari per dar vita ad un'idea, un'impresa, un progetto. L'avvento dei contratti intelligenti o *smart contract* rende possibile l'esecuzione e l'applicazione delle condizioni contrattuali automaticamente senza la necessità di intervento umano, grazie ad

Settlement), and the Financial Stability Board, 22.5.2017; Bresnahan T., Trajtenberg M., *General Purpose Technologies: Engines of Growth?*, 65(1) Journal of Econometrics, 83-108, 1995; Brummer C., Yadav Y., *Fintech and the Innovation Trilemma*, 107 GEO. L.J. 235, 275– 278, 2019; Carney M., *The Promise of Fintech – Something new under the sun?*, speech given for Deutsche Bundesbank G20 conference on *"Digitising finance, financial inclusion and financial literacy*", Wiesbaden, 25 gennaio 2017; European Parliament, *Report on FinTech: the influence of technology on the future of the financial sector*, (2016/2243(INI)), Committee on Economic and Monetary Affairs, Rapporteur: Cora van Nieuwenhuizen, RR\1124611EN, 2017; Kowalewski O., Pisany P., *The Rise of Fintech: A Cross-Country Perspective*, 2020; IESEG Working Paper Series 2020-ACF-07, 2020; Buterin V., *The Meaning of Decentralisation*, medium.com, 6 febbraio 2017; Carney M., *Enabling the Fintech transformation: Revolution, Restoration, or Reformation*, speech given at Mansion House 16 June 2016; Zhang, B., Baeck P., Ziegler T., Bone J., e Garvey K., *Pushing Boundaries: the 2015 UK Alternative Finance Industry Report*, U.K., University of Cambridge and Nesta, 2016.

2 Cfr. Schwab K., *The Fourth Industrial Revolution,* Portfolio Penguin, London 2017, 32; Schwab K., Davis N., *Shaping the Future of the Fourth Industrial Revolution. A Guide to Building a Better World*, Portfolio Penguin, London,2017, 65.

3 Sul tema cfr. amplius Alemanni B., Angelovski A., Di Cagno D., Galliera A., Linciano N., Marazzi F., Soccorso P., *La fiducia nel robo advice - Evidenze da uno studio sperimentale*, Quaderno Fintech Consob N. 7 (settembre 2020).

algoritmi e protocolli informatici ivi codificati[4]. Conseguentemente e per l'effetto, ne sono risultate modificate tutte le funzioni alle stesse connesse: profilazione, gestione della contrattazione, *customer relations*, *backoffice*, funzioni di controllo e *investor relations*. Tutte attività il cui svolgimento è stato fortemente digitalizzato attraverso il ricorso a documenti in formato elettronico ed alla firma elettronica, all'accesso ai servizi di investimento e pagamento on line. In tali settori, inoltre, da un lato l'ascesa delle *criptocurrencies* accentua il pericolo di dissociazione fra moneta e risparmio, fra moneta ed economia reale; dall'altro il ricorso ai *criptoasset* ha posto in discussione le nozioni stesse di prodotto finanziario e di offerta di prodotti finanziari al pubblico. La tecnologia è entrata anche nel diritto societario, modificando le strutture della stessa corporate governance, prevedendo la possibilità di dar vita a società quotate digitali in cui gli algoritmi entrano nel processo di formazione delle delibere del Consiglio di Amministrazione, o addirittura in cui il *board* è composto da algoritmi[5] sapientemente codificati ed in cui il voto dei soci viene trasmesso per corrispondenza. Algoritmi e codifiche erano d'altronde già da tempo impiegate nel mondo della finanza. Si pensi all'*Algotrading* (i.e. *Algorithmic trading*): una modalità di negoziazione basata sull'utilizzo di algoritmi e programmi informatici molto complessi che raccolgono ed elaborano le informazioni e i dati di mercato in tempo reale (HFT) e avviano in automatico gli ordini (di vendita o di acquisto di strumenti finanziari) sulle diverse piattaforme di negoziazione. Tale strategia di investimento negli USA ammonta oggi a più del 50% delle transazioni[6] e si stima che oltre l'80% delle negoziazioni nel mercato FOREX sia effettuato da algoritmi di trading[7].

Oltre ad impattare sulle strutture preesistenti, questa sinergia fra innovazione tecnologia ed *expertise* finanziaria ha dato inevitabilmente vita ad una rinnovata offerta di prodotti e servizi caratterizzati dalla digitalizzazione, dalla disintermediazione e dalla decentralizzazione, comportando, per l'effetto, anche una ricomposizione degli operatori e degli attori del mercato. Il *Fintech* ha, infatti, modificato la struttura del mercato, incentivando la comparsa di piattaforme[8] e costringendo le imprese ad una risposta strategica.

4 Per una disamina più approfondita si rimanda a Mik E., *Smart Contracts: Terminology, Technical Limitations and Real World Complexity,* in Law, Innovation & Technology, 2017; Lauslahti K., Mattila J., Seppälä T., *Smart Contracts. How will Blockchain Technology Affect Contractual Practices?*, 2017; Irti N., *Norma e luoghi. Problemi di geo-diritto*, Laterza, Roma-Bari, 2006; Grundmann S., Hacker P., The Digital Dimension as a Challenge to European Contract Law. The *Architecture*, in S. Grundmann (a cura di), European Contract Law in the Digital Age, Intersentia, Cambridge, 2018; UE Commission, *EUROPA 2020: Una strategia per una crescita intelligente, sostenibile e inclusiva, COM (2010) 2020.*

5 Il riferimento è alla società di Hong Kong Deep Knowledge Ventures (DKV) - una società di capitale di rischio di Hong Kong specializzata in medicina rigenerativa - che nel maggio 2014 ha aperto nuovi orizzonti nominando un algoritmo chiamato "VITAL (Validating Investment Tool for Advancing Life Sciences)" al suo consiglio. VITAL formula raccomandazioni in materia di investimenti analizzando enormi quantità di dati sulla situazione finanziaria, le sperimentazioni cliniche e la proprietà intellettuale delle future società. Come gli altri cinque membri del consiglio, l'algoritmo può votare se l'azienda fa un investimento in una società specifica o no. Per un approfondimento cfr. Schwab K., *The Fourth Industrial Revolution*, 2016, pg. 149; Harari Y.H., *Homo Deus: A Brief History of Tomorrow,* 2015, pg. 322

6 SEC, *Staff Report on Algorithmic Trading in U.S. Capital Markets*, Staff of the U.S. Securities and Exchange Commission, August 5, 2020.

7 Cfr. Bigiotti A., Navarra A., *"Optimizing Automated Trading Systems"*, Advances in Intelligent Systems and Computing, Springer International Publishing, October 19, 2018.

8 Per un approfondimento in tema di *multisided markets e multisided platform*, cfr. Evans D.S., Schmalensee R., *Matchmakers: The New Economics of Multisided Platforms*, Harvard Business Review Press, 2016; Evans D.S., *The Antitrust*

La rapida diffusione dell'*innovation technology* oltre i confini territoriali ed economici ha dunque imposto un ripensamento delle usuali tecniche di regolamentazione, rendendo necessaria una cooperazione tra Autorità nazionali ed un coordinamento fra i diversi ordinamenti nazionali in un'ottica di *levelling the playing field* e di armonizzazione.

Per fare ciò e al fine di addivenire ad una regolamentazione efficace ed efficiente è necessario preliminarmente interrogarsi sull'opportunità e il modo in cui disciplinare il fenomeno *Fintech.* Si tratta, in altre parole di domandarsi se siamo di fronte ad una "*revelation*", ossia (riprendendo la metafora iniziale) ad una evoluzione di una melodia già nota, ma suonata a volumi più alti, la quale rende necessario "semplicemente" riadattare i vecchi spartiti dei tradizionali schemi giuridici; oppure se si tratti, invece, di una rivoluzione, e quindi di una musica del tutto nuova che modifica ontologicamente gli schemi classici.

Il tema centrale se il *Fintech* sia semplicemente "*more of the same*" – ossia se si tratti di una diversa connotazione di un fenomeno già in atto non richiederebbe nuove regole – oppure se si sia di fronte ad una radicale trasformazione, che pone sfide uniche e richiede, quindi, normative adeguate[9] è stato ampiamente dibattuto.

Le criticità in tale ambito derivano soprattutto dalla complessità di incasellare entro una cornice dai contorni definiti le molteplici sfaccettature in cui il fenomeno si articola, sicché le risposte alle domande che precedono dipendono dall'angolo visuale dal quale si osserva il fenomeno[10].

La rivoluzione determinata dal *Fintech* si distingue nettamente dalle precedenti applicazioni di tecnologie al sistema finanziario sulla base di alcune caratteristiche chiave: (1) i dirompenti processi di *digitization* e *digitalization*; (2) il crescente

Economics of Multi-Sided Platform Markets, Yale Journal on Regulation Vol.20 Issue.2, Article4, 2003; Yang Y.S., *Rethinking models of relevant market definition for multisided platform*, International Journal of Trade, Economics and Finance, Vol. 9, No. 4, August 2018; Hagel J., *Business Ecosystems come of age. The power of platforms*, Deloitte University Press, 2015; Auer D., Petit N., *Two-Sided Markets and the Challenge of Turning Economic Theory into Competition Policy,* 2016.

9 Barba Navaretti G., Calzolari G., Pozzolo A.F., *FinTech and Banks: Friends or Foes?*, European Economy, vol. 2: 9-31, 2017; Jovanovic B., Rousseau P., *General Purpose Technologies*, Handbook of Economic Growth, edited by Philippe Aghion and Steven Durlauf, Volume 1, Elsevier, 2005; McQuinn, A., Guo W., Castro D., *Policy Principles for FinTech,* ITIF - Information Technology & Innovation Foundation, vol. 1-52, 2016; De Filippi P, Wright A., *Blockchain and the Law*, Harvard University Press, 2018; EBA, Discussion Paper on the *EBA's approach to financial technology (FinTech*), EBA/DP/2017/02, 4 August 2017; FSB, CGFS, Financial Stability Board e Bank of International Settlements (CGFS), *Fintech Credit. Market Structure, Business Models and Financial Stability Implications*, 22 maggio 2017.

10 Da un punto di vista transazionale, i servizi finanziari si affidano, infatti, sempre più alle tecnologie emergenti (ad esempio, intelligenza artificiale e big data) e a nuovi modelli di business (ad esempio, prestiti ICO e P2P), da un lato disgregando le funzioni finanziarie tradizionali, dall'altro creando nuove attività finanziarie. Da un punto di vista strutturale, inoltre, il settore finanziario si è trasformato da un'industria omogenea dominata da pochi grandi istituti finanziari in un'industria più ampia e disintermediata, che comprende tipi di operatori di mercato sempre diversi (Startup Fintech, aziende Techfin e istituti finanziari). Tali innovazioni, peraltro, tendono a crescere in modo esponenziale, creando nuove sfide legate al fatto che la regolamentazione non riesce a stare al passo dei cambiamenti economici e tecnologici con la stessa velocità di risposta cd "*pacing problem*". *Ofir M., Sadeh I., More of the Same or Real Transformation: Does FinTech Warrant New Regulation?, February 4, 2020.* Butenko A., e Larouche P., così spiegano le tipicità del *"pacing problem": <<This is a situation when technology develops faster than the corresponding regulation, [and] the latter hopelessly falling behind>>,* in *Regulation for Innovativeness or Regulation of Innovation?, 7 L. Innovation* & Tech. 52, 66-68, 2015.

utilizzo di AI; (3) il crescente sfruttamento di *big data analytics*; e (4) la disintermediazione.

I servizi finanziari si affidano, infatti, sempre più alle tecnologie emergenti (*AI* e *big data*) e a nuovi modelli di *business* per disintermediare le funzioni finanziarie tradizionali e creare nuove attività, modificando il modo in cui consumatori/utenti e operatori del settore interagiscono. Ciò ha comportato, grazie all'impiego di algoritmi decisionali che affiancano e sostituiscono gradualmente gli esseri umani nell'offerta di servizi finanziari, un notevole abbassamento dei costi e un efficientamento dei processi[11].

Oltre a trasformare l'industria finanziaria in termini di diversificazione e disintermediazione, questi cambiamenti stanno anche gradualmente modificando il contesto macroeconomico di riferimento, provocando il passaggio da quello che potrebbe essere definito come un settore finanziario "*puro*" ad uno "tecnologicamente orientato", in cui si scontrano nuovi e vecchi attori[12].

A ben vedere tutte le modifiche, le novità e le innovazioni sottendono, però, un obiettivo comune: quello della semplificazione, della massimizzazione della efficienza e della concorrenzialità nel panorama internazionale[13] attraverso un approccio modulare. Ciò si traduce in un modello di *business* ed organizzativo che punta alla riduzione dei costi e degli oneri dell'attività di impresa, attraverso la micro-segmentazione dei mercati e la creazione di servizi personalizzati per il pubblico.

In questa sinfonia forse è allora possibile affermare che, come in un'orchestra anche una singola nota può essere percepita diversamente a seconda dello strumento che la suona, così nel panorama finanziario si assiste ad una concomitante esecuzione

11 Per una disamina completa del fenomeno cfr. Alt R., Beck R., Smits M., *FinTech and the Transformation of the Financial Industry*, 28 Electronic Markets, 2018; Alyoshkin R., *Blockchain 2.0. The Purpose of Blockchain, 2017*; Arner, D.W., Barberis J., Buckley R.P., *The evolution of fintech: new post-crisis paradigm*, Georgetown Journal of International Law, vol. 47(4): 1271-1320, 2016; Boot A., *Understanding the Future of Banking Scale & scope economies, and fintech*, University of Amsterdam, mimeo, 2016; Carney M., *Building the Infrastructure to Realise FinTech's Promise*, International FinTech Conference, 2017; CB Insights, *How Blockchain Could Disrupt Banking*, 8 febbraio 2018; CB Insights, *Where Top US Banks Are Betting On Fintech*, 1 febbraio 2018; Dermine, J., *Digital Banking and Market Disruption: a Sense of Déjà Vu?*, in AA.VV. Financial Stability in the Digital Era, Banque de France, Financial Stability Review, vol. 20, 2016; European Commission, *Consultation document - Fintech: A more competitive and innovative financial sector*, Bruxelles, 23 marzo 2017; Finocchiaro G., Falce V., *Fintech: diritti, concorrenza, regole*, Zanichelli, 2019; Jacobides M., Knudsen T, Augier M., *Benefiting from Innovation: Value Creation, Value Appropriation and the Role of Industry Architectures*, 35 Research Policy, 2006; Mathew A., The Myth of the Decentralised Internet, 5(3) Internet Policy Review, 2016; Navaretti Barba G., Calzolari G., Mansilla-Fernandez J.M., Pozzolo A.F., "FinTech and Banks: Friends or Foes?", European Economy: Banks, Regulation, and the Real Sector, December 2017; Schwab K., The Fourth Industrial Revolution, Portfolio Penguin, London 2017; Zetzsche D.A., Arner D.W., Buckley R.P., Decentralized Finance (DeFi), IIEL Issue Brief 02/2020, European Banking Institute Working Paper Series 59/2020, University of Hong Kong Faculty of Law Research Paper No. 2020/010, University of Luxembourg Faculty of Law, Economics & Finance WPS, 2020.

12 Sul punto *cfr.* Magnuson W. (in *Regulating Fintech*, 71 VAND. L. REV. 1167, 2018. *Cfr* anche Brummer C., Yadav Y., *Fintech and the Innovation Trilemma*, 107 GEO. L.J. 235, 275– 278, 2019) ove si osserva *<< [...] regulating FinTech is different because FinTech applications reshape the structure of the financial industry as a whole. Advances in AI and big data analytics enable the creation of novel business models that allow new small startups to enter the market and disintermediate traditional services. These new startups, whose main area of expertise is often technology rather than finance, are gradually capturing a sizeable market share and transforming the financial industry from a concentrated market dominated by few "too-big-to-fail" institutes into a more dispersed market that includes a variety of small actors>>.*

13 "*Fintech è tecnologia per la semplificazione applicata ai servizi finanziari*", in *Lo sviluppo del Fintech. Opportunità e rischi per l'industria finanziaria nell'era digitale*, Quaderni Fintech Consob, pag. IX, op. cit.

di sparititi vecchi e nuovi, in cui melodie antiche e strumenti moderni coesistono, si sovrappongono e si scontrano, causando quello che oggi appare come una sorta di "frastuono" che genera un certo senso di disorientamento da parte degli operatori del settore. Ciò è amplificato dalla velocità con la quale tali realtà *fintech* si sviluppano e dagli alti livelli di sofisticazione che rendono ancora più arduo il compito del regolatore, il quale, prendendo le mosse dalle strategie messe in atto dagli intermediari già presenti nel settore, si trova a dover definire nuove politiche di regolamentazione, sia nazionali sia europee, tenendo in adeguata considerazione i diversi aspetti dell'innovazione tecnologica, della concorrenza, della *privacy* e protezione dei dati, della *cybersecurity*.

Le novità scaturenti dal fenomeno *fintech*, oltre a costituire opportunità da cogliere, rappresentano, infatti, anche sfide da affrontare sotto il profilo dei rischi sistemici e operazionali, della sicurezza e dell'affidabilità del sistema nel suo complesso.

Di qui la stringente necessità di predisporre una regolamentazione che possa essere in grado di affrontare in maniera uniforme e condivisa queste nuove problematiche, cosicché si possa sfruttare appieno l'alto potenziale del *Fintech*[14].

L'ontologica intersettorialità del fenomeno e la sua innata trasversalità, non solo tematica, ma anche e soprattutto geografica, rendono necessaria un'azione coordinata, o di "*coopetition*", a livello non solo europeo, ma internazionale, per adeguare gli strumenti della regolazione prima e della vigilanza poi al nuovo contesto economico-finanziario, che corre inevitabilmente più velocemente rispetto alle risposte dei singoli ordinamenti. Di fronte a questo scenario nuovo ed in continuo cambiamento, l'operazione concettuale che si richiede è allora quella di smontare per poi ricostruire le categorie giuridiche ricevute dalla tradizione al fine di adattarle e modellarle al nuovo contesto.

1.2 La *Digital disruption* nei mercati finanziari

Il termine Fintech enuclea tutte quelle attività nelle quali si assiste ad una offerta di servizi di finanziamento, di pagamento, di investimento e di consulenza ad alta intensità tecnologica. Tale innovazione riverbera i suoi effetti nel campo dei servizi sia finanziari sia bancari[15], modificandone la struttura. In particolare il lessema nasce dalla crasi delle parole 'finanza' e 'tecnologia' ed è traducibile nella formulazione generica "tecnologia applicata alla finanza"[16].

14 *"But the biggest prize arises from Fintech's potential to combine seamless, real-time payments, distributed commerce, more sophisticated client targeting and more accurate credit scoring. The more this can be realised the more the new financial system will support the new creative jobs people will need – and enjoy – in the coming Machine Age*", Carney M., *The Spectre of Monetarism'* speech given at the Roscoe Lecture, Liverpool John Morres University, 5 December 2016.

15 Settori maggiormente coinvolti sono: credito, servizi di pagamento, valute virtuali, consulenza, biometrica, supporto all'erogazione di servizi.

16 In *Lo sviluppo del Fintech. Opportunità e rischi per l'industria finanziaria nell'era digitale*, Quaderni Fintech Consob, pag. VIII, op.cit.

Nonostante in letteratura non vi sia unanimità[17] circa la definizione esatta da attribuire al fenomeno, molti sono concordi nel ritenere che con tale espressione si faccia in generale riferimento a «*un insieme indistinto di società accomunate dallo sviluppo di attività basate su nuove tecnologie informatiche e digitali, che vengono applicate in ambito finanziario*»[18].

Un fenomeno intersettoriale[19], dunque, che interessa sia l'offerta di servizi agli utenti finali sia i processi "produttivi" degli operatori finanziari. Da un lato, infatti, l'innovazione tecnologica ha avvicinato la clientela ai servizi finanziari, grazie all'utilizzo di piattaforme digitali e *App* per *smartphone*[20]; dall'altro ciò ha causato una crisi degli operatori tradizionali. Gli attori già nel mercato (cd. *incumbents*) hanno, infatti, dovuto rapidamente adeguare il proprio *business model* alla nuova struttura digitale, confrontandosi necessariamente con l'ascesa di nuovi *players*, per lo più *start-up*, portatori di nuovi modelli organizzativi che propongono una modularizzazione delle attività finanziarie ed una moltiplicazione dei canali di intermediazione diretta, offrendo servizi specializzati in specifici ambiti operativi[21].

17 Una definizione è fornita da Arner, il quale evidenzia come *"Fintech refers to the application of technology to finance"*, mettendo in rilievo che soggetti non vigilati utilizzano la tecnologia per fornire soluzioni finanziarie, che in passato erano offerte solo da intermediari finanziari regolamentati. In senso analogo si esprime Zetzsche rilevando che *"Fintech in its broadest sense refers to the use of technology to deliver financial solutions"*. Un'accezione più puntuale si ritrova, invece, nel FSB: *"Fintech is defined as technology-enabled innovation in financial services that could result in new business models, applications, processes or products with an associated material effect on the provision of financial services"*. In questa ottica, il Fintech costituisce un fenomeno "orizzontale" interno al settore dei servizi finanziari, che si sta sviluppando nel più ampio quadro della *digital economy*.

18 "*Per approfondire gli aspetti operativi si è fatto prevalentemente riferimento alle attività svolte dalle Fintech operanti in Italia (gradualmente censite nel corso del 2017 e aggiornate sino all'inizio di marzo 2018), chiarendo anche le specificità delle scelte regolamentari compiute nel contesto nazionale rispetto a quanto riscontrabile all'estero", in Lo sviluppo del Fintech. Opportunità e rischi per l'industria finanziaria nell'era digitale*, Quaderni Fintech Consob, op. cit., pag. 9.

19 «*Fintech is an umbrella term encompassing a wide variety of business models*» in ECB, *Guide to Assessments of Fintech Credit Institution Licence Applications*, Sept. 2017.

20 Capgemini - EFMA, *World FinTech Report 2017*, www.worldfintechreport2017.com; Davidson S., De Filippi P., Potts J., *Blockchains and The Economic Institutions of Capitalism*, 14(4) Journal of Institutional Economics, 2018.

Kane E., *Is Blockchain a General Purpose Technology?*, 2017; Lianos I., *Blockchain Competition*, in Research Paper Series: 8/2018, UCL, Centre for Law, Economics and Society, 2018; Morgan Stanley, *Blockchain: Unchained?*, 2017; OECD (2018), *Financial Markets, Insurance and Private Pensions: Digitalisation and Finance*, 2018; OICV-IOSCO, *IOSCO Research Report on Financial Technologies* (*Fintech*), 2017.

21 Il ricorso alla tecnologia consente, infatti, agli intermediari finanziari tradizionali (banche, compagnie di assicurazione e controparti centrali di compensazione) di operare su piattaforme *technology-led* e *peer-to-peer*, quali espressione della *sharing economy*. A partire dall'avvento dei cd. *Big-Tech* - iniziali esponenti dell'economia *data driven* – si è in particolare registrata una pressione competitiva verso la disaggregazione, che ha mutato il rapporto intermediario-cliente. In molti settori, inclusi i trasporti (es. app di *ride-sharing* come Uber) e l'ospitalità (es. app di *house-sharing* come Airbnb) le piattaforme/app digitali hanno disintermediato gli operatori storici, ciò soprattutto a fronte dell'inasprimento della crisi finanziaria globale, recentemente acuita a causa della pandemina da Covid-19, che ha creato l'opportunità per le *start-up* e le imprese di sviluppare prodotti finanziari innovativi per raggiungere il maggior numero di utenti e consumatori. Sul punto *Cfr.* Arner D.W., Barberis J.N., Buckley R.P., '*The Evolution of Fintech: A New Post-Crisis Paradigm?*'(2015) University of Hong Kong Faculty of Law Research Paper No. 2015/047; Buchak G., Matsos G., Seru A., '*Fintech, Regulatory Arbitrage and the Rise of Shadow Banks,* 2018. In relazione alle implicazioni derivanti da tali interconnessioni, cfr. Aggarwal N., in "*Fintech Credit and Consumer Financial Protection*", forthcoming in *Chiu and Deipenbrock (Eds) Routledge Handbook on Fintech and the Law (2020)* che evidenzia come "*[...] the general trend of datafication, digitisation and disintermediation in consumer credit markets is blurring the boundary between 'fintech' and 'traditional' consumer credit. To the extent that most credit providers are turning to data-driven, digital technology, all credit is or soon will be fintech credit*".

A tal proposito occorre sin da subito sgombrare il campo da alcuni equivoci: le imprese *Fintech*[22], originariamente nati come operatori finanziari che operavano in competizione e contrapposizione con gli *incumbent*, diversamente da quanto si è portati a pensare, non rappresentano una "nuova" industria, ma costituiscono semplicemente una componente nuova dell'industria finanziaria. Tali imprese si distinguono, però, per una caratteristica oggettiva: lo svolgimento di attività finanziarie attraverso soluzioni tecnologiche innovative in un'ottica di stimolo alla concorrenzialità e all'efficientamento del sistema finanziario e dei suoi meccanismi.

Tre sono allora i processi, tra di loro interconnessi, che possiamo individuare come caratterizzanti l'era *Fintech*: *digitisation*, *disintermediation* e *datafication.*

I termini anglosassoni, di più immediata comprensione, descrivono il complesso sistema di interrelazioni che governano i mercati finanziari, e dei quali occorre comprendere le potenziali opportunità ed i rischi, nonché il modo con il quale la regolamentazione possa al meglio amplificare i benefici e ridurre gli impatti negativi, tutelando gli utenti.

Con l'espressione *digitisation* o "digitalizzazione" si intende il passaggio dalla tecnologia analogica a quella digitale, "*dagli atomi ai bit*"[23]. Si tratta di una tendenza verificatasi negli ultimi decenni, ma che a seguito dei repentini cambiamenti nel contesto macroeconomico e normativo ha registrato, soprattutto nell'ultimo periodo imperversato dalla crisi sanitaria da Covid-19, una significativa accelerazione.

La seconda espressione, la *disintermediation* o "disintermediazione", indica il ridimensionamento del ruolo di intermediazione svolto dagli istituti di credito per effetto del calo dei depositi bancari, connesso da una parte allo sviluppo di forme di risparmio alternative, dall'altra allo sviluppo di nuove attività e istituzioni con compiti sempre più specializzati.

Infine, con il termine *datafication* o "dataficazione" si descrive la crescente dipendenza dai dati e dai metodi di calcolo basati sui dati nel processo decisionale finanziario. Il volume dei dati (personali e non) disponibili è, infatti, aumentato in modo esponenziale, quale causa ed al contempo conseguenza di una la società sempre più interconnessa, digitalizzata e "dataficata", grazie al miglioramento della potenza di

22 Ai fini di una migliore sistematizzazione, si è soliti poi classificare tali tipologie di "nuovi" operatori in due principali categorie: le *financial technology companies* (o più semplicemente imprese *Fintech*), che offrono servizi propriamente finanziari in competizione con gli *incumbent* e le *technology companies* (o le imprese *Tech*), aziende del settore tecnologico che sviluppano attività strumentali, servizi e applicativi utili per le attività finanziarie, spesso nella veste di fornitori o partner degli operatori *incumbent*, a supporto del loro sviluppo tecnologico e non in concorrenza tra loro. La fondamentale differenza che intercorre tra le categorie *supra* distinte risiede nella diversa accezione e utilizzazione che esse hanno della tecnologia: se per le prime rappresenta uno strumento, un fattore produttivo; per le seconde la tecnologia è, invece, l'oggetto stesso della produzione. Posto che solamente le prime possono essere ascritte al settore finanziario, dovendo le seconde essere ricomprese nel settore tecnologico più propriamente detto, occorrerà individuare con certezza le imprese essenzialmente Fintech, onde analizzare le loro caratteristiche e il rapporto con gli altri operatori del settore e di qui i destinatari delle nuove norme e delle nuove discipline.

23 Negroponte N., *Being Digital* (Alfred A. Knopf 1995); Balyuk T., Davydenko S., '*Reintermediation in Fintech: Evidence from Online Lending*', 2019.

calcolo, degli strumenti e delle infrastrutture necessari per acquisire e trattare tali dati[24].

A tal fine gli obiettivi fondamentali della tutela degli investitori e dei consumatori, della stabilità finanziaria e dell'integrità del mercato, quali risposte ai principali fallimenti del mercato, possono essere perseguiti sfruttando i nuovi canali ed i nuovi approcci imposti dalla digitalizzazione e dalla innovazione.

La finanza digitale introduce, infatti, nuove possibilità per correggere l'asimmetria delle informazioni, quale ostacolo alla tutela degli investitori o, più in generale, alla tutela dei consumatori di servizi finanziari. In questo campo, infatti, l'asimmetria informativa è forse il maggior ostacolo alla salvaguardia del sistema nel suo complesso, proprio in ragione dell'elevata specificità e tecnicità della materia. Se da un lato, infatti, il ricorso a sistemi crittografati, alla *DLT* e alla decentralizzazione dei servizi possono produrre benefici per il mercato e i consumatori/utenti in termini di concorrenza e offerta di prodotti e servizi[25], dall'altro l'impiego di nozioni e strumenti altamente tecnici impedisce di comprendere appieno il funzionamento dei procedimenti, causando, inevitabilmente dei vuoti di tutela[26].

La finanza digitale è, tuttavia, anche in grado di ridurre le asimmetrie informative, soprattutto incentivando e migliorando l'inclusione finanziaria[27]. In tal senso alcune iniziative *fintech,* assicurando l'accesso ai prodotti finanziari ad un pubblico più ampio, riducono il *gap* informativo sia sul lato dell'offerta sia su quello della domanda dei servizi finanziari stessi. In particolare, dal lato della domanda, la tecnologia digitale rende, infatti, possibile ai consumatori/utenti di regioni più remote e meno sviluppate di godere di un accesso paritario ai prodotti e ai servizi finanziari e alle informazioni, abbattendo i costi di accesso. Anzi, proprio nelle regioni scarsamente digitalizzate questi sviluppi sono stati particolarmente rapidi, per alcuni aspetti addirittura superando i mercati tradizionali (es. pagamenti, telefonia, etc.). Sul lato dell'offerta, invece, banche ed altri istituti hanno beneficiato del grande numero di informazioni derivante dalla raccolta ed analisi dei dati, per adattare i loro servizi alle esigenze della clientela e per abbattere i costi interni.

24 Il fenomeno per cui si sfruttano una serie indefinita di dati, raccolti e successivamente analizzati, è anche chiamato 'Big Data'. Sul punto *cfr.* Mayer- Schönberger V., Cukier K., *Big Data: A Revolution That Will Transform How We Live, Work and Think*, John Murray 2013.

25 Si è osservato come nel corso del tempo il decentramento possa ridurre le asimmetrie informative, ciò in ragione del fatto che i mercati decentralizzati elaborano l'informazione meglio di un'economia pianificata centralmente e quindi allocano le risorse in modo più efficiente (sul tema cfr. Hayek, F., *The Use of Knowledge in Society*, The American Economic Review, 35(4): 519–530, 1945). Ad oggi occorrerà attendere i primi sviluppi ed i conseguenti effetti al fine di verificare se l'emergere di piattaforme digitali possa facilitare il decentramento senza attriti e incentivare il coordinamento.

26 Amstad M., *Regulating Fintech: Objectives, Principles, and Practices,* Asian Development Bank Institute Working Paper Series 1016, October 2019, Tokyo

27 *Cfr.* Cohney S., Hoffman D., Sklaroff J., Wishnick D., *Coin-Operated Capitalism*, Columbia Law Review 119(3): 591–676, 2018; Cong W., He Z., *Blockchain Disruption and Smart Contracts*, Review of Financial Studies, 2018.

Se, quindi, la promessa della tecnologia può potenzialmente ridurre le disparità imprenditoriali, occorre però tenere conto degli ostacoli derivanti dalla elevata tecnicità e specificità delle competenze richieste, che possono ritardare o impedire la crescita inclusiva che poggia, come visto, sull'innovazione.

1.3 La trasformazione finanziaria come motore della regolamentazione

Il rapido e diffuso sviluppo dei servizi digitali ed il mutato contesto di mercato richiedono che la legislazione europea si evolva e stia al passo con i cambiamenti, affinché sia in grado di cogliere sia i benefici che ne derivano sia, al contempo, di affrontare le sfide ed i rischi che si generano dall'onda *disruptive* della *fintech*[28]. In tale scenario l'Europa sta dimostrando, attraverso la predisposizione di numerose iniziative, di voler stare al passo coi tempi introducendo moduli normativi e istituti in grado di assicurare una disciplina armonizzata del settore e intervenendo nei settori maggiormente impattati dalle nuove tecnologie: l'uso e la protezione dei dati, la rimozione delle barriere all'entrata e la lotta contro le asimmetrie informative. Si è preso atto del fatto che le norme attuali non sono né sufficienti né efficaci per regolamentare adeguatamente i nuovi modelli di *business* e i nuovi prodotti, sicché per rispondere alle nuove esigenze normative, è importante discostarsi dalle strategie tradizionali cercando di trovare e sperimentare approcci più innovativi per bilanciare i rischi e i benefici dell'innovazione tecnologica nel settore finanziario, senza pregiudizi[29]. Il compito è quello di modulare l'approccio con cui ci si rapporta al fenomeno, adattando e modificando, laddove possibile, le strutture già esistenti, e, senza operare ingiustificate discriminazioni, verificare se si stia assistendo all'offerta di prodotti del tutto nuovi oppure se si tratti delle stesse attività e servizi già offerti dagli altri operatori finanziari che vengono, però, immessi nel mercato sotto altro nome. A tal fine hanno preso il via

28 Omarova S. T., considera il *fintech* come una forza sistemica che sconvolge l'attuale paradigma tecnocratico dominante della regolamentazione finanziaria e offre, a tal fine, una tassonomia volta a spiegare (1) i cambiamenti chiave *fintech-driven* nella struttura e nel funzionamento del sistema finanziario, e (2) le sfide che questi cambiamenti sistemici pongono nella continua ricerca di una regolamentazione efficace. In particolare riconduce le sfide principali di ciascuna delle tendenze *fintech* alle seguenti: *the Scale/Scope Challenge; the Speed/Velocity Challenge; the Trust/Power Challenge; the Transparency/Governability Challenge.; the Boundary Challenge*, in *Technology v. Technocracy: Fintech as a Regulatory Challenge*, 6 J. Fin. Reg. 1 (2020), Cornell Legal Studies Research Paper No. 20-14, 2020.

29 Buckley R.P., Arner D.W., Veidt R., Zetzsche D.A., *Building FinTech Ecosystems: Regulatory Sandboxes, Innovation Hubs and Beyond,* op.cit.; Butenko A., e Larouche P., *Regulation for Innovativeness or Regulation of Innovation?,* 7 L. INNOVATION & TECH., 2015; Cambridge Centre for Alternative Finance, *Early Lessons on Regulatory Innovations to Enable Inclusive FinTech: Innovation Offices, Regulatory Sandboxes, and RegTech,* Cambridge, University of Cambridge, 2019; Deloitte, *RegTech Is The New FinTech. How Agile Regulatory Technology Is Helping Firms Better Understand and Manage Their Risks*, 2015; Colangelo G., Borgogno O., *Regulating FinTech: From Legal Marketing to the Pro-Competitive Paradigm*, 2020; Magnuson W., *Regulating Fintech*, 71 VAND. L. REV. 1167, 2018; Ofir M., Sadeh I., *More of the Same or Real Transformation: Does FinTech Warrant New Regulation?,* February 4, 2020; Gurrea-Martínez A., Remolina N., *Global Challenges and Regulatory Strategies to Fintech*, Banking & Finance Law Review, SMU Centre for AI & Data Governance Research Paper No. 2020/01, April 2020; Omarova S. T., *Technology v. Technocracy: Fintech as a Regulatory Challenge*, 6 J. Fin. Reg. 1 (2020), Cornell Legal Studies Research Paper No. 20-14, 2020; Omarova S. T., *Dealing With Disruption. Emerging Approaches to FinTech Regulation*, 61 WASH. U. J. L. & POL'Y 25, Cornell Legal Studies Research Paper No. 20-17, Cornell University - Law School, 2020; Zetzsche D.A., Arner D.W., Buckley R.P., Kaiser-Yücel A., *Fintech Toolkit/ Smart Regulatory and Market Approaches to Financial Technology Innovation*, Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ), Frankfurt, 2020.

hubs fintech[30] per l'innovazione e *sandboxes* di regolamentazione, così da coinvolgere più efficacemente gli operatori e testare le innovazioni in un ambiente controllato, valutando se le leggi esistenti siano appropriate per regolare tali prodotti e, in caso contrario, quali misure possano essere richieste[31]. Comprenderne gli impatti e gli obiettivi vuol dire, infatti, analizzare la capacità della società di rispondere alle sfide sistemiche che il *fintech* pone e tradurla in una strategia di regolamentazione coerente ed efficace[32], in grado di affermare il primato del diritto sulla tecnologia, il giudizio politico sulla capacità computazionale, e il benessere collettivo e la tutela degli individui sul profitto[33]. Si tratta di una operazione necessaria perché non rispondere tempestivamente a tali cambiamenti significherebbe restare inesorabilmente indietro e privare i mercati e i consumatori di nuovi servizi e tutele adeguate.

Le risposte normative a tali e tante esigenze sono state diverse[34].

La strategia inizialmente attuata dai regolatori di fronte alle novità tecnologiche che man mano si sono presentate è stata quella di intervenire in maniera mirata e circoscritta. Complice anche la cadenza periodica con le quali le novità, e con esse i nuovi problemi, si sono presentati, si è assistito nel tempo a risposte normative singole per singole problematiche, o, per riprendere la metafora di cui sopra, per ciascuno strumento veniva confezionato uno spartito. Sono figlie di questa impostazione tutte quelle misure dei primi anni del 2000, volte a regolamentare in maniera sempre più aderente alla prassi la realtà economica e finanziaria in continuo mutamento. Si tratta in particolare della *CSDR Regulation*[35], relativa al miglioramento del regolamento titoli

30 Un *hub fintech* è il punto focale per l'attività *fintech* all'interno di una regione. È l'ecosistema che comprende tutte le infrastrutture, le organizzazioni e le persone all'interno dell'*hub* o del centro, così come il modo in cui questi elementi sono organizzati e collegati tra loro. I centri sono spesso definiti come "città", ma possono essere anche ampie regioni (ad esempio Silicon Valley), paesi o zone circoscritte. Proprio come le organizzazioni hanno caratteristiche distintive che li differenziano dai loro concorrenti, i centri *fintech* possiedono una serie di fattori identificabili e correlati che contribuiscono al successo generale del centro. Uno di questi fattori è il contesto normativo. I regolatori sono chiamati nell'era fintech a posizionarsi all'interno dell'ecosistema dell'innovazione finanziaria, trovando il giusto equilibrio tra la protezione della stabilità del Sistema e la promozione dell'innovazione. Per un'analisi più dettagliata sulle modalità con le quali i regolatori possono dar vita a *fintech hubs*, *cfr.* Buckley R.P, Arner D.W., Veidt R., Zetzsche D.A., *Building FinTech Ecosystems: Regulatory Sandboxes, Innovation Hubs and Beyond*, University of Hong Kong Faculty of Law Research Paper No. 2019/100, 2019.

31 Cfr. Raghavendra R.P., *Law, Trust, and the Development of Crowdfunding*, 2018; Navaretti Barba G., Calzolari G., Mansilla-Fernandez J.M., Pozzolo A.F., "*FinTech and Banks: Friends or Foes?*", op.cit.; Claessens S., Frost J., Turner G., Zhu F., "*FinTech credit markets around the world: size, drivers and policy issues*", BIS Quarterly Review, September 2018; Pelkmans J., Renda A., *Does EU regulation hinder or stimulate innovation?, CEPS Special Report* No. 96 / November 2014.

32 *Cfr I confini tra diritto privato e pubblico nell'era digitale*, di Paolo Savona e Umberto Tombari, Il Sole24Ore, 23 ottobre 2020, dove si presenta l'idea di una regolamentazione unitaria, di un Codice Unitario, una sorta di Testo Unico del diritto del sistema finanziario, bancario e assicurativo, riprendendo un'antica idea di Carlo Azeglio Ciampi, che non deve però atteggiarsi a mera riproposizione (meglio coordinata) di vecchi contenuti, ma dovrà aprirsi al "nuovo" e prendere in centrale considerazione la finanza digitale in tutte le sue forme e declinazioni.

33 Sul tema cfr. amplius Freud S., Il disagio della civilità (Das Unbehagen in der Kultur), 1929.

34 Le misure normative legate al Fintech possono caratterizzarsi variamente per un approccio "*wait-and-see*", "*same risks, same rules*" (o "*duck typing*"), "*nuova funzionalità, nuove regole*" (cd. "*codifica*") che, oltre a garantire la solvibilità e la liquidità delle singole istituzioni finanziarie, mira alla solidità del sistema finanziario nel suo complesso. *Cfr. Amplius infra. Neutrality of financial regulation. Il (nuovo) ruolo del regolatore.*

35 Regulation (EU) No 909/2014 of the European Parliament and of the Council of 23 July 2014 on improving securities settlement in the European Union and on central securities depositories and amending Directives 98/26/EC and 2014/65/EU and Regulation (EU) No 236/2012.

nell'Unione europea e ai depositari centrali di titoli; della Direttiva UCITS, concernente il coordinamento delle disposizioni legislative, regolamentari e amministrative in materia di taluni organismi d'investimento collettivo in valori mobiliari[36]; della *SFTR Regulation*, in materia di trasparenza delle operazioni di finanziamento tramite titoli[37]; della *Benchmarks Regulation*, sugli indici usati come indici di riferimento negli strumenti finanziari e nei contratti finanziari o per misurare la performance di fondi di investimento[38]; della Direttiva *Transparency* sull'armonizzazione degli obblighi di trasparenza riguardanti le informazioni sugli emittenti i cui valori mobiliari sono ammessi alla negoziazione in un mercato regolamentato[39]. Ai ricordati interventi normativi, tutti caratterizzati da un approccio normativo unidirezionale, devono aggiungersi le misure previste dai pacchetti Mifid/Mifir[40], la direttiva PSD2[41] e le nuove disposizioni in materia di Privacy dettate dal Regolamento GDPR[42]: strategie messe a punto dall'UE (anche) al fine di implementare il ricorso all'intelligenza artificiale (*AI*) e incoraggiare le imprese a collaborare nello sviluppo di nuove tecnologie, a tutela e salvaguardia della fiducia dei cittadini nei mercati finanziari.

Successivamente e a fronte della esigenza di una risposta coordinata ed integrata – esigenza mai sopita ed acuita dalla crisi finanziaria che ha investito i mercati nell'ultimo decennio –, la Commissione si è prodigata nella emanazione di misure volte a superare la logica di regolamentazione per singoli settori (per "silos"). Nel solco di

36 Directive 2009/65/EC of the European Parliament and of the Council of 13 July 2009 on the coordination of laws, regulations and administrative provisions relating to undertakings for collective investment in transferable securities (UCITS).

37 Regulation (EU) 2015/2365 of the European Parliament and of the Council of 25 November 2015 on transparency of securities financing transactions and of reuse and amending Regulation (EU) No 648/2012.

38 Regulation (EU) 2016/1011 of the European Parliament and of the Council of 8 June 2016 on indices used as benchmarks in financial instruments and financial contracts or to measure the performance of investment funds and amending Directives 2008/48/EC and 2014/17/EU and Regulation (EU) No 596/2014.

39 Directive 2004/109/EC of the European Parliament and of the Council of 15 December 2004 on the harmonisation of transparency requirements in relation to information about issuers whose securities are admitted to trading on a regulated market and amending Directive 2001/34/EC.

40 La direttiva MiFID o *Markets in financial instruments directive* (2004/39/EC) ha disciplinato dal 31 gennaio 2007 al 2 gennaio 2018 i mercati finanziari dell'Unione europea. Dal 3 gennaio 2018 è entrata in vigore in tutta l'Unione la nuova direttiva MiFID II (2014/65/EU) che, insieme alla MiFIR o *Markets in financial instruments regulation* (regolamento EU n. 600/2014) ha preso il posto della precedente regolamentazione europea.

41 Direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio del 25 novembre 2015 relativa ai servizi di pagamento nel mercato interno, che modifica le direttive 2002/65/CE, 2009/110/CE e 2013/36/UE e il regolamento (UE) n. 1093/2010, e abroga la direttiva 2007/64/CE. La prima direttiva europea sui servizi di pagamento (Direttiva 2007/64/Ce), anche nota come PSD - Payment Services Directive, definiva un quadro giuridico comunitario moderno e coerente per i servizi di pagamento elettronici. La seconda direttiva sui servizi di pagamento, cosiddetta PSD2, entrata in vigore nell'Unione Europea il 13 gennaio 2016, si inserisce nell'ambito degli interventi di modernizzazione del quadro legislativo del mercato europeo dei pagamenti al dettaglio, volti a sviluppare sistemi di pagamento elettronico sicuri, efficienti, competitivi ed innovativi per consumatori, imprese ed esercenti. Gli ambiti di maggiore novità della PSD2 rispetto alla prima direttiva sui servizi di pagamento sono relativi alle nuove procedure di sicurezza per l'accesso al conto online ed i pagamenti elettronici e ai nuovi servizi di pagamento offerti nell'area dell'e-commerce e dello shopping online dalle banche e da nuovi operatori di mercato. La PSD2 è stata recepita nell'ordinamento nazionale con il D. lgs. n.218 del 15 dicembre 2017, entrato in vigore il 13 gennaio 2018. Le norme che regolano le nuove misure di sicurezza e la comunicazione sicura tra i soggetti coinvolti nella prestazione dei servizi di pagamento disciplinati dalla PSD2 sono contenute nel Regolamento delegato (UE) 2018/389 che ha trovato applicazione il 14 settembre 2019.

42 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)

siffatte politiche europee di crescita solidale necessaria[43], nel 2015 la Commissione ha varato la *Digital Single Market Strategy*[44], un'iniziativa figlia della policy *Shaping Europe's digital future*, che attraverso la chiara definizione di tre pilastri di azione[45] mira ad implementare la cultura digitale e la sicura digitalizzazione dell'Europa, a distribuire le opportunità ed i benefici che derivano dalla digitalizzazione dell'economia, nonché, quale obiettivo finale, per garantire all'Europa una posizione competitiva sul mercato internazionale.

Nel maggio 2017, nell'ambito della revisione intermedia della strategia per il mercato unico digitale, la Commissione ha poi identificato la sicurezza informatica e la lotta alla criminalità informatica come uno dei tre principali settori da implementare al fine di poter intraprendere nuove azioni nei prossimi anni[46], quali il riesame della strategia dell'Unione europea per la cyber-sicurezza e delle norme, certificazioni ed etichettature in materia di sicurezza informatica, al fine di proteggere maggiormente beni e servizi dai rischi di attacchi informatici. Tale operazione è culminata nella nuova strategia per la sicurezza informatica (*The EU's Cybersecurity Strategy for the Digital Decade*[47] del dicembre 2020), che rimane un settore prioritario per ulteriori azioni negli anni a venire sotto i nuovi orientamenti politici per la nuova Commissione europea

43 Bassan F., *Potere dell'algoritmo e resistenza dei mercati in Italia. La sovranità perduta sui servizi*, Rubbettino, luglio 2019.

44 Il 6 maggio 2015 la Commissione europea ha presentato la "Strategia per il mercato unico digitale in Europa" (COM(2015)192), definito come un mercato in cui, indipendentemente dalla cittadinanza o dal luogo di residenza, persone e imprese non incontrano ostacoli all'accesso e all'esercizio delle attività online, in condizioni di concorrenza leale e con un livello elevato di protezione dei consumatori e dei dati personali. *Cfr.* Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *A Digital Single Market Strategy for Europe /** COM/2015/0192 final *, Brussels, 6.5.2015; Comunicazione della commissione al parlamento europeo, al consiglio europeo, al consiglio, al comitato economico e sociale europeo e al comitato delle regioni, *Completare un mercato unico digitale sicuro per tutti*, Bruxxelles, 15 maggio 2018, COM(2018) 320 final; Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC (Text with EEA relevance.) PE/51/2019/REV/1.

45 In primo luogo la strategia digitale dell'UE mira a costruire una "Tecnologia che funzioni a vantaggio delle persone", in particolare investendo nelle competenze digitali, proteggendo le persone dalle minacce informatiche (hacking, ransomware, furto di identità), garantendo che l'intelligenza artificiale sia sviluppata in modo da rispettare i diritti delle persone e guadagnarsi la loro fiducia, accelerando l'introduzione della banda larga ultraveloce in tutta l'UE, espandendo la capacità di computing dell'Europa per sviluppare soluzioni innovative per i servizi pubblici. L'implementazione di tali misure dovrebbe condurre ad una "economia digitale equa e competitiva", in cui siano rafforzate le condizioni di concorrenzialità e responsabilità a vantaggio di tutte le imprese. A tal fine è necessario aumentare "l'accesso a dati di alta qualità", combattendo la disinformazione ed offrendo contenuti diversificati ed affidabili, e, al contempo, creare uno spazio europeo di dati per promuovere la ricerca, garantendo in ogni passaggio la salvaguardia dei dati personali e sensibili, per consentire ai cittadini un migliore controllo e una più efficace protezione.

46 In particolare nella comunicazione relativa alla revisione intermedia, la Commissione ha identificato tre ambiti principali in cui è necessaria un'azione più incisiva da parte dell'UE: 1) lo sviluppo completo delle potenzialità dell'economia dei dati europea, 2) la soluzione dei problemi della sicurezza informatica per proteggere i punti di forza dell'Europa, 3) la promozione delle piattaforme online in quanto attori responsabili di un ecosistema Internet equo.

47 Obiettivi della nuova strategia *cyber* europea sono quelli di affrontare sia la resilienza informatica sia quella fisica delle entità europee, delle reti e delle infrastrutture critiche, mirando a rafforzarne la leadership in materia di norme e standard internazionali nel cyberspazio, nonchè di rafforzare la cooperazione per promuovere un cyberspazio globale, aperto, stabile e sicuro, fondato sullo stato di diritto, sui diritti umani, sulle libertà fondamentali e sui valori democratici. In tale ottica, la Commissione ha inoltre presentato una proposta legislativa volta ad aggiornare la Direttiva NIS ("NIS 2") per raggiungere un più elevato livello comune di sicurezza informatica in tutta l'Unione e una nuova direttiva sulla resilienza delle entità critiche che coprono un'ampia gamma di settori per affrontare su larga scala i rischi attuali e futuri sia online sia offline. *Cfr.* Joint communication to the European parliament and the Council, *The EU's Cybersecurity Strategy for the Digital Decade*, Brussels, 16.12.2020 JOIN(2020) 18 final.

2019-2024[48]. Si collocano, altresì, nel solco di tale programma: la strategia globale per la cooperazione in materia digitale (*Global Digital Cooperation Strategy*[49]) e le iniziative rientranti nel quadro delle relazioni bilaterali con paesi terzi e contesti multilaterali; un'azione di sostegno alla trasformazione digitale delle economie in via di sviluppo (*Digital4Development Hub*[50])[51]. A queste si aggiunge il Libro Bianco sull'Intelligenza Artificiale (*AI*)[52], accompagnato da un Rapporto della Commissione sulle implicazioni dell'AI, dell'I*nternet of Things* (*IoT*) e della robotica per la sicurezza dei prodotti e il regime di responsabilità[53], del febbraio 2020.

48 Nell'ottica di cercare quindi di armonizzare le risposte normative finora varate e con l'intento di ricondurre ad un unico spartito la vasta serie di tonalità e strumentalità che medio tempore si sono diffuse, l'Unione Europea, per il tramite dei suoi organi istituzionali, ha dato vita ad un programma politico noto come Agenda Europea 2019-2024. Fra le sei priorità in essa individuate vi è , in primo luogo, l'impegno ad assicurare che l'Europa sia pronta per l'era digitale ("a Europe fit for the digital age") e che l'economia dell'Europa sia al servizio dei suoi cittadini ("a UE economy that works for people"). La Financial innovation, di cui il fenomeno del Fintech è l'espressione più concreta, porta senza dubbio i regolatori a dover affrontare entrambe le sfide. La nuova agenda strategica 2019-2024 definisce, a tal proposito, i settori prioritari che guideranno i lavori del Consiglio europeo e fornisce gli orientamenti per i programmi di lavoro delle altre istituzioni dell'UE. Gli obiettivi all'interno dei quali collocare poi le singole misure di policy hanno ad oggetto la protezione dei cittadini e delle libertà, lo sviluppo di una base economica forte e vivace, la costruzione di un'Europa green, equa, sociale e a impatto climatico zero, la promozione degli interessi e dei valori europei sulla scena mondiale. Ben consapevole del fatto che nei prossimi anni la trasformazione digitale subirà un'ulteriore accelerazione, con effetti di ampia portata, l'Unione dichiara di dover garantire la sovranità digitale dell'Europa, facendo sì che possa cogliere la sua parte di benefici da questa evoluzione. A tal riguardo si spiega perché le misure presentate nel programma politico siano plasmate in modo da incorporare i valori della società, promuovere l'inclusività e l'imprenditorialità, garantire l'innovazione e accrescere gli sforzi di ricerca, in particolare affrontando la frammentazione del settore della ricerca. Di qui la necessità dichiarata di voler adottare un approccio integrato, che guardi a tutti gli aspetti della rivoluzione digitale e dell'intelligenza artificiale: infrastrutture, connettività, servizi, dati, regolamentazione e investimenti; al contempo sviluppando un'economia dei servizi digitali, che promuova condizioni di parità, di leale concorrenza - nell'UE e a livello mondiale-; che garantisca l'accesso al mercato e combatta le pratiche commerciali scorrette e i rischi per la sicurezza.Per una più ampia disamina del tema sotto molteplici punti di vista, si consiglia la lettura di CEPS, What Comes After the Last Chance Commission? - Policy Priorities for 2019-2024, Edited by Steven Blockmans, Brussels, 2019.

49 Per maggiori informazioni cfr. https://ec.europa.eu/digital-single-market/en/foreign-policy.

50 Per maggiori informazioni sul D4D Hub cfr. https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2321, https://toolkit-digitalisierung.de/en/partner/d4d-hub/

51 Cfr. *Amplius* sul tema Renda A., Artificial Intelligence: Ethics, governance and policy challenges, Report of a CEPS Task Force, CEPS, Brussels, 2019.

52 Libro bianco sull'intelligenza artificiale - Un approccio europeo all'eccellenza e alla fiducia, Bruxelles, 19.2.2020 COM(2020) 65 final, consultabile al seguente link https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_it.pdf.

53 Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee, Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics, Bruxelles, 19.2.2020 COM(2020) 64 final. Nel report vengono messe a fuoco le caratteristiche e i vantaggi offerti dall'AI, dall'IoT e dalla robotica; nello specifico, viene analizzata la legislazione dell'Unione europea sul tema della sicurezza dei prodotti immessi nel mercato europeo. È inoltre affrontato il tema della responsabilità con riferimento ad eventuali danni che le nuove tecnologie potrebbero comportate e conseguentemente del nuovo livello di protezione che è necessario. Viene poi analizzato l'emergere di nuove tecnologie, quali l'IA, l'IoT e la robotica, e delle nuove sfide in termini di sicurezza del prodotto ma anche nuove sfide in termini di responsabilità come ad esempio la gestione della sicurezza. Viene sottolineata la necessità da un lato di creare un clima di fiducia per gli utenti e dall'altro di creare una certa stabilità negli investimenti di queste nuove tecnologie digitali da parte delle imprese.

Da ultimo, la Commissione è stata esortata ad esaminare il ruolo che le piattaforme online hanno rivestito negli ultimi anni ed in particolare se le potenziali questioni ad esse relative[54] possano essere risolte mediante una corretta e piena attuazione della legislazione vigente e un'efficace applicazione della normativa UE in materia di concorrenza.

L'obiettivo è garantire condizioni di parità e una concorrenza equa ed efficace tra le piattaforme *online*, evitando così la creazione di monopoli. L'aumento dell'impiego delle nuove tecnologie nei vari aspetti del diritto e dell'economia e la velocità con cui quest'operazione è avvenuta, ha, infatti, modificando il funzionamento, la regolamentazione e la supervisione dei mercati finanziari, comportando una sfida sempre maggiore per le autorità di regolamentazione[55] e financo determinando la necessità di ridefinire i concetti di mercato e soprattutto di mercato rilevante[56]. A questo proposito, nel corso del secondo semestre del 2020, la Commissione ha adottato il *Digital Services and Markets Act package* (dicembre 2020) volto ad assicurare un quadro giuridico moderno per garantire la sicurezza degli utenti online, istituire una *governance* in cui la protezione dei diritti fondamentali sia all'avanguardia e mantenere un ambiente per lo sviluppo delle piattaforme online equo e aperto. In particolare il *Digital Services Act*[57] e il *Digital Markets Act*[58] comprendono un insieme di nuove norme applicabili in tutta l'UE nel rispetto degli obiettivi della crescita, della sicurezza e della solidarietà[59]. Si affianca a tali misure anche il *Data Governance Act* di prossima emanazione, che ha l'obiettivo di porre una serie di misure per facilitare la condivisione dei dati in tutta l'UE, aumentare la fiducia nella condivisione dei dati, nonché di regole sulla neutralità e sulle pratiche commerciali per garantire un maggiore controllo sulle modalità di utilizzo dei dati.

54 Si tratta in particolare dei problemi legati al tema delle clausole contrattuali abusive e delle pratiche commerciali scorrette che sono state segnalate nei rapporti tra piattaforme e imprese.

55 Kowalewski O., Pisany P., *The Rise of Fintech: A Cross-Country Perspective*, IESEG Working Paper Series 2020-ACF-07, 2020.

56 In particolare è in corso da parte della Commissione Europea un'iniziativa di revisione ed esame della "*Notice on the definition of relevant market for the purposes of Community competition law*" del 1997, anche nota come "*the Market Definition Notice*", al fine di verificare se gli obiettivi, gli scopi e i contenuti di tale atto di soft law siano ancora aderenti al contesto macroeconomico generale o se, in ragione della spiccata digitalizzazione e dataficazione dell'economia e del diritto, sia necessario ed in che modo, aggionrarne i contenuti e gli obiettivi. *Cfr. Evaluation of the Commission Notice on the definition of relevant market for the purposes of Community competition law,* lead dg – responsible unit, DG comp – A1 and A2 – HT.5789, Indicative Planning Start date: Q1/2020 End date: Q2/2021).

57 Per maggiori informazioni cfr. https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en

58 Per maggiori informazioni cfr. https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en

59 Il pacchetto legislativo sui servizi digitali (DSA-DMA) si pone in continuità con le misure varate nell'ambito del Programma Fintech UE e riforma la direttiva sull'e-Commerce dell'Unione europea ormai risalente. L'obiettivo è ambizioso: plasmare l'economia digitale a livello UE e fissare gli standard per il resto del mondo, come ha fatto con la protezione dei dati *("to shape the digital economy at EU level as well as setting the standards for the rest of the world, as it did with data protection."* https://www.europarl.europa.eu/news/en/press-room/20201016IPR89543/digital-eu-must-set-the-standards-for-regulating-online-platforms-say-meps*).* La rapida digitalizzazione della società e dell'economia ha portato alla luce nuovi i limiti dell'attuale assetto regolatorio, rendendo così necessaria la predisposizione di una serie di interventi normativi che consentano di rivedere alcuni dei paradigmi fondamentali delle attuali teorie antitrust che non appaiono più adatte nel contesto digitale.

Tali strategie, insieme alla recente proposta del *New Competition Tool*[60], hanno come fine la creazione di uno spazio digitale più sicuro in cui siano tutelati i diritti fondamentali di tutti gli utenti dei servizi e la predisposizione ed il mantenimento di condizioni di parità per promuovere l'innovazione, la crescita e la competitività, sia nel mercato unico europeo sia a livello mondiale.

È, infine, in corso di definizione la Comunicazione sulla strategia europea per i dati (*Data Act*[61]), intesa a fornire incentivi per la condivisione orizzontale dei dati tra settori. La Commissione, infatti, nel qualificare l'accesso ai dati come un fattore cruciale per incentivare la concorrenza, sottolinea che attualmente non sono disponibili dati sufficienti per il loro riutilizzo innovativo, mentre *"le aziende hanno bisogno di un quadro che consenta loro di avviare, scalare, mettere in comune e utilizzare i dati, innovare e competere o cooperare a condizioni eque"*[62], pertanto, i dati dovrebbero essere disponibili a tutti, perché *"questo aiuterà la società a trarre il massimo dall'innovazione e dalla concorrenza e garantirà che tutti beneficino di un dividendo digitale"*. Per quanto concerne, infine, la politica commerciale, la Commissione sta elaborando la proposta di uno strumento giuridico per contrastare gli effetti distorsivi nel mercato interno dei sussidi concessi alle imprese di paesi terzi dai rispettivi governi, assicurando così un *level playing field* nei diversi settori, incluso il digitale.

Si tratta, con tutta evidenza, di una programmazione normativa di più ampio respiro che vuole superare le singolarità che fino ad ora hanno caratterizzato le precedenti regolamentazioni, al fine di realizzare una convergenza verso l'alto degli strumenti e degli obiettivi.

Perché, ormai, lo si è ben inteso, il problema delle tecnologie risiede nella loro natura *cross sectoral* e *cross boundaries*, essendo ontologicamente in grado di collegare e inter-operare più piattaforme site in diversi stati del mondo, operanti su fronti diversi, con regole giuridiche diverse, ma in virtù di una comune attività. E così, come c'è interazione e interconnessione nella realtà, allo stesso modo un approccio integrato deve riflettersi sul lato normativo.

Uno spartito unico, quindi, per legare tutti gli strumenti; un concerto per rispondere alla tecnologicizzazione e alla *digital innovation*.

60 L'iniziativa (i.e. proposta di regolamento) in esame è una delle misure volte ad assicurare che la politica e le norme in materia di concorrenza siano adeguate all'economia moderna. Il *New Competiotion Tool* affronta in particolare le lacune delle attuali norme dell'UE identificate sulla base dell'esperienza della Commissione in materia di concorrenza sul mercato digitale e su altri tipi di mercato. Essa scaturisce dal processo di riflessione a livello mondiale sulla necessità di modificare le attuali norme in materia di concorrenza per consentire azioni coercitive per preservare la competitività dei mercati, consentendo un intervento tempestivo ed efficace nei confronti dei problemi strutturali che caratterizzano alcuni mercati (soprattutto quello digitale) profondamente modificati dall'affermarsi dei giganti del web, dall'enorme concentrazione venutasi a creare nelle mani di poche aziende in grado di monitorare il comportamento dei propri clienti e concorrenti e di influire sulle politiche della domanda e dell'offerta di beni e servizi digitali, nonché dall'emergere di nuovi rischi per la concorrenza associati allo sviluppo dei mercati digitali.

61 European Commission, Communication 'A European strategy for data', COM(2020) 66 final, 13, 2020.

62 Nel testo originale *"[...] businesses need a framework that allows them to start up, scale up, pool and use data, to innovate and compete or cooperate on fair terms. [...] Therefore, data should be available to all, whether public or private, big or small, start-up or giant. This will help society to get the most out of innovation and competition and ensure that everyone benefits from a digital dividend." European Commission, Communication 'Shaping Europe's digital future'*, COM(2020) 67 final.

1.4 L'economia europea: una questione di dati

L'innovazione tecnologica, da sempre strettamente legata al mondo della finanza quale terreno di elezione per l'utilizzo e lo sviluppo delle nuove tecnologie, determina oggi importanti implicazioni anche nel settore economico-finanziario.

Già a partire dagli anni sessanta le tecnologie informatiche hanno, come noto, dato origine a nuove forme di capitalismo finanziario. Si è assisto, infatti, all'ascesa di beni e servizi, il cui valore economico è legato non più o non solo alle relazioni di titoli monetari e finanziari con materie prime, prodotti o *asset* reali, ma piuttosto al rapporto con altri valori di riferimento come valute, opzioni, *futures*, derivati, *swap*, obbligazioni ipotecarie, e da ultimo, *bitcoin*.

Oggi il processo di digitalizzazione delle relazioni economico-sociali dovuto all'uso estensivo dell'ICT (*Information and Communication Technology*) e dell'IOT (*Internet Of Things*) comporta mutamenti sia a livello imprenditoriale – favorendo l'integrazione tra diversi settori industriali, aprendo nuovi mercati e trasformando i modelli di *business* e l'organizzazione del lavoro aziendale – sia a livello consumeristico, determinando cambiamenti nel comportamento sociale e nello stile di vita delle persone. *Fintech* è, in tal senso, parte del processo di digitalizzazione dell'economia, da questo origina e si alimenta.

In ossequio alla cd. *open innovation*, il *Fintech* contribuisce alla creazione di una rete aperta di servizi modulari per imprese, individui, intermediari bancari, finanziari e assicurativi in una logica di cooperazione-concorrenza.

L'evoluzione tecnologica in atto, quindi, pur non mutando l'essenza dei mercati finanziari e la loro originaria funzione economica di garantire il capitale necessario per sviluppare fabbriche e imprese, ha, tuttavia, conferito loro una nuova veste in cui acquistano primario e autonomo rilievo la velocità e il volume delle transazioni finanziarie stesse[63].

Il progressivo affrancamento dall'economia reale, o come è stato detto, la "finanziarizzazione dell'economia"[64], è ancora più evidente se si guarda al potenziale degli *asset* virtuali – capaci di generare volumi diversi a velocità molto superiori rispetto a quella degli *asset* reali –, nonché all'uso massiccio delle nuove tecnologie e degli algoritmi, che rendono possibili infinite transazioni in un arco temporale di pochi nanosecondi.

63 Abadi J., Brunnermeier M., *Blockchain Economics*, 2018; Accenture, *Fintech and the Evolving Landscape: Landing Points for the Industry*, aprile 2016; Bofondi, M. e G. Gobbi, *The big promise of Fintech*, European Economy, vol. 2: 107-119, 2017; Claessens S., Frost J., Turner G., Zhu F.,, "*FinTech credit markets around the world: size, drivers and policy issues*", op-cit.; FCA, *Discussion Paper on distributed ledger technology*, DP17/3, 2017; FSB, FSB reports "*FinTech and market structure in financial services: Market developments and potential financial stability implications*", 2019; FSB, FSB reports "*Decentralised financial technologies. Report on financial stability, regulatory and governance implications*", 2019; PwC - PricewaterhouseCoopers, *Redrawing the lines: FinTech's growing influence on Financial Services*, Global FinTech Report, 2017; Schwab K., Davis N., *Shaping the Future of the Fourth Industrial Revolution. A Guide to Building a Better World*, Portfolio Penguin, London, 2017; Zetzsche D.A., Buckley R.P., Arner D.W., Barberis J.N., *From FinTech to TechFin: The Regulatory Challenges of Data-Driven Finance*, EBI Working Paper Series, n. 6, 2017.

64 P. Savona, "*Come riconciliare finanza e attività prodouttiva nell'era FIntech*", intervento alla Conferenza dell'ISTAO, Ancona, 20 gennaio 2020.

In siffatto settore in cui l'uomo e la tecnologia non corrono alla stessa velocità, assumono una centrale importanza gli algoritmi, i quali sono progettati dall'uomo per eseguire alcune operazioni prima di appannaggio dell'operatore persona fisica, al fine di raggiungere gli obiettivi in modo più efficiente, ad un minore costo ed in tempi assai più brevi.

Più in generale, al divario di ricchezza tra sistemi economici nazionali si è oggi affiancato anche un divario di velocità[65], in cui la misura dell'efficienza è data dalla capacità di massimizzare e velocizzare la produzione attraverso la programmazione e la digitalizzazione.

I cambiamenti che negli ultimi anni hanno interessato i mercati internazionali, decretando ora il successo ora il fallimento di imprese e gruppi operanti in vari settori e in diverse giurisdizioni, possono essere definiti come una *data revolution*.

L'integrazione economica e sociale conseguente al funzionamento del mercato interno ha condotto a un considerevole aumento dei flussi transfrontalieri di dati e, quindi, anche dei dati personali scambiati, in tutta l'Unione, tra attori pubblici e privati, persone fisiche, associazioni e imprese.

Si parla oggi di un mercato dei dati, composto essenzialmente dalle informazioni che gli utenti, più o meno consapevolmente, condividono nel sistema, e che è caratterizzato da profonde asimmetrie informative dovute non solo alla scarsa conoscenza del fenomeno, ma anche alla circostanza secondo cui la percezione circa il valore che i singoli dati assumono sono diversi da operatore a operatore e da operatore a utente.

Rispetto agli altri mercati, ed in particolare al mercato dei capitali, tale settore è diverso con riferimento all'oggetto: a differenza degli altri beni e servizi la cui valutazione è allineata all'economia reale, nel caso dei dati, il loro valore dipende dal contenuto informativo che allo stesso si attribuisce e dalla percezione che di esso si ha all'esterno[66]. La portata della condivisione e della raccolta di dati personali è, infatti, aumentata in modo significativo, tanto che le tecnologie dell'informazione e della comunicazione non costituiscono più un settore a sé stante, bensì sono la base stessa di tutti i sistemi economici e delle società innovative e moderne.

In una economia sempre più basata sulle informazioni, i flussi di dati sono, quindi, al centro dei processi aziendali delle imprese di qualsiasi dimensione e in tutti i settori della produzione e dell'offerta di servizi, divenendo vera e propria merce di scambio. Si sarebbe mai potuto pensare in passato di poter pagare l'acquisto di un qualsiasi bene con i propri dati personali, come se si trattasse di una sorta di moneta?

65 Taylor M.C, Speed kills, in Chronicle of Higher Education, 2015.

66 Sul *Financial Times*, nel 2013, usciva un articolo in cui si invitavano i lettori a provare a vedere, tramite un programma integrato, quanto valessero i priiorpi dati personali, *How much is your personal data worth? Use our calculator to check how much multibillion-dollar data broker industry might pay for your personal data,* JUNE 12 2013, https://ig.ft.com/how-much-is-your-personal-data-worth/.

Oggi ciò è stato reso possibile, ad esempio, dal *Data Dollar Store*[67], un negozio temporaneo dove per due giorni è stato possibile acquistare oggetti pagando esclusivamente con dati. La società battezzò questa originale moneta con il nome di "*Data dollar*".

Ora, senza giungere a provocatorie realtà[68], è innegabile come le principali società *fintech* basino, oggi, il loro modello di *business* sul commercio elettronico e/o sul *trading* di informazioni personali relative agli utenti/utilizzatori. La crescita dei mercati, da quello statunitense a quello cinese, è tutta incentrata sulla spinta propulsiva derivante dall'impiego dei dati quale valore aggiunto, sia in settori industriali, finanziari e commerciali sia anche nei settori tradizionali.

Appare evidente come la rapidità dell'evoluzione tecnologica e la globalizzazione abbiano comportato, *inter alia*, nuove sfide anche per la protezione dei dati personali. L'uso dei *big data* nella gestione del *business* aziendale non è un retaggio delle sole aziende *leader* del digitale; infatti, i flussi di dati pervadono e caratterizzano la vita di persone fisiche e giuridiche nei processi quotidiani. Quasi in una perfetta simbiosi, da un lato la tecnologia consente, tanto alle imprese private quanto alle autorità pubbliche, di utilizzare i dati personali nello svolgimento delle loro attività in modo massiccio e innovativo; dall'altro sempre più spesso, le persone (volontariamente o involontariamente, *rectius* indirettamente) rendono disponibili su larga scala informazioni personali, talvolta anche sensibili.

In tal senso, le catene del valore dei dati sono allora il risultato di diverse attività relative ai dati: la creazione e la raccolta; l'aggregazione e l'organizzazione; il trattamento; l'analisi, la commercializzazione e la distribuzione; l'utilizzo e il riutilizzo. Il funzionamento efficace ed efficiente del trattamento di dati costituisce, pertanto, un elemento fondamentale di qualsiasi catena del valore dei dati, di cui l'efficienza e l'efficacia nel trattamento dei dati stessi sono la chiave di volta.

La corretta gestione del ciclo-vita dei dati, la loro sicurezza e, soprattutto, la relativa comprensione sono dunque le nuove sfide con cui devono confrontarsi gli operatori del settore.

Posto che la tecnologia ha trasformato l'economia e le relazioni sociali, obiettivo della regolamentazione dovrebbe essere quello di facilitare la libera circolazione dei dati personali all'interno dell'Unione Europea e il loro trasferimento verso paesi terzi e organizzazioni internazionali, garantendo al tempo stesso un elevato livello di protezione dei "proprietari" dei dati stessi.

Simili considerazioni sono all'attenzione del legislatore eurounitario, il quale da tempo ha messo in atto un'opera di rivisitazione ed aggiornamento dei principali

67 Nel settembre 2017 aprì a Londra *The Data Dollar Store*, un negozio temporaneo ideato e promosso dalla società di cybersecurity Kaspersky Lab, all'interno del quale l'unica merce di scambio accettato per finalizzare l'acquisto era la condivisione di dati personali.

68 Ancora, sempre i dati, raccolti e analizzati sotto altro profilo, rendono possibile ad una madre interagire con l'ologramma di un congiunto passato a miglior vita. Il riferimento è al documentario televisivo intitolato "I met you" prodotto dalla Munhwa Broadcasting del 2016 ed alla puntata della serie TV Black Mirror, "Be right back", in cui la memoria digitale permette, attraverso l'elaborazione delle informazioni legate al defunto, di creare un alter ego digitale con il quale interagire.

plessi normativi a disciplina della materia. In particolare, nei Considerando di apertura al 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 (nel prosieguo anche Regolamento GDPR), si legge, quale manifesto dell'intervento dell'Unione in siffatto settore, che «*Tale evoluzione richiede un quadro più solido e coerente in materia di protezione dei dati nell'Unione, affiancato da efficaci misure di attuazione, data l'importanza di creare il clima di fiducia che consentirà lo sviluppo dell'economia digitale in tutto il mercato interno. È opportuno che le persone fisiche abbiano il controllo dei dati personali che li riguardano e che la certezza giuridica e operativa sia rafforzata tanto per le persone fisiche quanto per gli operatori economici e le autorità pubbliche*»[69].

Il diritto dell'Unione Europea impone, quindi, alle autorità nazionali degli Stati membri di vigilare sullo scambio e sul trattamento dei dati personali in piena armonizzazione. In tale quadro e nell'attesa della promulgazione del nuovo Regolamento *E-Privacy*, nonché del *Data Governance Act*[70], si inserisce la riforma europea sulla Privacy, attuata mediante il citato Regolamento GDPR, la cui *ratio* ispiratrice poggia sul corollario secondo cui «*Il trattamento dei dati personali dovrebbe essere al servizio dell'uomo*»[71].

Si osserva, infatti, come il diritto alla protezione dei dati "di carattere personale" non sia una prerogativa assoluta, ma vada piuttosto considerato alla luce della sua funzione sociale, contemperandolo con altri diritti fondamentali, in ossequio al principio di proporzionalità. Il regolamento detta, al riguardo, una disciplina in materia di dati personali nel rispetto di tutti i diritti fondamentali e nell'osservanza delle libertà e dei principi riconosciuti dalla Carta[72].

La più idonea chiave di lettura di tale normativa pare essere quella tipo logico-sistematico, focalizzando l'attenzione sul concetto di *accountability* come posto dal

69 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).

70 La proposta di Regolamento costituisce la prima delle misure preannunciate dalla Commissione nella Strategia europea per i dati e si configura quale primo tassello su cui edificare il modello europeo di governance dei dati. Un modello di gestione dati alternativo a quello delle big tech e fondato sui principi della tradizione eurounitaria e destinato a diventare un archetipo su scala internazionale sul modello del GDPR. In partcolare la proposta prevede la creazione di un meccanismo per il riutilizzo di alcune categorie di dati protetti detenuti dal settore pubblico, l'istituzione di un regime di notifica e controllo per i servizi di data sharing e la definizione di un sistema di registrazione volontaria delle organizzazioni che raccolgono ed elaborano i dati resi disponibili per scopi altruistici. A questo si affiancano una serie di previsioni dedicate all'istituzione di autorità competenti e alla creazione di un gruppo di esperti, l'European Data Innovation Board, dinamico, multidisciplinare ed in costante aggiornamento. Per ulteriori informazioni cfr. *Proposal for a regulation of the European Parliament and of the CounciL on European data governance (Data Governance Act) COM/2020/767 final,* https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52020PC0767&from=EN; https://ec.europa.eu/digital-single-market/en/news/commission-proposes-measures-boost-data-sharing-and-support-european-data-spaces.

71 Considerando 4, Reg. Ue 2016/679 *op.cit.*

72 Si tratta dei diritti sanciti dai Trattati e dalla Carta di Nizza, fra i quali, in particolare, il rispetto della vita privata e familiare, del domicilio e delle comunicazioni, la protezione dei dati personali, la libertà di pensiero, di coscienza e di religione, la libertà di espressione e d'informazione, la libertà d'impresa, il diritto a un ricorso effettivo e a un giudice imparziale, nonché la diversità culturale, religiosa e linguistica.

legislatore europeo. I nuovi istituti della portabilità dei dati, dell'illustrazione della logico-decisionale adottata, dei registri del trattamento, della valutazione di impatto *privacy* (la c.d. *DPIA*), spostano, infatti, il *focus* dallo scrutinio *ex ante* dell'Autorità Garante alla responsabilizzazione dei titolari, che "internalizzano" le proprie valutazioni, assumendo come parametro-guida il grado di rischio per i diritti e le libertà delle persone i cui dati sono oggetto di trattamento.

Il livello di *compliance* e di trasparenza che il GDPR richiede alle imprese consente inoltre, in questo settore, di utilizzare il rispetto degli obblighi di legge come vantaggio competitivo sul mercato. Se i dati sono nuovi beni giuridici ai sensi dell'art. 810 del Codice Civile, la protezione dei dati entra allora a far parte degli obiettivi oltre che dei beni dell'impresa, quale nuovo *asset* aziendale. E così, a livello imprenditoriale si assiste ad una rivoluzione delle organizzazioni interne che vedono nascere la figura del *Data Protection Officer (DPO*), e accrescere il peso della voce "*data protection"* nelle *due diligence* connesse alle operazioni di M&A o di quotazione su mercati regolamentati al fine di individuare, circoscrivere e neutralizzare, ove possibile il rischio d'impresa stesso.

Emerge, quindi, come la portata della regolamentazione sia inevitabilmente legata alla sua ontologica interconnessione con le altre aree non solo del diritto, ma anche dell'economia e del sociale in generale. Il quadro si complica se si considera che detta materia è spesso oggetto di una regolamentazione eterogenea a livello nazionale, con conseguenti ripercussioni in termini di tutela degli individui e fenomeni di *forum shopping.* L'aumento dell'importanza che i dati rivestono nel contesto economico-finanziario ha, altresì, accresciuto ed esteso su larga scala i problemi legati alla *privacy,* stimolando i regolatori e i supervisori nella ricerca di sempre nuove strategie[73].

Per rispondere a dette esigenze il legislatore europeo del GDPR ha operato attraverso lo strumento del Regolamento, che, come noto, a differenza delle direttive, non richiede(rebbe) una espressa norma nazionale di recepimento ed implementazione da parte degli Stati membri. Tuttavia, conscio delle diversità nazionali sul tema, il Regolamento in esame ha lasciato aperte aree in cui il legislatore nazionale è chiamato ad esercitare i suoi poteri legislativi per meglio perimetrare e precisare taluni aspetti che richiedono un'attenzione peculiare in relazione alle esigenze e alle altre norme nazionali vigenti (i.e. trattamento di dati particolari, come quelli sensibili, genetici e biometrici; possibilità di introdurre norme penali a presidio del rispetto delle norme sulla privacy, sulla base delle sensibilità e dell'ordinamento nazionale). Se da un lato questa riserva di sovranità ha consentito a ciascuno Stato di adattare la norma al proprio contesto socio-politico-economico, dall'altro, ha comportato, però, una falla nel

73 L'Europa, rispetto ad altre aree geografiche (i.e. Asia e U.S.A.) non dispone di abbastanza dati disponibili per essere riutilizzati ai fini dello sviluppo dell'AI e come spinta alla crescita ed alla innovazione. Questo comporta inevitabilmente un ritardo non solo normativo ma anche e soprattutto in termini di sviluppo economico e di effetti competitivi di mercato. A tal proposito l'approccio nel trattamento dei rischi deve tener conto del classico "paradosso della privacy" in cui le persone possono dividersi in due categorie: coloro che affermano di essere molto preoccupati per la propria privacy, e coloro che in gran parte ignorano questi rischi nel loro comportamento *online* (sul punto *cfr.* Athey S., Catalini C., Tucker C. E., *The Digital Privacy Paradox: Small Money, Small Costs, Small Talk.* National Bureau of Economic Research (NBER) Working Paper No. 23488, 2017; Barnes S. B., *A Privacy Paradox: Social Networking in the United States*, First Monday 11, ISSN 1396-0466 119, 2006).

processo di armonizzazione. È allora evidente come la previsione di rigidi standard e procedure finalizzate alla salvaguardia dei consumatori con riferimento alla raccolta, al trattamento e alla diffusione dei dati, da sola non basta a raggiungere gli obiettivi di armonizzazione e di "*levelling the playing field*".

Tali criticità si manifestano soprattutto nel settore dei mercati finanziari, in cui i temi della qualità-quantità dei dati disponibili e della velocità alla quale viaggiano le informazioni si atteggiano diversamente per operatori e utenti, rispettivamente in termini di vantaggi competitivi e di tutela.

Il problema della portabilità e del trattamento dei dati all'interno del sistema finanziario e dei servizi di investimento, attiene in particolare alla trasferibilità dei dati a terzi, quale modalità nelle quali può estrinsecarsi il trattamento ed in particolare il trattamento dei dati per finalità diverse.

Al riguardo la disciplina si ricava da una lettura sistematica di diverse norme provenienti da diversi plessi dispositivi, difettando sul punto una regolamentazione organica e puntualmente prevista. Da un lato, infatti, il GDPR introduce, a livello generale, presidi e limiti a tutela della liceità del trattamento dei dati; dall'altro il TUF e la normativa MIFID dettano regole per quanto concerne la raccolta di informazioni e dati dei clienti da parte degli intermediari nell'ambito della prestazione dei servizi di investimento. Inoltre, in ragione del fatto che quest'ultimi nulla prevedono in tema di trattamento dei dati, occorrerà di volta in volta, sussumere la fattispecie concreta di investimento all'interno della disciplina dettata dal GDPR.

Il fine perseguito dalla normativa citata è, tuttavia, comune e consiste nel promuovere la possibilità di controllo degli interessati sui propri dati personali, aumentandone la consapevolezza nelle fasi di circolazione e trasmissione dei dati stessi da un ambiente informatico all'altro. Il diritto alla portabilità dei dati consente, infatti, all'interessato di ricevere i dati personali forniti ad un titolare del trattamento, in un formato strutturato, di uso comune e leggibile da dispositivo automatico, e di trasmetterli ad un altro titolare del trattamento senza impedimenti. La *ratio* di tale diritto è, quindi, quella di consentire la trasmissione diretta dei dati da un titolare del trattamento all'altro, a supporto e ad incentivo della libera circolazione dei dati personali nell'UE e della concorrenza. Potenziando, infatti, il controllo dei singoli sui dati personali che li riguardano, si assicura agli interessati un ruolo attivo nell'ecosistema delle informazioni, il che permette di "riequilibrare" il rapporto fra interessati e titolari del trattamento, tramite il controllo esercitabile dagli interessati sui dati che li riguardano. Si noti che seppure possa apparire chiaro come il diritto alla portabilità abbia la finalità ultima di fungere da fattore di promozione della concorrenza fra i singoli servizi, proprio perché facilita il passaggio da un servizio all'altro, il nuovo Regolamento Privacy si preoccupa di disciplinare il trattamento dei dati personali e non la concorrenza fra le imprese.

Nel bilanciamento di interessi fra *bigdata* e *privacy* degli individui, occorre, infatti, contemperare l'importanza che l'uso e l'analisi dei dati ha acquisito in punto di competitività tra le aziende, con l'intangibilità del diritto alla tutela della riservatezza degli individui che osta alla configurazione dei uno scenario in cui i dati circolino liberamente e senza una base giuridica sottostante.

A tal riguardo, la Commissione distingue quattro scenari possibili che dal punto di vista dei mercati hanno ad oggetto il coinvolgimento efficiente dei dati: l'utilizzo da parte delle imprese delle informazioni nella disponibilità del settore pubblico (G2B); la condivisione di dati tra imprese (B2B); l'utilizzo da parte delle autorità pubbliche di dati detenuti da privati (B2G) e la condivisione di dati tra pubbliche amministrazioni (G2G). Per ciascuno dei quattro scenari sono in corso di adozione e revisione diverse misure atte a promuovere ulteriormente la condivisione dei dati, senza che ciò si risolva in una *deminutio* delle tutele.

In siffatto contesto i nuovi rischi per la stabilità del sistema sono associati alle dimensioni competitive o alla dimostrata connettività di un operatore del mercato finanziario: in altre parole l'essere "*too big to fail*" ("troppo grandi per fallire") o soprattutto "*too interconnected to fail*" ("troppo interconnessi per fallire")[74]. In termini di minacce legate alle dimensioni degli operatori, il Comitato per il Sistema Finanziario Globale e il *Financial Stability Board*, tra gli altri, ritengono che, in questa fase, se da un lato l'entità del credito *fintech*[75] in molte giurisdizioni sia ancora abbastanza basso per limitare l'impatto sistemico, dall'altro la crescita esponenziale del fenomeno potrebbe dare vita ad una serie di rischi il cui impatto non è ancora possibile prevedere. In termini di minacce connesse alla interconnettività, invece, si rileva che è la sicurezza cibernetica ad essere senza dubbio la sfida fondamentale per le autorità di regolamentazione, perché legata tanto alla stabilità finanziaria quanto all'integrità del mercato. Il settore finanziario è, infatti, l'obiettivo prediletto dalla criminalità informatica.

Ciò su cui allora deve focalizzarsi l'attenzione è la fiducia, cuore della regolamentazione e della vigilanza per il mantenimento dell'integrità del mercato.

Alla base delle transazioni finanziarie c'è, infatti, la fiducia, che, se nel mercato dei capitali conosce una lunga e dettagliata storia di regolamentazione, nel mercato dei dati manca, invece anche di un quadro globale di principi generali regolatori della materia. Nonostante l'elevata protezione prevista dal GDPR, la velocità con cui il

74 FSB, FSB reports, *Consider financial stability implications of BigTech in finance and third party dependencies in cloud services,* 2019; Omarova S. T., What Kind of Finance Should There Be?. Cornell Legal Studies Research Paper No. 20-09, What Kind of Finance Should There Be? 83 L. & CONTEMP. PROB. 195, 2020; Porter M., *The Five Competitive Forces that Shape Strategy,* 25 Harvard Business Review, 2008; Teece D., *Profiting from Technological Innovation: Implications for Integration, Collaboration, Licensing and Public Policy,* 15(6) Research Policy, 1986; Vives, X., The Impact of Fintech on Banking, European Economy, vol. 2: 97-105, 2017; Zhang, B., Wardorp R., Ziegler T., Lui A., Burton J., James A., Garvey K., Sustaining Momentum, the 2nd European Alternative Finance Industry Report, University of Cambridge, KPMG and CME Group Foundation, 2016.

75 Il *Fintech credit*, riconducibile alla categoria degli *alternative credit*, è l'attività creditizia agevolata da piattaforme elettroniche come i prestatori peer-to-peer, e, come si legge dal Report "*FinTech Credit: Market Structure, Business Models and Financial Stability Implications"* del CGFS e del FSB, "*has generated significant interest in financial markets, among policymakers and from the broader public. [...] The nature of FinTech credit activity varies significantly across and within countries due to heterogeneity in the business models of FinTech credit platforms. Although FinTech credit markets have expanded at a fast pace over recent years, they currently remain small in size relative to credit extended by traditional intermediaries.[...] The emergence of FinTech credit markets poses challenges for policymakers in monitoring and regulating such activity. Having good-quality data will be key as these markets develop. We hope that the information and analysis contained in this report will assist policymakers with their efforts.", cfr. amplius* Committee on the Global Financial System and Financial Stability Board (CGFS and FSB), *FinTech Credit: Market Structure, Business Models and Financial Stability Implications*, CGFS Papers, May 2017; Financial Action Task Force (FATF), *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers.* FATF, 2019.

fenomeno si evolve e l'ampiezza della portata *disruptive* della digitalizzazione impongono che gli strumenti a disposizione degli interessati per mantenere un pieno controllo sui propri dati ed esercitare in maniera effettiva i diritti riconosciuti dalla normativa europea dovranno necessariamente essere oggetto di una (forse periodica) revisione, aggiornamento e rafforzamento, per rispondere ai nuovi rischi e ai nuovi fenomeni che si andranno formando.

Posto, dunque, che l'attuale frammentazione normativa fra diversi Stati membri costituisce un serio ostacolo non soltanto allo sviluppo di un vero mercato unico ma anche alla competitività degli operatori europei con quelli americani o asiatici, è indispensabile che la regolazione sia elaborata a livello comunitario e armonizzato.

A tal riguardo, su proposta della Germania e della Francia presentata in seno al *Summit Digitale 2019*, ha visto da poco la luce GAIA X: un *cloud* a livello europeo il cui obiettivo è quello di creare un'infrastruttura che possa competere con i *cloud* USA nella gestione dei dati[76].

Se da un lato l'intento è chiaramente individuato in quello di pervenire ad una federazione di *cloud* nazionali, di protocolli tecnici, non altrettanto chiaro è il modo con il quale tale fine verrà perseguito. Diverse sono le idee e diverse sono le strutture ipotizzate: il dibattito al momento è alimentata da coloro che prospettano una soluzione "*GSM Like*", in cui sono dettate le regole standard e i protocolli applicativi che definiranno il quadro di regole applicabile in UE sia agli operatori UE sia agli operatori extra UE, e coloro che, invece, propendono per un modello in cui l'obiettivo non è creare le regole, ma dar vita ad una infrastruttura di piattaforme da cui poi dedurre le regole e le *best practices* in grado di garantire il perseguimento degli obiettivi di welfare in tutta l'UE.

Un approccio flessibile e modulare, dunque, capace di adattarsi al contesto e pronto a rispondere in maniera efficace ed efficiente alle nuove sfide che la *datification* impone. Una forte base economica e giuridica è, infatti, di importanza vitale per la competitività e la prosperità dell'Europa, soprattutto in un momento in cui il panorama mondiale è riplasmato da sfide in termini di tecnologie, sicurezza e sostenibilità.

C'è bisogno di un modello di regolazione integrato, "*embedded*" nella tecnologia, volto a rafforzare il mercato unico e che sappia elaborare una politica industriale a prova di futuro, capace di affrontare la rivoluzione digitale e garantire una politica industriale più assertiva, globale e coordinata.

76 Cfr. Joint Declaration EU cloud federation, *"Building the next generation cloud for businesses and the public sector in the EU"*, 15 Ottobre 2020.

2 *Neutrality of financial regulation*. Il (nuovo) ruolo del regolatore

2.1 Quale approccio regolatorio generale? *Regulation for coopetition*?

La *disrutption*[77] originata dalla *financial revolutiorn* e la sua rapida diffusione a livello globale ha imposto un ripensamento delle tradizionali tecniche di regolamentazione ed ha in qualche modo reso necessaria una cooperazione ed una coordinazione fra i vari regolatori nazionali al fine di livellare il *playing field*.

Questo ripensamento ha avuto più recentemente una ulteriore accelerazione a seguito della diffusione della pandemia da Covid-19 la quale ha avuto conseguenze rilevantissime anche sui settori dell'economia, rendendo urgente l'adozione di metodi di lavoro a distanza e la realizzazione di architetture digitali, distribuite, decentralizzate e innovative.

L'innovazione in ambito economico-giuridico ha determinato lo sviluppo di un processo attraverso il quale l'economia, nonostante la recente pandemia, è stata rivitalizzata dalla presenza di nuove tipologie di prodotti e servizi, nonché dall'introduzione di nuovi modi di fornire i prodotti e i servizi già esistenti[78]. In ambito finanziario la digitalizzazione ha creato sia opportunità che rischi. Tra i vantaggi vanno considerati: la maggiore velocità ed efficienza delle transazioni, le maggiori economie di scala nonché l'introduzione di strumenti automatizzati in grado di aiutare le aziende (così come le Autorità di vigilanza) ad intercettare in anticipo eventuali cattive condotte. Le aree di rischio includono invece: la sicurezza dei dati, gli incidenti operativi, la riservatezza di dati, prezzi e le pratiche di vendite, nonché la possibile esclusione dei soggetti non sufficientemente 'tecnologizzati' da taluni settori della finanza.

I problemi di "qualità" dei dati dovrebbero essere affrontati attraverso solidi meccanismi di verifica e i dati di testo dovrebbero essere scritti in un formato leggibile anche dalla macchina[79].

Tale nuovo contesto ha richiesto il dispiego di nuovi e più rapidi strumenti in grado di accompagnare le sorti del processo di *digitalization*, senza comprometterne lo sviluppo e senza creare vuoti di tutela.

Oggi può, infatti, accadere che le strutture di regolamentazione esistenti si dimostrino inadeguate ad accogliere e disciplinare i nuovi processi e le nuove realtà, oppure che i processi e i risultati che sono oggi auspicabili, diventino in un futuro involontariamente sgraditi. Il quadro è poi ulteriormente complicato dal fatto che, per

77 Termine, questo, introdotto in economia da Bower J.L., Christensen C.L., *Disruptive Technologies: Catching the Wawe*, in *Harvard Business Review*, January-February, 1995 per indicare quelle innovazioni tecnologiche così dirompenti da modificare l'assetto dei mercati esistenti ed i relativi valori di riferimento.

78 Schumpeter J., Capitalism, Socialism and Democracy, 1975.

79 *Cfr.* Sul punto ESMA, *ESMA responds to European Commission Consultation on the Digital Finance Strategy*, 29 giugno 2020 (consultabile sul sito internet https://www.esma.europa.eu/press-news/esma-news/esma-responds-european-commission-consultation-digital-finance-strategy).

quanto i regolatori cerchino di aggiornare i plessi normativi per affrontare le nuove sfide derivate dalla *digitalization*, il ritmo dell'innovazione sarà sempre più rapido rispetto alla risposta dell'azione di regolamentazione.

Se da un lato appare, dunque, evidente che sia senz'altro necessaria una risposta normativa, non vi è invece convergenza di opinioni per quanto riguarda i tempi e i modi coi quali essa debba estrinsecarsi. Adottare le regole troppo in fretta e prima che il fenomeno tecnologico sia stato correttamente compreso (non solo dal sistema finanziario ma anche, e soprattutto, dal regolatore), potrebbe, infatti, rivelarsi controproducente, perché si rischierebbe di imbrigliare eccessivamente il fenomeno e rallentare, per l'effetto, lo sviluppo dei settori finanziari che di quella crescita beneficerebbero. Per converso, attendere troppo a lungo, se da un lato consentirebbe al mercato un pieno sviluppo, dall'altro potrebbe avere l'indesiderato e rischioso effetto di lasciare il settore privo di una guida prima e di meccanismi di vigilanza e di *enforcement* dopo. Al tempo stesso, da un lato, lasciare il mercato del tutto libero vorrebbe dire fare vincere le tecnologie in grado di realizzare il prodotto o il servizio meno costoso ma anche mettere a rischio taluni principi su cui si fondano singoli Paesi e la stessa Unione Europea. Dall'altro, intervenire regolando alcune attività vorrebbe dire rendere le stesse maggiormente costose e probabilmente soccombenti sul mercato.

Pertanto dal punto di vista della regolamentazione la nuova sfida pare essere quella di scrivere norme che in qualche modo anticipino ed orientino le scelte tecnologiche. Per queste ragioni la scelta delle regole (e degli extra-costi dalle stessi derivanti) rappresenterà per il futuro una sorta di scelta di "politica industriale" per il Legislatore.

* * *

Se questi sono i termini del problema, ben si comprendono le difficoltà che i diversi 'Regolatori' del sistema finanziario stanno affrontando con riguardo allo sviluppo del *Fintech*.

Vale la pena allora ripercorrere qui brevemente quelle che sono state le diverse soluzioni normative immaginate nel corso del tempo per superare tali difficoltà.

Per lungo tempo, fino a quando il volume di mercato del *fintech* era relativamente piccolo, l'approccio predominante a livello mondiale è stato quello del c.d. "*wait and see*". Tale modello, basato sull'idea di 'passività normativa', prevedeva che le autorità di regolamentazione finanziaria non facessero altro che applicare il quadro normativo esistente limitandosi di fatto a monitorare il mercato. Molti regolatori sono inizialmente ricorsi a tale modello in modo anche al fine di non ostacolare il pieno sviluppo all'industria *fintech* prima di cimentarsi nella ricerca di una soluzione al quesito: applicare le regole esistenti, implementandole, oppure crearne di nuove?

L'attesa era stata considerata inizialmente anche come la strategia più funzionale per guadagnare tempo per avere un quadro più chiaro circa il modello giuridico da seguire. Tant'è che alcuni regolatori nazionali si erano posti addirittura in una posizione di 'osservazione' rispetto alle scelte compiute dagli altri regolatori sul mercato, ponendosi quasi in una posizione 'esterna' rispetto al fenomeno.

Con il passare del tempo e con la crescita esponenziale del fenomeno, l'idea che uno sviluppo del mercato senza una disciplina applicabile agli operatori e ai nuovi prodotti potesse promuovere l'innovazione è stata però superata. È stato, infatti, osservato in primo luogo come l'assenza di una regolamentazione rispetto al fenomeno avrebbe potuto lasciare i consumatori/risparmiatori (così come tutti gli altri *player* esistenti sul mercato) senza una adeguata protezione, danneggiando così in ultima analisi la fiducia nel sistema finanziario. In secondo luogo è stato rilevato che, posto che i processi di innovazione e trasformazione digitale sono avviati sia da istituzioni finanziarie 'tradizionali' (regolamentate e controllate), sia da nuovi concorrenti (non sempre soggetti allo stesso livello di regolamentazione e vigilanza di quelli 'tradizionali'), l'assenza di regolamentazione per gli attori che sviluppano attività funzionalmente equivalenti non solo si stava dimostrando iniqua, ma poteva addirittura dar luogo a fenomeni di arbitraggio regolamentare in assenza di una altrettanto adeguata supervisione. Infine, si è osservato che spesso l'assenza di una regolamentazione poteva altresì scoraggiare i consumatori e gli investitori dall'utilizzare i prodotti e i servizi forniti dai nuovi operatori di mercato o anche solo le nuove tecnologie[80].

Assodata la necessità di un intervento del Regolatore, ci si è quindi chiesto se l'attività riconnessa al *fintech* potesse essere in qualche modo ricondotta, in via interpretativa e *mutatis mutandis*, nell'ambito del quadro normativo esistente (posto che i precipitati del *fintech* sono essenzialmente rappresentazioni digitali o crittografiche di uno strumento, un'istituzione o una piattaforma di infrastruttura finanziaria già esistenti), oppure se fosse invece necessario sviluppare un nuova disciplina.

Per alcuni interpreti una prima possibile risposta normativa al fenomeno del *fintech* poteva fondarsi su un impianto normativo basato su norme di *divieto*. Secondo questo approccio un determinato prodotto o attività doveva essere vietato ogniqualvolta venivano individuati specifici rischi collegati alle nuove tecnologie; rischi cui il quadro normativo esistente non avrebbe potuto fare fronte.

Tale approccio, però, ha avuto ben poco seguito, in quanto ritenuto una sorta di strategia di regolamentazione 'subottimale', in cui le norme di divieto risultavano essere eccessivamente limitanti e poco organiche, perché attuabili sulla base di un approccio *case-by-case*, con un elevato rischio di disparità di trattamento anche a livello territoriale.

È stato questo il momento in cui si è finalmente giunti alla maturazione della convinzione che la stessa *velocità* con cui l'evoluzione tecnologica stava muovendosi rispetto ai tempi della corrispondente risposta normativa doveva essere posta al centro

80 Su come la mancanza di parità di condizioni per alcuni servizi bancari abbia accresciuto la rilevanza del settore bancario ombra (*shadow banking*), *cfr.* Wymeersch E., *Shadow Banking and Systemic Risk*, European Banking Institute Working Paper Series No. 1, 2017; Schwarcz S.L., *Shadow Banking and Regulation in China and Other Developing Countries*, Duke Law School Public Law & Legal Theory Series 2017-8, 2017. Inoltre, si è osservato che i fenomeni di autoregolamentazione possono portare ai tipici fallimenti dovuti a *free-riding*, problemi agente-principale e *moral-hazard* quando gli accordi istituzionali non forniscono meccanismi adeguati per il monitoraggio e l'applicazione delle norme, in particolare nel settore finanziario. Sul punto *cfr.* Tuch A., *The Self-Regulation of Investment Bankers*, 83 George Washington Law Review 101, 2014; Clements R., *Can a Cryptocurrency Self-regulatory Organization Work? Addressing its promises and likely challenges*, The finreg blog, global financial markets center, Duke University School of Law, 2018.

dell'attenzione delle istituzioni. Si è, allora, affermata l'idea che l'attività che le istituzioni e le *Authorities* dovevano essere chiamate ad effettuare avrebbe dovuto essere di tipo "attivo", poiché destinata a tradursi in meccanismi regolamentari in grado di favorire innovazioni che fossero tanto redditizie per il mercato quanto vantaggiose per i consumatori/investitori (in particolare nei mercati precedentemente sottoserviti), oltre che facilitare la fornitura di servizi finanziari in modo più economico ed efficiente.

Il primo passaggio compiuto dai Regolatori per seguire questo nuovo tipo di approccio regolamentare, fondato sull'utilizzo della regolamentazione già esistente con una specifica chiave interpretativa, è stato quello di: a) disciplinare il fenomeno del *fintech* in modo 'tecnologicamente neutro'; b) strutturare questa disciplina secondo il modello del c.d. "*duck typing*"[81], ossia sul principio del "*same risk-same rule*" in base al quale occorre utilizzare una medesima regola giuridica (obbligo di segnalazione, licenza o divieto) per far fronte ad un medesimo rischio (di mercato, di liquidità od operativo).

Regolando così la funzione, piuttosto che lo strumento, l'istituzione, o la piattaforma di infrastruttura, le innovazioni *fintech* avrebbero potuto essere regolate all'interno del perimetro normativo già esistente senza la necessità di una disciplina *ad hoc*.

Sebbene tale modello potesse sembrare la panacea di ogni problema regolatorio, presto se ne è individuato un difetto: nella prassi applicativa derivante dall'utilizzo delle nuove tecnologie e dalla interconnessione dei mercati finanziari sarebbero potute emergere nuove combinazioni di rischi – rispetto alle quali il modello del *duck typing* non avrebbe funzionato.

Si è allora considerata una ulteriore opzione: quella di introdurre normative specificamente plasmate sulle quelle nuove architetture sorte con l'innovazione tecnologica (*i.e.* nuove applicazioni della tecnologia *blockchain*, nuove combinazioni di modelli di business e nuove sfide operative digitali) dalle quali derivano nuove tipologie di rischi, figlie del processo di re-distribuzione e decentramento[82].

Taluni paesi hanno fatto invece una scelta più drastica emanando una legislazione *ad hoc* dedicata alle società *fintech*. Questa strategia ha il vantaggio di fornire una regola chiara ed omogenea a tutti gli operatori *fintech* di mercato, di modo che, il nuovo quadro normativo, se adeguatamente concepito, potrebbe fornire una risposta più consona alle esigenze e ai rischi dell'attuale settore dei servizi finanziari.

In relazione a questa scelta vi è stato però chi ha osservato come anche questa strategia di regolamentazione potesse risultare sub-ottimale in quanto, come già detto, stante la velocità di sviluppo delle nuove tecnologie e delle nuove interconnessioni tra settori generati dal *fintech*, tale disciplina rischia sempre di divenire rapidamente

81 Il termine "*duck-typing*" deriva dal linguaggio di programmazione dei computer e si riferisce al famoso test di Howey, spesso semplificato come il "test dell'anatra" (*if it looks like a duck, swims like a duck, and quacks like a duck, then it probably is a duck*).

82 Nuovi rischi operativi nei servizi finanziari digitali e nella catena del valore di mercato possono derivare, peraltro, dalla generazione e analisi di grandi quantità di dati sui clienti e sulle transazioni, ossia dai Bigdata. Sul punto cfr. Makarov I., Schoar A., *Trading and Arbitrage in Cryptocurrency Markets*, 2018, i quali hanno osservato che ad es. i movimenti dei prezzi nelle criptovalute sono in gran parte guidati non dai costi di transazione o dal rischio di *governance differenziale*, ma piuttosto evitando la regolamentazione, quindi dagli spazi generati dal ricorso all'arbitraggio normativo.

obsoleta e comunque rischia di non riuscire a coprire tutte le manifestazioni del *fintech*. Sono state, altresì, evidenziate le difficoltà che i Regolatori avrebbero potuto incontrare nell'elaborare una siffatta legislazione stante le oggettive limitate conoscenze e competenze tecnologiche oggi a disposizione. In ogni caso la risposta di singoli paesi a questi fenomeni globali, ad esempio, avrebbero avuto difficoltà ad applicarsi in paesi connotati da una diversa economia, normativa e assetto istituzionale.

Da tutto quanto detto sopra è emerso come incontrovertibile il fatto che, data la velocità alla quale corrono e si susseguono i cambiamenti tecnologici e i mercati, i precipitati dell'innovazione tecnologica probabilmente supereranno sempre qualsiasi quadro normativo di tipo 'statico' che venisse apprestato dal legislatore e che, pertanto, qualsiasi legislazione sarebbe destinata ad una rapidissima obsolescenza.

La strategia migliore, e per il momento quella più praticata dai diversi Regolatori, è stata quindi quella di assumere una posizione ancillare più che di rigido controllo, *affiancando e coadiuvando gli operatori* lungo il cammino della digitalizzazione attraverso uno sfruttamento efficiente della tecnologia, e, al contempo, cercando di apprendere dal fenomeno quanto più possibile in termini di vantaggi e rischi attraverso un processo di *learnig-by-doing*.

In questo senso la risposta al cambiamento si è risolta in primo luogo nell'offerta agli operatori di programmi governativi sperimentali, in grado di fornire un preliminare perimetro entro il quale muoversi: dai centri di innovazione (*innovation hubs*) alle sabbiere di regolamentazione (*regulatory sandboxes*).

Quando le risorse regolamentari sono scarse, la priorità dovrebbe essere la sperimentazione da parte delle istituzioni di nuovi modelli di regolamentazione al fine di perseguire gli obiettivi fondamentali della protezione degli investitori, dei consumatori e del sistema finanziario nel suo complesso. Una siffatta azione è necessaria non solo per migliorare la capacità di svolgere le funzioni di regolamentazione esistenti, ma anche per affrontare le nuove vulnerabilità create dai modelli di *business* che utilizzano tecnologie come il *machine learning* e gli *smart contracts* per fornire servizi finanziari nuovi secondo nuove modalità.

Cercando di porre l'attenzione ai profili più complessi del fenomeno regolatorio in esame, si può affermare che è stata proprio la differenza di velocità tra il susseguirsi dei cambiamenti tecnologici e la capacità di risposta degli ordinamenti ad aver reso accidentato il cammino della regolamentazione.

Emblematica è stata l'esperienza della sperimentazione adottata da talune Autorità di regolamentazione finanziaria (è il c.d. *Suptech*[83]) che si era senza dubbio originariamente dimostrata una risorsa preziosa per migliorare l'esecuzione di funzioni di regolamentazione finanziaria a lungo termine, ma i cui traguardi oggi sono stati già superati dai nuovi problemi e rischi creati dall'evoluzione delle tecnologie.

83 Per una distinzione tra i lessemi *"SupTech e "RegTech", cfr.* Allen, Hilary J., *Experimental Strategies for Regulating Fintech*, Feb. 6, 2020, p. 22 "[...] *SupTech" to refer to innovation by financial regulators that is informed by technological advances in big data analytics, machine learning and distributed ledger technology. [...] "RegTech" is used to describe technologies that are used by industry participants to facilitate their own regulatory compliance, as well as innovations that are used by the regulators themselves to improve their regulatory functions [...]".*

Questo deriva dal fatto che gli esperimenti di regolamentazione messi in campo incontrano due limiti: a) gli esperimenti di regolamentazione richiedono una adesione volontaria da parte dell'impresa privata a partecipare, sicché, quand'anche l'*Authority* decidesse di servirsi di tali istituti, questi non esplicherebbero alcun effetto nei confronti di quelle imprese che non scegliessero di collaborare con l'Autorità di regolamentazione stessa; b) spesso le stesse *Authorities* non posseggono, come già detto, risorse e competenze adeguate rispetto al nuovo fenomeno.

Per risolvere quest'ultimo problema si è comunque riflettuto sul fatto se alle *Authorities* convenisse utilizzare le risorse disponibili al proprio interno[84] per sfruttare al meglio la tecnologia e raggiungere gli obiettivi normativi di tutela dei consumatori/investitori e stabilità finanziaria, o se invece non fosse auspicabile (specializzandosi proprio anche al fine di comunicare con specialisti esterni e, in generale, attuare una politica di formazione del personale) o se invece avvalersi di risorse esterne. In quest'ultimo caso però potrebbe accadere che i fornitori selezionati per l'*outsourcing* sfruttino le loro competenze e conoscenze acquisite tramite l'attività svolta per le Autorità per offrire poi sul mercato soluzioni analoghe (il *software* Suptech) a favore di quella parte del mercato che è più redditizia, ossia i clienti privati.[85] Un modo possibile per evitare tale fenomeno potrebbe essere allora quello di collaborare con enti del settore pubblico con significativa capacità di ricerca e investire risorse nella formazione ed assunzione di personale qualificato.

Non immuni da critiche sono state anche le *sabbiere regolamentari*: strumenti molto utili dal punto di vista dell'implementazione guidata delle nuove strategie, ma che possono rivelarsi una forma particolarmente problematica di sperimentazione normativa laddove non prevedano norme volte a proteggere i consumatori, gli investitori o la stabilità finanziaria.

Come già detto sopra in relazione all'attività dei regolatori in generale, anche l'attività delle *Authorities* presenta queste problematiche. Infatti, la sperimentazione tecnologica potrebbe altresì essere indirizzata dalle Autorità di regolamentazione verso l'individuazione di soluzioni a vantaggio degli investitori, dei consumatori e della stabilità finanziaria in generale, che puntino al miglioramento dei processi di *disclosure* e di vigilanza[86] e che siano destinate a funzionare indipendentemente dal fatto che una società *Fintech* abbia scelto o meno di collaborare con il Regolatore[87]. A tal riguardo, di nuovo emerge il profilo problematico circa l'effettiva applicabilità delle norme in materia. La natura dell'innovazione tecnologica è, infatti, oggi caratterizzata da una portata globale e non vincolata in alcun modo a confini fisici, se non quelli infrastrutturali. La presenza fisica dell'operatore nei processi è divenuto un aspetto sempre più

84 De Castri S. et al., *Suptech solutions have emerged only recently, with a marked take-off in 2019*, in The suptech generations, bank for international settlements financial stability institute insights on policy implementation no. 99, 14, oct. 2019.

85 Cfr. Enriques L., *Financial Supervisors and RegTech: Four Roles and Four Challenges*, 2017.

86 Ad oggi, gli interventi di sperimentazione e sviluppo di nuovi modelli si sono concentrati principalmente sul miglioramento della raccolta e dell'analisi di quantità voluminose di dati.

87 Ad oggi, gli interventi di sperimentazione e sviluppo di nuovi modelli si sono concentrati principalmente sul miglioramento della raccolta e dell'analisi di quantità voluminose di dati.

intangibile, potendo egli movimentare in modo flessibile e con estrema facilità capitali finanziari, anche rilevanti, verso le giurisdizioni desiderate, sottraendosi ai profili di responsabilità e imputazione dei comportamenti propri dei tradizionali schemi giuridici. Sicché, quandanche si giungesse all'adozione delle auspicate misure regolamentari, non sarebbe possibile assicurare che la condotta degli operatori di mercato si conformi effettivamente alle norme, ben potendo verificarsi fenomeni di fuga dal sistema o realtà che, pur soddisfacendo formalmente i requisiti regolamentari, divergano nei fatti dagli obiettivi e dai limiti imposti dalla disciplina stessa. Sono, infatti, frequenti nel settore tecnologico i fenomeni di *shopping regulation* e di arbitraggio regolamentare[88], in ragione della capacità degli operatori di sfruttare il disallineamento giuridico che deriva dai nuovi modelli di *business* e dalle innovazioni per migliorare le combinazioni rischio-rendimento. Tali condizioni insieme alla facilità di accesso e alla libertà di movimento – sia logistica sia operativa – che queste nuove tecnologie assicurano agli operatori finanziari, contribuiscono a modificare la struttura dei mercati, imponendo una modifica anche delle regole antitrust[89].

In siffatto contesto aumentano, quindi, i rischi di fenomeni di "arbitraggio categoriali", in cui le imprese sfruttano la tecnologia per creare equivalenti più funzionali a prodotti e servizi già regolamentati, oppure per ottenere gli stessi risultati attraverso il ricorso a processi sottostanti non previsti e disciplinati dal regime di regolamentazione esistente.

Di fronte a tale scenario, in cui l'attività di impresa e la finanza non si snodano più entro confini ben definiti, ma anzi, si caratterizzano per una portata *cross boundaries* e *cross sectoral*, l'azione delle *Authorities* nazionali risulta avere scarsa efficacia se non viene coordinata a livello sovranazionale. Proprio la possibilità per gli operatori economici di potersi "muovere" liberamente fra i mercati, neutralizza, infatti, anche gli eventuali "balzi in avanti" regolamentari da parte di Autorità particolarmente diligenti.

La rapidità del cambiamento e l'impatto *disruptive* che l'innovazione produce nei settori non solo economici, ma anche sociali politici e giuridici, rende in definitiva quanto mai necessaria la costruzione di un plesso normativo fondato su princìpi generali, piuttosto che su specifiche disposizioni particolaristiche, e condiviso a livello europeo[90].

88 Due sono le categorie di arbitraggio regolamentare in cui è possibile scadere: "giurisdizionale" e "categoriale". Il primo sfrutta le differenze nelle leggi di diverse giurisdizioni; il secondo, invece, sfrutta una discrepanza legale tra il trattamento di due tipi di attività o prodotti che sono funzionalmente simili. Per una disamina approfondita sul tema *cfr.* Pollman E., *Tech, Regulatory Arbitrage, and Limit*s, 20. EUR. BUS. ORG. L. REV. 567, 571, 2019.

89 Senza fine di esaustività si ricorda in questa sede la revisione del Market Definition Notice del 1997 con lo scopo di determinare se la comunicazione rimanga idonea alla luce dei numerosi cambiamenti economici e di mercato (in particolare la globalizzazione e la digitalizzazione) che si sono verificati negli ultimi 23 anni; cfr. *Evaluation of the Commission Notice on the definition of relevant market for the purposes of Community competition law*, 2020. Nel solco di tali iniziative si pone anche la recente proposta di Regolamento, il *"New complementary tool to strengthen competition enforcement"* o New Competition tool, un'iniziativa volta a colmare le lacune delle attuali norme UE nell'applicazione delle regole di concorrenza UE nei mercati digitali al fine di garantire che la politica di concorrenza e le norme siano adeguate all'economia moderna, preservando la competitività dei mercati. Chiuso il periodo di pubblica consultazione, il regolamento dovrebbe vedere la luce nei primissimi mesi del 2021. Per ulteriori approfondimenti cfr. https://ec.europa.eu/competition/consultations/2020_new_comp_tool/kd0420574enn.pdf.

90 Il presupposto per una buona regolamentazione è avere chiare le esigenze e, soprattutto, gli obiettivi. In tal senso la letteratura economica indica almeno tre forme di fallimenti del mercato per i quali è auspicabile l'intervento dello

2.2 *Bottom-up and Co-regulation:* il circolo regolatorio ed il nuovo ruolo del regolatore

Per adeguare e rendere efficaci gli strumenti della regolazione e della vigilanza al nuovo scenario economico-finanziario, che corre più velocemente rispetto alle risposte dei singoli ordinamenti, è allora necessaria, in aperta discontinuità con il passato, una rivoluzione concettuale[91], prima ancora che normativa, e un'azione di *co-petition* tra le istituzioni nazionali non solo a livello europeo ma anche internazionale[92]. L'inadeguatezza dell'apparato regolamentare costruito nei primi anni 90 del secolo scorso è stata già a più riprese segnalata non solo dagli *stakeholders* – i quali, per primi si sono trovati a dover fare i conti con un sistema normativo obsoleto e lacunoso –, ma anche dalle Autorità europee e nazionali che si sono attivate con gruppi di esperti e pubbliche consultazioni destinate a riformare il plesso normativo di riferimento[93].

La regolamentazione c.d. verticale o per settori di materie, che ha contraddistinto le prime fasi della normazione in materia di mercati finanziari, è caratterizzata dalla presenza di una numerosa progenie di atti di tipo "verticale", ovvero riferiti a singole materie (bancaria, assicurativa e finanziaria in senso stretto) e ben caratterizzati in comparti (regolamentazione a "*silos*").

La realtà si scontra, però, con un dato di fatto: le Autorità di regolamentazione e le istituzioni pubbliche sono in genere poco propense al cambiamento e dispongono di minori finanziamenti rispetto al settore privato per promuovere o anche solo gestire una "*rivoluzione*" tecnologica interna, prima che esterna. Questa criticità diventa ancor più evidente quando l'innovazione procede molto rapidamente, come sta accadendo in questi anni. Il rischio, in questi casi, è quello che la dipendenza dei *player* pubblici dal settore privato, in termini di informazione e competenze, possa giungere sino al punto di determinare una sorta di "cattura della regolamentazione", tale per cui il Regolatore, pur di "restare al passo", inizia ad assumere la visione del mondo dell'industria che regola.

A tale riguardo, si può osservare come le risposte e i tentativi di addivenire ad una regolamentazione sul punto si poggiano necessariamente su un esercizio di interpretazione ed applicazione pratica e probabilistica delle normative esistenti ai nuovi casi che di volta in volta si profilano sullo scenario economico-finanziario.

Stato attraverso la predisposizione di una regolamentazione: l'asimmetria informativa, la presenza di esternalità ed il potere monopolistico. A questi obiettivi economici se ne sono nel tempo aggiunti altri come la tutela degli investitori e dei consumatori, la stabilità finanziaria e l'integrità del mercato, che le istituzioni e le autorità nazionali hanno ritenuto sempre più rilevanti e a favore della tutela dei quali hanno modellato la propria azione. La gerarchia di desiderabilità di questi obiettivi varia ovviamente a seconda del paese di riferimento, del suo contesto socio-politico-economico, nonché dal momento storico, ma, in ogni caso, si può oggi ragionevolmente affermare che la gran parte delle Autorità di regolamentazione ne ha implicitamente o esplicitamente riconosciuto il perseguimento come propria *mission*.

91 L'espressione "circolo regolatorio" è stata proposta in dottrina da F. Bassan, "Potere dell'algoritmo e resistenza dei mercati in Italia", op. cit.

92 Allen, Hilary J., Experimental Strategies for Regulating Fintech, February 6, 2020.

93 Yueh-Ping (Alex) Yang & Cheng-Yun Tsang, *RegTech and the New Era of Financial Regulators: Envisaging More Public-Private Partnership Models of Financial Regulation*, 21 U. PA. J. BUS. L. 354, 360-1, 2018.

Nel procedere a tali operazioni interpretative, piuttosto che assistere ad una regolamentazione calata dall'alto, non efficiente e non efficace per le ragioni viste in precedenza, sarebbe forse auspicabile ripensare ad una strategia che coinvolga anche gli *stakeholder*, non prima di aver preso coscienza del mutato ruolo che essi rivestono all'interno della società e più in particolare nel paradigma economico delle strategie delle imprese[94].

Se per la teoria economica classica l'impresa mira esclusivamente alla massimizzazione dei profitti, per le nuove teorie basate sul modello degli *stakeholder* tale aspetto non è più da solo sufficiente a determinare la qualità e la profittabilità dell'impresa, soprattutto nel lungo periodo; per cui al perseguimento del profitto deve accompagnarsi anche l'attenzione per il ruolo che l'impresa stessa svolge nella comunità in cui opera[95].

Se solo attraverso la soddisfazione delle aspettative di tutti gli *stakeholder* l'impresa è in grado di acquisire legittimazione sociale per operare sul mercato, si apre allora la porta ad un nuovo modello di gestione e di governo, sempre orientato al perseguimento del profitto, ma che tiene conto anche degli equilibri ambientali e sociali, bilanciando e rispondendo in modo efficace ed efficiente non solo alle esigenze dei clienti ma anche alle aspettative del gruppo degli *stakeholder*. Da questo punto di vista, infatti, la finalità imprenditoriale preminente non è solo la massimizzazione del profitto, ma anche la creazione di valore economico e sociale attraverso la gestione del sistema di relazioni con i diversi *stakeholder* e il loro massimo coinvolgimento nei processi decisionali (*stakeholder engagement*).

Simili considerazioni, *mutatis mutandis*, possono svolgersi anche con riferimento agli ordinamenti, dove l'attenzione ai rapporti con i vari *stakeholder* deve assurgere a nuova leva strategica per rispondere alle nuove criticità dettate dall'innovazione e dalla *digital disruption*. Sono, infatti, proprio gli *stakeholder,* quali principali attori della nuova rivoluzione, a sperimentare direttamente sul campo le innovazioni *fintech* e quindi a dover risolvere i problemi che da esse derivano con soluzioni che, in assenza di un chiaro quadro normativo, nascono dall'esperienza e dal *case law*. L'atteggiamento dei regolatori, caratterizzato da un approccio conservativo e attendista,

94 *Ex multis* si ricorda in questa sede come l'evoluzione degli studi sulla responsabilità sociale d'impresa (*Corporate social responsibility*) sia stata di recente segnata dalla teoria degli stakeholder (*stakeholder theory*), cambiando profondamente il rapporto fra l'impresa e i suoi vari portatori di interesse e introducendo il principio della responsabilità sociale nel management dell'impresa. L'impresa è, infatti, vista come «*un insieme complesso di relazioni tra gruppi di interesse con obiettivi diversi, ognuno dei quali contribuisce alla sua performance e si aspetta benefici (o almeno di non essere danneggiato senza indennizzo) come risultato dell'attività aziendale*» (*cfr. ex multis* D'Orazio E., *Verso una teoria degli stakeholder descrittiva: modelli ad uso dei manager di organizzazioni complesse*, in *notizie di POLITEIA*, XXI, 78, 2005; Freeman, R.E., Wicks, A., Parmar, B., McVea, J., *"Stakeholder Theory: The State of the Art and Future Perspectives*", in *notizie di Politeia*, XX, 2004; Harrison, J.S., e Freeman, R.E., "*Stakeholders, Social Responsibility, and Performance: Empirical Evidence and Theoretical Perspectives*", Academy of Management Journal, 1999; Englewood Cliffs, N.J., Prentice Hall.; Freeman, R.E., *Strategic Management: A Stakeholder Approach*, Boston, Pitman, 1984; Freeman, R.E., *"The Politics of Stakeholder Theory: Some Future Directions"*, Business Ethics Quarterly, 1994; Ansoff, H., *Implanting Strategic Management*, 1984.

95 Cfr. Sul tema Freeman E., *Strategic management .A stakeholder approach,* Pitman, 1984; Donaldson T., Preston L., *The Stakeholder Theory of the Corporation: Concepts, Evidence, and Implications*, Academy of Management Review, Vol.20, n.1, 1995; Mitchell R.K., Angle B.R., Wood D.J., Toward a *Theory of Stakeholder Identification and Saliance: Defining the Principle of Who and What Really Counts*, Academy of Management Review, Vol.22, n.4, 1997.

genera, infatti, come contraccolpo una maggiore spinta da parte degli operatori verso la sperimentazione e la ricerca di soluzioni volte a colmare tale vuoto o a superare gli ostacoli che da esso ne derivano, sia a livello pratico sia normativo.

Sarebbe, pertanto, auspicabile che la linea regolamentare da intraprendere venisse discussa, prima che decisa, di concerto con gli *stakeholder*, al fine di valutare quali siano le strategie maggiormente sostenibili nel tempo e più efficienti dal punto di vista economico-finanziario.

Si parla, infatti, oggi a tal proposito di "co-regolamentazione": il mercato dal basso trova le regole e sperimenta le soluzioni di disciplina ottimali e le *Authorities* recepiscono le spinte e le prassi attuate dai singoli partecipanti al mercato, per poi comunicarle al rispettivo Legislatore nazionale, il quale da ultimo le condivide in sede europea[96].

Il *circolo regolatorio*[97] comporta, pertanto, un rovesciamento dei ruoli: non sono più i Regolatori istituzionali a porre le norme dall'alto per modellare la realtà secondo il disegno astrattamente costruito e politicamente desiderabile, ma, al contrario, la produzione normativa viene ad essere fortemente influenzata dall'esperienza e dagli interessi concretamente espressi dagli operatori privati. Questi ultimi quando non trovano le regole atte ad assistere e regolare il proprio *business model*, inevitabilmente procederanno a dar vita a negoziati interni e a prassi di settore, che si imporrano anche all'esterno. In altre parole sarà la realtà a modellare la norma.

Ciò non vuol dire, tuttavia, che si debba abbracciare una regolamentazione altamente specifica e 'casistica', volta a disciplinare le singole e diverse fattispecie che possano sorgere – il che darebbe vita ad altri e ulteriori problemi legati all'obsolescenza normativa di fronte alla velocità del progresso economico e tecnologico –, ma anzi significa prediligere una regolamentazione per principi, in cui sia possibile di volta in volta calare e sussumere la regola generale nel caso di specie.

In questo modo si darebbe vita ad un (nuovo) modello di produzione normativa necessariamente *cross sectoral* e ultra-territoriale, per far sì che le barriere geografiche non divengano barriere economiche e sociali tali da ostacolare l'aggiornamento continuo degli ordinamenti di fronte all'inarrestabile processo innovativo sul piano tecnologico ed economico.

Questa impostazione traspare anche dalle tecniche di legislazione adottate dal Parlamento, dal Consiglio e dalla Commissione Europea nell'ultimo biennio: è stato, infatti, prediletto lo strumento del "regolamento" che ha il pregio di applicarsi uniformemente su tutto il territorio europeo e che è sempre più spesso preceduto da periodi di pubbliche consultazioni in cui viene dato molto spazio alle considerazioni espresse dagli *stakeholders* di settore, dalle altre autorità nazionali, dalle istituzioni e da

96 Renda A., *From impact assessment to the policy cycle: drawing lessons from the eu's better-regulation agenda*, SPP Technical Paper, Volume 9 • Issue 33 • October 2016; Hahn R., Renda A., *Understanding Regulatory Innovation: The Political Economy of Removing Old Regulations Before Adding New Ones*, August 2017.

97 F. Bassan, *Potere dell'algoritmo e resistenza dei mercati in Italia*, op. cit.

chiunque voglia contribuire al dibattito. Si è, infatti, compreso che in questa materia così vasta ed ontologicamente intersettoriale, solo l'incontro di competenze diverse è in grado di fornire un valido strumento di conoscenza, prima ancora che di regolazione.

2.3 *Principle-based & risk-based approach*. Quando il diritto rincorre la realtà

Chiarito, dunque, che non esiste un modello normativo 'universale'[98] in grado di affrontare le sfide lanciate dal *fintech*, la scelta della strategia di regolamentazione da adottare e l'opportunità di un approccio specifico dipendono da una varietà di fattori, tra cui il tipo di sotto-settore *fintech* da regolare[99] (i.e. *criptoassets*, pagamenti digitali, etc), le caratteristiche specifiche del paese di riferimento, gli obiettivi e le priorità delle Autorità di regolamentazione finanziaria.

Ma al di là di quella che è l'attività di ricerca di un modello normativo universale per il *fintech*, esistono, poi, anche esigenze legate a specifici settori dell'economia che necessitano di una normativa altrettanto specifica.

Così ad esempio, osservando i tentativi esperiti da talune Autorità nazionali (quali quelle degli Stati Uniti d'America e della Cina), si può affermare che esse abbiano principalmente avuto come obiettivo finale la promozione dell'efficienza economica e l'ordinato svolgimento della concorrenza nel mercato. Di contro la promozione della tutela dei risparmiatori in questi ultimi anni ha rivestito in tali Paesi un rilievo di secondo piano. Sebbene, infatti, alcune delle politiche di attuazione di tali programmi considerino anche questo aspetto, ad esempio ampliando l'accesso ai servizi finanziari e riducendo il loro costo, la tutela del consumatore/risparmiatore appare come esternalità positiva più che come un vero e proprio obiettivo da perseguire *in sè*[100].

L'efficienza e la tutela della concorrenza sono certamente obiettivi regolamentari fondamentali, ma è necessario che essi vengano controbilanciati (soprattutto in ambito europeo) anche col perseguimento degli obiettivi della stabilità finanziaria (micro e macro) e della tutela degli investitori/consumatori, che sono il carburante grazie al quale il sistema mercato funziona. Grazie ad esse, infatti, si garantisce la fiducia della collettività a partecipare a un sistema finanziario caratterizzato da evidenti asimmetrie informative.

98 Poiché il *fintech* racchiude un ampio spettro di attività, un approccio normativo unico rischierebbe di soffocare l'innovazione e scoraggiare i nuovi operatori di mercato. Di conseguenza, di fronte alle attuali risposte normative che differiscono ampiamente tra i tipi di attività e giurisdizioni, i regolatori hanno essenzialmente tre opzioni a questo proposito: ignorare il fenomeno e lasciare che si autoregoli ("*KeepItUnregulated*"), adottare l'approccio "*SameRisk-SameRules*", oppure cercare un nuovo sistema basato sul tipo di attività ("*NewFunctionality-NewRules*").

99 Cfr. Amstad, M., *Regulating Fintech: Ignore, Duck Type or Code*, Voxeu.com, March, 2019, che evidenzia come "*The first option is to leave fintech largely unregulated. In the early days of fintech, regulators in most jurisdictions chose "wait and see". [...] At that time, some fintech companies felt hampered in their activities as they could not benefit from the legal certainty of regulation, a criticism that contrasts with the sometimes anti-government approach of at least some fintech activities.*

100 Gordon J. N., *'Dynamic Precaution' in Maintaining Financial Stability: The Importance of FSOC*, in TEN YEARS AFTER THE CRASH, Sharyn O'Halloran & Thomas Groll eds., 2018.

Pertanto, nello sviluppo e nella predisposizione dei modelli di regolamentazione finanziaria, è necessario che anche questi profili non vengano compromessi ad esclusivo vantaggio dell'efficienza e della concorrenza basate sull'innovazione[101]. Se, infatti, il processo di innovazione avvantaggiasse esclusivamente l'"innovatore" e non generasse più ampi benefici anche per l'intera collettività, l'azione regolatoria posta in essere non potrebbe essere considerata una buona strategia di politica pubblica. Dal momento che non sembra realistico aspettarsi che l'innovazione del settore privato promuova scientemente l'obiettivo normativo della micro e macro/ stabilità finanziaria, se non indirettamente, mancando gli incentivi in tal senso e scontando inoltre la difficoltà di coordinare i loro concorrenti, è necessario che gli interventi per promuovere la stabilità del sistema finanziario nel suo complesso siano sempre assicurati dalle istituzioni e dalle autorità del settore.

Veicolo di tali idee e intenti in Europa è stato senza dubbio il Report dell'*Expert Group on Regulatory Obstacles to Financial Innovation* (di seguito anche ROFI EG)[102], anche noto come "*Le 30 Raccomandazioni*". Il *Report*, pubblicato nel dicembre 2019, rappresenta il prodotto della ricerca svolta dal Gruppo di esperti sulle modalità e sulle strade da seguire per creare un quadro europeo che soddisfi le esigenze di innovazione per la fornitura di servizi finanziari basati sulla tecnologia.

Secondo questi, le potenzialità ed i benefici del *Fintech*, se sfruttati appieno, potrebbero, infatti, avere un impatto reale sui mercati e sulle istituzioni finanziarie e su come vengono forniti i servizi finanziari stessi. Le 30 Raccomandazioni sono volutamente di ampia portata e, in ossequio ad una *principle-based regulation*, tracciano i principi da porre alla base della nuova regolazione, trasfondendoli in requisiti per delinearne i risultati attesi.

Esse investono tutti i settori del *Fintech*, tutte le tipologie di tecnologie e di *business*, con l'obiettivo di assicurare e mantenere condizioni di parità, accesso ai dati, inclusione finanziaria e uso etico dei dati. Sono, inoltre, supportate dalle analisi empiriche con l'intento di superare la situazione di incertezza, le differenze normative tra i mercati e il rischio di arbitraggio normativo, attraverso un'adeguata cooperazione tra le autorità di regolamentazione mondiali. A tal fine, i principali ambiti di ricerca e di intervento coinvolgono quattro macro-aree: (*i*) l'uso innovativo della tecnologia nella finanza, (*ii*) la creazione di un quadro unico e armonizzato, (*iii*) l'accesso ai dati, (*iv*) l'inclusione finanziaria e l'uso etico dei dati.

In particolare la prima area di indagine si incentra sulla necessità di adattare gli strumenti regolatori attualmente vigenti ai nuovi rischi connessi all'utilizzo delle nuove tecnologie nel sistema finanziario. In tal senso, si evidenzia l'opportunità per i *supervisors* di sviluppare programmi di formazione del personale sulle nuove tecnologie e la necessità per i soggetti vigilati di dotarsi di adeguati livelli di "*IT governance*".

101 Zetzsche, D.A., Buckley R.P., Arner D.W. e Barberis J.N., *From FinTech to TechFin: The Regulatory Challenges of Data-Driven Finance*, EBI Working Paper Series, n. 6, 2017.

102 L'incarico si pone nell'ambito delle iniziative sorte a livello europeo in occasione della pubblicazione del Fintech Action Plan della Commissione dell'8 marzo 2018.

L'indagine muove, poi, verso l'individuazione degli strumenti più adeguati ad assicurare un *level playing field*, soprattutto tra *FinTech start-ups* e *BigTech incumbents*; strumenti che vengono individuati nella predisposizione di una regolazione uniforme e nella standardizzazione della terminologia digitale. Per fare ciò occorre inevitabilmente partire dalla regolamentazione e dalla tutela di nuovi beni giuridici ed attività del ventesimo secolo: gli "spazi di dati"[103] e l'utilizzo dei Big Data.

Posto che l'industria finanziaria è ormai *"data-intensive"* essendo sia il settore finanziario, sia quello bancario, che quello assicurativo, dipendenti dai dati e dalle informazioni, assume una rilevanza centrale la necessità di conciliare l'accesso e l'utilizzo dei dati con la tutela della *privacy*, quale diritto fondamentale riconosciuto e garantito dal diritto europeo. Tale diritto è peraltro esaminato dal Gruppo di esperti anche sotto il profilo dell'utilizzo etico dei dati, a tal fine ritenendo che - sia a livello Europeo, sia a livello nazionale in chiave armonizzata - debba essere assicurata una *financial inclusion*, per evitare discriminazioni o di esacerbare l'esclusione di determinati gruppi di soggetti dall'accesso ai servizi finanziari.

Si tratta di regole trasversali che affrontano i principali problemi che la tecnologia porta con sé e che mirano a rendere più trasparenti le nuove opportunità e i nuovi rischi, consentendo così alla tecnologia di produrre i suoi effetti positivi, primo fra tutti una maggiore inclusione finanziaria.

Oltre a ciò, il Report del *ROFIEG* si differenzia dagli altri contributi sul tema in ragione della novità dell'approccio metodologico con cui i temi sono stati affrontati. In particolare ad essere nuova è la prospettiva di analisi: sganciandosi dalla tradizionale visione soggetto-centrica, l'indagine adotta la regola (già menzionata in precedenza) secondo cui "*agli stessi rischi debbono applicarsi le stesse regole*" (*same risks-same rules*). Si rifugge, quindi, dalla ricerca di una regolamentazione specifica e puntuale, in favore di un approccio più ampio e *cross-sectoral*. Di fronte ad un problema nuovo, è, infatti, necessario un criterio di risoluzione innovativo che sia in grado di comprendere le peculiarità del fenomeno al fine di fornire una risposta efficiente.

Il principio cardine che sta alla base di tale impostazione è quello della *neutralità tecnologica* della regolamentazione e supervisione finanziaria, cosicché non sia pregiudicato alcun tipo di tecnologia o di operatore. A tal fine le raccomandazioni elaborate dal Gruppo di esperti suggeriscono i perimetri di regolamentazione e di vigilanza che meglio dovrebbero consentire alle imprese operanti nel mercato unico dell'UE di beneficiare dell'innovazione finanziaria e di fornire ai loro clienti i prodotti più adeguati

103 Il concetto di spazio di dati nasce in relazione al sempre maggiore aumento del flusso di dati grazie al sempre maggiore numero di utenti e oggetti connessi, sia tra di loro, sia intersecandosi ed interconnettendosi nell'ambito di aree e materie fra loro anche molto diverse (si pensi ai dati raccolti da oggetti *werarable*, auto connesse, *health tracker*, ect). Ragionando sul modello insiemistico, si può parlare di "*spazi di dati*", settoriali e trasversali, in cui i dati pur appartenenti a categorie diverse sono fra loro abbinati, interconnessi ed impiegati per diverse finalità. Ai *big data* (raccolti in spazi di dati trasversali) si aggiungeranno, quindi, tutta una serie di informazioni periferiche (spazi settoriali), che comunque confluiranno nei *cloud* nazionali ed europeo A tal riguardo è allora indispensabile predisporre sistemi di protezione e sicurezza, diffusi a livello europeo, che assicurino una interoperabilità giuridica e semantica fra i dati, i formati e le regole di diritto costruite by design, cosicché possano essere garantiti i presidi minimi di sicurezza ed il rispetto dei principi fondamentali stabiliti a livello eurounitario prima, ad esempio quello della parsimonia nell'utilizzo dei dati come auspicato dal GDPR, ed estendibili poi a livello internazionale.

e accessibili, ricercando, allo stesso tempo, soluzioni che consentano di tutelare i consumatori, l'integrità e la competitività del mercato, senza ostacolarne l'innovazione.

La nuova legislazione o le nuove misure regolatorie dovrebbero essere quindi basate su principi e riferirsi ad attività (e non a prodotti o soggetti); dovrebbero essere inoltre *technology neutral* e *device agnostic*, nonchè "*risk-based*" e "*activity-based*" al fine di consentire una valutazione completa del rischio all'interno del sistema finanziario, ponendo l'accento su ciò che dovrebbe realmente interessare l'Autorità di regolamentazione: valutare il livello di rischio generato da determinati attori e attività e attuare, per l'effetto, strategie di regolamentazione per affrontare tali rischi[104].

Siffatto approccio si fonda altresì sui principi di "materialità" e "proporzionalità" per regolare adeguatamente le tecnologie finanziarie, caratterizzate da rapidi cambiamenti e sviluppi tecnologici. Seguendo questo schema, solo quando il rischio rappresentato dalle nuove tecnologie diventa *materiale*, una regolamentazione *proporzionale* al rischio deve essere messa in campo. Si è visto, infatti, che introdurre regole prima del tempo potrebbe soffocare l'innovazione e potenzialmente impedire il pieno sviluppo delle tecnologie. A ciò si aggiunga il fatto che per valutare l'importanza di ciascuna delle molteplici risposte normative e individuare quella maggiormente efficace sul piano dei risultati e degli effetti, è necessario tenere in considerazione il diverso grado di importanza che il *fintech* ricopre all'interno di ciascuna giurisdizione[105], sicché quale sia l'approccio migliore solo il tempo potrà dirlo.

Queste e altre ragioni depongono a favore della neutralità tecnologica quale principio normativo chiave. In primo luogo, il cambiamento tecnologico è molto veloce e sempre più imprevedibile, sicché potrebbe essere non più possibile né efficace rivedere e aggiornare costantemente i regolamenti al fine di evitarne la rapida obsolescenza; inoltre astenersi dallo scegliere una tecnologia rispetto all'altra, in termini di regolamentazione, escluderebbe la responsabilità potenziale in capo ai Regolatori, ossia il rischio che tale attività possa essere percepita in qualche modo come una garanzia implicita di copertura/sicurezza da parte del regolatore ad una data tecnologia.

Se queste sono le premesse, la disciplina in materia - che pure deve essere dettata ancorché limitata alla sola fissazione di principi base - necessita in ogni caso di un connotato di proporzionalità.

104 Entro tali limiti, pertanto, le autorità nazionali, adottando un approccio neutrale e *risk-based,* sono chiamate a stabilirei requisiti normativi in relazione ai servizi finanziari che presentano un rischio simile in relazione ai fattori quali la dimensione, l'importanza sistemica, la complessità e il profilo di rischio stesso. Questo approccio, infatti, non cerca solo di affrontare i rischia livello individuale e di tutela, ma anche quelli per l'intero sistema finanziario, assicurando all'autorità di regolamentazione un'attività di monitoraggio permanente.

105 Uno studio condotto dalla Cambridge University ha evidenziato come la risposta normativa principale sia ad oggi, con quasi il 50%, l'"*aspettare e vedere*", mentre il 42% della regolamentazione adotta un approccio *duck typing*; solo nel 10% delle giurisdizioni si osserva una risposta *fintech* "*su misura*". *Cfr.* Cambridge Centre for Alternative Finance, *Early Lessons on Regulatory Innovations to Enable Inclusive FinTech: Innovation Offices, Regulatory Sandboxes, and RegTech*, Cambridge, University of Cambridge, 2019; Institute of Digital Finance, *Digital Inclusive Finance Index Report 2011–2017*, Beijing: Institute of Digital Finance, Peking University, 2018.

Il concetto di proporzionalità mira, in questo contesto, a limitare l'intervento pubblico al fine di evitare eccessivi costi di conformità o oneri normativi per gli operatori del settore.

Seppur chiaro è l'aspetto teorico di questa impostazione, tuttavia, è difficile prevedere nella pratica una regolamentazione puramente basata soltanto su principi o, all'opposto, soltanto su regole[106]. Ogni regime normativo basato principalmente su principi dovrà avere altresì talune regole di attuazione, così come qualsiasi regime basato essenzialmente su regole dovrà individuare anche qualche principio. Il mix appropriato di ciascuno dipende da una serie di fattori, fra cui la maturità del mercato, le caratteristiche degli operatori di mercato e la qualità del regolatore.

Nonostante le caratteristiche specifiche di ciascuna giurisdizione (che fanno sì che la strategia scelta ed applicata possa variare da un paese a un altro e da un settore all'altro) rimane il fatto che una regolamentazione *principle-based* sia attualmente la più appropriata per disciplinare la maggior parte degli aspetti legati al *fintech* in ragione dell'incapacità delle Autorità di regolamentazione di mettersi al passo con il mercato e di dare spazio sufficiente al l'innovazione.

I princìpi, quali clausole generali, si atteggiano, infatti, a valvole di sfogo dell'ordinamento, consentendogli di adattarsi con pochi sforzi alla mutevolezza della realtà, al cambiamento dei costumi e degli interessi rilevanti, senza la necessità di un continuo adeguamento.

A tal fine diviene allora particolarmente importante individuare i principi cardine in grado di reggere il complesso sistema degli equilibri politici, economici, sociali e finanziari all'interno del settore *fintech*.

Gli obiettivi possono essere individuati in quelli classici della tutela degli investitori e dei consumatori, della stabilità finanziaria e dell'integrità del mercato, e, sebbene la loro attuazione e la loro gerarchia varino da giurisdizione a giurisdizione, anche i tre capisaldi della certezza giuridica[107], della neutralità tecnologica e della

106 Molte Autorità di regolamentazione stanno spostando l'attenzione su un modello di regolamentazione basato su di un'ampia serie di principi e di regole incentrate sui risultati, nonostante permangano, tuttavia, i fautori dell'approccio *rule-based* che ritengono che abbracciare un modello in cui sono gli operatori a dover perseguire gli obiettivi strategici (ad esempio, proteggere gli interessi dei consumatori), per poi spiegare al regolatore come raggiungere questi obiettivi, prescindendo dal rispetto delle procedure standard, non fornisca sufficiente certezza giuridica per i partecipanti al mercato.

107 In particolare la garanzia della certezza del diritto richiede una solida definizione dei perimetri normativi e un'applicazione trasparente della legge. Il contesto della *fintech*, la terminologia e la classificazione poco chiare dei singoli applicativi incoraggiano l'arbitraggio normativo e, in ultima analisi, ostacolano un quadro giuridico solido e per l'effetto, l'innovazione finanziaria stessa. Non sorprende quindi che molti progetti *fintech* siano desiderosi di essere regolamentati, in quanto ciò infonde la certezza giuridica necessaria per attirare gli investitori. D'atro canto, vi è, però, il rischio che gli approcci dei regolatori di codifica in una fase iniziale di sviluppo siano eccessivamente restrittivi e possano persino dirigere intenzionalmente o involontariamente l'innovazione, minandone gli sviluppi. Le sfide che quindi si pongono alla certezza del diritto possono essere, quindi, così annoverate. In primo luogo, la velocità con cui si sviluppa il fenomeno *fintech* in termini di modelli di business contrasta con le lunghe procedure per le nuove norme di regolamentazione comunemente seguite nei sistemi giurisdizionali; in secondo luogo l'elevato numero di istituzioni governative coinvolte, se da un lato contribuisce a garantire la formazione integrata della disciplina, dall'altra, ampliando notevolmente il perimetro regolamentare, rallenta e rende difficoltoso addivenire a norme che siano in grado di tenere conto di tutte le innegabili specificità regolatorie di cui i vari attori sono portatori. La terza sfida è poi rivolta ai regolatori e agli operatori di mercato, posto che il *Fintech* impone sempre più il ricorso a conoscenze e tecnicità

proporzionalità (spesso indicata anche come "*giudizio basato sul rischio*") risultano comuni fra i vari ordinamenti e ampiamente condivisi e accettati dalle autorità di regolamentazione.

Ciascuno di questi principi nel contesto della finanza digitale mira a creare condizioni di parità per gli operatori di mercato assicurandosi che tutti operino all'interno di uno stesso *framework* normativo (*levelling the playing field*), trattino le tecnologie in modo paritario e trovino un equilibrio tra l'esposizione al rischio e i requisiti normativi.

A tale riguardo recentemente la Commissione Europea ha dichiarato che tutte le iniziative del programma "*Shape Europe's Digital Future*"[108] sono volte al raggiungimento di un obiettivo strategico fondamentale: quello di garantire che il settore finanziario dell'UE abbracci tutte le opportunità offerte dalla rivoluzione digitale, così da posizionarsi al primo posto nel mercato europeo, assicurando ai consumatori e alle imprese europei i benefici della finanza digitale innovativa e garantendo nel contempo un'adeguata protezione dai rischi.

Quattro sono in particolare gli obiettivi da perseguire durante il mandato del Parlamento europeo e della Commissione fino al 2024: (i) affrontare la frammentazione del mercato unico digitale per i servizi finanziari al fine di offrire ai consumatori europei un accesso effettivo ai servizi transfrontalieri e promuovere l'espansione delle imprese finanziarie europee; (ii) garantire che il quadro normativo dell'UE agevoli l'innovazione digitale nell'interesse dei consumatori e dell'efficienza del mercato; (iii) creare uno spazio europeo di dati finanziari per promuovere l'innovazione basata su dati aperti; (iv) affrontare le nuove sfide e i rischi connessi alla trasformazione digitale. Nell'ambito di tali priorità, la Commissione si è inoltre impegnata a lavorare a stretto contatto con i nostri partner internazionali, dal momento che i vantaggi della finanza digitale sono meglio sfruttati se la loro diffusione si basa su principi e standard compatibili a livello internazionale.

La digitalizzazione dei servizi finanziari continua, infatti, ad apportare numerosi vantaggi all'economia attraverso la fornitura di servizi innovativi a prezzi competitivi ai clienti. Inoltre l'esperienza, ancora in essere, del Covid-19 ha dimostrato che i servizi digitali possono anche contribuire alla resilienza delle società in tempi di crisi.

informatiche, di codifica, oltre alla consueta ma rinnovata conoscenza del mercato da un punto di vista legale e finanziario. La regolamentazione finanziaria in molte giurisdizioni coinvolge, infatti, una varietà di istituzioni (tra cui la banca centrale, gli organismi di vigilanza finanziaria, altri dipartimenti governativi come l'amministrazione fiscale, l'autorità di regolamentazione legislativa e antiriciclaggio, etc). L'ambito di applicazione delle diverse autorità di regolamentazione, già variegato prima dell'era digitale, vede oggi nuove ed ulteriori sovrapposizioni e stratificazioni nella regolamentazione delle attività degli *asset* digitali. Sul punto *cfr.* Cambridge Centre for Alternative Finance, *Early Lessons on Regulatory Innovations to Enable Inclusive FinTech: Innovation Offices, Regulatory Sandboxes, and RegTech*, Cambridge, University of Cambridge, 2019.

108 Il programma, lo si è visto, include il Fintech Action Plan 2018, la relazione 2019 del Gruppo di Esperti sugli Ostacoli Normativi all'innovazione Finanziaria (ROFIEG), le Raccomandazioni per il 2020 del Forum di alto livello sull'Unione dei mercati dei capitali e la Strategia 2020 per le PMI per un'Europa digitale e sostenibile. Cfr. per maggiori informazioni https://ec.europa.eu/info/business-economy-euro/banking-and-finance/digital-finance_en; https://ec.europa.eu/info/sites/info/files/business_economy_euro/banking_and_finance/documents/210202-call-advice-esas-digital-finance_en.pdf.

Tuttavia, la digitalizzazione comporta anche nuovi rischi: la dipendenza dall'infrastruttura digitale associata alla raccolta e all'elaborazione di masse di dati altamente sensibili attraverso complesse catene del valore con più fornitori di servizi, la velocità dell'innovazione e le crescenti pressioni per ridurre i costi creano nuove vulnerabilità e rischi a livello di società. Questi rischi devono essere gestiti in modo adeguato dalle istituzioni finanziarie e dai loro fornitori di servizi.

Dal momento che i mercati finanziari sono fortemente interconnessi con altri settori critici (come le telecomunicazioni e le reti energetiche) è auspicabile che vengano rafforzati i requisiti per la gestione del rischio, soprattutto a livello sistemico, mediante un approccio *"whole-of-government-and-society"* (*i.e.* "a livello di governo e società"), che tenga quindi conto anche delle considerazioni di sicurezza nazionale.

A tal riguardo la recentissima proposta di regolamento DORA (*"Digital Operational Resilience Act")* si pone come punto di partenza per affrontare i rischi derivanti dalla digitalizzazione, in modo da fornire un approccio globale per affrontare anche la natura sistemica dei rischi in questione.

2.4 Raccolta, utilizzo e trasmissione dei dati

Un ordinamento che sappia coordinarsi con l'innovazione per raccogliere le nuove sfide che essa pone, semplicemente facendo perno sui principi fondamentali ed inderogabili entro i quali la realtà si muove, resiste nel tempo all'obsolescenza normativa ed interpretativa.

A partire da siffatte considerazioni e a cominciare dalla disciplina sulla concorrenza - che si è posta in qualche modo quale comune denominatore dei vari settori del mercato, in grado di coglierne i legami e gli aspetti di connessione - si è allora iniziato a prevedere una regolamentazione di tipo "orizzontale", in grado di collegare fra loro settori che erano strettamente interconnessi dal punto di vista economico e sociale, ma che dal punto di vista giuridico rimanevano indipendenti e isolati.

Le interdipendenze fra queste materie, infatti, sia a livello normativo che pratico dovevano necessariamente essere disciplinate da una normativa che fosse in grado di abbracciare i singoli aspetti di ogni settore, in un'ottica di armonizzazione.

Questa funzione pare oggi essere stata attribuita alla *normativa sulla protezione dei dati* (normativa che riguarda sia i dati personali[109] che quelli non personali[110]); dati la cui disponibilità è, infatti, sempre più rilevante per l'ottimizzazione dei processi e delle decisioni, per l'innovazione e per l'efficiente funzionamento dei mercati. In particolare i *Big Data* sono una caratteristica che non limitata soltanto a specifici settori ma che investe l'economia nel suo complesso, con il risultato che lo sviluppo dell'economia *data driven* ha implicazioni non solo sul funzionamento dei

109 *Cfr.* Regolamento generale sulla protezione dei dati personali (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016.

110 Cfr. Regolamento (UE) 2018/1807 del Parlamento europeo e del Consiglio, del 14 novembre 2018, relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea.

mercati e sul benessere dei consumatori, ma anche sotto il profilo sociale e democratico. Si tratta, in altre parole di una nuova forma in cui si manifesta il potere di mercato e che merita, dunque, un'attenta valutazione per le sue implicazioni economiche e sociali.

Si ricorda qui che con il termine "dati" si intende il complesso delle informazioni riferite ad un soggetto, a carattere personale e/o non personale, che vengono raccolte, analizzate e conservate in *database ad hoc* predisposti[111]. In ragione del ruolo centrale da essi ricoperto nella moderna economia, gli stessi vengono ricompresi fra i beni giuridici[112] e, sono, per l'effetto, suscettibili di valutazione economica, oggetto di scambi e transazioni, possono essere trasferiti a terzi, oggetto di atti di rinuncia da parte del titolare del diritto. Il valore dei dati in questione, occorre premetterlo, non deriva tanto dalle informazioni in sé e per sé detenute, quanto piuttosto dal lavoro di raccolta, analisi e utilizzo che di tali informazioni è stato fatto. Di qui l'importanza della circolazione dei dati all'interno del mercato, del loro trasferimento e del loro impiego.

L'economia mondiale dei dati è, infatti, caratterizzata da un ecosistema di diversi tipi di operatori di mercato che competono e collaborano per generare valore aggiunto. In siffatto contesto la capacità di accedere ai dati è divenuta per gli operatori di settore il *quid pluris* in termini di potere di mercato ed elemento chiave della competitività globale dell'UE. Nel quadro normativo europeo la protezione delle persone fisiche in relazione al trattamento dei loro dati personali assurge, infatti, a diritto fondamentale e ad elemento distintivo rispetto ad altri ordinamenti (come quello statunitense) che, invece, si preoccupano meno del tema relativo alla diffusione ed al trattamento dei dati (creando spazi per arbitraggi normativi).

111 Con la locuzione "Big Data" si fa riferimento, nell'assenza di definizioni normativamente vincolanti, alla raccolta, all'analisi e all'accumulo di ingenti quantità di dati, tra i quali possono essere ricompresi dati di natura personale (nell'accezione fornita dall'art. 4 del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE, di seguito anche "RGPD"), in ipotesi provenienti anche da fonti diverse. La natura massiva delle operazioni di trattamento reca con sè la necessità che tali insiemi di informazioni (sia memorizzate, sia in streaming) siano oggetto trattamento automatizzato, mediante algoritmi e altre tecniche avanzate, al fine di individuare correlazioni di natura (per lo più) probabilistica, tendenze e/o modelli. Operativamente, nel settore dell'ICT, per Big Data si intende una collezione di dati che non può essere acquisita, gestita ed elaborata da strumenti informatici, da software e da hardware "tradizionali" in un tempo tollerabile, benché non esista una soglia dimensionale predefinita affinché un insieme di dati possa essere ricondotto alla categoria dei Big Data. In chiave descrittiva è frequente rinvenire nella letteratura in materia, fortemente influenzata dall'esperienza nord-americana, il richiamo, in forma ellittica, ad alcune caratteristiche ricorrenti rispetto al fenomeno in esame. Esse sono sintetizzate nelle 4 "V": il volume, con riferimento all'enorme dimensione dei dati generati e raccolti; la varietà, con riguardo alle numerose tipologie dei dati disponibili, tra i quali, oltre ai dati strutturati tradizionali, vi sono anche dati semi-strutturati e non strutturati come audio, video, pagine web e testi; la velocità delle operazioni di trattamento; il valore che i dati assumono allorquando vengono elaborati ed analizzati, così da consentire l'estrazione di informazioni che possono contribuire all'efficienza e alla qualità di processi produttivi "tradizionali" ovvero qualificare intrinsecamente l'offerta di beni e/o servizi, in particolare in termini di innovazione e di personalizzazione. *Cfr. amplius* Beyer M.A. e Laney D., *"The importance of Big data: a Definition"*, Gartner Analysis Report, 2012; Gantz J., Reinsel D., "*Extracting value from chaos*" IDC Report, 2011; Min Chen, Shiwen Mao, Yunhao Liu, "*Big data: A survey" Mobile networks and applications*, 19.2: 171-209, 2014; OECD - Organization for Economic Co-operation and Development, *"Big data: Bringing competition policy to the digital era*", 2016; Delmastro M, Nicita A., *Big data. Come stanno cambiando il nostro mondo*, il Mulino, Bologna 2019.

112 In Italia vengono ricondotti alla nozione di cui all'art. 810 del Codice Civile secondo cui "*sono beni le cose che possono formare oggetto di diritti*".

La presenza di nuove tecnologie come l'intelligenza artificiale ("IA") e l'apprendimento automatico contribuisce a creare nuove possibilità per la trasformazione di *Big data* in informazioni preziose, se ed in quanto teleologicamente elaborate al fine di creare vantaggi competitivi.

La *data driven economy* e il dissolversi di chiari confini territoriali induce l'interprete a sfruttare la natura *cross-sectoral e cross-economics* del fenomeno come spinta per ricalibrare il ruolo svolto dalla regolamentazione, domandandosi se sia necessario prevedere ulteriori aree disciplinari in grado di interconnettere i vari *silos* o semplicemente modificare quelle già esistenti.

Prima nella disciplina della tutela dei consumatori ed ora nella protezione dei dati personali, si è individuato il *fil rouge* in grado di connettere i vari settori, tutti interessati dal profilo di tutela dei clienti/consumatori/investitori e dei relativi dati.

Tale *fil rouge* consiste nel diritto alla c.d. portabilità dei dati da parte del titolare; diritto che si manifesta in un duplice modo: a) come diritto dell'interessato a dal titolare del trattamento di tali dati una sorta di *dataset* contenente tali dati, ossia a "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" (art. 20, par. 1, GDPR); b) come diritto dell'interessato a trasmettere i propri dati personali tra più titolari del trattamento, senza che questi possano (in linea generale) opporgli impedimenti (sempre art. 20, par. 1, GDPR)[113].

Se queste sono le premesse, occorrerà indagare ora il quadro normativo di riferimento all'interno del quale avvengono e si compiono i processi di raccolta, utilizzo e trasferimento dei dati, al fine di verificare se la disciplina esistente sia in grado di assicurare la tutela dei singoli e la stabilità del sistema finanziario nel suo complesso.

La massiccia presenza dei dati, quali nuovi beni giuridici suscettibili di valutazione economica, ha, infatti, spostato il baricentro di interesse – sia del legislatore europeo sia dei legislatori nazionali – verso la tutela dei dati il cui impiego e la cui diffusione ha creato, di fatto, un nuovo mercato e con esso nuovi diritti che richiedono specifiche tutele.

La fornitura stessa di servizi finanziari tecnologicamente abilitati è altresì fortemente dipendente dai dati. Il mondo finanziario e bancario *utilizzano*, infatti, le informazioni quali parte dei propri processi decisionali quotidiani (dalla concessione di prestiti, alla gestione dei portafogli di investimento, ecc.). Il settore finanziario, inoltre, *genera* grandi quantità di dati, che vengono accumulati sia all'interno delle istituzioni finanziarie sia al loro esterno (ad esempio dai *social media*).

A tal fine e per quanto specificamente concerne il tema della *portabilità dei dati in ambito finanziario*, le considerazioni in merito alla raccolta dei dati dei clienti da parte di un intermediario in occasione della prestazione di un servizio di investimento e della loro eventuale utilizzabilità da parte dello stesso intermediario o di terzi

113 Sul tema si veda R. Cavallo Perin e D.U. Galletta (a cura di), *Il diritto dell'amministrazione pubblica digitale*, Torino, 2020, p. 77 e ss.

per finalità ulteriori rispetto a quelli in relazione ai quali è nata originariamente l'esigenza di raccogliere il consenso non possono prescindere da una ricognizione degli obblighi previsti dalla normativa in tema di protezione dei dati personali.

In particolare con riguardo alla disciplina della c.d. "*product governance*" prevista dalla Direttiva 2014/65/EU (c.d. "MiFID 2"), all'interprete si pongono i seguenti interrogativi: (*i*) può l'intermediario utilizzare i dati raccolti dai clienti nella prestazione dei servizi di investimento per meglio assolvere gli obblighi previsti in tema di *product governance*?; (*ii*) in caso affermativo, questi dati devono essere utilizzati in modo aggregato (e quindi anonimo) o è possibile per l'intermediario utilizzare i dati identificativi dei singoli clienti?; infine, (*iii*) è possibile per l'intermediario trasferire i dati a terzi?

Per rispondere a queste domande occorre in via preliminare ricordare che sia la Carta dei diritti fondamentali dell'Unione Europea sia il Trattato sul Funzionamento dell'Unione europea prevedono che ogni individuo abbia diritto alla protezione dei propri dati personali.

Il Regolamento generale sulla protezione dei dati personali n. 2016/679[114] (noto come "*GDPR*" - "*General Data Protection Regulation*") costituisce la *sedes materiae* della normativa europea in materia di protezione dei dati personali. Con la sua entrata in vigore, il GDPR ha sostituito la direttiva sulla protezione dei dati (95/46/CE) e, con riferimento al nostro ordinamento, ha abrogato gli articoli del codice per la protezione dei dati personali (d.lgs. n. 196/2003) con esso incompatibili.

Si tratta di un quadro normativo ambizioso che armonizza le regole sulla protezione dei dati nell'UE e che da un lato pone gli individui in una nuova posizione di controllo sui loro dati, in particolare rafforzando i loro diritti, dall'altro determina una serie di sfide per l'industria.

Secondo il GDPR i dati personali possono essere trattati solo in conformità a determinati principi generali (ad es. trasparenza, limitazione delle finalità e minimizzazione dei dati) e sulla base di un motivo legittimo, nel rispetto di determinati diritti dell'interessato, come il diritto all'informazione o il diritto all'oblio.

A seconda dell'origine dei dati personali, si può distinguere tra *dati dichiarati* (dati forniti attivamente e consapevolmente dal cliente), *dati osservati* (creati attraverso l'osservazione dell'attività del cliente, i.e. *web cookies*) e *dati desunti*, creati dal titolare del trattamento sulla base dei dati forniti dall'interessato (es. convalida, analisi, profilazione, ecc).

114 Approvato con Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016, pubblicato nella Gazzetta Ufficiale europea il 4 maggio 2016 ed entrato in vigore il 24 maggio 2016, è applicabile dal 25 maggio 2018.

Rimandando alle note per le importanti definizioni di "*Dato personale*"[115], "*Trattamento*"[116], "*Profilazione*"[117], "*Titolare del Trattamento*"[118] e "*Consenso dell'interessato*"[119] (di cui all'Articolo 4 del GDPR) ed alla nozione di "*Liceità del consenso*"[120] (di cui all'art 7 del GDPR), ciò che qui maggiormente interessa è il tema della "*liceità del trattamento*" dei dati, disciplinata dall'art. 6 del GDPR secondo cui il trattamento dei dati (per tale intendendosi anche la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, dei dati) deve considerarsi "lecito" soltanto in presenza di: 1) un consenso volontario dell'interessato che autorizza il trattamento dei dati; 2) un consenso necessitato dall'esecuzione di un contratto di cui l'interessato è parte o dall'esecuzione di misure precontrattuali adottate su richiesta dello stesso[121]; 3) obblighi a cui è sottoposto il soggetto titolare del trattamento derivanti da legge, regolamento o normativa comunitaria; 4) interessi vitali della persona interessata o di terzi; 5) un legittimo interesse prevalente del titolare o di terzi cui i dati vengono comunicati; 6) un interesse pubblico o un esercizio di pubblici poteri.

115 E' *"Dato personale": "qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale"* (enfasi aggiunta).

116 Per "*Trattamento*" si intende: "*qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione"* (enfasi aggiunta).

117 La "*Profilazione*" è: "*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 fisi*ca" (enfasi aggiunta).

118 Ai sensi dell'art. 4 del GDPR, con tale espressione si intende: "*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri".*

119 Per "*Consenso dell'interessato*" si intende: "*qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento*" (enfasi aggiunta).

120 L'Art. 7 prevede che: "*1. Qualora il trattamento sia basato sul consenso, il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali. 2. Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Nessuna parte di una tale dichiarazione che costituisca una violazione del presente regolamento è vincolante. 3. L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca. Prima di prestare il proprio consenso, l'interessato è informato di ciò. Il consenso è revocato con la stessa facilità con cui è accordato. 4. Nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto"* (enfasi aggiunta).

121 Si può ritenere tale base giuridica una sotto categoria del primo caso, essendo un consenso "necessario" e derivante dal rapporto contrattuale o pre-contrattuale con il "*Titolare del Trattamento*".

Nei primi due casi colui che intende 'trattare' i dati personali altrui, nel raccogliere il consenso dovrà fornire al loro titolare l'informativa specifica ai sensi degli art. 13[122] e 14[123] del GDPR e garantirne altresì la portabilità[124] (art. 20 GDPR).

122 Art. 13 GDPR: "*Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato": 1. In caso di raccolta presso l'interessato di dati che lo riguardano, il titolare del trattamento fornisce all'interessato, nel momento in cui i dati personali sono ottenuti, le seguenti informazioni: a) l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante; b) i dati di contatto del responsabile della protezione dei dati, ove applicabile; c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento; d) qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f), i legittimi interessi perseguiti dal titolare del trattamento o da terzi; e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali; f) ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'articolo 46 o 47, o all'articolo 49, paragrafo 1, secondo comma, il riferimento alle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali garanzie o il luogo dove sono state rese disponibili. 2. In aggiunta alle informazioni di cui al paragrafo 1, nel momento in cui i dati personali sono ottenuti, il titolare del trattamento fornisce all'interessato le seguenti ulteriori informazioni necessarie per garantire un trattamento corretto e trasparente: a) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo; b) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati; c) qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a), l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca; d) il diritto di proporre reclamo a un'autorità di controllo; e) se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati; f) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato. 3. Qualora il titolare del trattamento intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità e ogni ulteriore informazione pertinente di cui al paragrafo 2"* (enfasi aggiunta).

123 Articolo 14 "*Informazioni da fornire qualora i dati personali non siano stati ottenuti presso l'interessato": "1. Qualora i dati non siano stati ottenuti presso l'interessato, il titolare del trattamento fornisce all'interessato le seguenti informazioni: a) l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante; b) i dati di contatto del responsabile della protezione dei dati, ove applicabile; c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento; d) le categorie di dati personali in questione; e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali; f) ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un destinatario in un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'articolo 46 o 47, o all'articolo 49, paragrafo 1, secondo comma, il riferimento alle garanzie adeguate o opportune e i mezzi per ottenere una copia di tali garanzie o il luogo dove sono state rese disponibili. 2. Oltre alle informazioni di cui al paragrafo 1, il titolare del trattamento fornisce all'interessato le seguenti informazioni necessarie per garantire un trattamento corretto e trasparente nei confronti dell'interessato: a) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo; b) qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f), i legittimi interessi perseguiti dal titolare del trattamento o da terzi; c) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento dei dati personali che lo riguardano e di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati; d) qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a), l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prima della revoca; e) il diritto di proporre reclamo a un'autorità di controllo; f) la fonte da cui hanno origine i dati personali e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico; g) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato. 3. Il titolare del trattamento fornisce le informazioni di cui ai paragrafi 1 e 2: a) entro un termine ragionevole dall'ottenimento dei dati personali, ma al più tardi entro un mese, in considerazione delle specifiche circostanze in cui i dati personali sono trattati; b) nel caso in cui i dati personali siano destinati alla comunicazione con l'interessato, al più tardi al momento della prima comunicazione all'interessato; oppure c) nel caso sia prevista la comunicazione ad altro destinatario, non oltre la prima comunicazione dei dati personali. 4. Qualora il titolare del trattamento intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati ottenuti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità e ogni informazione pertinente di cui*

Negli altri casi, invece, non occorrerà il consenso del titolare dei dati e non si dovrà, quindi, garantire la portabilità dei dati stessi ma, in ogni caso, sarà necessario fornire allo stesso titolare l'informativa ai sensi degli art. 13 e 14 del GDPR, indicando il fondamento giuridico su cui si basa il trattamento.

Occorre inoltre considerare che, per quanto riguarda il problema della utilizzabilità dei dati raccolti "*per diverse finalità*", il consenso richiesto al titolare dei dati per aversi un trattamento lecito non potrà essere generico, ma specifico, ossia dovrà essere prestato in relazione ad ogni specifica finalità[125], di modo che, qualora il trattamento persegua una pluralità di finalità, il consenso dovrà essere prestato per ciascuna di esse[126]. A sua volta il Considerando 50 del GDPR chiarisce altresì che il trattamento dei dati personali per "finalità diverse" da quelle per le quali i dati personali sono stati originariamente raccolti "*dovrebbe essere consentito solo se compatibile con le finalità per le quali i dati personali sono stati inizialmente raccolti. In tal caso non è richiesta alcuna base giuridica separata oltre a quella che ha consentito la raccolta dei dati personali*". Ciò significa che ogniqualvolta il titolare del trattamento di dati altrui

al paragrafo 2. 5. I paragrafi da 1 a 4 non si applicano se e nella misura in cui: a) l'interessato dispone già delle informazioni; b) comunicare tali informazioni risulta impossibile o implicherebbe uno sforzo sproporzionato; in particolare per il trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, fatte salve le condizioni e le garanzie di cui all'articolo 89, paragrafo 1, o nella misura in cui l'obbligo di cui al paragrafo 1 del presente articolo rischi di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità di tale trattamento. In tali casi, il titolare del trattamento adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, anche rendendo pubbliche le informazioni; c) l'ottenimento o la comunicazione sono espressamente previsti dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento e che prevede misure appropriate per tutelare gli interessi legittimi dell'interessato; oppure d) qualora i dati personali debbano rimanere riservati conformemente a un obbligo di segreto professionale disciplinato dal diritto dell'Unione o degli Stati membri, compreso un obbligo di segretezza previsto per legge" (enfasi aggiunta).

124 Art. 20 "*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. 3. L'esercizio del diritto di cui al paragrafo 1 del presente articolo lascia impregiudicato l'articolo 17. Tale diritto non si applica al trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento. 4. Il diritto di cui al paragrafo 1 non deve ledere i diritti e le libertà altrui.*

125 Al riguardo, si riporta il considerando 32 del GDPR: *"Il consenso dovrebbe essere prestato mediante un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano, ad esempio mediante dichiarazione scritta, anche attraverso mezzi elettronici, o orale. Ciò potrebbe comprendere la selezione di un'apposita casella in un sito web, la scelta di impostazioni tecniche per servizi della società dell'informazione o qualsiasi altra dichiarazione o qualsiasi altro comportamento che indichi chiaramente in tale contesto che l'interessato accetta il trattamento proposto. Non dovrebbe pertanto configurare consenso il silenzio, l'inattività o la preselezione di caselle. Il consenso dovrebbe applicarsi a tutte le attività di trattamento svolte per la stessa o le stesse finalità. Qualora il trattamento abbia più finalità, il consenso dovrebbe essere prestato per tutte queste. Se il consenso dell'interessato è richiesto attraverso mezzi elettronici, la richiesta deve essere chiara, concisa e non interferire immotivatamente con il servizio per il quale il consenso è espresso"* (enfasi aggiunta).

126 Specifica disciplina è prevista per i c.d. dati "sensibili". L'Art. 9, rubricato "*Trattamento di categorie particolari di dati personali*" stabilisce al primo paragrafo che: "*È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona*". Il secondo paragrafo, prevede una serie di eccezioni, fra cui, per quanto qui interessa il consenso dell'interessato *("l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1*").

volesse utilizzare i dati per finalità diverse da quelle originariamente previste ed autorizzate, dovrà necessariamente verificare la *compatibilità* del nuovo trattamento rispetto alle finalità per la quale i dati personali sono stati inizialmente raccolti (*cfr.* art. 6, c. 4)[127].

Prima di tale ulteriore trattamento, il titolare è comunque chiamato dalla legge a fornire all'interessato le informazioni in merito a tale diversa finalità e ogni ulteriore informazione a ciò pertinente (artt. 13, comma 3, e 14, comma 4)[128].

2.5 L'attuale *framework* normativo in relazione alla prestazione di servizi ed attività di investimento

Passati brevemente in rassegna i presidi e i limiti previsti dal GDPR ai fini della "liceità del trattamento", dell'utilizzo dei dati "per diverse finalità" e della eventuale "trasmissione dei dati a terzi", è possibile ora esaminare - tra i tanti momenti di interazione tra le norme del GDPR e quelle esistenti in materia finanziaria - le interazioni esistenti tra le norme sopra citate del GDPR e gli obblighi previsti dal Testo Unico della Finanza ("TUF") e dalla MiFID 2 in materia di raccolta di informazioni e dati dei clienti da parte degli intermediari nello svolgimento dei servizi di investimento.

A tal riguardo, bisogna sin da subito rilevare che né il TUF né la MiFID 2 contengono specifiche previsioni in merito alla tutela della *privacy* dei dati dei clienti. Pertanto, al fine di risolvere i quesiti posti in precedenza [*i.e.:* (*i*) può l'intermediario utilizzare i dati raccolti dai clienti nella prestazione dei servizi di investimento per meglio assolvere gli obblighi previsti in tema di *product governance*?; (*ii*) in caso affermativo, questi dati devono essere utilizzati in modo aggregato (e quindi anonimo) o è possibile per l'intermediario utilizzare i dati identificativi dei singoli clienti?; (*iii*) è possibile per l'intermediario trasferire i dati a terzi?] occorrerà di volta in volta porre in relazione tali norme con quanto previsto delle dall'art. 6 del GDPR (*i.e.* delle n. 6 ipotesi

127 Art. 6, c 4: *"Laddove il trattamento per una finalità diversa da quella per la quale i dati personali sono stati raccolti non sia basato sul consenso dell'interessato o su un atto legislativo dell'Unione o degli Stati membri che costituisca una misura necessaria e proporzionata in una società democratica per la salvaguardia degli obiettivi di cui all'articolo 23, paragrafo 1, al fine di verificare se il trattamento per un'altra finalità sia compatibile con la finalità per la quale i dati personali sono stati inizialmente raccolti, il titolare del trattamento tiene conto, tra l'altro: a) di ogni nesso tra le finalità per cui i dati personali sono stati raccolti e le finalità dell'ulteriore trattamento previsto; b) del contesto in cui i dati personali sono stati raccolti, in particolare relativamente alla relazione tra l'interessato e il titolare del trattamento; c) della natura dei dati personali, specialmente se siano trattate categorie particolari di dati personali ai sensi dell'articolo 9, oppure se siano trattati dati relativi a condanne penali e a reati ai sensi dell'articolo 10; d) delle possibili conseguenze dell'ulteriore trattamento previsto per gli interessati; e) dell'esistenza di garanzie adeguate, che possono comprendere la cifratura o la pseudonimizzazione"*(enfasi aggiunta).

128 Al riguardo il Considerando 60 stabilisce che "*L'interessato dovrebbe ricevere le informazioni relative al trattamento di dati personali che lo riguardano al momento della raccolta presso l'interessato o, se i dati sono ottenuti da altra fonte, entro un termine ragionevole, in funzione delle circostanze del caso. Se i dati personali possono essere legittimamente comunicati a un altro destinatario, l'interessato dovrebbe esserne informato nel momento in cui il destinatario riceve la prima comunicazione dei dati personali. Il titolare del trattamento, qualora intenda trattare i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, dovrebbe fornire all'interessato, prima di tale ulteriore trattamento, informazioni in merito a tale finalità diversa e altre informazioni necessarie. Qualora non sia possibile comunicare all'interessato l'origine dei dati personali, perché sono state utilizzate varie fonti, dovrebbe essere fornita un'informazione di carattere generale"* (enfasi aggiunta).

di legittimo trattamento sopra elencate) per inferire la "liceità" o la "illiceità" del trattamento dei dati dei clienti.

Nessun dubbio sorge sulla liceità del trattamento dei dati raccolti dagli intermediari nella fase precontrattuale o contrattuale finalizzata alla prestazione di un servizio di investimento. Come noto, l'art. 21 del TUF nel dettare i criteri generali cui devono attenersi i soggetti abilitati nella prestazione dei servizi e delle attività di investimento e accessori, (i.e. "*diligenza, correttezza e trasparenza*"), prevede espressamente in capo a questi ultimi l'obbligo di "*acquisire le informazioni necessarie dai clienti e operare in modo che essi siano sempre adeguatamente informati*". Gli obblighi che il Legislatore ha posto in capo all'intermediario sono strumentali e finalizzati - nella logica delle c.d. "*Know your customer rule*" e "*Know your product rule*" - a servire al meglio l'interesse dei clienti e preservare l'integrità dei mercati.

In tali casi, l'intermediario in sede di primo contatto con i clienti presenterà agli stessi il questionario "*privacy*" dove fornirà le informative previste dal GDPR, indicherà loro le finalità del "trattamento" e ne raccoglierà il consenso ("necessitato") al fine di poter porre in essere i servizi di investimento.

Queste ipotesi integrano l'ipotesi di cui al n. 2 dell'art. 6 della GDPR sopra richiamato, ovvero l'ipotesi del consenso necessario per dare esecuzione ad un contratto di cui l'interessato è parte o per dare esecuzione a misure precontrattuali adottate su richiesta dello stesso.

Sempre in relazione alla raccolta di informazioni e di dati dei clienti lo stesso art. 21 del TUF, però, prevede due ulteriori obblighi in capo ai soggetti abilitati nella fase relativa al processo di creazione e strutturazione degli strumenti finanziari (si allude al momento della c.d. "*Product Governance*").

In particolare, il comma 2-*bis* dell'art. 21 del TUF prevede che quando i soggetti abilitati "*realizzano strumenti finanziari per la vendita alla clientela (...) fanno sì che tali prodotti siano concepiti per soddisfare le esigenze di un determinato mercato di riferimento di clienti finali individuato all'interno della pertinente categoria di clienti e che la strategia di distribuzione degli strumenti finanziari sia compatibile con i clienti target...* (e) *adottano inoltre misure ragionevoli per assicurare che lo strumento finanziario sia distribuito ai clienti all'interno del mercato target*". In relazione a tale attività il successivo comma 2-*ter* pone a capo del soggetto abilitato l'obbligo di "*conoscere gli strumenti finanziari offerti o raccomandati, valutarne la compatibilità con le esigenze della clientela cui fornisce servizi di investimento tenendo conto del mercato di riferimento di clienti finali di cui al comma 2*-bis, *e fare in modo che gli strumenti finanziari siano offerti o raccomandati solo quando ciò sia nell'interesse del cliente*".

Dalle citate disposizioni, introdotte con il fine di evitare il c.d. "*misseling*" di uno strumento finanziario e nell'ottica di offrire una migliore protezione al cliente, nonché dall'intero impianto normativo MiFID 2, si desume agevolmente che la raccolta delle informazioni e dei dati relativi ai clienti risulta necessaria in diversi momenti del rapporto intercorrente tra intermediario e cliente.

Essa è necessitata, infatti, sia per poter prestare i servizi di investimento (verificando l'adeguatezza e/o l'appropriatezza dello strumento finanziario consigliato o offerto)[129], sia per assolvere al meglio gli obblighi in tema di "*Product Governance*", tanto nel caso in cui il soggetto abilitato sia il produttore (c.d. "*manufacturer*") quanto nel caso in cui esso sia mero distributore (c.d. "*distributor*") dello strumento finanziario. [Per meglio comprendere la portata di tali obblighi si richiamano in nota le disposizioni previste al paragrafo 3 dall'art. 16, della MiFID II[130] (rubricato "*Requisiti organizzativi*"), e dall'art. 10 della direttiva delegata MiFID II 2017/593 (rubricato "*Obblighi di governance dei prodotti per i distributori*")[131]]

In particolare, il comma 2-*bis* dell'art. 21 del TUF prevede che quando i soggetti abilitati "*realizzano strumenti finanziari per la vendita alla clientela (...) fanno sì che tali prodotti siano concepiti per soddisfare le esigenze di un determinato mercato di riferimento di clienti finali individuato all'interno della pertinente categoria di clienti e che la strategia di distribuzione degli strumenti finanziari sia compatibile con i clienti*

129 Come noto, i soggetti abilitati non raccomandano i servizi di investimento o gli strumenti finanziari al cliente o potenziale cliente quando, nel prestare un servizio di consulenza in materia di investimenti o gestione del portafoglio, non ottengono le informazioni di cui all'articolo 25, paragrafo 2, della direttiva 2014/65/UE ("*qualora l'intermediario presti i servizi di consulenza in materia di investimenti o gestione del portafoglio e non ottenga le informazioni dal cliente, deve astenersi dall'effettuare il servizio richiesto*".

130 L'art. 16 par. 3. della MiFID 2 stabilisce che: *"Le imprese di investimento mantengono e applicano disposizioni organizzative e amministrative efficaci al fine di adottare tutte le misure ragionevoli volte ad evitare che i conflitti di interesse, quali definiti all'articolo 23, incidano negativamente sugli interessi dei loro clienti. Le imprese di investimento che realizzano strumenti finanziari da offrire in vendita alla clientela adottano, esercitano e controllano un processo di approvazione per ogni strumento finanziario e per ogni modifica significativa agli strumenti finanziari esistenti, prima della loro commercializzazione o distribuzione alla clientela. Il processo di approvazione del prodotto precisa per ciascuno strumento finanziario il determinato mercato di riferimento di clienti finali all'interno della pertinente categoria di clienti e garantisce che tutti i rischi specificamente attinenti a tale target siano stati analizzati e che la prevista strategia di distribuzione sia coerente con il target stesso. L'impresa di investimento riesamina inoltre regolarmente gli strumenti finanziari da essa offerti o commercializzati, tenendo conto di qualsiasi evento che possa incidere significativamente sui rischi potenziali per il mercato target, onde almeno valutare se lo strumento finanziario resti coerente con le esigenze del target e se la prevista strategia distributiva continui ad essere quella appropriata. Le imprese di investimento emittenti mettono a disposizione dei distributori tutte le necessarie informazioni sullo strumento finanziario e sul suo processo di approvazione, compreso il suo mercato target. Le imprese di investimento che offrono o raccomandano strumenti finanziari non realizzati in proprio, adottano opportune disposizioni per ottenere le informazioni menzionate al quinto comma e per comprendere le caratteristiche e il mercato target identificato* di *ciascuno strumento finanziario. Le politiche, i processi e le disposizioni menzionate nel presente paragrafo lasciano impregiudicati tutti gli altri obblighi della presente direttiva e del regolamento (UE) n. 600/2014 compresi quelli relativi a informativa, adeguatezza e appropriatezza, identificazione e gestione di conflitti di interesse e indebiti incentivi".*

131 Si riportano qui i paragrafi più pertinenti dell'Art. 10: "(...) 5. *Gli Stati membri prescrivono che le imprese di investimento riesaminino regolarmente i prodotti di investimento da esse offerti o raccomandati e i servizi prestati, tenendo conto di qualsiasi evento che possa incidere materialmente sui rischi potenziali per il mercato di riferimento determinato. Le imprese valutano almeno se il prodotto o il servizio resti coerente con le esigenze, le caratteristiche e gli obiettivi del mercato di riferimento e se la prevista strategia di distribuzione continui ad essere appropriata. Le imprese riconsiderano il mercato di riferimento e/o aggiornano i dispositivi di* governance *dei prodotti qualora rilevino di avere erroneamente identificato il mercato di riferimento per un prodotto o servizio specifico o qualora il prodotto o il servizio non soddisfi più le condizioni del mercato di riferimento determinato, ad esempio quando il prodotto non è più liquido o diviene molto volatile a causa delle oscillazioni del mercato. (...) 9. Gli Stati membri assicurano che i distributori forniscano ai produttori le informazioni sulle vendite e, se del caso, le informazioni sui riesami di cui sopra per corroborare i riesami dei prodotti svolti dai produttori. 10. Quando diverse imprese collaborano nella distribuzione di un prodotto o servizio, gli Stati membri assicurano che l'impresa di investimento avente il rapporto diretto con il cliente sia investita della responsabilità finale di adempiere agli obblighi di governance dei prodotti definiti dal presente articolo. Tuttavia, le imprese di investimento intermediarie devono: a) assicurare che le informazioni pertinenti sui prodotti passino dal produttore al distributore finale della catena; b) qualora il produttore richieda informazioni sulle vendite del prodotto al fine di adempiere ai propri obblighi di governance dei prodotti, consentirgli l'accesso; e c) applicare gli obblighi di governance dei prodotti ai produttori, se del caso, in relazione al servizio da esse fornito".*

target... (e) *adottano inoltre misure ragionevoli per assicurare che lo strumento finanziario sia distribuito ai clienti all'interno del mercato target*". In relazione a tale attività il successivo comma 2-*ter* pone a capo del soggetto abilitato l'obbligo di "*conoscere gli strumenti finanziari offerti o raccomandati, valutarne la compatibilità con le esigenze della clientela cui fornisce servizi di investimento tenendo conto del mercato di riferimento di clienti finali di cui al comma 2*-bis, *e fare in modo che gli strumenti finanziari siano offerti o raccomandati solo quando ciò sia nell'interesse del cliente*".

Dalle citate disposizioni, introdotte con il fine di evitare il c.d. "*misseling*" di uno strumento finanziario e nell'ottica di offrire una migliore protezione al cliente, nonché dall'intero impianto normativo MiFID 2, si desume agevolmente che la raccolta delle informazioni e dei dati relativi ai clienti risulta necessaria in diversi momenti del rapporto intercorrente tra intermediario e cliente.

Essa è necessitata, infatti, sia per poter prestare i servizi di investimento (verificando l'adeguatezza e/o l'appropriatezza dello strumento finanziario consigliato o offerto)[132], sia per assolvere al meglio gli obblighi in tema di "*Product Governance*", tanto nel caso in cui il soggetto abilitato sia il produttore (c.d. "*manufacturer*") quanto nel caso in cui esso sia mero distributore (c.d. "*distributor*") dello strumento finanziario. [Per meglio comprendere la portata di tali obblighi si richiamano in nota le disposizioni previste al paragrafo 3 dall'art. 16, della MiFID II[133] (rubricato "*Requisiti organizzativi*"), e dall'art. 10 della direttiva delegata MiFID II 2017/593 (rubricato "*Obblighi di governance dei prodotti per i distributori*")[134].]

132 Come noto, i soggetti abilitati non raccomandano i servizi di investimento o gli strumenti finanziari al cliente o potenziale cliente quando, nel prestare un servizio di consulenza in materia di investimenti o gestione del portafoglio, non ottengono le informazioni di cui all'articolo 25, paragrafo 2, della direttiva 2014/65/UE ("*qualora l'intermediario presti i servizi di consulenza in materia di investimenti o gestione del portafoglio e non ottenga le informazioni dal cliente, deve astenersi dall'effettuare il servizio richiesto*".

133 L'art. 16 par. 3. della MiFID 2 stabilisce che: "*Le imprese di investimento mantengono e applicano disposizioni organizzative e amministrative efficaci al fine di adottare tutte le misure ragionevoli volte ad evitare che i conflitti di interesse, quali definiti all'articolo 23, incidano negativamente sugli interessi dei loro clienti. Le imprese di investimento che realizzano strumenti finanziari da offrire in vendita alla clientela adottano, esercitano e controllano un processo di approvazione per ogni strumento finanziario e per ogni modifica significativa agli strumenti finanziari esistenti, prima della loro commercializzazione o distribuzione alla clientela. Il processo di approvazione del prodotto precisa per ciascuno strumento finanziario il determinato mercato di riferimento di clienti finali all'interno della pertinente categoria di clienti e garantisce che tutti i rischi specificamente attinenti a tale target siano stati analizzati e che la prevista strategia di distribuzione sia coerente con il target stesso. L'impresa di investimento riesamina inoltre regolarmente gli strumenti finanziari da essa offerti o commercializzati, tenendo conto di qualsiasi evento che possa incidere significativamente sui rischi potenziali per il mercato target, onde almeno valutare se lo strumento finanziario resti coerente con le esigenze del target e se la prevista strategia distributiva continui ad essere quella appropriata. Le imprese di investimento emittenti mettono a disposizione dei distributori tutte le necessarie informazioni sullo strumento finanziario e sul suo processo di approvazione, compreso il suo mercato target. Le imprese di investimento che offrono o raccomandano strumenti finanziari non realizzati in proprio, adottano opportune disposizioni per ottenere le informazioni menzionate al quinto comma e per comprendere le caratteristiche e il mercato target identificato di ciascuno strumento finanziario. Le politiche, i processi e le disposizioni menzionate nel presente paragrafo lasciano impregiudicati tutti gli altri obblighi della presente direttiva e del regolamento (UE) n. 600/2014 compresi quelli relativi a informativa, adeguatezza e appropriatezza, identificazione e gestione di conflitti di interesse e indebiti incentivi*".

134 Si riportano qui i paragrafi più pertinenti dell'Art. 10: *"(...) 5. Gli Stati membri prescrivono che le imprese di investimento riesaminino regolarmente i prodotti di investimento da esse offerti o raccomandati e i servizi prestati, tenendo conto di qualsiasi evento che possa incidere materialmente sui rischi potenziali per il mercato di riferimento determinato. Le imprese valutano almeno se il prodotto o il servizio resti coerente con le esigenze, le caratteristiche e gli obiettivi del mercato di riferimento e se la prevista strategia di distribuzione continui ad essere appropriata. Le imprese riconside-*

Inoltre, con riguardo alla declinazione dei suddetti obblighi di "*Product Governance*" ai sensi della MiFID II è altresì opportuno qui richiamare gli Orientamenti ESMA del 5 febbraio 2018 (Documento ESMA 35-43-620). In particolare, si fa riferimento alle indicazioni in tema di "*Riesame periodico da parte del produttore e del distributore volto alla rispettiva valutazione qualora i prodotti e i servizi raggiungano il mercato di riferimento*" previsti nei paragrafi 56[135], 57[136], 58[137], 59[138] e a quelle in tema di *"Identificazione del mercato di riferimento «negativo» e vendite al di fuori del*

rano il mercato di riferimento e/o aggiornano i dispositivi di governance *dei prodotti qualora rilevino di avere erroneamente identificato il mercato di riferimento per un prodotto o servizio specifico o qualora il prodotto o il servizio non soddisfi più le condizioni del mercato di riferimento determinato, ad esempio quando il prodotto non è più liquido o diviene molto volatile a causa delle oscillazioni del mercato. (...) 9. Gli Stati membri assicurano che i distributori forniscano ai produttori le informazioni sulle vendite e, se del caso, le informazioni sui riesami di cui sopra per corroborare i riesami dei prodotti svolti dai produttori. 10. Quando diverse imprese collaborano nella distribuzione di un prodotto o servizio, gli Stati membri assicurano che l'impresa di investimento avente il rapporto diretto con il cliente sia investita della responsabilità finale di adempiere agli obblighi di* governance *dei prodotti definiti dal presente articolo. Tuttavia, le imprese di investimento intermediarie devono: a) assicurare che le informazioni pertinenti sui prodotti passino dal produttore al distributore finale della catena; b) qualora il produttore richieda informazioni sulle vendite del prodotto al fine di adempiere ai propri obblighi di* governance *dei prodotti, consentirgli l'accesso; e c) applicare gli obblighi di* governance *dei prodotti ai produttori, se del caso, in relazione al servizio da esse fornito".*

135 Par. 56: "*In conformità dell'articolo 16, paragrafo 3, della MiFID II e degli articoli 9 e 10 della direttiva delegata MiFID II, è necessario che i produttori e i distributori riesaminino periodicamente i prodotti per verificare che il prodotto resti coerente con le esigenze, le caratteristiche e gli obiettivi del mercato di riferimento identificato e che la prevista strategia di distribuzione continui a essere appropriata".*

136 Par. 57: "*I produttori dovrebbero valutare, in modo proporzionato, le informazioni di cui necessitano per completare il riesame e come raccogliere tali informazioni. In linea con il considerando 20, della direttiva delegata MiFID II, le informazioni pertinenti potrebbero comprendere, ad esempio, le informazioni relative ai canali di distribuzione utilizzati, alla percentuale di vendite effettuata al di fuori del mercato di riferimento, alle informazioni sintetiche sui tipi di clienti, a una sintesi dei reclami pervenuti e ai quesiti suggeriti dal produttore a un campione di clienti per ottenere feedback. Tali informazioni possono essere in forma aggregata e non è necessario che siano fornite per ciascuno strumento o per ciascuna vendita".*

137 Par. 58. "*Per favorire i riesami da parte dei produttori contemplati dalla MiFID, i distributori devono fornire loro informazioni sulle vendite e, se del caso, qualsiasi informazione pertinente che possa essere ottenuta attraverso il riesame periodico del distributore. I distributori dovrebbero inoltre tenere in considerazione i dati e le informazioni da cui possono dedurre di aver erroneamente identificato il mercato di riferimento per un prodotto o servizio specifico o qualora il prodotto o il servizio non soddisfa più le condizioni del mercato di riferimento determinato, ad esempio quando il prodotto non è più liquido o diviene molto volatile a causa delle oscillazioni del mercato. Dette informazioni sono soggette al principio di proporzionalità, possono generalmente essere in forma aggregata e non è solitamente necessario che vengano fornite per ciascuno strumento o per ciascuna vendita. Le informazioni relative a strumenti specifici dovrebbero essere fornite nei casi di particolare importanza per determinati strumenti singoli (ad esempio, qualora il distributore giunga alla conclusione che un mercato di riferimento per un prodotto specifico sia stato erroneamente definito)"* (enfasi aggiunta).

138 Par. 59: *"In relazione alla comunicazione di informazioni sulle vendite al di fuori del mercato di riferimento del produttore, i distributori dovrebbero essere in grado di comunicare qualsiasi decisione adottata finalizzata alla vendita al di fuori del mercato di riferimento o ad ampliare la strategia di distribuzione raccomandata dal produttore nonché le informazioni sulle vendite al di fuori del mercato di riferimento (ivi comprese le vendite all'interno del mercato di riferimento negativo), tenendo in considerazione le eccezioni di cui al paragrafo 54".*

mercato di riferimento positivo" previste nei paragrafi 73[139] e 74[140] dei citati Orientamenti.

Dall'analisi delle disposizioni richiamate si evince che anche in materia di *product governance* la raccolta di informazioni del cliente da parte dell'intermediario distributore, nonché la trasmissione di tali dati ad un terzo soggetto (il c.d. "*manufacturer*") nei casi in cui lo strumento finanziario offerto o consigliato non sia stato "progettato in casa"[141], sono entrambe attività da considerarsi lecite se ed in quanto debitamente descritte al cliente al momento della richiesta di autorizzazione al trattamento dei dati.

Alla luce del descritto *framework* normativo ne deriva che al fine di considerare lecito il trattamento dei dati dei clienti raccolti dall'intermediario possono formularsi le seguenti considerazioni.

In primis, nessun dubbio può sorgere circa la liceità del trattamento dei dati qualora nella relazione con il proprio cliente l'intermediario ne raccolga il consenso (facendo sottoscrivere a questi il modulo della "*privacy*") anche in relazione ad un possibile successivo utilizzo al fine di assolvere gli obblighi in tema di *product governance*. Tale ipotesi rientra tra i casi di legittimo utilizzo dei dati indicati ai numeri 1 e 2 dell'art. 6 GDPR.

In secundis, laddove invece l'intermediario non avesse raccolto dal cliente uno specifico consenso al trattamento dei dati ai fini della *product governance*, si potrebbe comunque ritenere che la "liceità" di un tale trattamento potrebbe comunque discendere dal disposto di cui al n. 3 dell'art. 6 del GDPR, ritenendo che in materia si sia comunque in presenza di obblighi a cui è sottoposto l'intermediario titolare del trattamento e che derivano da "*legge, regolamento o normativa comunitaria*"[142]. Probabilmente, però, in questo secondo caso dovrebbe essere garantita al cliente il maggior 'anonimato' possibile, ossia trasferendo *sinteticamente* ed *in forma aggregata* solamente i dati (economici, di propensione al rischio, ecc.) strettamente necessari per progettare i nuovi prodotti finanziari.

A favore della utilizzabilità e trasferibilità dei dati a terzi in modo aggregato e quindi anonimo dei dati soccorrono le esplicite previsioni dei par. 56 e 57 degli Orientamenti ESMA sopra menzionati, laddove si prevede che le informazioni possono essere

139 Par. 73: "*È importante che, qualora il distributore venga a conoscenza, ad esempio mediante l'analisi dei reclami dei clienti o a partire da altri dati o fonti, del fatto che la vendita di un determinato prodotto al di fuori del mercato di riferimento identificato ex ante è divenuta un fenomeno significativo (ad esempio, in termini di quantità di clienti interessati), tale elemento sia tenuto debitamente in considerazione nel corso del riesame periodico da esso svolto sui prodotti e sui servizi correlati offerti. In tali casi, il distributore può, ad esempio, giungere alla conclusione che il mercato di riferimento identificato inizialmente non fosse corretto e che sia necessario riesaminarlo o che la strategia di distribuzione correlata non fosse adeguata per il prodotto e debba essere oggetto di una nuova valutazione*" (enfasi aggiunta).

140 Par. 74: "*Gli scostamenti rispetto al mercato di riferimento (al di fuori del positivo o all'interno del negativo) che possono essere significativi per il processo di governance del prodotto del produttore (segnatamente quelli ricorrenti) dovrebbero essere comunicati al produttore tenendo in considerazione le eccezioni di cui al paragrafo 54 (enfasi aggiunta).*

141 È questo il caso dello schema "produttore-distributore-cliente" dove le prime due funzioni sono svolte da due soggetti diversi.

142 Come sopra ricordato, qualsiasi sia la base giuridica su cui si fonda il Trattamento, deve essere comunicata al cliente ai sensi degli art. 13 e 14 del GDPR.

fornite al produttore ("terzo") in forma aggregata e senza invece la necessità che siano fornite per ciascuno strumento o per ciascuna vendita.

Del resto l'art. 23 del GDPR[143], prevede espressamente che il diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o il responsabile del trattamento possano limitare, mediante misure legislative, la portata degli obblighi e dei diritti previsti, qualora tale limitazione rispetti l'essenza dei diritti e delle libertà fondamentali e si qualifichi come una misura necessaria e proporzionata in una società democratica per salvaguardare una serie di interessi considerati primari e che devono essere preferiti alle ragioni dell'interessato.

Tra gli altri, uno degli interessi considerati primari dal par. 1 lett. *e)* dell'art. 23 del GDPR, ossia il "*rilevante interesse economico o finanziario dell'Unione o di uno Stato membro, anche in materia monetaria, di bilancio e tributaria, di sanità pubblica e sicurezza sociale*", sembrerebbe, infatti, potersi concretizzare ogniqualvolta le norme della MiFID 2 mirino a salvaguardare la stabilità e il corretto funzionamento dei mercati finanziari. Analoga considerazione può essere svolta con riferimento alla lett. *i)* del medesimo Par 1 ("*la tutela dell'interessato o dei diritti e delle libertà altrui*) con riferimento alla quasi totalità delle disposizioni della MiFID 2 che hanno come fine ontologico la protezione e la tutela del risparmiatore.

Le considerazioni sinora svolte ci consentono quindi di rispondere in senso affermativo alle domande sopra formulate. In particolare, con riferimento alla domanda circa l'"utilizzabilità dei dati ai fini degli obblighi di *Product Governance*", si può ritenere che non vi siano dubbi sulla possibilità di lecito utilizzo dei dati, laddove l'intermediario abbia raccolto un consenso specifico (e distinto) in relazione a tali finalità oppure laddove trasmetta tali dati in forma aggregata ed anonima per adempiere ad un obbligo giuridico sullo stesso incombente (e, tra l'altro, posto a tutela del cliente medesimo).

Qualora invece l'intermediario volesse utilizzare i dati a disposizione per finalità di mero *marketing* o per scopi diversi rispetto a quelli individuabili negli obblighi previsti dalla disciplina di settore, potrebbe evidentemente farlo lecitamente solo dopo aver ottenuto il consenso da parte del cliente secondo le modalità e i limiti descritti dal GDPR.

143 Art. 23 GDPR, 1 par.: *"Il diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o il responsabile del trattamento può limitare, mediante misure legislative, la portata degli obblighi e dei diritti di cui agli articoli da 12 a 22 e 34, nonché all'articolo 5, nella misura in cui le disposizioni ivi contenute corrispondano ai diritti e agli obblighi di cui agli articoli da 12 a 22, qualora tale limitazione rispetti l'essenza dei diritti e delle libertà fondamentali e sia una misura necessaria e proporzionata in una società democratica per salvaguardare: a) la sicurezza nazionale; b) la difesa; c) la sicurezza pubblica; d) la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica; e) altri importanti obiettivi di interesse pubblico generale dell'Unione o di uno Stato membro, in particolare un rilevante interesse economico o finanziario dell'Unione o di uno Stato membro, anche in materia monetaria, di bilancio e tributaria, di sanità pubblica e sicurezza sociale; f) la salvaguardia dell'indipendenza della magistratura e dei procedimenti giudiziari; g) le attività volte a prevenire, indagare, accertare e perseguire violazioni della deontologia delle professioni regolamentate; h) una funzione di controllo, d'ispezione o di regolamentazione connessa, anche occasionalmente, all'esercizio di pubblici poteri nei casi di cui alle lettere da a), a e) e g); i) la tutela dell'interessato o dei diritti e delle libertà altrui; j) l'esecuzione delle azioni civili".*

* * *

Un'altra attività nello svolgimento della quale l'intermediario si trova a dovere trattare dati dei propri clienti è quella concernente i servizi di pagamento[144].

Anche in questa materia, come in quella vista sopra sui servizi e attività di investimento, la disciplina di settore (*i.e.* la Direttiva europea sui servizi di pagamento nel mercato interno 2015/2366/UE - c.d. PSD2 - recepita il 13 gennaio 2018) deve essere coordinata con il GDPR.

La prestazione di servizi di pagamento ben può comportare, infatti, il trattamento di dati personali e di questo ne è ben consapevole il legislatore comunitario che al Considerando 90 della PSD2 ha tenuto a precisare che nell'applicazione della Direttiva occorre rispettare i diritti fondamentali e osservare *"i principi riconosciuti dalla Carta dei diritti fondamentali dell'Unione europea, incluso (...), il diritto alla protezione dei dati personali"*.

Il Considerando 89 della PSD2, inoltre, nel ribadire che le norme sul trattamento dei dati personali debbano trovare applicazione anche ai fini della Direttiva medesima, prevede che qualora vi sia trattamento di dati personali "*è opportuno che sia specificato lo scopo preciso, siano citate le basi giuridiche pertinenti, vi sia conformità con i requisiti di sicurezza pertinenti di cui alla direttiva 95/46/CE*[145] *e siano rispettati i principi di necessità, proporzionalità, limitazione delle finalità e proporzionalità del periodo di conservazione dei dati*".

Ai fini che qui interessano, la norma del GDPR che assume maggiore rilevanza è l'art. 94, rubricato "*Protezione dei dati*" che al primo paragrafo prevede espressamente che *"gli Stati membri autorizzano il trattamento dei dati personali da parte di sistemi di pagamento e di prestatori di servizi di pagamento se necessario per garantire la prevenzione, l'indagine e l'individuazione dei casi di frode nei pagamenti. La fornitura di informazione a persone fisiche in merito al trattamento dei dati personali e al trattamento di tali dati personali e di qualsiasi altro trattamento di dati personali ai fini della presente direttiva è effettuata in conformità della direttiva 95/46/CE, delle norme nazionali di recepimento della direttiva 95/46/CE e del regolamento (CE) n. 45/200"*.

Il secondo paragrafo dello stesso articolo ribadisce, a sua volta, il principio del consenso del titolare dei dati per ogni loro trattamento, prevedendo che *"i prestatori di servizi di pagamento hanno accesso, trattano e conservano i dati personali necessari alla*

144 Il tema dell'evoluzione dei servizi di *"Financial Data Aggregation (FDA)"* e di *"account information"* viene in trattato nella Collana Consob dedicata al FinTech. In particolare si veda il *Quaderno Fintech*, n. 4, "*Financial Data Aggregation e Account Information Services Questioni regolamentari e profili di business*", Consob, marzo 2019.

145 La PSD2 è anteriore all'entrare in vigore del GDPR, pertanto i richiami qui presenti, devono ritenersi validi per il GDPR che ha abrogato e sostituito la Direttiva 95/46/CE. Ai sensi dell'art. 94 del *GDPR* la "*direttiva 95/46/CE è abrogata a decorrere da 25 maggio 2018*» e i «*riferimenti alla direttiva abrogata si intendono fatti al presente regolamento. I riferimenti al gruppo per la tutela delle persone con riguardo al trattamento dei dati personali istituito dall'articolo 29della direttiva 95/46/CE si intendono fatti al comitato europeo per la protezione dei dati istituito dal presente regolamento"*.

prestazione dei rispettivi servizi di pagamento, solo dietro consenso esplicito dell'utente dei servizi di pagamento".

Con riferimento, infatti, all'operatività nella prestazione dei servizi di "disposizione di ordine di pagamento" o di "informazione sui conti", gli art. 66[146], 67[147] del PSD2 rispettivamente ribadiscono che "le terze parti" possono accedere solo su consenso esplicito del cliente.

A tal riguardo si noti, peraltro, che l'accesso consentito alle "terze parti" è ben delimitato dal par. 2 dell'art. 67[148]. Tale norma, infatti, prevede una serie di limitazioni all'uso dei dati e in particolare alla lett. f) stabilisce che il prestatore dei servizi di informazione sui conti "*non usa, accede o conserva dati per fini diversi da quelli della prestazione del servizio di informazione sui conti esplicitamente richiesto dall'utente dei servizi di pagamento, conformemente alle norme sulla protezione dei dati"*. Dalla portata di tale norma se ne desume quindi, *a contrario*, uno speculare divieto di accedere alle informazioni di "tipo diverso" o per "fini diversi".

Anche in questo caso, quindi, come visto in precedenza per gli obblighi previsti dalla MiFID, per identificare un "trattamento lecito" dei dati, si devono svolgere le medesime considerazioni sulla necessità di una valida base giuridica. Laddove il cliente abbia prestato uno specifico consenso all'utilizzo ed eventuale trasferimento a terzi dei propri dati, la terza parte potrà effettuare lecitamente il trattamento di tali dati all'interno del perimetro del consenso ricevuto. Qualora invece non sia stato prestato il consenso, o questo sia stato limitato solo a specifiche finalità, per ritenere di essere in presenza di un "trattamento lecito" occorre di volta in volta verificare la sussistenza delle condizioni per l'operatività delle diverse basi giuridiche n. 3 o n. 5 dell'art. 6 del

146 L'art. 66 rubricato *"Disposizioni per l'accesso ai conti di pagamento in caso di servizi di disposizione di ordine di pagamento"* al par. 2 stabilisce che *"Se il pagatore presta il consenso esplicito all'esecuzione di un pagamento in conformità dell'articolo 64, il prestatore di servizi di pagamento di radicamento del conto esegue le azioni specificate al paragrafo 4 del presente articolo per garantire il diritto del pagatore di avvalersi del servizio di disposizione di ordine di pagamento"*. Inoltre, il par. 3 prevede tra l'altro che: *"Il prestatore di servizi di disposizione di ordine di pagamento: (...) c) provvede affinché qualunque altra informazione sull'utente dei servizi di pagamento, ottenuta nella prestazione di servizi di disposizione di ordine di pagamento, sia fornita esclusivamente al beneficiario e solo su consenso esplicito dell'utente dei servizi di pagamento"* (enfasi aggiunta).

147 L'art. 67 rubricato "*Disposizioni per l'accesso alle informazioni sui conti di pagamento e all'utilizzo delle stesse in caso di servizi di informazione sui conti*", al par. 1 prevede che. *"Gli Stati membri assicurano che l'utente di servizi di pagamento abbia il diritto di ricorrere a servizi che consentono l'accesso ai servizi di informazione sui conti di cui al punto 8 dell'allegato I. Il diritto non si applica qualora il conto di pagamento non sia accessibile online*". Il par. 2 prosegue specificando che il prestatore di servizi di informazione sui conti: *"a) presta servizi unicamente sulla base del consenso esplicito dell'utente dei servizi di pagamento"*.

148 Art. 67, par. 2: "*Il prestatore di servizi di informazione sui conti: a) presta servizi unicamente sulla base del consenso esplicito dell'utente dei servizi di pagamento; b) provvede affinché le credenziali di sicurezza personalizzate dell'utente dei servizi di pagamento non siano accessibili ad altre parti ad eccezione dell'utente e dell'emittente delle credenziali di sicurezza personalizzate e la trasmissione di tali informazioni da parte del prestatore di servizi di informazione sui conti avvenga attraverso canali sicuri ed efficienti; c) per ogni sessione di comunicazione, si identifica presso il prestatore o i prestatori di servizi di pagamento di radicamento del conto dell'utente di servizi di pagamento e comunica in maniera sicura con il prestatore o i prestatori di servizi di pagamento di radicamento del conto e l'utente dei servizi di pagamento conformemente all'articolo 98, paragrafo 1, lettera d); d) accede soltanto alle informazioni sui conti di pagamento designati e sulle operazioni di pagamento a questi associati; e) non richiede dati sensibili relativi ai pagamenti, collegati ai conti di pagamento; f) non usa, accede o conserva dati per fini diversi da quelli della prestazione del servizio di informazione sui conti esplicitamente richiesto dall'utente dei servizi di pagamento, conformemente alle norme sulla protezione dei dati.*

GDPR sopra richiamate (ovvero la presenza di obblighi normativi o l'interesse legittimo prevalente del titolare).

* * *

In definitiva da quanto sopra detto è possibile affermare che il *diritto alla portabilità dei dati* è stato incardinato dalle normative europee in capo al cliente che può "cederlo", prestando il proprio esplicito a *terze parti*; queste ultime, pertanto, potranno trattarne i dati dei clienti soltanto in forza di un tale consenso prestato e nei limiti dello stesso.

Questo formale incardinamento pone però alcuni problemi pratici: a) quello del trattamento dei dati da parte di sistemi che intendano sperimentare l'utilizzano l'intelligenza artificiale (posto che il principio di limitazione delle finalità rende difficile invocare la validità dell'autorizzazione concessa e difficilmente il suo titolare risulta avere autorizzato un tale tipo di trattamento); b) quello di trattamento ed elaborazione dei Big data, ad esempio, in ambito finanziario

Per questa ragione al fine di promuovere un approccio omogeneo delle norme del GDPR in tutta l'UE e sostenere fattivamente il settore delle tecnologie innovative, si rivelano quanto mai utili orientamenti interpretativi mirati per risolvere le questioni ancora aperte[149].

Tuttavia, al di là di un approccio *cross sectoral*, che cerca, attraverso la previsione di interconnessioni normative, di mantenere in piedi un sistema normativo ormai superato, sarebbe forse ancor più preferibile ripensare a quelle che sono le priorità e le direttrici di questa nuova *data driven economy* al fine di pervenire ad un disegno legislativo in grado di mantenersi al passo con i tempi.

Nell'intento di rispondere a tali esigenze, il Parlamento europeo e il Consiglio hanno da ultimo presentato una proposta di regolamento in materia di *governance* dei dati, il *Data Governance Act*[150], la prima di una serie di misure annunciate nella *Strategia europea per i dati del 2020* che si rivolge a diversi tipi di intermediari di dati che gestiscono dati sia personali sia non personali, al fine agevolare la condivisione dei dati nonché di rafforzare la fiducia nei confronti di quegli intermediari di condivisione dei dati che si prevede saranno utilizzati nei diversi spazi di dati.

149 In particolare si osserva come rimangano ancora aperte le questioni inerenti alla distinzione tra dati di prova e dati di formazione e le implicazioni per il trattamento dei dati in tal caso (ad es. verificare che l'esenzione di cui all'articolo 5(1)(b) sarebbe applicabile quando i dati vengono utilizzati solo per la formazione e quando non vengono prese decisioni); alla possibilità o meno di ricorrere alla ricerca finanziata privatamente nel contesto dell'uso dei dati e della sperimentazione nell'uso del l'IA e di altre tecnologie; all'esame circa un'applicazione dell'articolo 6(4) del GDPR che non sia incompatibile con lo "scopo originario". *Cfr.* Expert Group on Regulatory Obstacles to Financial Innovation (ROFIEG), *30 Recommendations on Regulation, Innovation and Finance - Final Report to the European Commission*, European Commission, Directorate-General for Financial Stability, Financial Services and Capital Markets Union European Commission, 1049 Bruxelles, Belgium, 2019.

150 Proposta di Regolamento del Parlamento europeo e del Consiglio relativo alla *governance* europea dei dati (Atto sulla governance dei dati) del 25 novembre 2020 [COM(2020) 767 final 2020/0340 (COD)].

Il Regolamento si inserirà nel tessuto normativo già disegnato dal Legislatore europeo in materia di dati personali interagendo, in particolare, con il Regolamento generale sulla protezione dei dati (GDPR) e con la direttiva ePrivacy relativa alla vita privata e alle comunicazioni elettroniche, rafforzando così la solidità e affidabilità del delineato quadro giuridico per la protezione dei dati personali e creando al contempo un modello per il resto del mondo.

La proposta in parola andrà inoltre ad integrare, senza sovrapporsi ad essa[151], la direttiva (UE) 2019/1024 del Parlamento europeo e del Consiglio, del 20 giugno 2019, relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico (direttiva sull'apertura dei dati).

L'obiettivo è quello di migliorare le condizioni e i meccanismi per la condivisione dei dati nel mercato interno, creando un quadro armonizzato per lo scambio di dati. In particolare, il nuovo Regolamento andrà a disciplinare, in un'ottica di *levelling the playing field*, la condivisione dei dati nel settore pubblico, i servizi di intermediazione per la condivisione di dati tra imprese e interessati (e forniti a fronte di remunerazione) e il "*data altruism*", ovvero la raccolta e il trattamento dei dati messi a disposizione per scopi altruistici da persone fisiche e giuridiche[152].

Se è pur vero che il Regolamento si andrà ad applicare senza pregiudizio per il GDPR, tuttavia, è possibile intuirne il cambio di paradigma già a partire dall'ambito di applicazione e dalle definizioni.

In primo luogo, l'applicazione del regolamento ricomprenderà tutti i dati, personali e non personali. In secondo luogo esso disciplinerà il "*riutilizzo*", la "*condivisione*" e l'"*accesso*" dove: a) per "riutilizzo" s'intende l'uso da parte di persone fisiche o giuridiche di dati detenuti da enti del settore pubblico, per scopi commerciali o non commerciali diversi dallo scopo iniziale nell'ambito del compito pubblico per il quale i dati sono stati prodotti; b) per "condivisione dei dati", la fornitura da parte di un titolare dei dati a un utente dei dati ai fini dell'utilizzo congiunto o individuale dei dati condivisi, sulla base di accordi volontari, direttamente o tramite un intermediario; c) per

151 La presente proposta riguarda, infatti, i dati oggetto di diritti di terzi detenuti da enti pubblici e non rientra pertanto nel campo di applicazione della direttiva citata. Il DGA non mira inoltre a concedere, modificare o sopprimere i diritti sostanziali in materia di accesso ai dati e del loro utilizzo, per i quali sarà prevista per un'eventuale legge sui dati nel corso del 2021 (*cfr. Una strategia europea per i dati*, 2020, *op.cit.*)

152 Con espressione "altruismo dei dati" si fa riferimento all'uso dei dati prestati e raccolti – a seguito di consenso da parte degli interessati o comunque previa autorizzazione dei titolari – a titolo gratuito e per scopi di interesse generale (i.e. scopi scientifici, di ricerca o di miglioramento dei servizi pubblici). In particolare si prevede che per poter raccogliere dati per scopi altruistici le organizzazioni dovranno essere costituite per soddisfare obiettivi di interesse generale, operare senza scopo di lucro ed essere indipendenti da qualsiasi entità che operi a tale scopo. Dovranno inoltre essere in grado di garantire che le attività relative a tale categoria di dati si svolgano attraverso una struttura giuridicamente indipendente e separata. Le organizzazioni che rispettino detti requisiti dovranno poi richiedere l'iscrizione nel registro delle organizzazioni di *data altruism* in uno degli Stati membri dell'UE (laddove, invece, la sede sia stabilita in un Paese terzo, dovrà essere nominato un Legale rappresentante in uno degli Stati membri). A tal riguardo saranno istituite apposite Autorità di controllo, responsabili della creazione di tale registro nonché della vigilanza e del monitoraggio delle attività di dette organizzazioni.

"accesso", infine, l'operazione di "*processing by a data user of data that has been provided by a data holder*"[153], in conformità a specifici requisiti tecnici, legali o organizzativi, senza che ciò necessariamente implichi la trasmissione o il download di tali dati.

In tali *spazi di dati*, tre sono i principali interventi di normazione: *i*) le condizioni per il riutilizzo all'interno dell'Unione di determinate categorie di dati detenuti da enti del settore pubblico; *ii*) l'identificazione di un quadro di notifica e vigilanza per la fornitura di servizi di condivisione dei dati; *iii*) l'identificazione di un quadro per la registrazione volontaria delle entità che raccolgono ed elaborano i dati resi disponibili per scopi altruistici.

Per quanto di specifico interesse nel presente lavoro, si segnala che nel *Data Governance Act* i servizi per la condivisione dei dati, cd. "*data sharing services*", saranno suddivisi in tre categorie, tutte sottoposte al regime di notifica e vigilanza:

i) servizi di intermediazione tra persone giuridiche e potenziali *data users*, incentrati sullo scambio di dati attraverso la creazione di piattaforme o banche dati, e sulla creazione di infrastrutture specifiche per l'interconnessione dei titolari dei dati e degli utenti dei dati;

ii) servizi di intermediazione tra interessati a rendere disponibili i propri dati personali e potenziali *data users*, attraverso l'abilitazione e il supporto all'esercizio dei diritti dell'interessato ai sensi del GDPR, in particolare del diritto alla portabilità dei dati; e

iii) *data cooperatives*, servizi a supporto degli interessati o di imprese, che conferiscono alla cooperativa il potere di negoziare i termini e le condizioni per il trattamento dei dati rappresentandone gli interessi.

Se però, da un lato, il *Data Governance Act* configura il regime di responsabilità nonché le forme di separazione strutturale che devono adottare coloro che organizzano forme di gestione e condivisione dei dati, dall'altro, ancora non paiono essere ben delineati i presupposti ed i confini di tale normativa. In particolare non vi è chiarezza sul perimetro dei *data spaces*, sulla *governance* degli spazi di dati e circa la correlazione fra gli spazi (anche con riferimento all'applicazione della normativa antitrust).

Non vi è neppure certezza giuridica su chi avrà la proprietà (*ownership*) di tali dati e sulla base di quali principi o *entitlements* i dati potranno essere gestiti. Manca, altresì, una chiara delineazione circa l'(eventuale) esistenza di obblighi di condivisione tra le piattaforme e la loro compatibilità con i principi e le regole imposte dal GDPR, nonché sul regime di condivisione automatica e immediata dei dati sotto il profilo del *Regtech*.

Come è tipico ed insito in questa materia, solo il tempo e la prassi potranno colmare le lacune, aiutando il Legislatore nella creazione delle norme, che non dovrà

153 Le figure principali delineate dal DGA sono il *"data holder"* e il *"data user"*: il primo, definito come la persona giuridica o una persona interessata che, in conformità con il diritto dell'Unione o nazionale applicabile, ha il diritto di concedere l'accesso o di condividere determinati dati personali o non personali sotto il suo controllo. Il secondo come la persona fisica o giuridica che ha accesso legale a determinati dati personali o non personali ed è autorizzata a utilizzare tali dati per scopi commerciali o non commerciali.

sempre più cercare di anticipare e financo precedere l'innovazione, in modo tal da generare fiducia intorno alle nuove tecnologie. Non sono, infatti, i dati in quanto tali a generare ricchezza, ma è la fiducia nello scambio di informazioni e un utilizzo consapevole della tecnologia che determineranno le sorti dell'economia digitalizzata.

3 La tutela dei diritti fondamentali nella Financial Data Era

3.1 Premesse

L'avvento di una nuova epoca governata dai dati ha inciso fortemente sul percorso dell'umanità. Resta ancora incerta la possibile evoluzione della tecnologia, ma si nota come lo sviluppo e l'implementazione dello spazio cibernetico e dei suoi precipitati assumano sempre più importanza in ogni aspetto della vita dell'individuo. Sono proprio i dati, agglomerato di bit, che viaggiano ad altissima velocità, che si frammentano e si ricompongono secondo differenti dinamiche, attraverso gli algoritmi, le API, i servizi digitali e l'intelligenza artificiale. Un cambiamento così profondo ha scardinato le certezze preesistenti e ha apportato innovazioni in molti settori. Dunque, la quarta rivoluzione industriale[154], non poteva non travolgere anche il settore finanziario, proiettandoci nella c.d. Financial Data Era[155].

Gli sviluppi potenziali sembrano illimitati. In particolare, l'utilizzo massivo dell'ICT apre le porte a nuovi modelli imprenditoriali e ridisegna quelli esistenti.

Altra conseguenza di tale cambiamento è il passaggio alla Fintech[156], sintesi di finanza e tecnologia, intesa come declinazione della tecnologia alla finanza[157]. Si tratta di un fenomeno rapido e dirompente, che ha condotto a una repentina e vicendevole implementazione dei due elementi che la compongono.

Il legislatore europeo ha posto l'attenzione su ulteriori nuovi aspetti della finanza digitale, con l'intento di creare un *Digital Single Market* competitivo e innovativo[158], dando vita a un complesso sistema di fonti di riferimento. Questo è sicuramente

154 La prima è stata quella del carbone utilizzato per la macchina a vapore (fine Settecento), la seconda quella del motore a scoppio, dell'elettricità e del petrolio (prima metà del Novecento), la terza è quella dell'energia atomica (in coincidenza della Seconda guerra mondiale). La quarta rivoluzione inizia con il rilancio dell'IA a seguito del fenomeno della diffusione dei big data, dell'IoT e della robotica, secondo K. Schwab, La quarta rivoluzione industriale, Franco Angeli, Milano 2019, che ha coniato il termine.

155 Sul punto si veda V. Falce, G. Finocchiaro, La Digital Revolution nel settore finanziario. Una nota di metodo, in Analisi Giuridica dell'economia, fascicolo 1, giugno 2019, pp. 313 ss.

156 Per una definizione di Fintech si veda Financial Stability Board, Fintech credit Market structure: business models and financial stability implications, 22 maggio 2017. Cfr. D.W. Arner, J. Barberis, R.P. Buckley, The Evolution of Fintech: A New Post-Crisis Paradigm?, in Georgetown Journal of International Law, 1271, 2016; D.A. Zetzsche, R.P. Buckley, D.W Arner, J.N. Barberis, From Fintech to Techfin: The regulatory challenges of Data-Driven Finance, European Banking Institute, Working Paper Series, n. 6, 2017

157 Il termine Fintech nasce, infatti, dall'unione delle parole «finanza» e «tecnologia» e deve intendersi genericamente come «tecnologia applicata alla finanza», così C. Schena, A. Tanda, C, Arlotta, G. Potenza, Lo sviluppo del Fintech – Opportunità e rischi per l'Industria Finanziaria nell'era digitale, in Quaderni Fintech, a cura della Consob, 2018, p. VIII. Cfr. G. Alpa, Prefazione. Fintech: un laboratorio per i giuristi, in G. Finocchiaro, V. Falce, Fintech: diritti, concorrenza, regole. Le operazioni di finanziamento tecnologico, Bologna, 2019, pp. XIII ss.

158 Comunicazione della Commissione 2018, 109 final. Cfr. Comunicazione della Commissione 2015, COM(2015) 192 final.

dovuto al continuo progresso delle nuove tecnologie che ha indotto la promozione di iniziative incidenti *de iure condendo* sul progresso nel Fintech.

Tra gli interventi più rilevanti deve essere senz'altro menzionato il nuovo pacchetto legislativo sulla *Digital Finance*[159], che vuole eliminare la frammentazione nel settore del mercato unico digitale, procedendo con un *update* della disciplina.

Per perseguire tale obiettivo, la strategia della Commissione europea contempla tre proposte di regolamento, rispettivamente: sui mercati delle cripto-attività[160], su un regime pilota per le infrastrutture di mercato basate su DLT (*Distributed Ledger Technology*)[161] e sulla resilienza operativa digitale per il settore finanziario[162]. È anche prevista una proposta di direttiva[163] rivolta a novellare una serie di provvedimenti precedenti, tra cui la PSD2[164].

Il progresso ha coinvolto anche il settore dei pagamenti, che pure ha giocato un ruolo fondamentale nell'evoluzione del mercato digitale. Basti citare le Direttive EMD2[165] e PSD[166], che hanno introdotto novità regolatorie, sia nell'ambito della moneta elettronica, che nella fornitura dei servizi di pagamento da nuovi *player*, questi ultimi poi codificati nella PSD2. Deve inoltre ricondursi a tale quadro normativo quello sulla *Single Euro Payments Area* (SEPA) in cui confluisce anche quello dei pagamenti transfrontalieri[167].

159 Comunicazione della Commissione, relativa a una strategia in materia di finanza digitale per l'UE. del 24.9.2020, COM(2020) 591 final

160 Commissione europea, Proposta di Regolamento del Parlamento europeo e del Consiglio relativo ai mercati delle cripto-attività e che modifica la direttiva (UE) 2019/1937, del 24.9.2020, COM(2020) 593 final.

161 Commissione europea, Proposta di Regolamento del Parlamento europeo e del Consiglio relativo ad un regime pilota per le infrastrutture di mercato basate sulla tecnologia di registro distribuito, del 24.9.2020, COM(2020) 594 final.

162 Commissione europea, Proposta di Regolamento del Parlamento europeo e del Consiglio relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n.1060/2009, (UE) n.648/2012, (UE) n.600/2014 e (UE) n.909/2014, del 24.9.2020, COM(2020) 595 final.

163 Commissione europea, Proposta di Direttiva del Parlamento europeo e del Consiglio che modifica le direttive 2006/43/EC, 2009/65/EC, 2009/138/EU, 2011/61/EU, EU/2013/36, 2014/65/EU, 2015/2366/EU e 2016/234/EU, del 24.9.2020, COM(2020) 596 final.

164 Direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio del 25 novembre 2015 relativa ai servizi di pagamento nel mercato interno, che modifica le direttive 2002/65/CE, 2009/110/CE e 2013/36/UE e il regolamento (UE) n. 1093/2010, e abroga la direttiva 2007/64/CE, in G.U. n. L 337/23 del 23.12.2015, pp. 35 ss.

165 Direttiva 2009/110/CE del Parlamento europeo e del Consiglio del 16 settembre 2009 concernente l'avvio, l'esercizio e la vigilanza prudenziale dell'attività degli istituti di moneta elettronica, che modifica le direttive 2005/60/CE e 2006/48/CE e che abroga la direttiva 2000/46/CE, in G.U. n. L 267 del 10.10.2009, pp. 7-17.

166 Direttiva 2007/64/CE del Parlamento europeo e del Consiglio del 13 novembre 2007 relativa ai servizi di pagamento nel mercato interno, recante modifica delle direttive 97/7/CE, 2002/65/CE, 2005/60/CE e 2006/48/CE, che abroga la direttiva 97/5/CE, in G.U., n. L 319 del 05.12.2007, pp. 1 ss.

167 Regolamento (CE) n. 2009/924 del Parlamento europeo e del Consiglio del 16 settembre 2009 relativo ai pagamenti transfrontalieri nella Comunità e che abroga il regolamento (CE) n. 2560/2001, in G.U. L 266 del 9.10.2009, pp. 11-18. Regolamento (UE) n. 260/2012 del Parlamento europeo e del Consiglio del 14 marzo 2012 che stabilisce i requisiti tecnici e commerciali per i bonifici e gli addebiti diretti in euro e che modifica il regolamento (CE) n. 924/2009, in G.U. n. L 94 del 30.3.2012, pp. 22-37. Regolamento (UE) n. 248/2014 del Parlamento europeo e del Consiglio del 26 febbraio 2014 che modifica il regolamento (UE) n. 260/2012 per quanto riguarda la migrazione ai bonifici e agli addebiti diretti a livello di Unione, in G.U. L 84 del 20.3.2014, pp. 1-3. Regolamento (UE) 2019/518 del Parlamento europeo e del Consiglio del 19 marzo 2019 che modifica il regolamento (CE) n. 924/2009 per quanto riguarda talune commissioni applicate sui pagamenti transfrontalieri nell'Unione e le commissioni di conversione valutaria, in G.U. L 91 del 29.3.2019, pp. 36-41.

In tale contesto si inserisce la *Retail Payment Strategy*, attraverso la quale la Commissione intende raggiungere «1) soluzioni di pagamento sempre più digitali e istantanee di portata paneuropea; 2) mercati innovativi e competitivi dei pagamenti al dettaglio; 3) sistemi di pagamento al dettaglio efficienti e interoperabili e altre infrastrutture di sostegno; e 4) pagamenti internazionali efficienti, anche per le rimesse»[168]. Sono numerosi gli interventi previsti e riguardano, *inter alia*, il riesame della PSD2 e il potenziamento del Regolamento eIDAS[169].

Sul quadro descritto inciderà la nuova proposta di Regolamento sul *Digital Services Act* (DSA)[170] che disciplina responsabilità e responsabilizzazione dei servizi di intermediazione online, prevedendo, dal punto di vista del secondo profilo, la disciplina degli obblighi di *due diligence* specifici per tutti i *provider* di servizi di intermediazione, per i servizi di *hosting*, per le piattaforme online e per le «*very large online platform*», informati a una logica progressiva e cumulativa che intende sommare gli obblighi della categoria precedente a quella successiva.

Numerose sono le riforme in cantiere che manifestano una ipertrofia normativa intenta a seguire, talvolta affannosamente, gli sviluppi della tecnologia.

Ogni cambiamento radicale che investe la società comporta uno squilibrio nei paradigmi esistenti e richiede, tuttavia, una riflessione anche sulle conseguenze giuridiche (seguendo il noto binomio che lega *ius* e *societas*).

Anche nel contesto della strategia per il mercato unico digitale assume rilevanza la normativa sui dati personali e sul loro trattamento, la cui disciplina attuale è, a sua volta, conseguenza della nascita di un mondo che ha reso indispensabile una nuova ponderazione del diritto alla privacy[171].

Il modello europeo attuale innalza il diritto alla protezione dei dati personali al rango di diritto fondamentale, riconoscendolo espressamente, a livello di fonti del diritto primario, agli artt. 7 e 8 della Carta dei diritti fondamentali dell'Unione europea (CDFUE)[172] e all'art. 16, par. 1, del Trattato sul funzionamento dell'Unione europea

168 Comunicazione della Commissione, relativa a una strategia in materia di pagamenti al dettaglio per l'UE, del 24.9.2020, COM(2020) 592 final.

169 Regolamento (UE) n. 2014/910 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE, in G.U. n. L 257 del 28.08.2014, pp. 73 ss.

170 European Commission, Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, del 15.12.2020, COM(2020) 825 final.

171 Sul punto si veda S.D. Warren, L.D. Brandeis, The right to privacy, in Harvard Law Review, Vol. 4, No. 5. (Dec. 15, 1890), p. 193 ss. Per un approfondimento sulle origini del diritto alla privacy si veda C. Faralli, La privacy dalle origini ad oggi. Profili storico-filosofici, in N.Z. Galgano (a cura di), Persona e mercato dei dati. Riflessioni sul GDPR, Milano, 2019, pp. 1 ss. Per l'evoluzione storica della teoria dei diritti della personalità si veda G. Resta, Diritti della personalità: problemi e prospettive, in Diritto dell'informazione e dell'informatica, 2007, pp. 1045 ss.

172 Carta dei diritti fondamentali dell'Unione europea, in G.U. n. C 202 del 07.06.2016, pp. 389 ss. L'art. 7, rubricato "Rispetto della vita privata e della vita familiare" recita «Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle proprie comunicazioni». L'art. 8, rubricato "Protezione dei dati di carattere personale" recita «1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. 2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica. 3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente».

(TFUE)[173]. È principalmente il GDPR[174] a dettagliare, a livello secondario, tale diritto, tutelandone sia la protezione che - in un'ottica moderna di creazione di un mercato unico digitale - la circolazione. Il Regolamento 2016/679 è compendiato dalla Direttiva *e-privacy*[175], *lex specialis* del primo segnatamente al trattamento dei dati personali degli utenti dei servizi di comunicazione elettronica. La materia attualmente regolata dalla direttiva è oggetto di una proposta di regolamento da parte della Commissione, attualmente al vaglio del Parlamento europeo e del Consiglio[176].

La tensione tra tutela della privacy e le esigenze del mercato è interiorizzata dal GDPR, ma si palesa anche nel rapporto di questo con le altre normative che la sottintendono. Risulta, nello specifico, particolarmente complesso l'inquadramento delle nuove figure previste dalla PSD2 - i *Third Party Provider* – secondo gli schemi del GDPR.

3.2 Il nesso tra GDPR e PSD2

La disciplina PSD2 e quella del GDPR seguono alcuni approcci comuni. Il riferimento è ai principi di trasparenza, di sicurezza e di neutralità tecnologica a cui entrambe le normative si uniformano[177].

La PSD2 funzionalizza tali principi con l'intento di aggiornare l'attuale quadro normativo per rafforzare la fiducia dei consumatori nel mercato dei pagamenti, colmando le lacune regolamentari e garantendo maggiore certezza giuridica, in modo da assicurare un terreno fertile per la diffusione dei nuovi strumenti di pagamento[178].

La necessità di una seconda direttiva, dopo la PSD, è stata sentita specialmente dopo l'evoluzione e l'espansione del settore dei pagamenti online, grazie alla

173 Versione consolidata del trattato sul funzionamento dell'Unione europea, in G.U. n. C 326 del 26.10.2012 pp. 1 ss. L'art. 16, par. 1, che recita «Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano».

174 Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), in G.U. n. L 119 del 04.05.2016, pp. 1 ss.

175 Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche), in G.U. n. L 201, del 31.07.2002, pp. 37 ss.

176 Commissione europea, 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 2002/58/CE (regolamento sulla vita privata e le comunicazioni elettroniche), del 10.1.2017, COM(2017) 10 final.

177 Sul rapporto critico tra PSD2 e GDPR si veda C. Sertoli, PSD2, sicurezza e privacy, in G. Finocchiaro, V. Falce, Fintech: diritti, concorrenza, regole. Le operazioni di finanziamento tecnologico, Bologna, 2019, pp. 157 ss.; R. Petti, Identità digitale e biometria nei servizi di pagamento, in G. Finocchiaro, V. Falce, Fintech: diritti, concorrenza, regole. Le operazioni di finanziamento tecnologico, Bologna, 2019, pp. 453 ss.; M. Rabitti, A. Sciarrone Alibrandi, I servizi di pagamento tra PSD2 e GDPR: Open Banking e conseguenze per la clientela, in F. Capriglione (a cura di), Liber amicorum Guido Alpa, Padova, 2019, pp. 711 ss.

178 Cfr. Considerando 6 della PSD2. Si veda S. Vanini, L'attuazione in Italia della seconda direttiva sui servizi di pagamento nel mercato interno: le innovazioni introdotte dal d. lgs. 15 dicembre 2017, n. 218, in NLCC, 2018, p. 839 ss.; S. Balsamo Tagnani, Il mercato europeo dei servizi di pagamento si rinnova con la PSD2, in Contratto e impresa/Europa, 2018, p. 609 ss.; F. Porta, Obiettivi e strumenti della PSD2, in Quaderni di Ricerca Giuridica della Consulenza Legale della Banca d'Italia, Le nuove frontiere dei servizi bancari e di pagamento tra PSD2, criptovalute e rivoluzione digitale, a cura di F. Maimeri e M. Mancini, n. 87/2019, pp. 21 ss.

diffusione sempre più capillare del commercio elettronico e la nascita di nuovi servizi accessori.

Una delle novità più importanti della PSD2, che si muove in linea di continuità con la precedente direttiva[179], è l'aver disciplinato i *Third Party Provider* (TPP), quali nuovi soggetti frapposti tra la banca e il cliente. La direttiva affranca il fenomeno noto come *Open banking*.

La Seconda Direttiva Pagamenti individua due differenti attività che possono essere effettuate dai TTP:

(i) il servizio di disposizione di ordine di pagamento (*Payment Initiation Service* o PIS), che dispone l'ordine su richiesta dell'utente di servizi di pagamento, con riferimento a un conto detenuto presso un altro prestatore di servizi[180];

(ii) il servizio di informazione sui conti (*Account Information Service* o AIS), che fornisce informazioni consolidate, relativamente a uno o più conti di pagamento detenuti dall'utente presso un altro prestatore di servizi di pagamento, o presso più prestatori di servizi di pagamento, consentendo all'utente di avere un quadro generale della sua situazione finanziaria in un determinato momento[181].

Per usufruire dei nuovi servizi offerti dai TPP, è di norma sufficiente procedere con l'autenticazione tramite le credenziali fornite per accedere al conto di radicamento online, controllato dal prestatore di servizi di pagamento del conto (*Account Servicing Payment Service Provider* o ASPSP), non essendo necessaria l'esistenza di un rapporto contrattuale intercorrente tra questo e il TPP.

La PSD2 disciplina, agli artt. 66 e 67, il diritto di accesso ai conti di pagamento per i servizi AIS e PIS, richiedendo come prerequisito indispensabile l'accessibilità online dei conti stessi. Da questo punto di vista, la questione dell'infrastruttura assume primaria importanza, in quanto consente la comunicazione tra interfacce differenti, al fine di uno scambio vicendevole di informazioni contenute nei *database* di diversi interlocutori.

Dal punto di vista tecnico, tale operazione è resa possibile dalle *Application Programming Interface* (API), interfacce informatiche che consentono di accedere a un software o a un sistema tecnico. Pertanto, le API fungono da intermediari per la circolazione e la regolazione di flussi di dati tra vari sistemi informatici, anche altrimenti incompatibili.

Le API hanno dimostrato notevoli vantaggi nei diversi settori in cui sono state utilizzate. Uno degli ambiti in cui hanno riscosso maggiore successo è quello della condivisione di dati tra imprese, risultando uno strumento sicuro e affidabile, con benefici rilevanti in termini di opportunità e di efficienza[182].

179 Che ha riconosciuto l'attività degli Istituto di Pagamento (IP) e degli Istituti di Moneta Elettronica (IMEL).

180 Art. 4, par.1, n. 15, della PSD2.

181 Art. 4, par. 1, n. 16, della PSD2. Cfr. Considerando 28 della PSD2.

182 Cfr. Commissione europea, Documento di lavoro dei servizi della Commissione, Orientamenti sulla condivisione dei dati del settore privato nell'economia europea dei dati, del 25.4.2018, SWD(2018) 125 final e Study on data sharing

Le API consentono, inoltre, lo sviluppo di nuovi modelli di business, data la loro versatilità. In particolare, le API aperte consentono l'interazione con soggetti terzi, garantendo alti livelli di interoperabilità[183].

Anche nell'ambito dei rapporti tra ASPSP e TPP, ai sensi della PSD2, si fa ricorso ad API[184] per consentire la creazione di un canale di condivisione dei dati dei clienti delle banche con i TPP, secondo quella che sarebbe, per l'opinione maggioritaria[185], la tecnologia più affidabile per adempiere l'obbligo di fornire l'accesso ai dati del cliente gravante sulle banche[186].

La messa in comunicazione di sistemi differenti conduce alla movimentazione di un gran flusso di dati, tra cui assumono particolare rilievo, per le loro peculiarità precipue, i dati personali[187], il cui trattamento[188] è regolato dal GDPR.

Il riferimento, in particolare, è ai dati dei soggetti che vengono coinvolti nei processi sottesi ai servizi posti in essere dai TPP, tra i quali confluiscono non solo quelli del titolare del conto, ma anche quelli dei potenziali beneficiari o, comunque, di altri

between companies in Europe, commissionato dalla Commissione europea e realizzato da Everis, disponibile su https://op.europa.eu/en/publication-detail/-/publication/8b8776ff-4834-11e8-be1d-01aa75ed71a1/language-en.

183 Si veda O. Borgogno, Regimi di condivisione dei dati ed interoperabilità: il ruolo e la disciplina delle API, in Diritto dell'Informazione e dell'Informatica (Il), fasc.3, giugno 2019, pp. 689 ss.

184 Si veda sul punto la Sezione 2 del Capo V del Regolamento delegato (UE) 2018/389 della Commissione che riporta specifici per gli standard aperti di comunicazione comuni e sicuri.

185 Si veda G. Colangelo, O. Borgogno, Open Banking, portabilità dei dati e regime di accesso ai conti di pagamento, in G. Finocchiaro, V. Falce, Fintech: diritti, concorrenza, regole. Le operazioni di finanziamento tecnologico, Bologna, 2019, pp. 117 ss.; Poncibò C., Borgogno O., The Day After Tomorrow of banking: On FinTech, Data Control and Consumer Empowement, N. Aggarwal, Eidenmüller, L. Enriques, J. Payne, K. van Zwieten (edited by) Autonomous System and the Law, 2019, p. 55 ss. Cfr. M. Noctor, PSD2: Is the banking industry prepared?, in Computer Fraud & Security, n. 6/2018, pp. 9 ss.

186 Invero, il Governo del Regno Unito, per mezzo dell'Her Majesty's Treasury (HMT), a ridosso dell'entrata in vigore della PSD2, ha creato l'Open Banking Working Group (OBWG) per la realizzazione di un modello pro-concorrenziale standardizzato basato sulle API. Tale progetto fu seguito dalla pubblicazione di una bozza di raccomandazioni da parte della Competitions and Markets Authoruty (CMA), seguita dalla pubblicazione di un report finale nell'agosto 2016 (CMA, Retail banking investigation. Final report, del 9 agosto 2016, in https://assets.publishing.service.gov.uk/media/57ac9667e5274a0f6c00007a/retail-banking-market-investigation-full-final-report.pdf.). Il progetto Open Banking portava avanti il proposito di consentire agli ASPSPs di condividere i dati dei conti dei propri clienti in modo sicuro con i TPP, in modo che questi potessero erogare i propri servizi. Per raggiungere tale traguardo si è ritenuto necessario sviluppare degli standard per le APIs. Cfr. M. Zachariadis e O. Pinar, The API Economy and Digital Transformation in Financial Services: The case of Open Banking, in SWIFT Institute Working Paper, n. 2016-001, 15 giugno 2017.

187 La definizione di «dato personale» è riportata nell'art. 4, par. 1, n. 1, del GDPR che lo identifica come «qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale». Deve ricordarsi che il GDPR non si applica al trattamento di informazioni anonime o ai dati personali anonimizzati in modo tale da impedire l'identificazione dell'interessato.

188 Per trattamento, ai sensi dell'art. 4, par. 1, n. 2, del GDPR, si intende «qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione».

individui che siano entrati in contatto con l'utente del TPP, il quale deve trattare gli stessi perché strumentali con l'attività da questo posta in essere[189].

Il nesso più evidente tra la disciplina del GDPR e quella della PSD2 è individuabile nelle disposizioni dell'art. 94[190] - contenuto nel Capo 4 intitolato appunto "Protezione dei dati" - e dai considerando 89[191] e 90[192] della Seconda Direttiva Pagamenti, che tuttavia, *ratione temporis*, fa riferimento alla Direttiva n. 95/46/CE (Direttiva Privacy)[193] antesignana del GDPR[194].

Rivolgendo l'attenzione all'attività dei TPP, si nota che, sia per quelle di PIS che di AIS, gli artt. 66 e 67 della PSD2 contengono alcune misure a tutela dei dati personali. In particolare, l'art. 66, par. 3, lett. f) e g), stabilisce che il PISP «non chiede all'utente dei servizi di pagamento dati diversi da quelli necessari a prestare il servizio di disposizione di ordine di pagamento» e «non usa né conserva dati né vi accede per fini diversi dalla prestazione del servizio di disposizione di ordine di pagamento come esplicitamente richiesto dal pagatore».

Invece l'AISP, secondo l'art. 67, par. 2, lett. d) e f) della PSD2, «accede soltanto alle informazioni sui conti di pagamento designati e sulle operazioni di pagamento a questi associati» e «non usa, accede o conserva dati per fini diversi da quelli della prestazione del servizio di informazione sui conti esplicitamente richiesto dall'utente dei servizi di pagamento, conformemente alle norme sulla protezione dei dati». È opportuno chiarire da subito che quando ci si riferisce a questi ultimi servizi, alcuni potrebbero non rientrare nell'ambito applicativo della PSD2. Sono certamente ricompresi

189 Si pensi anche all'attività di info conti, che consente l'accesso alle movimentazioni complessive dell'utente

190 Art. 94 della PSD2: «1. Gli Stati membri autorizzano il trattamento dei dati personali da parte di sistemi di pagamento e di prestatori di servizi di pagamento se necessario per garantire la prevenzione, l'indagine e l'individuazione dei casi di frode nei pagamenti. La fornitura di informazione a persone fisiche in merito al trattamento dei dati personali e al trattamento di tali dati personali e di qualsiasi altro trattamento di dati personali ai fini della presente direttiva è effettuata in conformità della direttiva 95/46/CE, delle norme nazionali di recepimento della direttiva 95/46/CE e del regolamento (CE) n. 45/2001. 2. I prestatori di servizi di pagamento hanno accesso, trattano e conservano i dati personali necessari alla prestazione dei rispettivi servizi di pagamento, solo dietro consenso esplicito dell'utente dei servizi di pagamento».

191 Secondo il considerando 89 della PSD2, «La prestazione di servizi di pagamento da parte dei prestatori di servizi di pagamento può comportare il trattamento di dati personali. La direttiva 95/46/CE del Parlamento europeo e del Consiglio, le norme nazionali che danno attuazione alla direttiva 95/46/CE e il regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio si applicano al trattamento dei dati personali ai fini della presente direttiva. In particolare, qualora ai fini della presente direttiva vi sia trattamento di dati personali, è opportuno che sia specificato lo scopo preciso, siano citate le basi giuridiche pertinenti, vi sia conformità con i requisiti di sicurezza pertinenti di cui alla direttiva 95/46/CE e siano rispettati i principi di necessità, proporzionalità, limitazione delle finalità e proporzionalità del periodo di conservazione dei dati. Inoltre, la protezione dei dati fin dalla progettazione e la protezione dei dati di default dovrebbero essere integrate in tutti i sistemi di trattamento dei dati sviluppati e utilizzati nel quadro della presente direttiva.»

192 Secondo il considerando 90 della PSD2 «La presente direttiva rispetta i diritti fondamentali e osserva i principi riconosciuti dalla Carta dei diritti fondamentali dell'Unione europea, incluso il diritto al rispetto della vita privata e familiare, il diritto alla protezione dei dati personali, la libertà d'impresa, il diritto a un ricorso effettivo e il diritto di non essere giudicati o puniti due volte per lo stesso reato. La presente direttiva deve essere applicata conformemente a tali diritti e principi».

193 Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, in G.U. n. L 281 del 23.11.1995, pp. 31 ss.

194 Si ricordi che ai sensi dell'art. 94, par. 2, del GDPR i riferimenti alla Direttiva Privacy, abrogata a decorrere dal 25 maggio 2018, si devono intendere fatti al GDPR stesso.

quelli di pianificazione del budget e di monitoraggio della spesa, ma non i servizi di valutazione del merito creditizio e i servizi di audit.

3.3 Il ruolo dei TPP nella GDPR *compliance*

Il trattamento dei dati personali deve essere informato ai principi generali descritti dall'art. 5 del GDPR[195]:

(a) il principio di liceità, correttezza[196] e trasparenza, che impone di informare i soggetti interessati sulle modalità di raccolta, utilizzo e consultazione dei dati in modo comprensibile;

(b) il principio di finalità, che implica una raccolta indirizzata a finalità determinate, esplicite e legittime e, in caso di trattamenti ulteriori, solo per quelle compatibili;

(c) il principio di adeguatezza, di pertinenza e di non eccedenza, per il quale occorre ridurre al minimo la raccolta e il trattamento di dati personali (c.d. minimizzazione);

(d) il principio di esattezza e di aggiornamento, al fine di garantire l'accuratezza delle informazioni trattate;

(e) il principio di identificazione dell'interessato e di giusta durata del trattamento, che deve protrarsi per il tempo necessario a conseguire le finalità alla base dello stesso;

195 Il considerando 39 specifica: «qualsiasi trattamento di dati personali dovrebbe essere lecito e corretto. Dovrebbero essere trasparenti per le persone fisiche le modalità con cui sono raccolti, utilizzati, consultati o altrimenti trattati dati personali che le riguardano nonché la misura in cui i dati personali sono o saranno trattati. Il principio della trasparenza impone che le informazioni e le comunicazioni relative al trattamento di tali dati personali siano facilmente accessibili e comprensibili e che sia utilizzato un linguaggio semplice e chiaro. Tale principio riguarda, in particolare, l'informazione degli interessati sull'identità del titolare del trattamento e sulle finalità del trattamento e ulteriori informazioni per assicurare un trattamento corretto e trasparente con riguardo alle persone fisiche interessate e ai loro diritti di ottenere conferma e comunicazione di un trattamento di dati personali che le riguardano. È opportuno che le persone fisiche siano sensibilizzate ai rischi, alle norme, alle garanzie e ai diritti relativi al trattamento dei dati personali, nonché alle modalità di esercizio dei loro diritti relativi a tale trattamento. In particolare, le finalità specifiche del trattamento dei dati personali dovrebbero essere esplicite e legittime e precisate al momento della raccolta di detti dati personali. I dati personali dovrebbero essere adeguati, pertinenti e limitati a quanto necessario per le finalità del loro trattamento. Da qui l'obbligo, in particolare, di assicurare che il periodo di conservazione dei dati personali sia limitato al minimo necessario. I dati personali dovrebbero essere trattati solo se la finalità del trattamento non è ragionevolmente conseguibile con altri mezzi. Onde assicurare che i dati personali non siano conservati più a lungo del necessario, il titolare del trattamento dovrebbe stabilire un termine per la cancellazione o per la verifica periodica. È opportuno adottare tutte le misure ragionevoli affinché i dati personali inesatti siano rettificati o cancellati. I dati personali dovrebbero essere trattati in modo da garantirne un'adeguata sicurezza e riservatezza, anche per impedire l'accesso o l'utilizzo non autorizzato dei dati personali e delle attrezzature impiegate per il trattamento». Cfr. L. Bolognini, E. Pelino, Dato personale e trattamento, in L. Bolognini, E. Pelino, C. Bistolfi, Il Regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali, Milano 2016, pp. 90 ss.

196 *Fair* nella versione del testo in inglese, forse più evocativo. Si veda M. Soffientini (a cura di), Privacy. Protezione e trattamento dei dati, Vicenza, 2018, p. 93 che riconosce nell'espressione correttezza quel principio, immanente nel nostro ordinamento, di cui agli artt. 1175 e 1375 cod. civ.

(f) il principio di sicurezza adeguata, attraverso l'adozione di misure tecniche e organizzative idonee, secondo la nota *privacy by design* e *privacy by default* [197];

(g) il principio dell'*accountability* del titolare del trattamento, rispetto al quale egli deve dimostrare di aver predisposto misure efficaci e adeguate rispetto alle disposizioni del GDPR. Da ciò muove l'obbligo dello stesso di predisporre e mettere in atto tutte le misure di sicurezza e politiche interne idonee a tutelare i dati personali degli interessati.

Un primo problema concerne l'individuazione del ruolo che sia la banca che i *Third Party Provider* assumono secondo le dinamiche del GDPR. Come anticipato, nell'attuare i servizi da loro offerti - che siano di disposizione di ordini di pagamento o di informazione di conti – questi si trovano a dover trattare dati personali, principalmente dei loro utenti/interessati[198].

Nel Regolamento, i soggetti attivi che operano direttamente sui dati personali, sono il titolare del trattamento (*controller*) e il responsabile del trattamento (*processor*)[199].

L'*European Data Protection Board* (EDPB)[200] ha recentemente adottato delle linee guida proprio su questi due concetti[201], precedentemente oggetto di riflessione anche da parte dell'*Article 29 Data Protection Working Party* (A29WP) nel Parere 1/2010[202].

197 Il concetto di *privacy by design*, quale modello proattivo volto a integrare la *privacy compliance* nello sviluppo delle tecnologie, delle infrastrutture e delle pratiche commerciali, è dovuto al lavoro di Ann Cavoukian (cfr. Privacy by design, the 7 Fundationak Principles, in http://dataprotection.industries/wp-content/uploads/2017/10/privacy-by-design.pdf. Si veda il suo Privacy by design: the definitive workshop. A foreword by Ann Cavoukian, Ph.D., in IDIS 3, 2010, pp. 247 ss. che ha preceduto la risoluzione adottata da The 32nd International Conference of Data Protection and Privacy Commissioners (Resolution on Privacy by Design, Jerusalem, Israel 27-29 October 2010, in https://edps.europa.eu/sites/edp/files/publication/10-10-27_jerusalem_resolutionon_privacybydesign_en.pdf, che vedeva la stessa Dott.ssa Cavoukian (nella veste di Information and Privacy Commissioner of Ontario, Canada), quale proposer della risoluzione che ha riconosciuto tale principio come essenziale per la protezione della privacy, incoraggiando l'adozione di tale modello come *default* e invitando alla sua promozione. Tale principio venne riconosciuto *inter alia* dalla Federal Trade Commission come una delle tre passi fondamentali da seguire per la protezione della privacy online e inserito nel U.S. Commercial Privacy Bill of Rights Act of 2014 (S.2378) «to establish a regulatory framework for the comprehensive protection of personal data for individuals under the aegis of the Federal Trade Commission, to amend the Children's Online Privacy Protection Act of 1998 to improve provisions relating to collection, use, and disclosure of personal information of children, and for other purposes». Il GDPR accoglie tale principio all'art. 25, anche come declinazione di quella neutralità tecnologica che consente una progettazione delle misure e in base alla tecnologia al momento disponibile.

198 Tra cui sono annoverabili nome, cognome, indirizzo, e-mail, telefono, numero di documento ecc.

199 Per un'esaustiva disamina su queste due figure si veda L. Greco, I ruoli: titolare e responsabile, in G. Finocchiaro (opera diretta da), in Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali, Bologna, 2017, pp. 251 ss., E. Pelino, I soggetti del trattamento, in L. Bolognini, E. Pelino, C. Bistolfi, Il Regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali, Milano 2016, pp. 119 ss.

200 L'EDPB è un organo indipendente che contribuisce all'applicazione coerente delle norme sulla protezione dei dati in tutta l'Unione europea, pubblicando linee guida e raccomandazioni, identificando le migliori pratiche relative all'interpretazione e all'applicazione del GDPR e promuovendo la cooperazione tra le autorità competenti per la protezione dei dati dell'UE. Dal 25 maggio 2018, l'EDPB ha sostituito l'Article 29 Working Party.

201 EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, version 1.0 (for public consultation), adopted on 2 September 2020.

202 A29WP, Parere 1/2010 sui concetti di "responsabile del trattamento" e "incaricato del trattamento", adottato il 16 febbraio 2010, 00246/20/IT WP 169.

Il concetto di titolare/*controller* è stato mutuato dalla Convenzione 108 del Consiglio d'Europa del 1981[203], dove era prevista la figura del *controller of the file*, poi divenuto *controller of the processing of personal data*, ovvero il titolare del trattamento dei dati personali.

Il titolare è - nella formulazione attuale - definito come «la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri»[204].

Il titolare decide gli elementi fondamentali del trattamento ed esercita un potere decisorio sui motivi e le modalità di trattamento dei dati personali. Egli può essere indicato dalla legge, o la sua individuazione può essere meramente fattuale, manifestazione di un momento decisorio, che non richiede una designazione o un conferimento della titolarità stessa.

La figura del responsabile del trattamento non trova, invece, un suo predecessore nella Convenzione 108. La sua presenza nel GDPR e nella precedente Direttiva Privacy, si deve all'avvertita necessità di garantire eguale protezione agli interessati nei casi in cui i loro dati personali fossero stati trattati da soggetti terzi per conto del titolare.

Il responsabile del trattamento è definito dall'art. 3, par. 8, del GDPR, come «la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento». La sua nomina avviene tramite un atto di designazione da parte del titolare – o da altro responsabile autorizzato da quest'ultimo – affinché questo possa agire secondo le istruzioni impartite, fornendo altresì assistenza attraverso le modalità descritte dalla normativa e dalla nomina. All'interno di questo perimetro, il responsabile gode di un margine operativo abbastanza ampio.

L'alterità rispetto al titolare e l'effettuazione dell'attività di trattamento per conto di quest'ultimo sono *condiciones sine quibus non* è possibile agire quale responsabile. Non meno importante è l'elemento volitivo esterno, giacché in assenza della decisione della sua nomina, le operazioni a esso delegate potrebbero essere eseguite direttamente dal titolare.

Oltre che sull'*an*, il titolare decide sul *quantum* da delegare, ben potendo scegliere di affidare al responsabile la totalità, o solamente una parte, delle operazioni di trattamento. Quanto al *quomodo*, il *modus operandi* del responsabile è cristallizzato nel contenuto dell'atto di nomina. La fattispecie è sussumibile nel *genus* del contratto

203 La Convenzione 108 di Strasburgo del 1981 ha lo scopo di garantire il rispetto dei diritti e delle libertà fondamentali della persona fisica, indipendentemente dalla sua nazionalità, con riferimento all'elaborazione automatica dei dati personali che la riguardano. È stata ratificata anche da Stati appartenenti al Consiglio d'Europa ed è stata di recente novellata da un protocollo di modifica - adottato il 18 maggio 2018 - che l'ha informata ai nuovi principi del GDPR.

204 Così l'art. 4, par. 1, n. 7, del GDPR.

di mandato e deve riportare: (a) la durata del trattamento, (b) la natura e le finalità e (c) il tipo di dati personali e le categorie di interessati[205].

La scelta del responsabile è *intuitus personae* e deve tenere presente la competenza specialistica, l'affidabilità e le risorse di cui questi dispone per poter svolgere la sua funzione. Ciò impone al titolare di ponderare attentamente se il potenziale responsabile possa o meno soddisfare tali requisiti, prima di esternalizzare le operazioni di trattamento.

Nonostante la presenza di un rapporto negoziale risulti fondamentale per delineare i compiti assegnati al responsabile, deve sottolinearsi come questo non possa in alcun modo impedire l'applicazione del principio funzionalista che, al fine di prevenire assegnazioni fittizie, con conseguenti limitazioni di responsabilità, consente in ogni caso di riconsiderare la figura del responsabile nominato nel caso in cui questi - travalicando le funzioni proprie di tale ruolo - determini autonomamente le finalità e i mezzi del trattamento, divenendo sostanzialmente anch'egli un titolare[206].

In questi casi si verifica una titolarità condivisa in cui i diversi attori incidono su singole operazioni o insiemi di operazioni sui dati personali, che possono aver luogo contemporaneamente o in varie fasi[207]. In caso di simultaneità ricorre la figura del contitolare (*joint controller*).

Il concetto di contitolarità è riconosciuto dall'art. 26 del GDPR e si verifica qualora due o più titolari determinino congiuntamente le finalità e i mezzi del trattamento.

La partecipazione congiunta al trattamento può sostanziarsi in una decisione comune presa da due o più titolari o derivare dalla convergenza di decisioni, laddove queste si completino a vicenda e risultino necessarie affinché il trattamento avvenga in modo tale da avere un impatto tangibile sulla determinazione delle finalità e dei mezzi dello stesso. Il criterio discretivo rilevante, rispetto all'assetto di due titolari distinti, è che il trattamento non sarebbe possibile senza la partecipazione di entrambe le parti, nel senso che tale operazione compiuta da ciascuna parte è inseparabile, o meglio inestricabilmente legata.

La morfologia della *joint controllership* risulta, sin dalla sua enucleazione, ambigua, in quanto sottintende tutte le situazioni in cui il titolare operi con l'intervento di un ulteriore soggetto che determini a sua volta proprie le finalità e i mezzi, assumendo molteplici fattezze. Anche in questo caso devono necessariamente andarsi a scrutinare i rapporti fattuali tra le parti nel trattamento dei dati personali.

Per tentare di facilitare tale operazione, il GDPR ha accolto l'esigenza di avere un documento che definisca *a priori* tali rapporti, evitando in questo modo contrattazioni artate che ostacolerebbero l'applicazione effettiva della normativa. Pertanto, è stato previsto l'obbligo, da parte dei contitolari, di descrivere i loro rapporti in materia

205 Considerando 81 e art. 28 del GDPR.

206 A29WP, Parere 1/2010 sui concetti di "responsabile del trattamento" e "incaricato del trattamento", cit., p. 26.

207 Cfr. A29WP, Parere 1/2010 sui concetti di "responsabile del trattamento" e "incaricato del trattamento", cit., p. 19.

di trattamento attraverso un accordo scritto da rendere disponibile *vis-à-vis* ai soggetti interessati, consentendo altresì – al fine di evitare circonvenzioni della normativa – a questi ultimi, indipendentemente dalle disposizioni dell'accordo, di poter esercitare i propri diritti nei confronti e contro ciascun titolare coinvolto.

La disposizione di cui all'art. 26 del GDPR è un esempio di implementazione del principio di trasparenza che, come afferma il considerando 29 della normativa in questione, si propone di rendere facilmente accessibili le informazioni e le comunicazioni relative al trattamento dei dati personali[208].

Volendo identificare il TPP in uno dei soggetti esaminati poc'anzi - atteso che la banca deve rivestire, dal momento dell'apertura del conto corrente, la figura del titolare - le differenti possibili interazioni renderebbero potenzialmente configurabili sia la sua nomina a responsabile del trattamento, sia la titolarità diretta di tale attività.

La prima eventualità, ovvero la nomina a responsabile del TPP, presupporrebbe invero l'instaurazione di un rapporto fiduciario con il titolare, la banca, in quanto in tal caso sarebbe come se la prima facesse eseguire, su ordine dell'utente, alcuni servizi (quelli previsti dalla PSD2) al TPP – che in tal caso perderebbe forse il requisito della terzietà - nominandolo responsabile. Tale circostanza sottintenderebbe, da parte del titolare, una valutazione a monte dell'affidabilità del TPP, che a tale scopo dovrebbe prestare garanzie sufficienti per mettere in atto quanto previsto dal GDPR di riferimento e dalle istruzioni impartite dallo stesso. Si ricordi, tuttavia, che per la PSD2 non è indispensabile un legame negoziale tra ASPSP e il TPP[209].

A parere di chi scrive, tale situazione risulterebbe implausibile, in considerazione del fatto che i TPP svolgono un'attività propria, che è ontologicamente estranea a quella prestata dalla banca. Considerando che il responsabile opera per conto del titolare e in base a finalità definite da quest'ultimo, per verificarsi tale ipotesi, le finalità del TPP dovrebbero paradossalmente coincidere con quelle della banca, come pure la base giuridica.

Una differente ricostruzione - che poi dovrebbe coincidere con l'*id quod plerumque accidit* - suggerirebbe invece che, nell'ambito dei servizi prestati, il TPP determini finalità e mezzi propri del trattamento, facilmente rinvenibili nel necessario rapporto contrattuale che lo lega al cliente, qualificandosi *ex se* come titolare.

Ulteriore passaggio è comprendere se la titolarità del TPP possa essere definita autonoma o congiunta.

Come detto in precedenza, la peculiarità della contitolarità è l'interazione nel medesimo trattamento. Da vagliare è anche la soluzione della titolarità asimmetrica, ovvero il caso di una, sia pur parziale, sovrapponibilità delle finalità. Devono, infatti, considerarsi le varie interazioni prospettabili tra i potenziali contitolari, che possono

208 L. Greco, I ruoli: titolare e responsabile, cit., p. 260.

209 Cfr. art. 66, par. 5, della PSD2: «La prestazione di servizi di disposizione di ordine di pagamento non è subordinata all'esistenza di un rapporto contrattuale a tale scopo tra i prestatori di servizi di disposizione di ordine di pagamento e i prestatori di servizi di pagamento di radicamento del conto».

manifestarsi come rapporti più o meno stringenti, e insistere su fasi più o meno coincidenti del trattamento, rendendo necessaria la valutazione caso per caso dei rapporti tra i titolari[210].

La circostanza che i due ipotetici titolari, la banca e il TPP, realizzino molteplici trasferimenti di dati, tra cui i dati personali, di per sé non implica necessariamente la contitolarità. Nella prassi applicativa non è sempre semplice distinguere le situazioni di contitolarità da quelle in cui i singoli titolari agiscono separatamente. In effetti, l'elaborazione dei dati a catena, senza comunanza di finalità o strumenti, deve essere letta come un trasferimento tra distinti titolari.

Dunque, quando la banca consente l'accesso ai dati personali dei suoi clienti al TPP, affinché questo possa svolgere la sua attività (di disposizione di ordini di pagamento o di info conti), sembra manifestarsi una *separate-controllership*.

Tuttavia, la contitolarità non dovrebbe essere escludibile *a priori*. Infatti, nel caso in cui venga realizzata una base infrastrutturale di raccordo comune, questi diverrebbero corresponsabili del trattamento nella misura in cui determinano gli aspetti fondamentali dei mezzi del trattamento[211].

In conclusione, salvi casi particolari, il rapporto tra la banca e il TPP dovrebbe ricondursi al paradigma dei due titolari indipendenti, non rinvenendosi alcun elemento fondamentale comune tra finalità e mezzi del trattamento che induca a ritenere indispensabile la contitolarità.

Proprio in virtù di tale considerazione, occorre approfondire gli aspetti concernenti le basi giuridiche dei trattamenti e le dinamiche sottese al trasferimento dei dati tra banca e TPP.

3.4 La base giuridica del trattamento dei dati personali

Secondo il GDPR, il trattamento dei dati personali, affinché sia lecito, deve fondarsi sul consenso dell'interessato o su un'altra base legittima prevista dallo stesso Regolamento, dal diritto dell'Unione o degli Stati membri[212].

210 Cfr. A29WP, Parere 1/2010 sui concetti di "responsabile del trattamento" e "incaricato del trattamento", cit., pp. 20-21.

211 EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, cit., pp. 20-21, riporta l'esempio dell'agenzia di viaggi che invia i dati personali del suo cliente alla compagnia area e a una catena di hotel per la prenotazione di un pacchetto vacanze. Ricevuta conferma, l'agenzia rilascia i documenti di viaggio e i voucher per i propri clienti. In questo caso, ciascuno degli attori tratta i dati personali per lo svolgimento delle proprie attività e con i propri mezzi ed è un titolare del trattamento. Se, tuttavia, l'agenzia creasse con le catene alberghiere e le compagnie aeree una piattaforma online comune, concordando gli aspetti fondamentali degli strumenti da utilizzare, i tre soggetti risponderebbero congiuntamente solo per quanto riguarda i trattamenti effettuati su tale piattaforma, rimanendo individualmente responsabili per le residue attività. Così, se banca e TPP dovessero creare congiuntamente un'interfaccia comune, definendo gli elementi fondamentali dei mezzi del trattamento, potrebbero configurare una contitolarità asimmetrica. In tal caso, dovrebbero, *ex* art. 26 del GDPR, predisporre un accordo interno da rendere *vis-à-vis* disponibile agli interessati.

212 Cfr. l'art. 8 della CDFUE e il considerando 40 del GDPR. Per un approfondimento sull'argomento si veda L. Bolognini, E. Pelino, Dato personale e trattamento, in L. Bolognini, E. Pelino, C. Bistolfi, Il Regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali, Milano 2016, pp. 43 ss.; Id., Condizioni di liceità, in

La disposizione di riferimento è l'art. 6 del GDPR[213], secondo cui «il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:

a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;

b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;

c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;

d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;

L. Bolognini, E. Pelino, C. Bistolfi, Il Regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali, Milano 2016, pp. 277 ss.; F. Bravo, Il consenso e le altre condizioni di liceità del trattamento di dati personali, in G. Finocchiaro (opera diretta da), Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali, Bologna, 2017, pp. 101 ss.

213 Che si riferisce alla generalità dei dati personali trattati, ivi compresi i c.d. dati giudiziari, dovendosi integrare le sue disposizioni con quelle di cui all'art. 10 e dell'art. 9 del GDPR, sulle categorie dei dati personali particolari, ovvero i dati sensibili, genetici e biometrici, che è stato formulato premettendo il divieto generale a trattare dati personali «che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona», prevedendo, sotto forma di eccezione, un'elencazione di dieci ipotesi riportate al paragrafo 2, di trattamento lecito di dati personali, nei casi in cui: «a) l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1; b) il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato; c) il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso; d) il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato; e) il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato; f) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali; g) il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato; h) il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità, fatte salve le condizioni e le garanzie di cui al paragrafo 3; i) il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale; j) il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.»

e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;

f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore».

Tra le condizioni di legittimità enumerate dal GDPR, sicuramente quella del consenso trova maggiore riscontro dal punto di vista applicativo.

Il consenso viene definito dall'art. 4, par. 1, n. 11 del GDPR come «qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento». Per tale motivo, all'interessato deve essere somministrata un'idonea informativa, che lo renda edotto riguardo l'identità del titolare, le finalità e le basi giuridiche, la durata e i diritti degli interessati.

Negli altri cinque casi previsti dall'art. 6 del GDPR, il trattamento viene effettuato in un contesto specifico ed è possibile a prescindere dal consenso o tramite differente manifestazione dello stesso[214].

In particolare, la condizione di liceità che si fonda sull'esecuzione di un contratto impone al titolare di valutare quale trattamento è necessario per l'esecuzione dello stesso, nel rispetto dei già menzionati principi di cui all'art. 5 del GDPR, tra cui quello di correttezza - che induce a riconoscere le ragionevoli aspettative dell'interessato - quello di limitazione delle finalità e di minimizzazione dei dati, che assumono particolare rilevanza con riferimento ai servizi online, giacché questi non vengono negoziati su base individuale[215].

Infatti, nella valutazione del consenso contrattuale, a mente dell'art. 7, par. 4, del GDPR «si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto»[216]. Pertanto, il trattamento deve essere effettivamente indispensabile per l'esecuzione dello stesso. In caso contrario, la base giuridica contrattuale non è

214 L. Bolognini, E. Pelino, Condizioni di liceità, cit., p. 288.

215 EDPB, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, version for public consultation, adopted on 9 April 2019, p. 5. Cfr. A29WP, Opinion 03/2013 on purpose limitation, adopted on 2 April 2013, 00569/13/EN WP 203, pp. 15-16: «The purpose of the collection must be clearly and specifically identified: it must be detailed enough to determine what kind of processing is and is not included within the specified purpose, and to allow that compliance with the law can be assessed and data protection safeguards applied. For these reasons, a purpose that is vague or general, such as for instance 'improving users' experience', 'marketing purposes', 'IT-security purposes' or 'future research' will-without more detail-usually not meet the criteria of being 'specific'».

216 Cfr. Considerando 44 del GDPR.

sufficiente a legittimare il trattamento, che deve necessariamente giustificarsi su altra base[217].

Circoscrivendo il discorso ai TPP, il considerando 87 della PSD2 stabilisce che la direttiva riguarda «gli obblighi e le responsabilità contrattuali tra l'utente dei servizi di pagamento e il corrispondente prestatore di servizi di pagamento», inducendo a ritenere che la base giuridica sia quella contrattuale *ex* art. 6, par. 1, lett. b) del GDPR. In proposito, la direttiva, nel disciplinare l'accesso ai conti di pagamento e l'uso delle informazioni dei conti, riporta che il PISP, ex art. 66, par. 3, lett. f) e g), «non chiede all'utente dei servizi di pagamento dati diversi da quelli necessari a prestare il servizio di disposizione di ordine di pagamento» e «non usa né conserva dati né vi accede per fini diversi dalla prestazione del servizio di disposizione di ordine di pagamento come esplicitamente richiesto dal pagatore». L'art. 67, par. 2, lett. d) e f) dispone che l'AISP «accede soltanto alle informazioni sui conti di pagamento designati e sulle operazioni di pagamento a questi associati» e «non usa, accede o conserva dati per fini diversi da quelli della prestazione del servizio di informazione sui conti esplicitamente richiesto dall'utente dei servizi di pagamento, conformemente alle norme sulla protezione dei dati». Questo sottintende che le finalità per cui le informazioni degli account sono fornite all'AISP devono essere oggetto di un contratto con l'utente.

Gli artt. 66, par. 3, lett. f) e 67, par. 2, lett. d) sembrano interiorizzare e modulare il concetto di "stretta necessità per l'esecuzione del contratto" del GDPR, mentre il contenuto degli artt. 66, par. 3, lett. g) e 67, par. 2, lett. f) impedisce l'ulteriore utilizzo dei dati personali raccolti sulla base del consenso contrattuale.

Questo induce l'EDPB a ritenere che ogni ulteriore trattamento da parte dei TPP dovrà necessariamente fondarsi su una differente base giuridica, quale ad esempio il consenso o l'obbligo di una legge (degli Stati membri o del diritto dell'Unione europea)[218].

La questione delle condizioni di liceità del trattamento coinvolge anche le dinamiche di accesso ai dati personali detenuti dalle banche durante le operazioni di tra TPP e l'ASPSP. L'accesso deve infatti essere garantito anche in assenza di un rapporto contrattuale intercorrente tra questo e il TPP[219]. L'effettivo esercizio delle prerogative garantite ai TPP dalla PSD2, verrebbe in caso contrario compromesso.

217 EDPB, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, cit., p. 9, riporta l'esempio del rivenditore online da cui un soggetto interessato acquista alcuni oggetti. Se l'interessato vuole pagare con carta di credito con consegna a casa, il rivenditore dovrà trattare le informazioni relative alla carta di credito e l'indirizzo di fatturazione per le finalità del pagamento, trattando altresì l'indirizzo dell'interessato per la consegna, potendo fondare il trattamento sulla base legale di cui all'art. 6, par. 1, lett. b). Qualora invece il cliente intenda ritirare l'acquisto presso un punto di consegna, l'indirizzo dell'interessato non sarebbe più necessario per l'esecuzione del contratto e pertanto per il trattamento di tale dato personale sarebbe necessaria una differente base legale.

218 EDPB, Guidelines 06/2020 on the interplay of Second Payment Services Directive and GDPR, cit., p. 11 riporta l'esempio dell'obbligo di legge di cui alla Direttiva (UE) 2015/849 del Parlamento europeo e del Consiglio del 20 maggio 2015 relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo, che modifica il regolamento (UE) n. 648/2012 del Parlamento europeo e del Consiglio e che abroga la direttiva 2005/60/CE del Parlamento europeo e del Consiglio e la direttiva 2006/70/CE della Commissione

219 Cfr. art. 66, par. 5, della PSD2, per i PISP, secondo cui «La prestazione di servizi di disposizione di ordine di pagamento non è subordinata all'esistenza di un rapporto contrattuale a tale scopo tra i prestatori di servizi di disposizione di

Anche in questo caso è doveroso interrogarsi su quale sia la base giuridica che legittima questo ulteriore trattamento da parte della banca. Invero, risulterebbe implausibile che detto trasferimento possa essere disciplinato da un contratto in forza tra la banca e l'utente. Allo stesso modo, ipotizzare una base consensuale da prestare di volta in volta renderebbe le dinamiche intercorrenti tra ASPSP e TPP particolarmente farraginose.

In questi casi, secondo l'EDPB, la condizione di legittimità, che consente l'accesso ai PISP e agli AISP per l'esecuzione dei loro servizi per conto degli utenti, è l'obbligo di legge di cui all'art. 6, par. 1, lett. c), del GDPR, secondo cui è lecito il trattamento necessario per adempiere a un obbligo legale al quale è soggetto il titolare del trattamento, in questo caso le disposizioni della PSD2 e, segnatamente, dagli artt. 66, par. 1 e 67, par. 1. Tali disposizioni impongono agli Stati membri di assicurare tali diritti attraverso l'implementazione di una legge nazionale di trasposizione della Seconda Direttiva Pagamenti, divenendo proprio questa la legge che obbliga l'ASPSP a un ulteriore trattamento[220].

Un altro degli aspetti problematici nel coordinamento tra la PSD2 e il GDPR è sicuramente l'interpretazione del già menzionato art. 94, par. 2, della PSD2 secondo cui «i prestatori di servizi di pagamento hanno accesso, trattano e conservano i dati personali necessari alla prestazione dei rispettivi servizi di pagamento, solo dietro consenso esplicito dell'utente dei servizi di pagamento». In particolare, ci si domanda se il termine «consenso esplicito», utilizzato nella PSD2 assuma o meno lo stesso significato di quello assunto nel GDPR, dove questo viene richiesto unicamente nei casi di trattamento di dati personali particolari (art. 9).

Sul punto si è espresso l'EDPB concludendo che la terminologia utilizzata dalla PSD2 si riferisce al consenso contrattuale, che deve essere prestato previa conoscenza esplicita, da parte degli interessati, delle clausole riguardanti le specifiche categorie di dati personali che verranno trattati e delle finalità del trattamento individuate dal titolare. Tali clausole «dovrebbero essere chiaramente distinguibili dalle altre questioni trattate nel contratto e dovrebbero essere esplicitamente accettate dall'interessato[221]. Il concetto di consenso esplicito ai sensi dell'articolo 94, paragrafo 2, della PSD2 è quindi un requisito aggiuntivo di natura contrattuale e non è lo stesso del consenso (esplicito) ai sensi del GDPR»[222]; non rappresenta dunque la base giuridica del trattamento dei dati personali, ma è specificamente correlato alla protezione degli stessi.

ordine di pagamento e i prestatori di servizi di pagamento di radicamento del conto» e l'art. 67, par. 4, della PSD2, per gli AISP, secondo cui «La prestazione di servizi di informazione sui conti non è subordinata all'esistenza di un rapporto contrattuale a tale scopo tra i prestatori di servizi di informazione sui conti e i prestatori di servizi di pagamento di radicamento del conto»

220 EDPB, Guidelines 06/2020 on the interplay of Second Payment Services Directive and GDPR, cit., p. 11.

221 EDPB, Guidelines 06/2020 on the interplay of Second Payment Services Directive and GDPR, cit., p. 14. Cfr. A. Burchi, S. Mezzacapo, P. Musile Tanzi, V. Troiano, Financial Data Aggregation e Account Information Services. Questioni regolamentari e profili di business, in Quaderni FinTech, a cura della Consob, n. 4, marzo 2019, p. 35 secondo cui «Appare quindi così delinearsi una disciplina differenziata, segnatamente nel senso della previsione di una protezione extra o rafforzata, per il trattamento di "dati personali"».

222 EDPB, Letter to 't Veld, (Member of the European Parliament), 5 July 2018, EDPB-84-2018, p. 4 (traduzione dell'autore).

Un'ultima questione riguarda il fondamento legale del trattamento dei dati personali della c.d. *silent party*, ovvero quel soggetto terzo i cui dati personali sono processati senza che questi abbia rilasciato alcun consenso. Viene definito tale il beneficiario di un pagamento operato tramite servizio PIS o il soggetto terzo di cui vengono visualizzate informazioni attraverso il servizio AIS. Anche in tale circostanza il trattamento dei dati personali deve trovare base giuridica idonea, sebbene non vi sia alcun rapporto che lega il TPP con la parte silente.

Secondo l'EDPB, la base legale per il trattamento dei dati della *silent party* da parte dei TPP andrebbe identificata nell'interesse legittimo del titolare o del soggetto terzo per l'esecuzione del contratto con l'utente del servizio[223]. Sulla base di questa, il titolare può trattare i dati personali dell'interessato o di terzi, a patto che non metta a rischio, nel perseguimento delle sue finalità, i diritti fondamentali dei soggetti i cui dati sono trattati. Il considerando 47 riporta il caso in cui «esista una relazione pertinente e appropriata tra l'interessato e il titolare del trattamento, ad esempio quando l'interessato è un cliente o è alle dipendenze del titolare del trattamento». In tali casi, il titolare è obbligato a operare un bilanciamento tra il suo interesse e quello dell'interessato, o del terzo. Tale valutazione deve tenere conto se l'interessato, al momento e nell'ambito della raccolta dei dati personali, avrebbe ragionevolmente potuto attendersi un trattamento per tali finalità. Ciò implica che il legittimo interesse del titolare è limitato e determinato dalle ragionevoli aspettative dell'interessato. A tal fine, il titolare del trattamento deve predisporre tutte le misure opportune affinché i dati personali della *silent party* non vengano trattati per finalità ulteriori a quelle per cui sono stati originariamente raccolti[224].

Infine, giova osservare che tali dati personali non potrebbero essere utilizzati per uno scopo diverso da quello per cui sono stati inizialmente raccolti, considerate anche le ulteriori limitazioni sui trattamenti derivanti dai già menzionati artt. 66, par. 3, lett. g) e 67, par. 2, lett. f), della PSD2, che definiscono, come visto, limiti più stringenti in termini di accesso, conservazione e utilizzo.

3.5 I diritti dell'interessato: la portabilità dei dati

Il GDPR disciplina al Capo III, dagli artt. 12-23, i diritti dell'interessato[225], ereditandone la maggior parte dalla precedente Direttiva Privacy e introducendo il nuovo diritto alla portabilità.

223 EDPB, Letter to 't Veld, cit., p. 3.

224 EDPB, Guidelines 06/2020 on the interplay of Second Payment Services Directive and GDPR, cit., p. 15 che suggerisce la crittografia o altre tecniche idonee a raggiungere un livello appropriato di sicurezza e minimizzazione.

225 Per un approfondimento sul tema si veda A. Ricci, I diritti dell'interessato, in G. Finocchiaro (opera diretta da), Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali, Bologna, 2017, pp. 179 ss.; E. Pelino, I diritti dell'interessato, in L. Bolognini, E. Pelino, C. Bistolfi, Il Regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali, Milano 2016, pp. 171 ss.

In sintesi, i diritti dell'interessato sono:

a. il diritto di accesso, che trova la sua disciplina nell'art. 15 del GDPR[226], secondo cui l'interessato può ottenere dal titolare la conferma di un trattamento che lo riguarda e, nel caso, venire a conoscenza delle informazioni inerenti allo stesso[227].

b. il diritto di rettifica, ex art. 16 del GDPR[228], che si sostanzia nel diritto alla correzione dei dati personali inesatti dell'interessato e nel complementare diritto di ottenere l'integrazione dei dati incompleti;

c. il diritto alla cancellazione, se ricorrono i presupposti indicati dall'art. 17 del GDPR[229];

d. il diritto di limitazione di trattamento, che opera nei casi riportati dell'art. 18 del GDPR[230].

Si aggiunge a quelli già menzionati il nuovo diritto alla portabilità dei dati previsto dall'art. 20 del GDPR[231].

226 Diritto analogo è riportato all'art. 8, par. 1, lett. b) della Convenzione 108.

227 Segnatamente l'art. 15 del GDPR riporta: «(a) le finalità del trattamento; (b) le categorie di dati personali in questione; (c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali; (d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo; (e) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento; (f) il diritto di proporre reclamo a un'autorità di controllo; (g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine; (h) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.»

228 Diritto analogo è riportato all'art. 8, par. 1, lett. C) della Convenzione 108.

229 I motivi individuati dell'art. 17 del GDPR sono i seguenti: «(a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati; (b) l'interessato revoca il consenso su cui si basa il trattamento conformemente all'articolo 6, paragrafo 1, lettera a), o all'articolo 9, paragrafo 2, lettera a), e se non sussiste altro fondamento giuridico per il trattamento; (c) l'interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2; (d) i dati personali sono stati trattati illecitamente; (e) i dati personali devono essere cancellati per adempiere un obbligo giuridico previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento; (f) i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8, paragrafo 1.»

230 Le ipotesi riportate dall'art. 18 del GDPR sono: «(a) l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al titolare del trattamento per verificare l'esattezza di tali dati personali; (b) il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo; (c) benché il titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria; (d) l'interessato si è opposto al trattamento ai sensi dell'articolo 21, paragrafo 1, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.»

231 «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. 3. L'esercizio del diritto di cui al paragrafo 1 del presente articolo lascia impregiudicato l'articolo 17. Tale diritto non si

Si tratta della vera novità introdotta dal Regolamento Privacy che sottintende una molteplicità di pretese da parte dell'interessato[232]. Tali sono: (a) la possibilità di ricevere i dati personali che lo riguardano, (b) la successiva trasmissione dei dati ricevuti dall'interessato a un altro titolare e (c) il diritto di richiedere il trasferimento diretto dei propri dati personali da un primo titolare a un secondo.

Il diritto in esame opera con delle limitazioni. Infatti, la portabilità può essere richiesta su dati personali il cui trattamento si fonda unicamente sulla base giuridica del consenso o contrattuale. Inoltre, è necessario che il trattamento sia effettuato con mezzi automatizzati, escludendo pertanto la sua operatività in caso di archivi cartacei. Infine, possono essere trasferiti unicamente dati personali riguardanti l'interessato o forniti dallo stesso.

Tale ultima circostanza pone un duplice dubbio interpretativo che coinvolge sia la tematica della perimetrazione dei dati personali effettivamente "portabili", sia la tematica dei diritti di soggetti terzi, che in ogni caso non devono essere pregiudicati dal trasferimento, anche per espressa disposizione dell'art. 20, par. 4, del GDPR.

Per quanto concerne la prima tematica, la norma in parola sembra escludere la possibilità di trasmissione di dati inferenziali o comunque derivati. Tuttavia, l'A29WP suggerisce un'interpretazione meno stringente della disposizione, ricomprendendo nel novero dei "dati forniti dall'interessato" anche quelli che derivano dall'osservazione delle attività dello stesso, includendo, così, anche i dati grezzi generati, ad esempio, da un contatore intelligente o da altri oggetti connessi (quali ad esempio i dati sulle registrazioni delle attività svolte, sulla cronologia della navigazione o sulle ricerche effettuate, i dati relativi al traffico, quelli inerenti all'ubicazione, alla frequenza cardiaca o altri dati rilevati da specifici dispositivi)[233]. Come è stato sostenuto, la tematica è strettamente connessa al settore bancario, in quanto gli istituti bancari tendono a implementare e a raffinare i dati, a volte anche perché obbligati *ex lege*, e pertanto la portabilità di dati raffinati comporterebbe un ingiustificato arricchimento informativo a danno dell'operato delle banche europee[234].

applica al trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento. 4. Il diritto di cui al paragrafo 1 non deve ledere i diritti e le libertà altrui».

Si vedano sull'argomento L. Somaini, The right to data portability and user control: ambitions and limitations, in Rivista di diritto dei media, n. 3, 2018, p. 164 ss., A.G. Monteleone, Il diritto alla portabilità dei dati: tra diritti della persona e diritti del mercato, in LUISS Law Review, n. 2/2017, pp. 202 ss.; S. Troiano, Il diritto alla portabilità dei dati, in N.Z. Galgano (a cura di), Persona e mercato dei dati. Riflessioni sul GDPR, Milano, 2019, pp. 195 ss.; M. Giorgianni, Art. 20 - Diritto alla portabilità dei dati, in A. Barba, S. Pagliantini (a cura di), Commentario del Codice civile - Modulo delle persone - vol. 2, pp. 408 ss.; E. Pelino, I diritti dell'interessato, cit., pp. 245 ss.

232 Distinguono tre differenti pretese Somaini L., cit., p. 165 secondo cui «the provision encompasses three distinct rights: the right to receive personal data in a structured and machine-readable format, the right to transmit personal data to another data controller and the right to transmit personal data directly from one data controller to another». Cfr. F. Pezza, sub Art. 20, in GDPR e normativa privacy. Commentario, a cura di G.M. Riccio, G. Scorza e E. Belisario, Milano, 2018, p. 203.

233 A29WP, Linee guida sul diritto alla portabilità dei dati, adottato il 13 dicembre 2016, versione emendata e adottata il 5 aprile 2017, 16/IT, WP 242 rev.01, pp. 9-10.

234 Cfr. E. Palmerini, G. Aiello, V. Cappelli, Il FinTech nel contesto della data-driven economy, cit., pp. 25-26.

Riguardo alla seconda tematica, sono posti dei dubbi in merito alla possibile estrapolazione dei dati personali appartenenti a soggetti terzi. In questo caso, secondo l'A29WP, il trattamento di questi dati da parte del nuovo titolare è permesso se chi si avvale di tale diritto perseguirà le medesime finalità dopo aver eseguito la portabilità (ad esempio la richiesta per il trasferimento del registro dei contatti per poterne usufruire in un servizio analogo). Diverso sarebbe il caso in cui il titolare utilizzasse tali dati per finalità differenti, come quella di marketing da parte del nuovo titolare, trattamento che risulterebbe inevitabilmente illecito[235].

Limiti interpretativi a parte, deve sottolinearsi come questo diritto si differenzi dagli altri previsti dal GDPR. Se rapportato al diritto di accesso - di cui risulta un'evoluzione - testimonia la tendenza verso l'*empowerment* dell'interessato garantendogli il potere di indirizzare la movimentazione dei propri dati personali[236].

Tuttavia, da un diverso punto di vista, non può tacersi che l'implementazione di questo diritto richiede necessariamente un'architettura tecnica di sostegno, che consenta ai titolari di sviluppare e scambiare dei formati interoperabili di dati, non solo personali. Lo sviluppo dell'interoperabilità condurrebbe all'espressione delle potenzialità dell'art. 20 anche in chiave pro-competitiva, in quanto consentirebbe di contrastare più efficacemente le pratiche di *vendor lock-in* e di rimozione delle barriere tecnico-giuridiche per stimolare la concorrenza tra i diversi fornitori di servizio. Tale intento è tra l'altro sottinteso dal considerando 68 del GDPR[237].

235 A29WP, Linee guida sul diritto alla portabilità dei dati, cit., p. 12, riporta l'esempio dei dati personali riguardanti i soggetti che hanno effettuato un bonifico a favore del titolare di un conto corrente. In questo caso, la richiesta di portabilità delle informazioni relative al conto da parte del titolare, se avanzata per utilizzare le informazioni per le medesime finalità (ad es. per disporre di un registro delle operazioni compiute) non comporta la lesione dei diritti dei terzi. Sul punto, invero, vi sono analogie con il la condizione della silent party analizzata nel paragrafo precedente.

236 Cfr. Pelino, I diritti dell'interessato, cit., p. 250. Cfr. anche A.G. Monteleone, Il diritto alla portabilità dei dati, cit., p. 205.

237 Considerando 68 del GDPR: «Per rafforzare ulteriormente il controllo sui propri dati è opportuno anche che l'interessato abbia il diritto, qualora i dati personali siano trattati con mezzi automatizzati, di ricevere in un formato strutturato, di uso comune, leggibile da dispositivo automatico e interoperabile i dati personali che lo riguardano che abbia fornito a un titolare del trattamento e di trasmetterli a un altro titolare del trattamento. È opportuno incoraggiare i titolari del trattamento a sviluppare formati interoperabili che consentano la portabilità dei dati. Tale diritto dovrebbe applicarsi qualora l'interessato abbia fornito i dati personali sulla base del proprio consenso o se il trattamento è necessario per l'esecuzione di un contratto. Non dovrebbe applicarsi qualora il trattamento si basi su un fondamento giuridico diverso dal consenso o contratto. Per sua stessa natura, tale diritto non dovrebbe essere esercitato nei confronti dei titolari del trattamento che trattano dati personali nell'esercizio delle loro funzioni pubbliche. Non dovrebbe pertanto applicarsi quando il trattamento dei dati personali è necessario per l'adempimento di un obbligo legale cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento. Il diritto dell'interessato di trasmettere o ricevere dati personali che lo riguardano non dovrebbe comportare l'obbligo per i titolari del trattamento di adottare o mantenere sistemi di trattamento tecnicamente compatibili. Qualora un certo insieme di dati personali riguardi più di un interessato, il diritto di ricevere i dati personali non dovrebbe pregiudicare i diritti e le libertà degli altri interessati in ottemperanza del presente regolamento. Inoltre tale diritto non dovrebbe pregiudicare il diritto dell'interessato di ottenere la cancellazione dei dati personali e le limitazioni di tale diritto di cui al presente regolamento e non dovrebbe segnatamente implicare la cancellazione dei dati personali riguardanti l'interessato forniti da quest'ultimo per l'esecuzione di un contratto, nella misura in cui e fintantoché i dati personali siano necessari all'esecuzione di tale contratto. Ove tecnicamente fattibile, l'interessato dovrebbe avere il diritto di ottenere che i dati personali siano trasmessi direttamente da un titolare del trattamento a un altro.»

In questi termini, un notevole passo in avanti verso la libera circolazione dei dati è dato dall'introduzione del Regolamento (UE) n. 2018/1807[238] che trae spunto dalle considerazioni alla base dell'art. 20 del GDPR, riconoscendo dall'art. 6 il diritto alla portabilità «uno degli elementi fondamentali che agevolano la scelta degli utenti e stimolano la concorrenza effettiva nei mercati dei servizi di trattamento di dati»[239].

L'utilizzo della portabilità per finalità competitive, d'altro canto, non è nuovo allo scenario europeo. Merita infatti menzione il diritto alla portabilità del numero già introdotto dall'art. 30 della Direttiva n. 2002/22/CE (Direttiva Servizio Universale)[240] che consente all'utente di cambiare l'operatore telefonico, senza rinunciare al proprio numero. Altro precedente, più recente, è quello relativo al diritto di portabilità del conto corrente, regolato dalla Direttiva (UE) n. 2014/92 (Direttiva PAD)[241].

Finalità pro-competitive si riscontrano, come visto in precedenza, anche nella PSD2, che ha appunto ampliato il mercato bancario estendendolo anche ai servizi offerti dai nuovi *player*, i TPP, a cui le banche di radicamento del conto devono dare accesso. In tal caso, tuttavia, l'interoperabilità si esprime secondo una fenomenologia differente. Rimane infatti l'obbligo di disporre di un conto corrente di radicamento, dal quale non si può prescindere, per poter usufruire dei servizi messi a disposizione dai TPP. Il trasferimento dati tra banca e TPP, poi, può essere protratto nel tempo e opera dinamicamente.

3.6 La sicurezza informatica

La sicurezza informatica è un argomento particolarmente delicato, atteso il ruolo sempre più permeante che le tecnologie dell'informazione e della comunicazione stanno assumendo. Tale pervasività impone l'adozione di contromisure atte a ridurre e gestire il rischio di minacce informatiche attraverso operazioni di cibersicurezza. A fornire la definizione di tali attività è l'art. 2 del Regolamento 2019/881[242], descrivendole come «necessarie per proteggere la rete e i sistemi informativi, gli utenti di tali sistemi e le altre persone interessate dalle minacce informatiche».

Circoscrivendo la tematica, deve sottolinearsi come anche all'interno del GDPR e della PSD2 sono dedicate all'argomento precipue disposizioni.

238 Regolamento (UE) 2018/1807 del Parlamento europeo e del Consiglio, del 14 novembre 2018, relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea, in G.U. n. L 303 del 28.11.2018, pp. 59 ss.

239 Considerando 29, reg. 2018/1807.

240 Direttiva 2002/22/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002, relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica (direttiva servizio universale), in G.U. n. L 108 del 24.04.2002, pp. 51 ss.

241 Direttiva 2014/92/UE del Parlamento europeo e del Consiglio, del 23 luglio 2014, sulla comparabilità delle spese relative al conto di pagamento, sul trasferimento del conto di pagamento e sull'accesso al conto di pagamento con caratteristiche di base, in G.U. n. L 257 del 28.08.2014, pp. 214 ss.

242 Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cibersicurezza»), in G.U. n. L 151, del 07.06.2019, pp. 15 ss.

Il tema della sicurezza diviene canone orientativo del trattamento dei dati personali[243]. Questo rappresenta uno dei principi cardine del Regolamento che, come anticipato[244], richiede l'adozione di misure adeguate secondo i modelli della *privacy by design* e della *privacy by default*, predisponendo un sistema complesso, espressione dell'*accountability* del titolare. Quest'ultimo deve infatti concepire una serie di misure tecniche e organizzative, come previsto dall'art. 32 del GDPR[245], tenendo conto, *inter alia*, dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento. Anche l'intero sistema organizzativo del personale, e i vari livelli di autorizzazione, assumono un significativo valore in termini di prevenzione dei rischi legati alla sicurezza.

L'adeguata sicurezza, ai sensi del GDPR, è altresì garantita dalla valutazione d'impatto sulla protezione dei dati (*Data Protection Impact Assessment* o DPIA) prevista dall'art. 35. Questa viene richiesta qualora il trattamento preveda l'utilizzo di strumenti tecnologici e vi sia un rischio potenzialmente elevato per i diritti e le libertà delle persone (interessati o soggetti terzi), data la natura, l'oggetto, il contesto e le finalità del trattamento. In particolare, giova sottolineare come l'obbligo di procedere alla DPIA sia previsto in tutti i casi in cui vengono trattati dati personali particolari e giudiziari di agli artt. 9, par. 1, e 10 del Regolamento.

Il GDPR disciplina anche il comportamento che il titolare dovrà seguire in caso di violazione dei dati personali (c.d. *personal data breach*), ovvero «la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati»[246]. In tale caso, il titolare deve notificare all'autorità competente la violazione, entro le settantadue ore successive alla conoscenza del fatto, elaborando un report da condividere con l'*authority*. Qualora la violazione porti a un rischio elevato per i diritti e le libertà degli interessati, questi dovranno essere avvertiti dal titolare secondo le modalità di cui all'art. 34 del GDPR.

In ambito finanziario la violazione di dati, personali e non, implica delle gravi ripercussioni sull'utente. Per tale motivo nella PSD2 il ruolo della sicurezza rimane centrale. Per offrire servizi di pagamento elettronici sicuri ed evitare rischi di frode - incrementando perciò la fiducia dei consumatori nel settore - la direttiva ha demandato all'Autorità Bancaria Europea (*European Banking Authority* o EBA) il compito di pre-

243 Si vedano sull'argomento A. Mantelero, Il nuovo approccio della valutazione del rischio nella sicurezza dei dati. Valutazione d'impatto e consultazione preventiva, in Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali, Bologna, 2017, pp. 251 ss.; L. Bolognini, E. Pelino, C. Bistolfi, Le obbligazioni di compliance in materia di protezione dei dati, in L. Bolognini, E. Pelino, C. Bistolfi, Il Regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali, Milano 2016, pp. 323 ss.

244 Si veda il paragrafo 2.

245 Quali «a) la pseudonimizzazione e la cifratura dei dati personali; b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.»

246 Così l'art. 4, par. 1, n. 12), del GDPR.

sentare delle norme tecniche di regolamentazione alla Commissione, affinché quest'ultima le adotti[247]. Difatti, con Regolamento Delegato n. 2018/389[248], sono state adottate le *Regulatory Technical Standards* (RTS) per stabilire i requisiti che i prestatori di servizi di pagamento devono rispettare nell'applicazione degli standard aperti di comunicazione e del meccanismo di Autenticazione Forte del cliente (*Strong Customer Authentication* o SCA), definita dall'art. 4, par. 1, n. 30, come «un'autenticazione basata sull'uso di due o più elementi, classificati nelle categorie della conoscenza (qualcosa che solo l'utente conosce), del possesso (qualcosa che solo l'utente possiede) e dell'inerenza (qualcosa che caratterizza l'utente), che sono indipendenti, in quanto la violazione di uno non compromette l'affidabilità degli altri, e che è concepita in modo tale da tutelare la riservatezza dei dati di autenticazione».

Viene stabilito dunque un riconoscimento con credenziali a doppio fattore tramite ad esempio una password, un *token* ed elementi biometrici. Per le operazioni con un indice maggiore di rischio, come le operazioni di pagamento elettronico a distanza, viene richiesto un elemento aggiuntivo che colleghi dinamicamente la transazione a un importo e a un beneficiario specifico (il c.d. *Dynamic Linking*), come l'autenticazione attraverso le *one-time password* (OTP), chiavi crittografiche o firme elettroniche.

Sono state tuttavia contemplate deroghe al principio dell'autenticazione forte in caso di livello basso di rischio, determinato in correlazione con l'importo, la frequenza dell'operazione e il canale di pagamento utilizzato. Sono esentate: (a) le transazioni che prevedono un importo di esigua entità (art. 16 delle RTS), (b) i pagamenti ricorrenti dello stesso valore (art. 14 delle RTS), e (c) i pagamenti verso beneficiari di fiducia (art. 13 delle RTS).

L'ambito applicativo della SCA è circoscritto alle operazioni: (a) di accesso al conto di pagamento on line, (b) di disposizione di un'operazione di pagamento elettronico e (c) che vengono effettuate tramite un canale a distanza che possano comportare un rischio di frode nei pagamenti o altri abusi.

247 Contenute nel Final Report dell'EBA, Draft Regulatory Technical Standards on Strong Customer Authentication and common and secure communication under Article 98 of Directive 2015/2366 (PSD2), del 23 febbraio 2017, EBA/RTS/2017/02.

248 Regolamento delegato (UE) 2018/39 della Commissione, del 27 novembre 2017 che integra la direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione per l'autenticazione forte del cliente e gli standard aperti di comunicazione comuni e sicuri, in G.U. n. L 69, del 13.06.2018, pp. 23-43.

M. Cassese, G. Colangelo(*)

4 Il diritto alla portabilità dei dati nella Digital Single Market Strategy

4.1 Premesse

La quarta rivoluzione industriale[249] promuove la digitalizzazione delle più variegate relazioni economico-sociali e le affranca dai limiti spazio-temporali propri dell'era analogica grazie all'utilizzo estensivo dell'*Information and Communication Technology* (ICT) e dell'*Internet of Things* (IoT), che consentono alla collettività di porre in essere processi comunicativi, produttivi e commerciali in modo istantaneo e a costi estremamente ridotti.

Il nuovo ecosistema digitale venutosi a creare tende ad una costante innovazione che ha la peculiarità di essere calibrata sulle necessità degli individui, intesi sia come singoli che come collettività. Come noto, tali necessità sono monitorate e, non di rado, dedotte dalle piattaforme digitali che possono ormai agevolmente ricorrere allo sfruttamento massivo dei dati mediante l'utilizzo di una serie estremamente variegata di tecniche che ne consentono la raccolta, l'accumulo (Big Data[250]) e la elaborazione.

Perno centrale di questo ecosistema è, quindi, costituito dai dati, la cui elaborazione consente l'ottenimento di risultati predittivi che rappresentano per le imprese un vero e proprio driver per l'economia in quanto potenzialmente in grado di stravolgere i paradigmi di ogni settore di attività e della vita quotidiana, apportando indubbi benefici per la collettività e per le medesime imprese. L'elaborazione dei dati, infatti, non solo consente alle imprese di acquisire vantaggi competitivi sul mercato elaborando, ad esempio, servizi digitali *ad hoc*, ma permette altresì alle organizzazioni pubbliche, agli Stati ed alle organizzazioni internazionali di rispondere in maniera più efficace alle sfide sociali, economiche, sanitarie, climatiche e ambientali del secondo

(*) Marco Cassese, dottorando Università Europea e Innovation and Competition Policy Centre-ICPC (marcocassese1@gmail.com);

Giuseppe Colangelo, Jean Monnet Chair in European Innovation Policy and Associate Professor of Law and Economics (University of Basilicata); Transatlantic Technology Law Forum Fellow (Stanford University and University of Vienna); Adjunct Professor of Markets, Regulations and Law (Luiss) (giuseppe.colangelo1975@gmail.com).

249 Per un'ampia disamina della quarta rivoluzione industriale si veda, inter alia: Parlamento Europeo, Industry 4.0 Digitalisation for productivity and growth, 2015; F. Butera, Lavoro e organizzazione nella quarta rivoluzione industriale: la nuova progettazione socio-tecnica, in L'Industria, 3, 2017.

250 Per un approfondimento specifico sul tema dei *Big Data* si rinvia a: AGCM, AGCOM, Garante per la protezione dei dati personali, *Indagine conoscitiva sui Big Data,* 10 febbraio 2020, Doc. Web: 9264297. Tale indagine ha preso avvio con la delibera n. 375/15/CONS dell'AGCOM con specifico riferimento allo sviluppo delle piattaforme digitale e dei servizi di comunicazione elettronica. Sulle single fasi della raccolta dei dati da parte delle piattaforme *online*, invece, si veda: M. Forti, *Le piattaforme online alla prova del Regolamento (UE) 2016/679. Quali tutele per la condivisione dei dati nell'economia collaborativa?*, in *Rivista di diritto dei media*, 2/2019, p. 5.

millennio, contribuendo allo sviluppo di società prospere e sostenibili[251]. Si pensi ad esempio al settore finanziario, che in seguito alla crisi finanziaria del 2008 ha assistito a forti scosse innovative che hanno avviato una dirompente rimodulazione nei fornitori dei servizi, nei prodotti offerti e nei processi aziendali[252]. Si pensi anche al settore sanitario, ove grazie alle nuove tecnologie di tracciamento e di elaborazione dei dati si è recentemente registrato uno sviluppo esponenziale della medicina personalizzata e di nuove tecniche di contenimento dei virus infettivi[253].

Se i benefici derivanti dai servizi digitali e, in più generale, dalla Data Driven Economy sono ormai indubbi, tuttavia, è altrettanto noto che dietro questa ondata innovativa si celano anche molte insidie[254]: le caratteristiche intrinseche del nuovo mondo economico digitalizzato costituiscono un terreno fertile per il compimento di pratiche commerciali scorrette, di abusi concorrenziali, di frodi e di violazioni dei dati personali. Creare *policy* e regolamentare il nuovo ecosistema, incanalandolo nei corretti binari valoriali, costituisce pertanto una delle maggiori sfide che le principali potenze mondiali si trovano a dover fronteggiare e ciò, come è stato da molti rilevato, è essenziale sia per preservare i diritti fondamentali degli individui che per infondere un clima di generale fiducia nei confronti del nuovo ecosistema, propedeutico a promuoverne uno sviluppo esponenziale[255].

In tale contesto, l'Unione europea si colloca tra le potenze mondiali maggiormente attive grazie all'adozione, fin dal 2015, di una strategia finalizzata alla creazione di un mercato unico digitale (*Digital Single Market Strategy*) fondato sui seguenti tre pilastri: 1) un migliore accesso a prodotti e servizi online; 2) migliori condizioni normative affinché le reti e i servizi digitali possano svilupparsi e prosperare; 3) promozione della crescita e della sicurezza dell'economia digitale europea[256]. Gli obiettivi

251 Per una panoramica sui benefici e sui rischi che porta la digitalizzazione si veda, tra gli altri: OECD, *Digital Economy Outlook 2017*, October 2017; si vedano inoltre: European Commission, *Communication: Shaping Europe's digital future,* 19 Febbruary 2020. Con specifico riferimento al settore finanziario si rinvia a: Schena, A. Tanda, C. Arlotta, G. Potenza, *Lo sviluppo del FinTech - Opportunità e rischi per l'industria finanziaria nell'era digitale*, op. cit., marzo 2018.

252 Tale fenomeno, che rappresenta un sottoinsieme della attuale rivoluzione industriale, è ormai comunemente definito come FinTech e consiste nella crescente offerta di nuovi servizi di finanziamento, di pagamento, di investimento e di consulenza, tutti caratterizzati per la loro alta intensità tecnologica. Per un'analisi delle peculiarità dei nuovi attori nel mondo finanziario si veda: D. A. Zetzsche, R.P. Buckley, D.W. Arner, J.N. Barberis, *From FinTech to TechFin: The Regulatory Challenges of Data-Driven Finance*. in *EBI Working Paper Series*, n. 6, 2017.

253 A tal riguardo, la recente esperienza italiana ha assistito al lancio dell'applicazione "immuni", che salvaguardando la *privacy* dei suoi utenti, consente il tracciamento dei circoli di contagio per fronteggiare più efficacemente l'emergenza sanitaria causata dal virus Covid-19.

254 Ibidem.

255 Il tema è stato affrontato da varie prospettive. Tra i vari, per un approfondimento, si veda: V. Falce, G. Finocchiaro, *La digital devolution nel settore finanziario. Una nota di metodo*, op. cit, giugno 2019; H. Zech, *A legal framework for a data economy in the European Digital Single Market: rights to use data, Journal of Intellectual Property Law & Practice*, Volume 11, Issue 6, June 2016; U. Von der Leyen, *A Union that strives for more, My agenda for Europe, Political Guidelines for the next European Commission 2019 – 2024*; OECD, *Digital Economy Outlook 2017*, October 2017; European Commission, *Communication: Shaping Europe's digital future,* 19 February 2020; B. Custers, H. Ursic, *Big data and data reuse: a taxonomy of data reuse for balanging big data benefits and personal data protection*, in *International Data Privacy Law*, 6(1), 2016; R. Mattera, *Il trattamento dei dati in ambito bancario e finanziario,* in *Circolazione e protezione dei dati personali tra libertà e regole del mercato. Commentario al Regolamento UE n. 679/2016 e al d.lgs. n. 101/2018,* a cura di R. Panetta, Milano, 2019.

256 Commissione Europea, Comunicazione *"A Digital Single Market Strategy for Europe* ", 6 maggio 2015, COM(2015) 192 final.

enunciati dalla strategia sono stati ad oggi parzialmente raggiunti e sono i più variegati includendo, a titolo esemplificativo, la promozione dell'e-commerce, l'eliminazione del *geoblocking*, la modernizzazione delle norme sul *copyright*, l'aggiornamento delle norme dettate nel settore audiovisivo, la creazione di un *level playing field* relativo al settore delle piattaforme online e la realizzazione di un ambiente digitale sicuro[257]. In estrema sintesi, la strategia mira alla creazione nello spazio europeo di un mercato unico digitale regolato da un apparato normativo capace di coniugare strumenti che promuovono lo sviluppo di nuovi servizi digitali e l'utilizzo estensivo dei dati con presidi per gli utenti e per gli operatori che siano in grado di garantire il rispetto dei principi e dei valori posti alla base della tradizione giuridica europea[258].

Accanto alla necessità di promuovere lo sviluppo delle infrastrutture digitali, la Commissione europea ha fin da subito indicato che uno dei primari obiettivi per la piena attuazione del mercato unico digitale risiedesse nella rimozione degli ostacoli "al flusso dei dati attraverso le frontiere e allo sviluppo di servizi nuovi [...]", costituiti per la maggior parte dalla "mancanza di sistemi e servizi aperti e interoperabili e di portabilità dei dati fra servizi"[259]. In altre parole, secondo la Commissione europea non può esistere un mercato unico digitale se, dapprima, non si estenda l'applicazione del principio europeo della libera circolazione anche ai dati in modo tale da configurare uno spazio unico (europeo) aperto ai dati provenienti da tutto il mondo, nel quale questi ultimi, sia personali che non, includendo i dati commerciali sensibili, possano circolare liberamente[260].

257 Ad oggi, nell'ambito della DSM, sono state già adottate numerose iniziative relative al diritto d'autore, al divieto delle pratiche di *geoblocking*, alla protezione dei dati personali e non personali, etc. Per un approfondimento circa gli obiettivi raggiunti si rinvia al sito della Commissione europea https://ec.europa.eu/digital-single-market/ e a V. Elam, *Digital Single Market: a long way to go*, in *Revista d'Internet, Dret i Politica* e *Revista de Internet, Derecho y Politica*, 2018, p. 43 ss.

258 Si ricorda che il 10 maggio 2017 la Commissione europea ha pubblicato la revisione intermedia della sua strategia per il mercato unico digitale, individuando tre ambiti principali in cui dover agire in maniera più incisiva, che sono: 1) sviluppare in maniera completa la *data economy*; 2) risolvere i problemi relativi alla sicurezza informatica; e 3) promuovere le piattaforme *online* in quanto attori responsabili di un ecosistema Interne equo. Con particolare riguardo al settore finanziario, si segnala che è stata recentemente adottata dalla Commissione europea una comunicazione dedicata esclusivamente alla elaborazione di una strategia in materia di finanza digitale dell'UE, che evidenzia come il futuro della finanza nell'Unione sia digitale ed illustra, *inter alia*, le seguenti quattro priorità per la trasformazione digitale nel settore finanziario: (i) affrontare la frammentazione del mercato unico digitale nell'ambito dei servizi finanziari, allo scopo di fornire ai consumatori europei l'accesso a servizi transfrontalieri e di aiutare le imprese finanziarie europee ad espandere la loro operatività digitale; (ii) garantire che il quadro normativo dell'UE agevoli l'innovazione digitale nell'interesse dei consumatori e dell'efficienza del mercato; (iii) creare uno spazio europeo di dati finanziari al fine di promuovere l'innovazione guidata dai dati, partendo dalla strategia europea per i dati, che includa il potenziamento dell'accesso ai dati e della condivisione dei dati all'interno del settore finanziario; (iv) affrontare le nuove sfide e i rischi legati alla trasformazione digitale. Cfr. *Comunicazione relativa a una strategia in materia di finanza digitale per l'UE*, Bruxelles, 24.9.2020 COM(2020) 591 final.

259 Quanto detto si riscontrava già nella sopracitata Comunicazione *"A Digital Single Market Strategy for Europe*". Una ulteriore conferma si trova in alcuni recenti documenti: U. Von der Leyen, *A Union that strives for more, My agenda for Europe, Political Guidelines for the next European Commission 2019 – 2024,* op. cit. e della European Commission, *Communication: Shaping Europe's digital future,* 19 Febbruary 2020, nei quali si evince chiaramente che la strategia in materia di dati è di centrale importanza per la piena attuazione della DSM.

260 Il principio della libera circolazione dei dati si ricava dall'articolo 1, paragrafo 3, del regolamento per la protezione dei dati personali n. 2016/679/EU, in cui è previsto che la libera circolazione dei dati personali "*non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali*". In particolare, come si approfondirà nel corso della presente trattazione, questo regolamento, assieme al regolamento sulla circolazione dei dati non personali n. 2018/1807/EU, contribuisce a realizzare un regime di libera circolazione di "tutti"

Gli sforzi e le proposte presentate dalla Commissione europea per la realizzazione di questo primario obiettivo hanno rapidamente condotto a numerosi dibattiti dovuti alla estrema eterogeneità dei dati presenti nel mondo digitale (commerciali, personali, sensibili, anonimi, pseudonimizzati) cui si associano diversi diritti e valori, anch'essi da dover preservare. In breve, il legislatore europeo ha escluso l'adozione di un approccio open[261], basato cioè sulla previsione di un generale obbligo di condivisione dei dati, preferendo l'adozione di una serie di fonti normative che, congiuntamente, definiscono un regime di portabilità dei dati nello spazio giuridico europeo, che applica ai dati il principio di libera circolazione bilanciandolo con gli altri diritti e valori (quali la protezione dei dati personali, i diritti di privativa intellettuale, la protezione del consumatore, l'osservanza delle regole concorrenziali e di sicurezza) di volta in volta coinvolti in base alla natura, alle finalità e alla tipologia dei dati stessi. Tra gli atti normativi di maggior rilievo che ne sono scaturiti si annoverano, per la loro portata orizzontale, il Regolamento europeo per la protezione dei dati personali[262] (o GDPR) ed il Regolamento sulla libera circolazione dei dati non personali[263], che assieme instaurano nel mercato interno un regime di portabilità dei dati personali e non personali[264]. Si aggiungono, inoltre, una serie di normative di carattere verticale che, direttamente o indirettamente, prevedono regimi specifici di portabilità e di condivisione dei dati che integrano quanto previsto dai suddetti regolamenti con riferimento a specifici settori di mercato. Tra le più rilevanti, con riguardo al settore pubblico, si registrano la Direttiva Open Data[265], che stabilisce norme e modalità pratiche per favorire il riutilizzo delle informazioni contenute nei documenti posseduti da enti pubblici e dalle imprese pubbliche, e la recente Proposta di Atto sulla Governance sui Dati[266], che integra la predetta direttiva con il fine di creare un quadro armonizzato per lo scambio di dati ed il riutilizzo dei medesimi e di istituire un regime di notifica e vigilanza per la fornitura di servizi di condivisione dei dati. Con riferimento al settore bancario e finanziario[267],

i dati nell'UE. Le basi per l'instaurazione di tale regime si sono poste con l'adozione della Comunicazione della Commissione del 10 gennaio 2017 "*Costruire un'economia dei dati europea*" (COM(2017) 9 final. Si veda, inoltre: Commissione europea, Comunicazione "*Una strategia europea per i dati*", 19 febbraio 2020, COM(2020) 66 final, p. 1 – 5.

261 *Ibidem*, p. 4 ss. In particolare, occorre osservare che la scelta di campo di non adottare un obbligo generalizzato di condivisione dei dati segue la tesi dottrinaria che considera la *privacy* e la protezione dei dati personali come diritti fondamentali della persona e che propone l'interpretazione estensiva dell'art. 8 della Carta dei diritti fondamentali, la qualificazione estensiva del diritto alla *privacy*, la valorizzazione del consenso e del recesso ed il rafforzamento dei controlli sul mercato digitale, concludendo con l'affermazione "meglio controllare il processo che liberalizzarlo concedendo diritti di proprietà".

262 Regolamento generale sulla protezione dei dati (UE) 2016/679.

263 Regolamento (UE) 2018/1807 relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea.

264 In materia di dati, occorre menzionare anche il regolamento sulla cybersicureza (UE) 2019/881 e la direttiva sull'apertura dei dati (UE) 2019/1024, che contribuiscono a dare impulso allo sviluppo dell'economia dei dati seppur, la prima, concentrandosi sui profili della sicurezza, e la seconda, sul settore pubblico.

265 Direttiva (UE) 2019/1024 relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico.

266 Proposta di Regolamento relativo alla *governance* europea dei dati, Bruxelles, 25.11.2020 COM(2020) 767 final 2020/0340 (COD).

267 All'uopo, è doveroso segnalare che il 24 settembre 2020 è stato recentemente adottato a livello europeo un pacchetto legislativo su *Digital Finance*, che include sia una *Digital Finance Strategy* che una *Retail Payment Strategy*. composti da tre proposte di regolamento ed una proposta di direttiva. Tali iniziative legislative sono in particolare finalizzate alla creazione di uno spazio unico europeo dei dati finanziari, promuovendo l'*Open Finance* e l'utilizzo delle nuove tecnologie quali i *cryptoasset*, *stablecoin* e la DLT.

invece, assumono particolare rilievo la Direttiva relativa ai mercati degli strumenti finanziari[268] (MiFIDII) e la Direttiva relativa ai servizi di pagamento[269] (PSD2), che hanno indubbi riflessi sul fenomeno FinTech e che prevedono, la prima, in materia di servizi di investimento, una elevata trasparenza del mercato e maggiori tutele nella circolazione dei dati, e la seconda, in materia bancaria, la possibilità per soggetti terzi di prestare servizi di pagamento consentendogli l'accesso e l'utilizzo di infrastrutture bancarie già esistenti[270]. Infine, sempre a livello verticale, si registrano interventi legislativi sia con riferimento al settore audiovisivo, che ha assistito all'adozione del Regolamento sui contenuti audiovisivi che instaura nel mercato interno un regime di portabilità transfrontaliera dei servizi di contenuti *online* per gli utenti[271], sia in quello delle comunicazioni elettroniche, che è invece in attesa della prossima adozione della proposta di Regolamento e-privacy[272], la quale comporterà notevoli novità rispetto all'attuale disciplina contenuta nella Direttiva e-Privacy del 2002 in materia di *marketing*, e-Commerce, *call center* e di pubblicità *online.*

Ebbene, chiarito il quadro normativo dedicato alla portabilità dei dati nel mercato unico digitale, stante l'impossibilità di analizzarne tutti gli aspetti in un singolo intervento, i successivi paragrafi sono dedicati a offrire una panoramica generale delle normative che, aventi carattere orizzontale, ne delineano i tratti essenziali e sono applicate trasversalmente. L'analisi comprenderà, pertanto, le norme in tema di portabilità dei dati previste nel GDPR (paragrafo II), quelle previste nel Regolamento sulla libera circolazione dei dati non personali (paragrafo III) e, infine, una breve disamina delle novità che le recenti iniziative legislative della Commissione potrebbero apportare al mercato europeo dei dati (paragrafo IV).

4.2 Il diritto alla portabilità dei dati nel Regolamento europeo per la protezione dei dati personali

4.2.1 Nozione, *ratio* e ruolo nel mercato unico digitale

Il diritto alla portabilità dei dati personali è disciplinato all'art. 20 del GDPR e si presenta come un diritto complesso, che include[273], in primo luogo, il diritto di ricevere dal titolare del trattamento i propri dati personali in un formato strutturato, di

268 Direttiva (UE) 2014/65 relativa ai mercati degli strumenti finanziari.

269 Direttiva (UE) 2015/2366 sui servizi di pagamento.

270 La direttiva ha, inter alia, avuto l'effetto di eliminare il monopolio della gestione dei conti correnti online delle banche, il cui mercato è oggi aperto anche ai c.d. Third Service Providers, compiendo così un deciso passo in avanti verso l'Open Banking. Per un approfondimento sul tema si rinvia alle trattazioni successive nel presente Quaderno.

271 Regolamento (UE) 2017/1128 relativo alla portabilità transfrontaliera di servizi di contenuti online nel mercato interno.

272 Proposta di relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche, Regolamento Bruxelles, 10.1.2017 COM(2017) 10 final 2017/0003.

273 E' oggetto di discussione in dottrina se il diritto alla portabilità contenga due oppure tre pretese. Gli autori che ritengono che esso si componga di tre pretese: *G. Malgieri, Il diritto alla portabilità dei dati personali*, in *Manuale per il trattamento dei dati personali*, a cura di Comandé e Malgieri, Milano, 2018, p. 54; S. Troiano, *Il diritto alla portabilità dei dati personali*, in *Persona e mercato dei dati. Riflessioni sul GDPR*, op. cit., p. 195; P. De Hert, V. Papakonstantinou, G. Malgieri, L. Beslay, I. Sanchez, *The right to data portability in the GDPR: Towards user-centric interoperabilità of digital services*, in *Computer Law & Security Review*, 2018, p. 196; L. Somaini, *The right of data portability and user control: ambitions and limitations*, op.cit., p. 165. Tra gli autori che ritengono che esso si componga di due pretese si

uso comune e leggibile da dispositivo automatico e, in secondo luogo, il diritto di trasmettere i predetti dati ad un altro titolare (trasmissione indiretta) o, se tecnicamente fattibile, di ottenerne la trasmissione diretta dal primo titolare ad un altro (trasmissione diretta).

L'istituto trova la sua collocazione sistematica tra i diritti di controllo attribuiti agli interessati e viene generalmente considerato come un'evoluzione del diritto di accesso[274]. Evoluzione, che consente oggi di affermare l'evidente differenza tra i medesimi diritti. Mentre il diritto di accesso si limita ad attribuire agli interessati presidi finalizzati a garantire la conoscenza della qualità e del tipo dei propri dati personali detenuti da terzi, il diritto alla portabilità dei dati personali attribuisce agli interessati diritti ben più incisivi, per i quali l'operazione di accesso rappresenta un mero presupposto applicativo[275]. Il diritto alla portabilità dei dati personali, difatti, attribuisce sia il diritto di ricevere i propri dati personali, sia quello di richiederne la trasmissione (in maniera diretta o indiretta), consentendo all'interessato di incidere direttamente sulla sfera giuridica dei titolari di trattamento, che saranno obbligati ad adempiervi. Il diritto in esame può pertanto essere collocato tra i diritti che attuano il c.d. principio della autodeterminazione informativa[276], che orienta ormai da anni gli studiosi e il legislatore verso una rinnovata e più ambiziosa nozione di *privacy,* tale da comprendere non solo il diritto alla riservatezza, ma anche il diritto alla protezione dei dati personali, inteso come complesso di diritti aventi il fine di attribuire agli individui una tutela

veda: F. Pezza, *Diritto alla portabilità dei dati*, in *GDPR e normativa Privacy. Commentario,* a cura di Riccio, Scorza e Belisario, Milano, 2018, p. 201 ss.; G.M. Riccio, (e F. Pezza), *Portabilità dei dati personali e interoperabilità*, in *I dati personali nel diritto europeo*, a cura di Cuffaro, D'Orazio e Ricciuto, Torino, 2019, p. 397 ss.; L. Bianchi, *Il diritto alla portabilità dei dati*, in *Circolazione e protezione dei dati personali, tra libertà e regole del mercato,* in Commentario al Regolamento UE n. 2016/679 (GDPR) e al novellato d.lgs. n. 196/2003 (Codice Privacy), a cura di Panetta, Milano, 2019, p. 225; G. Palma, *La portata fortemente innovativa del diritto alla portabilità dei dati come articolato nel GDPR e nelle linee guida WP29*, in *Data Protection Law – Riv. Giuridica,* n. 2/2019, p. 52.

274 Sul diritto alla portabilità come evoluzione del diritto di accesso si veda, tra gli altri, M. Giorgianni, *Il "nuovo" diritto alla portabilità dei dati personali. Profili di diritto comparato*, in *Contratto e impresa,* 4/2019, p. 1401 e ss.; e A. Ricci, *I diritti dell'interessato*, in *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018 n. 101*, a cura di Finocchiaro, Milano, 2019, p. 219. Per una efficace disamina delle differenze tra il diritto alla portabilità dei dati personali ed il diritto di accesso si veda M. Giorgianni, *Il "nuovo" diritto alla portabilità dei dati personali. Profili di diritto comparato*, op. cit., p. 1403 e ss.; L. Bianchi, *Il diritto alla portabilità dei dati*, in *Circolazione e protezione dei dati personali, tra libertà e regole del mercato*, op. cit., p. 226.

275 Si pensi, invero, che è ben possibile esercitare la portabilità sui propri dati personali senza accedervi, inoltrando semplicemente la richiesta al titolare di trattamento.

276 Tale principio è ricavato dalla disciplina dettata nell'art. 8 della Carta dei diritti fondamentali dell'Unione europea e nell'art. 16, par 1, del Trattato sul funzionamento dell'Unione europea, che qualificano i dati personali come espressione della persona e specificazione del diritto della personalità. Si veda, tra i vari, M. Giorgianni, *Il "nuovo" diritto alla portabilità dei dati personali. Profili di diritto comparato*, op. cit., p. 1397; M. Borghi, *Portabilità dei dati e regolazione dei mercati digitali*, in *Mercato concorrenza regole*, a. XX, n. 2, 2018, p. 225 -226; V. Falce, G. Finocchiaro, *La digital devolution nel settore finanziario. Una nota di metodo*, op. cit., p. 320; G. Finocchiaro, *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, in *Le riforme del diritto italiano*, Bologna, 2017, p. 6; Graef, I., Husovec, M., & Purtova, N. (2018). Data *portability and data control: Lessons for an emerging concept in EU law. German Law Journal*, *19*(6), 1365 ss. https://static1.squarespace.com/static/56330ad3e4b0733dcc0c8495/t/5c05ba070e2e72aaf4f621dc/1543879175464/3_Vol_19_No_06_Graef_ET_Final.pdf.

dinamica delle proprie informazioni personali (es. mediante l'attribuzione di diritti di controllo e di gestione)[277].

Quanto detto consente di cogliere a pieno la *ratio* dell'istituto: il diritto alla portabilità dei dati personali ha l'obiettivo di rafforzare i diritti degli individui nell'ecosistema digitale, consentendogli di accedere, controllare e gestire i propri dati personali. In quest'ottica si può agevolmente affermare che i nuovi diritti di controllo attribuiti agli interessati ai sensi dell'art. 20 del GDPR assumono un ruolo di estremo rilevo nell'ambito del terzo pilastro della strategia per il mercato unico digitale[278], contribuendo significativamente a rafforzare la fiducia degli individui nei servizi digitali mediante la predisposizione di maggiori diritti a loro tutela. Ma vi è di più. Il diritto alla portabilità dei dati personali, consentendo agli interessati di far circolare i propri dati da un ambiente IT ad un altro, ha inevitabilmente instaurato un regime di libera circolazione dei dati personali nell'Unione[279]. Questo regime, come sarà approfondito nel corso della trattazione, produce rilevanti effetti che vanno oltre la materia della *privacy*, incidendo sulle dinamiche concorrenziali del mercato unico digitale mediante la prevenzione e il contrasto di alcune delle pratiche anticoncorrenziali poste in essere dagli operatori di settore[280].

277 Rodotà, *Il mondo nella rete. Quali i diritti, quali i vincoli*, op. cit., p. 28-29. Si deve inoltre notare che parla di "controllo sui propri dati personali" il *Considerando* n. 68 del GDPR, relativo alla portabilità dei dati e che tale inquadramento non è discusso in dottrina (si veda nota 25).

278 E' discusso se il diritto alla portabilità dei dati personali sia un diritto nuovo o meno. In particolare, non sono mancati autori che hanno evidenziato come, in realtà, il diritto alla portabilità poteva essere già ricompreso, implicitamente, nell'art. 8 della Carta dei diritti fondamentali dell'Unione europea e, espressamente, nella Direttiva in materia di servizi telefonici, che ha previsto la portabilità del numero telefonico consentendo agli utenti di cambiare il gestore del servizio conservando il proprio numero telefonico (c.d. mobile data portability), e nella PSD2, che ha introdotto in materia bancaria la portabilità dei dati dei conti del cliente presso un istituto bancario a favore dei servizi di pagamento. Cfr. tra i vari: M. Giorgianni, *Il "nuovo" diritto alla portabilità dei dati personali. Profili di diritto comparato*, op. cit., p. 1398 ss.; L. Bianchi, *Il diritto alla portabilità dei dati*, op.cit., p. 227, in cui la portabilità viene ricondotta tra i *"control rights"* e dove viene ben illustrato che il concetto di portabilità non è nuovo, ma nuovi sono gli elementi caratterizzanti del diritto alla portabilità dei dati personali. Inoltre, tra gli autori che individuano la novità del diritto alla portabilità dei dati personali proprio nella intrinseca polifunzionalità della portabilità si annoverano, tra gli altri: S. Troiano, *Il diritto alla portabilità dei dati personali*, in *Persona e mercato dei dati. Riflessioni sul GDPR*, op. cit., p. 202 e 207 e ss.; A. Ricci, *I diritti dell'interessato*, in *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018 n. 101*, op. cit., p. 219 – 220.

279 Il principio della libera circolazione dei dati personali si ricava dall'art. 1, paragrafo 3, del GDPR, che prevede espressamente 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" ed il diritto alla portabilità dei dati personali ne rappresenta il principale strumento attuativo.

280 Sugli effetti concorrenziali derivanti dall'introduzione del diritto alla portabilità dei dati personali si veda, tra i vari: R. H. Weber, *Data Portability and Big Data Analytics. New Competition Policy Challenges*, op. cit., p. 63 ss.; L. Bianchi, *Il diritto alla portabilità dei dati*, in *Circolazione e protezione dei dati personali, tra libertà e regole del mercato*, op. cit., p. 235; M. Borghi, *Portabilità dei dati e regolazione dei mercati digitali*, op. cit., p. 245 ss.; O. Lynskey, *Alagning data protection rights with competition law remedies? The GDPR right to data portability,* in *European Law Review*, 42(6), 2017, p. 794 ss.; Diker Vanberg, Aysem and Ünver, Mehmet B. (2017) *The right to data portability in the GDPR and EU competition law : odd couple or dynamic duo?*, in *European Journal of Law and Technology*, 8 (1). ISSN 2042-115X, p. 6 ss.; Graef, Inge and Verschakelen, Jeroen and Valcke, Peggy, *Putting the Right to Data Portability into a Competition Law Perspective* (2013). *Law: The Journal of the Higher School of Economics*, Annual Review, 2013, p. 6 ss. Questi profile sono stati anche evidenziati in varie relazioni destinate alla Commissione e ai governi degli Stati membri. Su tutte, si veda: Cremer, deMontjoye, Schweitzer, *Competition policy for the digital era*; Furman, *Unlocking digital competition*.

4.2.2 Ambito di applicazione

Il diritto alla portabilità di cui all'art. 20 del GDPR si compone non solo di nuovi poteri di controllo che incidono su soggetti terzi, ma anche di un nuovo oggetto: i dati personali. Questi sono definiti all'articolo 4, n. 1), del medesimo GDPR come "*qualsiasi informazione riguardante una persona fisica identificata o identificabile*" ove, come è stato affermato[281], l'uso dell'espressione "qualsiasi informazione" sottende la volontà del legislatore di attribuire un'accezione estesa alla nozione di dato personale, tale da comprendere "*potenzialmente ogni tipo di informazioni, tanto oggettive quanto soggettive, sotto forma di pareri o di valutazioni, a condizione che esse siano "concernenti" la persona interessata*"[282]. La generica formulazione della definizione di dato personale e la sua crescente interpretazione estensiva elaborata in sede europea non permettono una nitida ricostruzione dell'ambito applicativo del diritto alla portabilità dei dati personali. Ad ogni modo, esse consentono fin da subito di affermarne una portata che si estende in tutti i settori dell'economia ove sono presenti dati connessi "*[...] a una determinata persona in ragione del suo contenuto, della sua finalità o del suo effetto*"[283], e anche a quelli in cui vi sono dati anonimi e non personali, a condizione che questi siano trattati dai titolari utilizzando strumenti di *data analytics* che consentono l'identificazione dell'interessato[284].

L'ambito di applicazione della norma è tuttavia circoscritto da alcune limitazioni territoriali e oggettive[285]. Le prime si ricavano dalla disciplina generale prevista dall'articolo 3 del GDPR, che prevede l'applicazione del regolamento, per un verso, al trattamento dei dati personali che viene effettuato da un titolare di trattamento (o da un responsabile) stabilito nell'Unione europea, a prescindere dal fatto che il trattamento avvenga effettivamente nel medesimo territorio; per altro verso, al trattamento dei dati personali che viene effettuato da un titolare (o da un responsabile) che non è stabilito nell'Unione europea, ma solo nel caso in cui detto trattamento abbia ad oggetto i dati personali di un interessato che si trova nell'Unione europea e quando riguardi, alternativamente, l'offerta di beni o la prestazione di servizi al suddetto interessato nell'Unione europea[286] o il monitoraggio del suo comportamento nella misura in cui tale comportamento abbia luogo all'interno dell'Unione europea. In particolare,

281 Causa C-434/16, *Peter Nowak c. Data Protection Commissioner* (2017), §34. Tale pronuncia segue il filone dottrinario, notoriamente garantista, già citato nella nota 15, secondo il quale il dato personale deve essere inteso come una proiezione della persona, che ne compone l'identità digitale. Nello stesso senso, si veda G. Alpa, *La "proprietà" dei dati personali*, cit., p. 17, 33, il quale osserva che una conferma alla concezione "garantista" della tutela dei diritti della personalità si può ricavare dalla previsione sulla responsabilità extracontrattuale per la violazione degli obblighi previsti nel GDPR, dal momento che l'art. 82 del medesimo individua l'antigiuridicità del fatto nel trattamento effettuato in violazione delle disposizioni del regolamento stesso.

282 Ibidem.

283 Ibidem.

284 Come vedremo, far rientrare determinate categorie di dati piuttosto che altre entro l'ambito applicativo della portabilità può condurre alla produzione di effetti concorrenziali diametralmente opposti, privilegiando un mercato aperto che stimola la concorrenza ovvero un mercato chiuso che incentiva all'innovazione.

285 Per un approfondimento si rinvia, su tutti a: L. Somaini, *The right of data portability and user control: ambitions and limitations*, op.cit., p. 184 ss.

286 All'uopo, la norma precisa che detta offerta non debba contenere necessariamente l'obbligo di un pagamento da parte dell'interessato.

da una lettura a contrario della predetta disposizione si deduce che il diritto alla portabilità può in concreto trovare applicazione solamente in una delle seguenti ipotesi: 1) quando i dati personali sono trattati nell'Unione europea da un titolare di trattamento (o da un responsabile) che sia stabilito nell'Unione europea; 2) quando i dati personali sono trattati al di fuori dell'Unione europea da un titolare di trattamento (o da un responsabile) che sia stabilito nell'Unione europea; e 3) quando i dati personali riguardanti un interessato che si trova nell'Unione europea sono trattati da un titolare di trattamento (o da un responsabile) che sia stabilito al di fuori dell'Unione europea al fine di offrire beni o servizi ai medesimi interessati nel territorio dell'Unione ovvero per monitorare il comportamento dei medesimi quando questo abbia luogo nell'Unione.

Quanto alle limitazioni oggettive, queste sono invece disciplinate direttamente dall'articolo 20 del GDPR che, come anticipato, è stato elaborato dal legislatore europeo nella piena consapevolezza di dover bilanciare i differenti interessi coinvolti nell'ambito del trasferimento dei dati personali, come l'interesse alla libera circolazione dei dati personali, l'interesse a incentivare l'innovazione nell'ambito dei servizi digitali e l'interesse a rafforzare la protezione dei dati personali e la loro sicurezza[287]. La norma, in particolare, delimita l'ambito applicativo del diritto alla portabilità ai soli dati personali che siano trattati mediante l'impiego di mezzi automatizzati e sulla base del consenso prestato dell'interessato per una o più specifiche finalità[288] ovvero ai fini dell'adempimento di obblighi contrattuali che derivino da un accordo stipulato tra il titolare e l'interessato[289]. Al di fuori dei predetti casi, pertanto, i dati personali non possono essere oggetto di portabilità (i.e. nel caso in cui i dati personali siano trattati in maniera non automatizzata ovvero quando i medesimi siano trattati per adempiere a funzioni pubbliche ovvero a un obbligo di legge[290]). Una eccezione all'anzidetta affermazione si riscontra tuttavia con riguardo ai dati personali oggetto di trattamento parzialmente automatizzato che, secondo l'orientamento prevalente, sono anch'essi soggetti alla disciplina di cui all'art. 20 del GDPR. Tale orientamento si basa in particolare su una duplice argomentazione: la prima, di carattere letterale, rileva come l'art.

287 Cfr. *Considerando* n. 4 del GDPR, in cui è prevista l'applicazione del principio di proporzionalità nel bilanciamento tra i diversi diritti e valori che si applicano in materia di dati personali. In particolare, nel medesimo *Considerando* si prevede che "Il trattamento dei dati personali dovrebbe essere al servizio dell'uomo. Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità. Il presente regolamento rispetta tutti i diritti fondamentali e osserva le libertà e i principi riconosciuti dalla Carta, sanciti dai trattati, in particolare il rispetto della vita privata e familiare, del domicilio e delle comunicazioni, la protezione dei dati personali, la libertà di pensiero, di coscienza e di religione, la libertà di espressione e d'informazione, la libertà d'impresa, il diritto a un ricorso effettivo e a un giudice imparziale, nonché la diversità culturale, religiosa e linguistica".

288 Cfr. art. 6, comma 1, lett. a), GDPR. Qualora si tratti di dati sensibili, il consenso dovrà essere invece prestato ai sensi dell'art. 9, comma 2, lett. a) del medesimo Regolamento.

289 Cfr. art. 6, comma 1, lett. b), GDPR.

290 Quanto detto trova conferma nel *Considerando* n. 68 del GDPR che prevede che "[...]Tale diritto dovrebbe applicarsi qualora l'interessato abbia fornito i dati personali sulla base del proprio consenso o se il trattamento è necessario per l'esecuzione di un contratto. Non dovrebbe applicarsi qualora il trattamento si basi su un fondamento giuridico diverso dal consenso o contratto. Per sua stessa natura, tale diritto non dovrebbe essere esercitato nei confronti dei titolari del trattamento che trattano dati personali nell'esercizio delle loro funzioni pubbliche. Non dovrebbe pertanto applicarsi quando il trattamento dei dati personali è necessario per l'adempimento di un obbligo legale cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento [...]".

20 del GDPR non faccia menzione di un eventuale impiego "esclusivo" di mezzi automatizzati per il trattamento dei dati personali; la seconda, di carattere sistematico, evidenzia come l'art. 20 del GDPR debba essere letto in combinato disposto con l'art. 2, comma 1, del medesimo Regolamento, che enuncia il principio della parificazione dei trattamenti "interamente" automatizzati con quelli che lo sono anche solo "parzialmente"[291].

In secondo luogo, l'esercizio della portabilità dei dati personali deve necessariamente riguardare solo i dati personali che sono forniti dall'interessato. Tenendo a mente l'eterogeneità delle forme di raccolta dei dati attuate nel mercato unico digitale (fornitura diretta, fornitura indiretta, raccolta passiva di dati dalle attività dell'utente, etc.) non sorprenderà che, fin dall'emanazione della norma, anche tale limitazione abbia destato numerose perplessità. In particolare, non sono mancate critiche da parte degli operatori di settore che hanno evidenziato come la genericità della nozione di "dati forniti dall'interessato" instauri un clima di incertezza relativo all'inclusione o meno, entro l'ambito di applicazione del diritto alla portabilità, di tutte quelle forme di raccolta dei dati personali diverse dalla fornitura diretta. A tal riguardo, un po' di chiarezza è stata fatta dal *Working Party 29* (WP29) nelle cui Linee Guida si illustra[292], in estrema sintesi, che per "dati forniti dall'interessato" non si devono intendere solamente tutti i dati attivamente e consapevolmente trasmessi dall'individuo, ma anche quelli raccolti dalle attività dell'utente durante la fruizione di un servizio o l'utilizzo di un dispositivo (c.d. dati osservati), quali ad esempio le informazioni attinenti alle ricerche sul web, i dati di traffico telefonico, i dati di localizzazione e i dati inerenti le transazioni effettuate tramite conto corrente bancario. Sono invece esclusi dai "dati forniti dall'interessato" tutti quei dati (c.d. derivati o inferiti) che il titolare deduce da altri dati utilizzando tecniche di analisi volte ad individuare correlazioni statistico-probabilistiche ivi ricorrenti (si pensi, ad esempio, ai dati relativi ai profili creati dal titolare sulla base di un'attività di monitoraggio della navigazione dell'utente; nel settore finanziario, ai dati utilizzati al fine di attribuire uno *score* creditizio)[293].

La scelta di non includere i dati derivati tra i dati che rientrano nell'oggetto della portabilità discende dall'obiettivo che il diritto alla portabilità si pone nel bilanciare l'interesse alla libera circolazione dei dati, finalizzato a stimolare la concorrenza fra i servizi, con quello di tutelare i diritti di proprietà intellettuale, indirizzato invece a incentivare l'innovazione. In altre parole, tenuto conto che la creazione dei dati derivati comporta un investimento economico per le imprese (titolari di trattamento) si è

291 Article 29 Data Protection Working Party, *Guidelines on the right to data portability*, WP 242 rev.01, 5 April 2017, p. 9, in cui è affermata la non esclusività dell'impiego di mezzi automatizzati.

292 Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali istituito ai sensi dell'art. 29 della direttiva 95/46/CE. Art. 29 Data Protection Working Party, organo sostituito, a seguito dell'entrata in vigore del GDPR, dal Comitato per la protezione dei dati personali (o EDPB).

293 Per la definizione dei dati derivati si rinvia a: AGCM, AGCOM, Garante per la protezione dei dati personali, *Indagine conoscitiva sui Big Data,* op. cit., p. 55. Per un approfondimento circa la tassonomia dei dati personali e la categorizzazione dei medesimi in dati forniti dall'interessato, dati osservati e dati derivati, si vedano, tra gli altri: OCSE, *Data-driven Innovation for Growth and Well-being, Interim Synthesis Report,* October 2014; Article 29 Data Protection Working Party, *Guidelines on the right to data portability*, WP 242 rev.01, 5 April 2017, p. 10; World Economic Forum, *Near-Term Priorities for Strengthening Trust*, reperibile in https://reports.weforum.org/rethinking-personal-data/near-term-priorities-for-strengthening-trust/.

scelto di escluderli dall'ambito di applicazione della portabilità in modo da consentire alle medesime imprese di ricavarne un vantaggio competitivo[294]. A conferma di quanto detto, come è stato efficacemente osservato in materia bancaria, rendere portabili anche i dati derivati avrebbe comportato, in prima battuta, un disequilibrio mondiale secondo cui i giganti tecnologici extra europei avrebbero beneficiato di tale sistema senza alcun obbligo di reciprocità; in seconda battuta, un disequilibrio tra le imprese nel medesimo spazio europeo, dal momento che le ingenti somme da alcune di esse investite in strumenti tecnologici per la rielaborazione dei dati non si sarebbero tradotte in alcun vantaggio competitivo perché, in seguito a richieste di portabilità, avrebbero dovuto trasmettere gratuitamente i propri risultati a imprese presumibilmente concorrenti[295]. Se le scelte di fondo sono state gradite in linea di massima dagli operatori[296], occorre osservare che la tematica è ancora oggetto di ampie discussioni dal momento che il WP29 ha precisato che la valutazione circa l'appartenenza all'una piuttosto che all'altra categoria va effettuata caso per caso, sulla base delle circostanze specifiche. Nella prassi, infatti, il confine tra i dati osservati e quelli derivati non è così nitido e si viene inevitabilmente a creare una zona d'ombra in cui vi rientrano una molteplicità di dati la cui categorizzazione è incerta o, quantomeno, dubbia[297]. Il fatto che sussistano tali difficoltà di categorizzazione è indubbiamente uno dei temi più caldi nell'ambito della portabilità dei dati personali in quanto l'inclusione di determinati tipi di dati in una categoria piuttosto che in un'altra esclude, o meno, l'applicazione del diritto e, conseguentemente, produce rilevanti effetti sul mercato concorrenziale con il rischio di violare il principio generale della parità di trattamento[298]. A parere dello scrivente è pertanto auspicabile l'adozione (anche a livello di soft law da parte dell'EPDB) di criteri parzialmente flessibili, sulla scorta della tecnica utilizzata nell'ambito del Digital Service Act Package[299], che consentano una agevole categorizzazione di tutti i tipi di dati, anche futuri, in modo tale da garantire un equo trattamento di tutti i titolari di trattamento e una uniforme intensità della tutela dei dati personali in favore degli interessati.

In terzo luogo, secondo una lettura a contrario dell'art. 20 del GDPR, i dati personali oggetto di portabilità non possono consistere né in dati anonimi né in dati

294 Le tecniche automatizzate di *Big Data analytics* basate su dati personali possono essere impiegate per identificare trend comportamentali degli interessati e per estrarre conoscenza predittiva, allo scopo di orientare decisioni in riferimento a persone o gruppi. Tale processo determina implicazioni in riferimento al rispetto dei diritti fondamentali, tra i quali il diritto alla vita privata, alla protezione dei dati e alla loro sicurezza, la libertà di espressione e di non discriminazione. Per un approfondimento di tali tematiche si rinvia ai documenti indicati nella nota precedente.

295 European Banking Federation, *Data Usage, Access & Sharing in the Digital Economy*, doc. N. 039811, Jan 2020, p. 2 ss.

296 Ciò si è rinvenuto in particolar modo in ambito bancario. Si veda la nota 43.

297 L. Bianchi, *Il diritto alla portabilità dei dati*, op. cit. p. 231, che con riferimento alle limitazioni del diritto alla portabilità parla espressamente di zona d'ombra riferendosi alla difficile opera da parte degli interpreti di distinguere i dati osservati da quelli derivati.

298 Difatti, qualora più operatori che concorrono nel medesimo settore raccolgano dati personali mediante tecniche di raccolta molto similari, ma non identiche, sorgerebbe il rischio di una differente qualificazione di detti dati (gli uni come dati osservati e gli altri come dati derivati), palesandosi pertanto una violazione del principio della parità di trattamento: l'operatore che ha raccolto ed elaborato i dati qualificati come dati osservati dovrà sottostare a obblighi e responsabilità più stringenti rispetto a quelli applicabili all'operatore concorrente.

299 A tal riguardo, si rinvia al paragrafo IV della presente trattazione.

che non sono riferiti all'interessato[300]. Tale esclusione è fondata sulla definizione stessa di dati personali che, come anzidetto, comprende tutti quei dati che *"identificano o rendono identificabile una persona fisica [...]"* e, pertanto, non sembra richiedere un particolare approfondimento. Tuttavia, una questione che è stata fortemente dibattuta in tale ambito riguarda la categorizzazione dei dati "pseudonimizzati"[301], che rappresentano una categoria *sui generis* di dati in quanto sono veri e propri dati personali trattati in modo tale da non essere attribuibili all'interessato senza l'utilizzo di informazioni aggiuntive (che, secondo quanto previsto dal GDPR, devono in ogni caso essere conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile). Nonostante le iniziali difficoltà, il WP29 sembra aver trovato una soluzione che, nello specifico, qualifica i dati pseudonimizzati come dati che possono costituire oggetto di richieste di portabilità alla condizione che i medesimi possano essere chiaramente riconducibili all'interessato (ad esempio, nel caso in cui l'interessato medesimo metta a disposizione del titolare di trattamento del dato pseudonimizzato un elemento che lo identifichi)[302].

Infine, l'ultima limitazione al diritto alla portabilità trova espressa previsione normativa nell'art. 20, paragrafo 4, del GDPR ai sensi del quale la richiesta di portabilità non deve ledere i diritti e le libertà di terzi[303]. Come chiarito nel Considerando n. 68 del GDPR, non si tratta di una limitazione relativa allo scopo o alla finalità del riutilizzo dei dati, ma di una limitazione alle violazioni di diritti e libertà di terzi che possono in concreto accadere nel caso in cui la trasmissione di dati da un titolare all'altro comporti una preclusione in capo a terzi di esercitare uno dei diritti previsti nel regolamento e, in particolare, nei casi in cui nel data set trasferito siano inclusi dati personali di terzi. Al fine di evitare di commettere tali violazioni, le Linee Guida del WP29 raccomandano l'individuazione di una base giuridica di trattamento dei dati personali di terzi, che sia diversa dal consenso o dal contratto posti alla base del trattamento dei dati personali relativi al soggetto che richiede la portabilità (ad esempio, il legittimo interesse ai sensi dell'articolo 6, par. 1, lett. (f) quando la finalità del titolare del trattamento consiste nel fornire un servizio al titolare che permetta a quest'ultimo di trattare i dati personali con finalità puramente personali)[304]. Ad ogni modo, come è stato sostenuto[305], i suddetti rischi sembrano assumere rilevanza solo in una ipotesi circoscritta, ovverosia qua-

300 Della definizione di "dati anonimi" non vi è traccia nel GDPR. Tuttavia, essa può essere ricavata dal *Considerando* n. 26, in cui si prevede che i "[...] principi di protezione dei dati non dovrebbero pertanto applicarsi a informazioni anonime, vale a dire informazioni che non si riferiscono a una persona fisica identificata o identificabile o a dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato".

301 Secondo l'art. 4, paragrafo 5, del GDPR, i dati pseudonimizzati sono i dati personali che sono trattati "in modo tale che non possano più essere attribuiti a un interessato specifico 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 che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile".

302 Article 29 Data Protection Working Party, *Guidelines on the right to data portability*, WP 242 rev.01, 5 April 2017, p. 9.

303 Art. 20, paragrafo 4, del GDPR. Per un approfondimento sul tema, si rinvia a: M. Borghi, *Portabilità dei dati e regolazione dei mercati digitali*, op. cit., p. 254 ss.

304 In tal caso, è opportuno evidenziare che il trattamento dei dati personali sarà sotto la responsabilità esclusiva dell'interessato a condizione che il trattamento non sia in nessuna maniera decisa dal titolare del trattamento.

305 Article 29 Data Protection Working Party, *Guidelines on the right to data portability*, WP 242 rev.01, 5 April 2017, p. 9.

lora il nuovo titolare tratti i dati personali per altre finalità rispetto al primo (ad esempio, per trasmettere promozioni marketing dedicate); diversamente, nei casi in cui il nuovo titolare tratti i dati personali per le medesime finalità (ad esempio, nel caso di trasferimento di contatti e/o storico di transazioni da un Third Party Provider ad un altro), i diritti e le libertà di terzi saranno difficilmente compromessi.

Nell'ambito di quest'ultima limitazione del diritto alla portabilità merita considerazione il caso specifico in cui si pregiudichino i diritti di proprietà intellettuale e i segreti commerciali del titolare del trattamento cui è stata richiesta la portabilità. Questa situazione non è infatti rara tenuto conto che essa può in concreto accadere tutte le volte in cui l'interessato esercita il diritto alla portabilità trasmettendo, direttamente o indirettamente, a un nuovo titolare di trattamento un data set su cui il primo titolare di trattamento vanta diritti di proprietà intellettuale. Come è stato efficacemente osservato[306], tali casi possono in concreto ravvisarsi nelle tre seguenti ipotesi: 1) quando la portabilità sia in conflitto con diritti posseduti dal titolare del trattamento su banche dati (es. raccolta sistematica e metodica in una banca dati può essere oggetto di diritto d'autore o di diritto sui generis); 2) quando la portabilità sia in conflitto con dati personali che contengono informazioni protette come know how riservato o segreti commerciali (es. dati osservati mediante particolari sistemi di data analytics); 3) nel caso in cui il titolare del trattamento sia licenziatario di diritti sui dati che sono oggetto di portabilità, in particolare quando i dati comprendano materiale protetto dal diritto d'autore). Contrapponendo ancora una volta i due distinti obiettivi del mercato unico digitale consistenti nell'incentivo all'innovazione e nello stimolo alla concorrenza dei servizi digitali, il legislatore europeo sembrerebbe aver optato in tali ipotesi per la limitazione del diritto alla portabilità, consentendo ai titolari di diritti di proprietà intellettuale o di segreti industriali di respingere le richieste di portabilità anche in assenza di comportamenti abusivi da parte dell'interessato.

4.2.3 Modalità di esercizio del diritto alla portabilità dei dati personali

La disciplina prevista dall'art. 20 del GDPR e la lettera del Considerando n. 68 del medesimo Regolamento consentono di delineare le modalità di esercizio del diritto alla portabilità dei dati. In linea generale, si distingue l'ipotesi di trasmissione indiretta dei dati personali, che deve avvenire sulla base di "formati interoperabili" e "senza impedimenti" da parte dei titolari di trattamento, da quella di trasmissione diretta, che può essere posta in essere solo "se tecnicamente fattibile".

Il primo requisito richiesto affinché possa concretamente esercitarsi il diritto alla trasmissione indiretta dei propri dati personali consiste quindi nella necessità che i titolari di trattamento coinvolti in detta operazione adottino formati interoperabili[307]. Sebbene il GDPR non offra alcuna definizione di interoperabilità, questa può essere

306 M. Borghi, *Portabilità dei dati e regolazione dei mercati digitali*, op. cit., p. 256 ss.

307 In realtà è bene specificare che più che un requisito l'interoperabilità dei formati rappresenta una raccomandazione da parte dell'Unione, che in tale materia acquisisce una notevole rilevanza persuasiva in quanto estremamente importante per attuare a pieno il diritto alla portabilità dei dati. Cfr. *Considerando* 68 del GDPR, che prevede espressamente un incoraggiamento *"[...] a sviluppare formati interoperabili che consentano la portabilità dei dati"*.

rintracciata nella Decisione 922/2009/EC[308], che la definisce come "*la capacità di organizzazioni diverse e disparate di interagire in vista di obiettivi comuni concordati e reciprocamente vantaggiosi, ricorrendo alla condivisione di conoscenze e informazioni tra le organizzazioni, per mezzo dei processi aziendali che su di esse si basano, tramite lo scambio di dati fra i rispettivi sistemi TIC*". In particolare, abbracciando tale definizione, l'adozione di formati interoperabili si potrebbe definire come l'utilizzazione da parte dei titolari di trattamento di formati che siano in grado di interagire con quelli degli altri titolari e che permettano tecnicamente di scambiarsi i dati[309], consentendo così un più agevole passaggio da un ambiente IT ad un altro. A parere dello scrivente, è questa l'interoperabilità intesa nel GDPR che, come tale, costituisce un caposaldo della portabilità dei dati rappresentando un presupposto imprescindibile al fine di dare piena attuazione al mercato unico europeo di dati e un elemento essenziale per l'attuazione del diritto alla loro portabilità.

Ciò detto, occorre tuttavia evidenziare che in merito alla interoperabilità il legislatore non ha in realtà previsto alcun obbligo giuridico di utilizzare formati specifici né tantomeno di trattare i dati con sistemi compatibili[310], optando invece per l'autoregolamentazione. Nonostante si potrebbe prima facie rimanere sorpresi di questa scelta di politica legislativa, come è stato invece osservato[311], la previsione di un obbligo generalizzato di utilizzare uno specifico formato avrebbe creato delle barriere alla circolazione dei dati nel mercato unico digitale perché, di fatto, è impensabile prestabilire un formato unico per tutti i titolari di trattamento, ciascuno avente differenti capacità economiche, tecniche e gestionali; inoltre, neppure demandare la scelta del formato da utilizzare esclusivamente al mittente ovvero al recipient del dataset trasferito avrebbe rappresentato una previsione adeguata, comportando, nel primo caso, effetti di un lock-in nascosto e, nel secondo caso, il c.d. "effetto Torre di Babele"[312], producendo in ogni caso scarsi risultati in termini di apertura del mercato. Ciò detto, in base ad alcune raccomandazioni provenienti da vari autori e dal Gruppo dei garanti

308 J. Palfrey, U. Gasser, *interop. The Promise and Perils of Highly Interconnected Systems*, New York, Basic Bookes, 2012, p. 5.

309 Come sarà evidenziato nelle successive trattazioni, l'interoperabilità intesa nell'ambito del GDPR non è assimilabile all'interoperabilità cui si riferisce la normativa bancaria, che dispone che gli enti pubblici mettano a disposizione i propri documenti "*in formati aperti e leggibili*", ma solo "*ove possibile e opportuno*" e "*nella misura del possibile*" (art. 5 della PSD2).

310 Article 29 Data Protection Working Party, *Guidelines on the right to data portability*, WP 242 rev.01, 5 April 2017, p. 16 – 17, in cui si suggeriscono due diversi approcci di trasferimento dei dati: 1) trasmissione diretta dell'intero insieme di dati portabili; 2) utilizzo di uno strumento automatizzato che consenta l'estrazione dei dati pertinenti. Le metodologie di trasmissione suggerite riguardano principalmente i sistemi di messaggistica sicura, *server* SFTP, *webAPI* o *webPortal* sicuri. Attraverso tali sistemi, il titolare del trattamento può consentire il *download* delle informazioni attraverso una funzionalità implementata direttamente all'interno dell'area riservata utente, il quale può procedere con il *download* in autonomia. Come osservato nelle medesime Linee Guida, quando la mole di dati è considerevole o in caso di sistemi complessi o di grandi dimensioni, il titolare potrà mettere a disposizione dell'utente (o del nuovo titolare indicato dall'utente) un'interfaccia di programmazione di applicazioni (API), dove, una volta inserite le credenziali di sicurezza (per consentire l'accesso solo agli aventi diritto), verrà messo a disposizione il file richiesto per la sua trasmissione cifrata all'interno dell'ambiente informatico individuato dall'interessato.

311 L. Bianchi, *Il diritto alla portabilità dei dati*, op. cit. p. 235.

312 In un contesto cioè in cui ciascun donor sarebbe tenuto a conoscere e parlare tutte le possibili lingue ovvero al potenziale ricorso a tutti i formati disponibili, anche nella prospettiva di una loro evoluzione tecnologica.

europei[313], si ritiene che l'autoregolamentazione in tema di interoperabilità dei formati si tradurrà prevalentemente nell'adozione di criteri di standardizzazione aventi le finalità di instaurare forme "*[...] di collaborazione tra i produttori e le associazioni di categoria"* e di far adottare ai titolari di trattamento "*[...] un insieme condiviso di standard e formati interoperabili"* e sistemi di *data management* che siano capaci di selezionare adeguatamente i dati da trasferire[314]. L'adozione di tale strategia è particolarmente vantaggiosa in quanto consentirebbe, per un verso, di agevolare l'introduzione di sistemi interoperabili perché sviluppati e condivisi tra gli stessi operatori (titolari di trattamento) e, per altro verso, di garantire un certo grado di funzionalità nella circolazione dei dati, agevolando gli interessati o, nel caso di trasferimento diretto, i secondi titolari di trattamento, a selezionare i soli dati oggetto della richiesta di portabilità[315].

Il secondo requisito relativo alle modalità di esercizio della portabilità è espressamente disciplinato dall'art. 20 del GDPR e consiste, come premesso, nella previsione che ogni trasmissione di dati personali abbia luogo "senza impedimenti" da parte del primo titolare di trattamento. Nella prassi, l'interpretazione estensiva data a tale requisito comporta il sorgere di una duplice obbligazione in capo al titolare di trattamento: egli dovrà rispettare un generico dovere di astensione consistente nel non porre in essere alcun comportamento o attività idonea ad impedire il trasferimento dei dati personali e, in presenza di impedimenti derivanti da soggetti terzi o dal caso fortuito o dalla forza maggiore, dovrà inoltre adottare, per quanto di propria competenza e nei limiti della ragionevolezza, un comportamento positivo finalizzato a rimuoverli. Se quanto detto mette di per sé in luce il notevole impatto che tali obblighi hanno nei confronti dei titolari di trattamento, occorre evidenziare che questo è ulteriormente intensificato dall'accezione estesa attribuita dal WP29 alla nozione di "impedimenti", in cui vengono inclusi non solo gli impedimenti fisici e tecnici, ma anche qualsiasi altro tipo di impedimenti, come ad esempio quelli di carattere legale o finanziario[316].

L'ultimo requisito, previsto dall'art. 20 del GDPR esclusivamente con riferimento alle ipotesi di trasferimento diretto dei dati personali, concerne, come detto, la "fattibilità tecnica". Questa dovrà in particolare essere oggetto di una valutazione effettuata caso per caso dal medesimo titolare che deve tenere conto della sicurezza della comunicazione tra i sistemi dei due titolari coinvolti e della capacità tecnica del

313 Tra i vari si veda: O. Borgogno, *Regimi di condivisione dei dati ed interoperabilità: il ruolo e la disciplina delle A.P.I.*, in Dir. Inf., 2019, p. 690 ss. Si veda, inoltre: R. H. Weber, *Data Portability and Big Data Analytics. New Competition Policy Challenges*, op. cit., p. 71; M. Borghi, *Portabilità dei dati e regolazione dei mercati digitali*, op. cit., p. 233 – 242; L. Bianchi, *Il diritto alla portabilità dei dati,* op. cit. p. 234 ss.; M. Giorgianni, *Il "nuovo" diritto alla portabilità dei dati personali. Profili di diritto comparato*, op. cit., p. 1411; De Hert, V. Papakonstantinou, G. Malgieri, L. Beslay, I. Sanchez, *The right to data portability in the GDPR: Towards user-centric interoperabilità of digital services*, op.cit., 2018, p. 194 ss.; L. Somaini, *The right of data portability and user control: ambitions and limitations*, op.cit., p. 187 – 188.

314 All'uopo occorre osservare che l'UE ha in programma di finanziare l'istituzione di spazi interoperabili comuni di dati a livello dell'UE in settori strategici. Si veda Commissione europea, Comunicazione "*Una strategia europea per i dati*", 19 febbraio 2020, COM (2020) 66 final, p. 19.

315 G. Palma, *La portata fortemente innovativa del diritto alla portabilità dei dati come articolato nel GDPR e nelle linee guida WP29*, in *Data Protection Law – Riv. Giuridica*, n. 2/2019, p. 55 ss.

316 Seguendo alla lettera detto orientamento tutte le pattuizioni contrattuali che oggi subordinano contrattualmente l'adempimento alla richiesta di portabilità al pagamento di un corrispettivo ovvero ad altre condizioni devono essere considerate in violazione dell'art. 20 del GDPR. Cfr. Article 29 Data Protection Working Party, *Guidelines on the right to data portability*, WP 242 rev.01, 5 April 2017, p. 15.

destinatario relativa alla ricezione dei dati oggetto della richiesta di trasferimento. Rispetto ai primi due requisiti analizzati, i quali contribuiscono senza dubbio a incrementare il flusso dei dati personali nell'Unione, questo requisito sembra invece orientarsi in direzione diametralmente opposta, ponendosi piuttosto come una limitazione al diritto alla portabilità, sia pure con esclusivo riferimento all'ipotesi in cui è richiesto il trasferimento diretto dei dati personali[317]. La valutazione circa la fattibilità tecnica di un determinato tipo di trasferimento ricade, invero, nei medesimi titolari di trattamento, che beneficiano di un certo grado di discrezionalità nell'accettare o respingere le richieste e che possono quindi respingere richieste legittime di portabilità. A tal riguardo, al fine di prevenire detti abusi ed evitando allo stesso tempo una regolamentazione troppo rigida, si auspica la predisposizione di ulteriori linee guida dirette ad indicare agli operatori privati precisi parametri oggettivi per la valutazione inerente alla fattibilità tecnica di un trasferimento diretto[318], che potranno rappresentare il punto di riferimento per i medesimi operatori al fine di individuare nei propri codici di condotta le buone prassi da seguire nell'ambito dei trasferimenti diretti di dati personali.

4.2.4 Effetti concorrenziali del diritto alla portabilità dei dati personali

Come premesso, il diritto alla portabilità dei dati personali, quale conseguenza dell'attribuzione di una tutela dinamica ai dati personali, pone le basi all'instaurazione di un regime di circolazione dei dati personali che sembra inevitabilmente agire sulla struttura del mercato unico digitale, condizionandone le dinamiche concorrenziali[319]. In particolare, sono due gli effetti auspicati che il diritto alla portabilità dovrebbe produrre: dal punto di vista del consumatore, la riduzione dei costi di switching e, dal punto di vista delle imprese, la riduzione delle barriere all'entrata.

Quanto al primo effetto, occorre preliminarmente chiarire che i costi di *switching* consistono in tutte quelle pratiche poste in essere dai prestatori di servizi digitali che hanno l'effetto di ostacolare i propri utenti nel passaggio ad un altro fornitore di servizi. Tali pratiche, nella prassi, si traducono nella predisposizione di aggravi di natura tecnica (ad esempio, l'adozione di un formato non interoperabili), economica (ad esempio, rendere eccessivamente oneroso il passaggio ad un altro fornitore di servizi digitali rispetto al costo del servizio stesso) e/o legale (ad esempio, la predisposizione di clausole contrattuali che limitino o escludono la portabilità dei propri dati ad un altro fornitore).

Ciò chiarito, tenuto conto di quanto detto nei paragrafi precedenti, sembra indiscutibile che la struttura del diritto alla portabilità dei dati personali (attribuzione

317 Sulle criticità mosse a tale diritto si veda O. Borgogno, *Regimi di condivisione dei dati ed interoperabilità: il ruolo e la disciplina delle A.P.I.*, op.cit., p. 695 ss.

318 Non è mancato chi ha tuttavia indicato la pericolosità di utilizzare un approccio esclusivamente di *soft law* in quanto lascerebbe agli operatori privati completamente liberi di adottare API (*Application Programming Interface*) poco sicure o difettose amplificando il rischio di sistematiche violazioni. *Ibidem*.

319 Si rinvia alla nota 31.

agli interessati di diritti di controllo sugli stessi e raccomandazione ai titolari di utilizzare formati interoperabili) sia potenzialmente idonea a contrastare e ridurre tali pratiche. Infatti, grazie a detto istituto i fornitori non potranno più opporsi, salvi i casi già analizzati in precedenza, alle richieste di portabilità esercitate dai propri utenti e nemmeno potranno prevedere aggravi tecnici, economici e legali all'esercizio di detto diritto. A titolo esemplificativo, occorre rammentare che, grazie all'introduzione di tale istituto, tutte le clausole contrattuali che prevedevano l'impossibilità di trasmettere i dati personali sono da considerarsi apposte in violazione dell'art. 20 del GDPR.

Come è stato rilevato[320], la riduzione dei costi di switching produrrebbe, a sua volta, effetti benefici a catena per il mercato concorrenziale perché contribuirebbe a contrastare due ulteriori e più generiche pratiche anti-concorrenziali che sono molto frequenti nel mercato unico digitale visto il ruolo ivi predominante dei c.d. effetti *network*: le pratiche di *lock-in* e le barriere all'entrata. Queste pratiche, assieme, hanno infatti fino ad oggi reso il mercato unico digitale un mercato con una concorrenza attenuata, impedendo alle piccole e medie imprese di entrare ad operare nel mercato (digitale) ovvero di competere in maniera equa con le grandi imprese (OTT). La prevenzione e rimozione di queste pratiche rappresenterebbe pertanto il secondo effetto, consequenziale al primo, prodotto dal diritto alla portabilità dei dati personali e che si atteggerebbe quindi, in ambito concorrenziale, come una regola concorrenziale a priori applicabile indistintamente a tutti coloro che trattano dati personali a prescindere dalla sussistenza di posizioni dominanti o di pratiche anticoncorrenziali di esclusione[321]. Orbene, occorre tuttavia evidenziare che, nonostante gli effetti benefici anzidetti, il diritto alla portabilità dei dati non è rimasto scevro da critiche dagli esperti della concorrenza, che hanno evidenziato la pericolosità di avallare un sistema normativo che imponga l'interoperabilità dei formati o, comunque, di altre forme di apertura perché esso disincentiverebbe le imprese all'innovazione. Le medesime critiche hanno inoltre evidenziato che non si devono sottovalutare nemmeno i costi e le difficoltà che possono insorgere durante l'implementazione delle tecniche e dei metodi standardizzati finalizzati a garantire l'interoperabilità in quanto, soprattutto con riferimento ai piccoli e medi prestatori di servizi, questi potrebbero risultare eccessivamente onerosi (si pensi, ad esempio, agli ingenti costi che si devono affrontare in tema di *compliance*)[322]. A tali considerazioni, tuttavia, sembra potersi obiettare che, in primo luogo, il diritto alla portabilità dei dati personali non comporta la cessazione del rapporto di trattamento dei dati con il primo titolare, salvo che ovviamente l'interessato non richieda la cancellazione dei propri dati; pertanto, i titolari di trattamento, seppur non in via esclusiva e fintantoché permanga una base giuridica del trattamento, potranno, a seguito dell'esercizio della portabilità da parte dei propri utenti, continuare a trattenere i loro

320 M. Borghi, *Portabilità dei dati e regolazione dei mercati digitali*, op. cit., p. 241.

321 M. Borghi, *Portabilità dei dati e regolazione dei mercati digitali*, op. cit., p. 245.

322 L'orientamento in esame giunge a tali conclusioni osservando inoltre come nel mercato unico digitale le imprese hanno spesso bisogno di esercitare un controllo esclusivo sui dati forniti dai propri consumatori per sviluppare servizi innovativi e come molti di questi richiedono una certa dimensione di scala, che può essere acquisita e mantenuta solo "trattenendo" i propri utenti all'interno del proprio servizio e che di certo non può essere raggiunta nei primi anni di attività della società. Conseguentemente, si afferma che il controllo esclusivo sui dati e la dimensione di scala sembrano necessari per le imprese al fine di raggiungere un certo posizionamento sul mercato digitale e produrre ricavi rilevanti.

dati personali. In secondo luogo, come è stato efficacemente osservato[323], si rileva che, quale contraltare al disincentivo verso l'innovazione "proprietaria", l'interoperabilità caldeggiata dalla normativa europea e stimolata dagli strumenti di *soft law*, può e dovrà essere orientata verso una innovazione " aperta", nella quale tutti i prestatori di servizi, anche di piccole e medie dimensioni, potranno beneficiare delle innovazioni dei concorrenti. Nella consapevolezza dell'utopistica visione di un'innovazione totalmente "aperta" nell'ambito del mercato unico digitale, è bene ad ogni modo evidenziare che l'intera disciplina in tema di portabilità dei dati, che comprende il GDPR e tutte le altre normative che oggi regolano la portabilità in specifici settori di mercato, non sembra esclusivamente diretta a stimolare la concorrenza tra gli operatori, ma anche ad incentivare tutti gli operatori ad una "innovazione condivisa", consistente nella previsione e condivisione da parte degli stessi di standard tecnici ed organizzativi comuni al fine di condividere più efficacemente i dati[324].

4.2.5 Ulteriori profili del diritto alla portabilità dei dati personali

Per completezza, l'analisi del diritto alla portabilità dei dati personali non può prescindere da una sintetica disamina delle norme che disciplinano la posizione del *titolare-donor* dei dati personali oggetto della richiesta di portabilità[325].

In primo luogo, il *titolare-donor* (al pari del *titolare-recipient*) è soggetto a precisi obblighi di informativa nell'ambito di un'operazione di portabilità dei dati personali. Tali obblighi costituiscono corollario del principio generale di trasparenza e si ricavano precisamente dalla lettura in combinato disposto degli articoli 13, 14 e 20 del GDPR, che, in breve, pongono in capo ai titolari di trattamento l'obbligo di informare l'interessato, in maniera "c*oncisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro*", di essere titolare e di poter esercitare il diritto alla portabilità dei dati[326]. In particolare, detto obbligo deve essere osservato in due momenti distinti: quando avviene la fornitura o la raccolta dei dati personali e quando avviene la chiusura di un account ovvero la cessazione del servizio di trattamento[327]. Con riferimento al primo momento, il titolare di trattamento dei dati dovrà adempiere al suddetto obbligo secondo tempistiche differenti a seconda che i dati personali siano stati raccolti direttamente presso l'interessato ovvero aliunde, ad esempio presso soggetti terzi[328]. Nel primo caso, qualora i dati siano raccolti direttamente presso l'interessato, il titolare sarà tenuto a fornire l'informativa "*nel momento in cui i dati personali*

323 M. Borghi, *Portabilità dei dati e regolazione dei mercati digitali*, op. cit., p. 244.

324 All'uopo occorre rammentare che, come già analizzato nel paragrafo II.2 del presente intervento, nell'ipotesi in cui il diritto alla portabilità dei dati personali incida sui diritti di proprietà intellettuale e sui segreti commerciali del titolare del trattamento cui è stata richiesta la portabilità, il titolare del trattamento potrà respingere la richiesta di portabilità ai sensi dell'art. 20 del GDPR.

325 Non si ritiene necessario analizzare nella presente trattazione in quanto, essendo il nuovo titolare di trattamento, saranno ad esso applicabili tutte le norme del GDPR.

326 Articoli 13 e 14 del GDPR.

327 L. Bianchi, *Il diritto alla portabilità dei dati*, op. cit. p. 230; G. Palma, *La portata fortemente innovativa del diritto alla portabilità dei dati come articolato nel GDPR e nelle linee guida WP29*, op. cit., p. 54.

328 *Ibidem*.

sono ottenuti"; nel secondo caso, invece, il titolare dovrà fornire l'informativa entro un termine ragionevole e comunque non superiore ad un mese dall'ottenimento dei dati[329]. Per quanto concerne l'informativa (di identico contenuto rispetto a quella precedente) da fornire al momento della chiusura dell'account o della cessazione del servizio di trattamento, è bene invece precisare che dovrà essere fornita in un momento antecedente rispetto all'effettiva chiusura dell'account e ciò nonostante il dettato normativo, che indica espressamente il momento della "chiusura dell'account". Questa lettura normativa risulta invero necessaria per tutelare i diritti degli utenti e consentirgli di non perdere definitivamente i propri dati personali detenuti dal fornitore di servizi digitali con cui hanno deciso di chiudere i propri account.

Quanto detto sin qui in merito agli obblighi di informativa gravanti sui titolari di trattamento non deve però indurre nell'errore di ritenere che il *titolare-donor* sia obbligato a cancellare i dati personali degli utenti che gli richiedano il trasferimento dei propri dati personali e/o la cancellazione del proprio account. Infatti, come illustrato nelle già richiamate Linee Guida, a seguito dell'esercizio della portabilità dei dati personali ben possono permanere le ragioni ovvero le condizioni di legittimità del trattamento in corso, pur accanto alla facoltà dell'utente di usufruire di un nuovo servizio di trattamento dei dati personali, in aggiunta al primo, con un diverso fornitore (ad esempio, quando l'interessato voglia trasferire la rubrica di un proprio account di posta elettronica ad un ulteriore account, senza dismettere quello precedentemente in uso) [330]. In altre parole, l'esercizio del diritto alla portabilità non interrompe la prosecuzione dei rapporti originari tra l'interessato con il primo titolare del trattamento e, qualora quest'ultimo desideri cancellare i propri dati personali, troverà applicazione la disciplina prevista dall'art. 17 del GDPR a prescindere dalla base giuridica di trattamento dei dati di cui si chiede la portabilità[331].

Ciò chiarito, sembra inoltre opportuna qualche breve considerazione relativamente alla posizione del *titolare-donor* con riferimento al contenuto delle informazioni oggetto di portabilità. La normativa, infatti, non prevede espressamente obblighi di verifica preliminari rispetto alla trasmissione dei dati personali della qualità delle informazioni da trasferire; tutt'al più, come si evince dai principi generali di trattamento di cui all'art. 5 del GDPR, questi saranno comunque tenuti in ogni tempo, e quindi anche subito prima di effettuare la trasmissione dei dati, a garantire l'osservanza e il rispetto della liceità del trattamento, della sua correttezza, trasparenza, esattezza, ecc. Sebbene la scelta di non prevedere obblighi specifici in capo al *titolare-donor* in relazione al contenuto dei dati oggetto di portabilità sia stata chiaramente sostenuta dalle associazioni di categoria e dagli operatori leader nel settore[332], occorre evidenziare che non

329 Articolo 14, paragrafo 3, del GDPR.

330 Tra i vari, si veda: L. Bianchi, *Il diritto alla portabilità dei dati*, op. cit. p. 229.

331 Tra le basi giuridiche è incluso il consenso del titolare. Invero, la normativa presuppone che l'interessato abbia piena consapevolezza che il consenso prestato al primo titolare resti valido sino alla sua revoca ovvero sino alla scadenza del periodo di conservazione fissato in relazione al conseguimento delle finalità del trattamento.

332 Tra i vari, si rileva che l'*European Banking Federation* ha qualificato come corretta la scelta di non gravare i titolari della responsabilità per il trattamento dei dati dall'interessato. Allo stesso tempo, viene tuttavia caldeggiato il fatto che di ciò gli interessati ne abbiano consapevolezza e che vengano attuati in materia comportamenti responsabili.

sono mancate critiche da parte di alcuni autori che ne hanno evidenziato la pericolosità, affermando che detta scelta avrebbe avuto ricadute negative sui diritti degli interessati tenuto conto che, non di rado, i *titolari-recipient* non sempre dispongono degli strumenti e delle competenze necessarie per compiere una valutazione sul potenziale dannoso dei dati ricevuti[333]. A modo di vedere dello scrivente, le problematiche avanzate dal suddetto orientamento potrebbero essere ridimensionate mediante l'applicazione del principio di integrità e riservatezza dei dati personali, da cui si ricava generalmente come corollario che ogni trattamento dei dati deve avere una sicurezza adeguata al rischio. Alla luce di detto principio, infatti, si deve tenere a mente che i titolari di trattamento devono dotarsi non solo di strutture informatiche adeguate a ridurre al minimo i rischi di distruzione, perdita o accesso non autorizzato ai dati[334], ma anche di strutture tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al rischio[335]. Ne consegue, quindi, che una pedissequa applicazione di detto principio potrebbe avere un forte impatto in tema di portabilità dei dati personali potendosi tradurre nell'attribuzione di specifici obblighi in capo ai titolari di trattamento relativi all'adozione di determinate strutture informatiche, organizzative e di sicurezza come, ad esempio, quello di adottare sistemi rafforzati di autenticazione degli utenti[336].

E' indiscusso, invece, dato il chiaro tenore normativo dell'art. 12 del GDPR, l'obbligo in capo al *titolare-donor* a cui sia stata richiesta la portabilità di fornire le "*informazioni relative all'azione intrapresa*" all'interessato richiedente "*senza giustificato ritardo*" e comunque "*entro un mese dal ricevimento della richiesta*" ovvero, in casi di particolare complessità, entro il termine massimo di tre mesi purché l'interessato venga informato delle motivazioni di tale proroga entro un mese dal ricevimento della richiesta iniziale.

Come già anticipato nei paragrafi precedenti, è bene precisare nuovamente che il *titolare-donor* ha la facoltà di respingere le richieste di portabilità dei dati personali dei propri utenti, ma a condizione che siano presenti determinati impedimenti

All'uopo si veda European Banking Federation, *Comments to the Working Party 29 Guidelines on the Right to Data Portability*, doc. N. 025448E, Feb 2017, p. 4.

333 L. Bianchi, *Il diritto alla portabilità dei dati*, op. cit. p. 231. Ovviamente, detti rischi sono accentuati nei casi di trasferimento indiretto, ove il primo recipient dei dati trasferiti è proprio il medesimo interessato.

334 L'art. 5, par. 1, lett f), del GDPR, stabilisce che i dati personali sono "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".

335 Il principio generale viene poi specificato nell'art. 32 del GDPR, secondo il quale: "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".

336 L'adeguatezza di tali misure di sicurezza (i fattori di autenticazione si basano di norma su "qualcosa che sai" – PIN, *password* ecc. – ovvero su "qualcosa che hai" – *badge*, *key fob* ecc. – o, ancora, su "qualcosa che sei" – impronta digitale, retina ecc.) si giustificherebbe in particolare dal fatto che instaurerebbe meccanismi di prevenzione da accessi e richieste di portabilità abusivi, evitando così notevoli rischi in tema di violazioni dei dati personali. L'importanza di tali sistemi è in particolar modo visibile in ambito bancario in cui, rinviando agli interventi successivi per un approfondimento sul tema, si rammenta che la PSD2 ha introdotto alcune nuove misure di sicurezza relative all'autenticazione degli utenti, quali il concetto di *Dynamic link* e la SCA (*Strong Customer Authentication*).

(ad esempio, come anticipato, quando il trattamento sia connesso all'esercizio di pubblici poteri ovvero sussistano ostacoli di natura tecnica, giuridica, o finanziaria). In tale ipotesi il diniego dovrà essere espresso entro il termine massimo di un mese e dovranno essere indicati all'interessato i motivi del rifiuto nonché la possibilità di ricorrere all'autorità giudiziaria ovvero presentare reclamo all'autorità di controllo[337]. Nell'ipotesi inversa, qualora la richiesta di portabilità sia evasa da parte del *titolare-donor*, è opportuno invece rilevare che non sorge automaticamente alcun obbligo in capo al *titolare-recipient* di accettare i dati personali a lui indirizzati, essendo quest'ultimo sempre libero di scegliere se accettarli o meno.

Infine, quanto al *titolare-recipient*, sembra in tale sede doveroso evidenziare solamente che questo assumerà la qualifica di titolare di trattamento dei dati personali e che, conseguentemente, sarà tenuto all'osservanza di tutte le norme contenute nel GDPR. Tra queste, avuto riguardo al momento della ricezione dei dati, sembra assumere particolare rilevanza l'obbligo di agire in conformità al principio di necessità e pertinenza del trattamento dei dati personali, che, a parere dello scrivente, si pone come una vera e propria limitazione alla portabilità. Invero, ai sensi del predetto obbligo, i dati personali oggetto di portabilità che non risultino necessari o pertinenti al servizio richiesto dall'interessato dovranno essere rifiutati dal *titolare-recipient*. Ovviamente, la problematica non sembra destinata ad assumere rilevanza nei casi in cui il nuovo titolare tratti i dati personali per le stesse finalità del primo titolare di trattamento; negli altri casi, invece, essa è destinata ad avere un forte impatto, che può tuttavia essere mitigato dalle innovazioni in tema di interoperabilità ed in particolare dalle innovazioni nell'ambito delle tecniche di estrazione dei dati, che permetterebbero ai titolari di trattamento di non rifiutare in toto la richiesta di trasferimento dei dati, ma solo il trasferimento di quelli incompatibili con le proprie finalità di trattamento.

4.3 Il diritto alla portabilità dei dati non personali

4.3.1 Il Regolamento europeo relativo alla libera circolazione dei dati non personali: brevi cenni

Nella data driven economy anche la raccolta e la elaborazione dei dati non personali assume un ruolo fondamentale: le medesime tecniche utilizzate per la raccolta ed elaborazione dei dati personali sono parimenti efficaci con riferimento ai dati non personali e permettono di generare risultati estremamente utili per le imprese, pubbliche e private, specialmente quando tali attività sono associate a servizi e prodotti[338]. Si pensi, ad esempio, ai dati utilizzati nelle statistiche o nelle relazioni sulle

337 In quest'ultimo caso, opererà un'inversione dell'onere della prova di talché sarà compito del titolare dimostrare la legittimità del proprio diniego.

338 L'incipit del *Considerando* n. 1 del regolamento relativo alla circolazione dei dati non personali (EU) n. 2018/1807 è altrettanto di impatto quando afferma che: "l'economia si sta velocemente digitalizzando. Le tecnologie dell'informazione e della comunicazione non costituiscono più un settore a sé stante, bensì sono la base stessa di tutti i sistemi economici e delle società innovativi e moderni. I dati elettronici sono al centro di tali sistemi e, quando sono analizzati o utilizzati in associazione a servizi e prodotti, possono generare un ingente valore. Allo stesso tempo, il rapido sviluppo dell'economia dei dati e di tecnologie emergenti come l'intelligenza artificiale, i prodotti e i servizi relativi all'Internet

vendite, che consentono di valutare la popolarità di un prodotto e le sue caratteristiche; ai dati del trading ad alta frequenza, che consentono di valutare l'andamento del mercato e di attuare strategie finanziarie competitive; ai dati sull'agricoltura di precisione, che contribuiscono significativamente monitorare e ad ottimizzare l'uso di pesticidi, nutrienti e acqua.

Accanto alla predisposizione di un quadro normativo dedicato alla libera circolazione dei dati personali, non stupisce allora che la strategia per il mercato unico digitale si sia posta l'obiettivo aggiuntivo di adottare un quadro normativo unitario applicabile anche alla circolazione dei dati non personali, garantendo un approccio globale e coerente con il principio della libera circolazione di tutti i dati all'interno del territorio dell'Unione, necessario, come più volte affermato, per promuovere lo sviluppo del nuovo ecosistema digitale[339].

Per l'attuazione di tale obiettivo, tenuto conto dei numerosi ostacoli legali, contrattuali e tecnici incontrati dai fornitori di servizi di trattamento dei dati non personali, l'Unione ha adottato un ulteriore regolamento: il Regolamento europeo relativo alla libera circolazione dei dati non personali[340]. Lo strumento del regolamento era stato ritenuto il più opportuno per contrastare e rimuovere tutti i suddetti ostacoli, che erano visti dall'Unione come una delle priorità da affrontare dal momento che limitavano fortemente la circolazione dei dati non personali e, quindi, lo sviluppo dell'intero mercato unico digitale. A conferma di ciò, si pensi che a seguito dell'adozione del GDPR, lo scenario in materia di dati non personali era ancora diametralmente opposto a quello perseguito dalla strategia per il mercato unico digitale: mancava un'effettiva concorrenza tra i fornitori di servizi cloud, vi era una vasta diffusione delle pratiche di "*vendor lock-in*" e, in generale, la mobilità e la circolazione dei dati non personali era fortemente compromessa.

In sintesi, come rilevato nelle linee guida elaborate con riferimento al Regolamento in esame[341], questo scenario era diretta conseguenza di tre distinte prassi: per un verso, l'adozione da parte degli Stati membri di politiche di localizzazione dei dati non personali si traduceva nella previsione di veri e propri obblighi di localizzazione geografica dei dati ai fini di trattamento o, comunque, nella previsione di norme aventi l'effetto di rendere più difficile il trattamento dei dati al di fuori di un determinato territorio o area geografica (es. l'obbligo di utilizzare dispositivi tecnologici certificati o omologati in un determinato Stato membro); per altro verso, le prassi contrattuali degli operatori di settore (fornitori di servizi di trattamento), che predisponevano sempre più frequentemente clausole contrattuali che limitavano o impedivano ai propri

degli oggetti, i sistemi autonomi e la tecnologia 5G sollevano nuove questioni giuridiche relative all'accesso ai dati e al loro riutilizzo, alla responsabilità, all'etica e alla solidarietà".

339 Quanto detto si evince anche nel *Considerando* n. 7 del regolamento relativo alla circolazione dei dati non personali (EU) n. 2018/1807, in cui si afferma che la previsione di un "unico insieme di regole per tutti i partecipanti al mercato costituisce un elemento essenziale per il corretto funzionamento del mercato interno, affinché siano garantite la certezza del diritto e la parità di condizioni all'interno dell'Unione [...]".

340 Regolamento (EU) 2018/1807 relativo a un quadro applicabile alla libera circolazione dei dati non personali.

341 Commissione europea, Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union, May, 2019, p. 4.

utenti di trasferire i loro dati ad un altro fornitore di servizi di trattamento o di ritrasferirli verso i propri sistemi informatici; infine, per altro verso ancora, i molteplici impedimenti tecnici riscontrati nell'ambito delle operazioni di trasferimento dei dati, che erano spesso causati dagli stessi fornitori di servizi di trattamento e che avevano l'effetto di disincentivare gli utenti a cambiare fornitore di servizi perché troppo dispendioso a livello economico e/o temporale[342].

Alla luce di ciò, nel regolamento sono stati previsti tre distinti strumenti[343]: in primo luogo, un generale divieto agli Stati membri di imporre obblighi sui luoghi in cui i dati dovrebbero essere localizzati; in secondo luogo, un meccanismo di cooperazione per garantire che le autorità competenti continuino a poter esercitare tutti i diritti di cui godono per quanto riguarda l'accesso ai dati trattati in un altro Stato membro; e, infine, incentivi per l'industria nell'intento di sviluppare codici di autoregolamentazione sul cambio di fornitore di servizi e la portabilità dei dati[344]. Tali strumenti, nel prevenire e contrastare le suddette prassi, hanno instaurato un ulteriore regime di libera portabilità dei dati, che si applica ai dati non personali e che ha come presupposto la previsione di un generale divieto degli obblighi di localizzazione dei medesimi.

Procedendo con ordine, è necessario in primo luogo chiarire cosa si intenda per dati non personali. Come previsto nel regolamento in oggetto, la loro definizione si ricava da una lettura *a contrario* di quella prevista nel GDPR per i dati personali, nel senso che costituiscono dati non personali tutti i dati che non rientrano nella nozione di dati personali ivi prevista[345]. Come è stato osservato[346], i dati non personali possono essere catalogati in base alla loro origine in due tipologie: dati anonimi *ex-ante*, che rappresentano i dati che in origine non si riferivano a una persona fisica identificata o identificabile (ad esempio, i dati sulle condizioni meteorologiche prodotti da sensori installati sulle turbine eoliche, i dati sulle esigenze di manutenzione delle macchine

342 A titolo esemplificativo, la Commissione ha individuato numerose restrizioni relative ai luoghi di archiviazione o di elaborazione dei dati, che interessano la mobilità dei dati in diversi settori: a) le autorità di vigilanza che raccomandano ai fornitori di servizi finanziari di archiviare i dati a livello locale; b) le norme in materia di segreto professionale (come ad esempio nel caso del settore sanitario) che prevedono l'archiviazione o l'elaborazione dei dati a livello locale; c) le norme generali che impongono l'archiviazione locale delle informazioni generate dal settore pubblico, indipendentemente dalla sensibilità delle stesse; d) le norme che impongono di utilizzare dispositivi tecnologici che siano omologati o certificati in un determinato stato membro. All'uopo, si veda il *Considerando* n. 4 del regolamento (EU) 2018/1807. Inoltre, come è anche rilevato nel Considerando n. 5 del medesimo regolamento "la mobilità dei dati all'interno dell'Unione era anche ostacolata da restrizioni relative al settore privato, quali aspetti giuridici, contrattuali e tecnici che ostacolano o impediscono agli utenti di servizi di trattamento di dati di trasferire i propri dati da un fornitore di servizi a un altro o di ritrasferirli verso i propri sistemi informatici, non da ultimo al termine del loro contratto con il fornitore di servizi". Tra gli ostacoli alla libera circolazione dei dati non personali espressamente indicati nei *Considerando* del regolamento in esame vi rientrano in particolare 2 differenti categorie: 1) gli obblighi in materia di localizzazione dei dati posti in essere dalle autorità dei singoli Stati membri; e 2) le pratiche di *vendor lock-in* nel settore privato.

343 O. Borgogno, *Regimi di condivisione dei dati ed interoperabilità: il ruolo e la disciplina delle A.P.I.*, op.cit., p. 697 – 698.

344 .

345 Articolo 3, let. 1), del regolamento (EU) 2018/1807.

346 Commissione europea, *Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union*, op. cit., p. 4.

industriali, etc.); ovvero, dati anonimi *ex-post*, ovverosia dati che inizialmente si qualificavano come dati personali, ma che poi sono stati anonimizzati[347].

Prima di esaminare brevemente la portabilità dei dati non personali, occorre soffermarsi sul divieto degli obblighi di localizzazione dei medesimi che, come anticipato, sembra costituire il presupposto giuridico per garantire la libera circolazione (e, quindi, la portabilità) dei dati non personali all'interno del territorio dell'Unione. Ai sensi dell'art. 4 del regolamento, per obblighi di localizzazione si intende "*qualsiasi obbligo, divieto, condizione, limite o altro requisito, previsto dalle disposizioni legislative, regolamentari o amministrative di uno Stato membro o risultante dalle prassi amministrative generali e coerenti in uno Stato membro e negli organismi di diritto pubblico, anche nell'ambito degli appalti pubblici, fatta salva la direttiva 2014/24/UE, che impone di effettuare il trattamento di dati nel territorio di un determinato Stato membro o che ostacola il trattamento di dati in un altro Stato membro*". La definizione, come evidenziato anche dalle già citate linee guida[348], è molto ampia e ricomprende ogni forma di obbligo di localizzazione, sia diretta che indiretta. Tra i tipi di obblighi di localizzazione vietati vi rientrano pertanto non solo tutte quelle previsioni consistenti nell'obbligo di conservare i dati in una specifica posizione geografica (ad es. i server devono essere situati in uno specifico Stato membro) o nell'obbligo di conformarsi a requisiti tecnici nazionali unici (ad es. i dati devono utilizzare specifici formati nazionali), ma anche quelle previsioni che, in seguito ad una valutazione effettuata caso per caso, è dimostrato che avrebbero come effetto quello di ostacolare il trattamento dei dati non personali in qualsiasi altro Stato membro (ad esempio, quelle che includono un obbligo di utilizzare dispositivi tecnologici che siano certificati o omologati in un determinato Stato membro o quelle che, di fatto, richiedono l'osservanza di ulteriori requisiti specifici)[349]. Secondo quanto previsto nel regolamento, detti obblighi di localizzazione dovranno essere eliminati entro il 30 maggio 2021 al fine di porre solide basi per salvaguardare all'interno dell'Unione la libertà di stabilimento dei servizi di trattamento dei dati non personali[350]. L'unico limite a tale previsione è espressamente previsto nel primo comma dell'art. 4 del regolamento, che prevede che restano salvo gli obblighi di localizzazione nei casi in cui gli stessi "*siano giustificati da motivi di sicurezza pubblica nel rispetto del principio di proporzionalità*". Il concetto di pubblica sicurezza, come indicato nella giurisprudenza della Corte di giustizia dell'Unione europea, riguarda sia la sicurezza interna di uno Stato membro che quella esterna, come pure le questioni di

347 I dati anonimizzati sono dati che sono stati resi anonimi (e, quindi, sono dati non personali) in modo che non possano essere attribuiti a una persona specifica, neppure ricorrendo a informazioni aggiuntive. La valutazione se i dati siano stati adeguatamente resi anonimi dipende dalle condizioni specifiche ed uniche di ogni singolo caso. *Ibidem.* Le linee guida del regolamento (EU) 2018/1807 inoltre precisano che "l'anonimizzazione dei dati personali è diversa dalla pseudonimizzazione, in quanto i dati che sono stati resi anonimi in modo adeguato non possono essere attribuiti a una persona specifica, neppure ricorrendo a informazioni aggiuntive e sono pertanto dati non personali. Questo aspetto è delicato perché garantire un corretto processo di anonimizzazione del dato non è semplice e non va sottovalutato da chi vuole percorrere questa strada per escludere l'applicazione dal GDPR".

348 European Commission, *Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union*, May, 2019, p. 5.

349 Ciò detto, si deve tuttavia osservare che, come è stato chiarito dalle citate linee guida al regolamento (EU) 2018/1807, il divieto degli obblighi di localizzazione non incide anche sulle imprese e, quindi, esse rimarranno libere nello stabilire contrattualmente dove effettuare il trattamento dei dati da loro gestiti.

350 *Considerando* n. 3 del regolamento (EU) 2018/1807.

incolumità pubblica; in particolare, essa presuppone l'esistenza di una minaccia reale e sufficientemente grave a uno degli interessi fondamentali della società, quale il pregiudizio al funzionamento delle istituzioni e dei servizi pubblici essenziali nonché all'incolumità della popolazione, come il rischio di perturbazioni gravi dei rapporti internazionali o della coesistenza pacifica dei popoli, o ancora il pregiudizio agli interessi militari[351]. La portata della limitazione al divieto degli obblighi di localizzazione è quindi limitata ai suddetti casi e, come anzidetto, dovrà essere comunque proporzionata alle finalità perseguite[352].

Per gli obblighi di localizzazione che non soggiacciono al suddetto divieto, si noti che il regolamento prevede un regime di trasparenza finalizzato a far conoscere ai titolari di trattamento tutti gli obblighi di localizzazione presenti nel territorio dell'Unione, agevolando quindi il libero flusso dei dati non personali all'interno dell'Unione. A livello pratico, l'informativa relativa agli obblighi di localizzazione in un determinato territorio sarà rilasciata da ciascun Stato membro attraverso la predisposizione di un portale unico nazionale on-line d'informazione, che dovrà essere aggiornato e facilmente accessibile da tutte le imprese.

4.3.2 La portabilità dei dati non personali. Interazione tra il GDPR ed il Regolamento europeo relativo alla libera circolazione dei dati non personali

Oltre a prevedere un generale divieto degli obblighi di localizzazione, il Regolamento in esame si occupa, all'articolo 6, della portabilità dei dati non personali. In linea di massima, essa si differenzia dal diritto alla portabilità previsto dall'art. 20 del GDPR per i seguenti aspetti: l'oggetto del diritto, la struttura e il funzionamento del medesimo e, infine, i titolari dei diritti ad esso connaturati.

Il primo elemento distintivo tra i due diritti alla portabilità dei dati si basa sull'oggetto: il diritto alla portabilità dei dati non personali ha ad oggetto tutti i dati che non rientrano entro l'ambito di applicazione del GDPR e che, come già detto nel paragrafo precedente, data la loro varietà non sono inquadrabili in una categoria unitaria dal momento che possono consistere tanto in dati anonimi *ex-ante* che in dati anonimi *ex-post*.

351 Per "pubblica sicurezza", ai sensi dell'articolo 52 TFUE, si intende la sicurezza sia interna che esterna di uno Stato membro, come pure le questioni di incolumità pubblica, in particolare al fine di agevolare le indagini, l'accertamento e il perseguimento di reati. In sostanza il concetto di "pubblica sicurezza" presuppone l'esistenza di una minaccia reale e sufficientemente grave a uno degli interessi fondamentali della società, quale il pregiudizio al funzionamento delle istituzioni e dei servizi pubblici essenziali nonché all'incolumità della popolazione, come il rischio di perturbazioni gravi dei rapporti internazionali o della coesistenza pacifica dei popoli, o ancora il pregiudizio agli interessi militari.

352 Conformemente alla giurisprudenza della Corte di giustizia dell'Unione europea, il principio di proporzionalità impone che le misure adottate siano atte a garantire il conseguimento dell'obiettivo perseguito e non vadano al di là di quanto necessario a tale scopo. Si veda, *inter alia*, CGUE 08 luglio 2010, Causa C-343/09, *Afton Chemical Limited contro Secretary of State for Transport*, punto 45. In questo senso, pertanto, l'obbligo assoluto di localizzazione dovrebbe costituire sempre una *extrema ratio*.

Il secondo elemento distintivo tra i due diritti alla portabilità riguarda, invece, la loro differente struttura e funzionamento. Il diritto alla portabilità dei dati non personali, contrariamente a quanto accade per quello relativo ai dati personali, non trova una puntuale disciplina dedicata a tali profili, che è invece demandata quasi interamente all'autoregolamentazione. Quest'ultima, secondo quanto previsto dall'art. 6 del Regolamento in esame, dovrebbe assumere la forma di codici di condotta indicanti "*le migliori prassi per agevolare il cambio di fornitore di servizi e la portabilità dei dati in un formato strutturato, di uso comune e leggibile elettronicamente, anche in formati standard aperti ove necessario o richiesto dal fornitore di servizi che riceve i dati*" e "*gli obblighi d'informazione minimi per garantire che gli utenti professionali ricevano informazioni sufficientemente dettagliate, chiare e trasparenti prima della conclusione di un contratto di trattamento di dati, per quanto riguarda le procedure e i requisiti tecnici, i tempi e gli oneri applicati nel caso in cui un utente professionale intenda cambiare fornitore di servizi o ritrasferire i dati nei propri sistemi informatici*"[353]. È previsto, inoltre, che i medesimi contemplino "*gli approcci in materia di sistemi di certificazione che agevolano il confronto di prodotti e servizi di trattamento dei dati per gli utenti professionali...* " e le "*tabelle di marcia in materia di comunicazione, con un approccio multidisciplinare volto a sensibilizzare a proposito dei codici di condotta".* La portabilità dei dati non personali con particolare riferimento ai servizi *cloud* troverà pertanto applicazione con le modalità che saranno previste nei singoli codici di condotta di cui, ad oggi, è prematura una disamina[354]. Ad ogni modo, seppur il meccanismo tecnico di fondo (trasmissione di un dato da un ambiente IT ad un altro) non dovrebbe cambiare rispetto al funzionamento della portabilità ex art. 20 del GDPR, sembra potersi presumere che le modalità di esercizio e il funzionamento del diritto alla portabilità dei dati non personali tenderanno ad assumere connotati e forme proprie, nettamente differenti e sicuramente più variegate rispetto a quelle previste nel GDPR in quanto il loro ambito di applicazione non sembra incidere in maniera rilevante sui diritti fondamentali degli individui.

Quanto appena affermato trova ulteriore conforto nel terzo elemento distintivo della portabilità dei dati non personali da quello relativo ai dati personali, che si ravvisa nel fatto di non attribuire diritti a una platea indeterminata di soggetti, ma

353 A titolo esemplificativo, il *Considerando* n. 31 del regolamento (EU) 2018/1807 chiarisce che i codici di condotta, per essere efficaci, dovrebbero trattare almeno gli aspetti fondamentali in tema di portabilità, tra cui i processi e il luogo dei *back up* dei dati, i formati dei dati e i supporti disponibili, la configurazione informatica richiesta e la larghezza di banda minima della rete, il tempo necessario per avviare il processo di trasferimento e il periodo in cui i dati saranno disponibili per il trasferimento, nonché le garanzie di accesso ai dati in caso di fallimento del fornitore.

354 Nel mercato dei servizi *cloud*, la Commissione europea ha iniziato a facilitare le attività dei gruppi di lavoro dei portatori di interesse *cloud* del mercato unico digitale, che riuniscono esperti e utenti professionali *cloud*, tra cui le piccole e le medie imprese. In questa fase, un sottogruppo sta elaborando codici di autoregolamentazione sulla portabilità dei dati e sul cambio di fornitore di servizi *cloud* (gruppo di lavoro SWIPO), mentre un altro sottogruppo sta lavorando allo sviluppo della certificazione di sicurezza dei servizi *cloud* (gruppo di lavoro CSPCERT) . In particolare, occorre osservare che il gruppo di lavoro SWIPO sta sviluppando codici di condotta che riguardano l'intero spettro dei servizi *cloud*: infrastrutture come servizi (IaaS), piattaforme come servizi (PaaS) e *software* come servizi (SaaS). Si veda, a tal riguardo, European Commission, *Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union*, May, 2019, p. 4 ss., in cui si auspica che i diversi codici di condotta siano integrati da clausole contrattuali tipo in modo tale da consentire una sufficiente specificità tecnica e giuridica nell'attuazione e nell'applicazione pratiche dei codici di condotta. L'elaborazione delle clausole contrattuali tipo è stata prevista dopo lo sviluppo dei codici di condotta (il cui termine era previsto entro il 29 novembre 2019).

solamente in favore di una categoria specifica: gli utenti professionali[355]. Tale caratteristica comporta una indebitabile limitazione dell'ambito applicativo del diritto alla portabilità dei dati non personali esclusivamente alle relazioni "*business – to – business*", ovverosia alle relazioni intercorrenti tra un utente professionale e un fornitore di servizi (ad esempio il fornitore di servizi cloud) e non anche alle relazioni tra interessati e titolare di trattamento, come accade in tema di portabilità dei dati personali.

Sebbene gli elementi anzidetti sembrano distinguere nitidamente i due diritti alla portabilità, in realtà, si deve evidenziare che nella prassi non è sempre semplice individuare la normativa applicabile. Ormai, l'estensivo ricorso all'ICT ha invero comportato la creazione di innumerevoli *dataset* composti sia da dati personali che da dati non personali[356](c.d. insiemi di dati misti), che hanno sollevato la questione circa il rapporto tra il Regolamento sulla libera circolazione dei dati non personali ed il GDPR. Secondo la soluzione maggiormente accreditata, che si basa sul tenore dell'art. 2, paragrafo 2, del Regolamento, che dispone che "*Nel caso di un insieme di dati composto sia da dati personali che da dati non personali, il presente regolamento si applica alla parte dell'insieme contenente i dati non personali [...]"*, i due regolamenti si applicherebbero, ciascuno senza interferenze da parte dell'altro, ai dati rientranti nel proprio ambito di applicazione. Detta soluzione sembra aver trovato ulteriore conforto in alcuni recenti orientamenti pubblicati dalla Commissione europea[357], in cui è stato chiarito che nell'eventualità di cambio, da parte di un'impresa, del fornitore di servizi *cloud*, qualora tale fornitore abbia aderito ad un codice di condotta conformemente al Regolamento la portabilità dovrà essere attuata per i dati non personali in base alle previsioni del codice di condotta e per i dati personali in base alle prescrizioni contenute nel GDPR; analogamente, nell'eventualità di cambio del fornitore dei servizi di gestione delle relazioni con i clienti (CRM), i trasferimenti dei dati dovranno conformarsi sia al GDPR (per i dati personali) sia al Regolamento relativo ai dati non personali.

Nonostante l'orientamento anzidetto rappresenti, anche a parere dello scrivente, quello migliore, occorre tuttavia evidenziare che esso non sembra risolvere il rapporto tra il GDPR ed il Regolamento sulla libera circolazione dei dati non personali nelle ipotesi in cui in un determinato dataset siano presenti dati personali e non personali "*indissolubilmente legati*" fra loro. Tale status, seppur non definito da nessuno

355 Questi sono definiti dall'articolo 3 del regolamento sui dati non personali come la *"persona fisica o giuridica compreso un'autorità pubblica e un organismo di diritto pubblico che utilizza o richiede servizi di trattamento di dati per fini connessi alla sua attività commerciale, industriale, artigianale, professionale o a una sua funzione*".

356 Tra gli insiemi di dati misti, ad esempio, si annoverano: a) documenti fiscali d'impresa, che contengono il nome e il numero di telefono dell'amministratore delegato; b) insiemi di dati di una banca, in particolare quelli che contengono informazioni sui clienti e dettagli delle transazioni, come servizi di pagamento (carte di credito e di debito), applicazioni di *partner relationship management* (PRM) e contratti di prestito, documenti che includono dati misti relativi sia a persone fisiche che giuridiche; c) dati statistici resi anonimi di un istituto di ricerca e dati non trattati inizialmente raccolti, come le risposte dei singoli intervistati alle domande di un'indagine statistica; d) una banca dati di conoscenze di un'impresa riguardante i problemi IT e le loro soluzioni basate sulle singole relazioni degli incidenti informatici; e) dati relativi all'Internet delle cose, dove alcuni dati consentono di fare ipotesi sulle persone identificabili (ad es. presenza a un particolare indirizzo e modelli di utilizzo); e) analisi dei dati del registro operativo delle attrezzature di produzione nell'industria manifatturiera.

357 Giova evidenziare che ai sensi dell'art. 8, paragrafo 3, del regolamento (EU) 2018/1807 sono stati pubblicati gli orientamenti il 29 maggio 2019, che sono stati già più volte citati.

dei due regolamenti, indica quella situazione in cui un insieme di dati misti sia configurato in modo tale da rendere impossibile una separazione dei dati ivi contenuti ovvero da renderla eccessivamente onerosa[358]. Ebbene, in tale ipotesi sembrerebbe invece conveniente fare ricorso a quanto previsto nella seconda parte dell'art. 2, paragrafo 2, del regolamento che prevede espressamente l'applicazione del GDPR a tutti i dati (personali e non personali) "*indissolubilmente legati*"[359]. Tale norma, infatti, sembra risolvere la suddetta questione con il pregio di incentivare tutti i titolari di trattamento a provvedere alla separazione dei dati appartenenti agli insiemi di dati misti[360].

4.4 Le nuove iniziative in tema di condivisione dei dati nel mercato unico digitale

Chiarito il rapporto tra le due normative fondamentali in tema di portabilità dei dati, senza avere la pretesa di esaminare dettagliatamente tutte le normative menzionate in premessa, in un'ottica sistematica, sembra opportuno fare un passo in avanti analizzando (brevemente) alcune delle iniziative legislative proposte dalla Commissione che, se adottate, potrebbero assumere una notevole rilevanza in materia.

In primo luogo, si fa riferimento alla recente Proposta di Atto sulla Governance sui Dati[361], la quale, tra le varie novità, propone due tipi di interventi. Il primo è finalizzato a promuovere e incentivare il "riuso" dei dati pubblici che, se soggetti a vincoli di riservatezza commerciale, statistica, proprietà intellettuale o sottoposti alla disciplina della protezione dei dati personali, spesso non ricadono nell'ambito di applicazione della Direttiva Open Data in quanto oggetto di specifici accordi con gli enti pubblici che prevedono l'esclusiva di tali tipologie di dati in proprio favore o, comunque, una restrizione del loro riutilizzo da parte dei legittimari. Detto intervento si traduce a livello normativo nella previsione di un generale divieto in capo agli enti pubblici di stipulare accordi aventi il predetto contenuto; l'unico caso in cui è fatta salva la loro liceità è quello in cui detti accordi siano stipulati per servizi pubblici rilevanti e, comunque, per periodi di tempo non superiore a tre anni. Il secondo tipo di intervento è, invece, dedicato al settore privato e prevede l'instaurazione nel mercato unico digitale di nuove modalità di condivisione dei dati tra privati e tra questi e il settore pubblico.

358 Ad esempio, quando la società acquista servizi di gestione delle relazioni con i clienti e sistemi di rendicontazione delle vendite, dovrebbe spendere altrettanto per comprare *software* separati per i CRM (dati personali) e per i sistemi di rendicontazione delle vendite (dati aggregati/non personali) basati sui dati CRM. È altresì probabile che separare l'insieme di dati ne diminuisca sensibilmente il valore. Inoltre, la natura mutevole dei dati rende ancora più difficile distinguere chiaramente e quindi separare le diverse categorie di dati.

359 Per regola generale, sulla base di quanto detto, i diritti e gli obblighi previsti nel GDPR si dovrebbero applicare all'insieme di dati misti indissolubilmente legati tra loro anche quando i dati personali rappresentano soltanto una piccola parte del medesimo insieme dei dati. Tale interpretazione risulta inoltre conforme con i principi alla base del diritto alla protezione dei dati personali sanciti dalla Carta dei diritti fondamentali dell'Unione europea e con il tenore letterale di cui al *Considerando* n. 8 del GDPR.

360 Invero, tenuto conto che nessuno dei due regolamenti relativi ai dati personali e non personali prevede l'obbligo di separazione, senza la previsione normativa in esame i titolari avrebbero potuto evitare di compiere le operazioni di separazione dei dati misti senza incorrere in alcuna sanzione.

361 Proposta di Regolamento relativo alla *governance* europea dei dati, Bruxelles, 25.11.2020 COM(2020) 767 final 2020/0340 (COD).

All'uopo, non solo sono previsti meccanismi di riconoscimento e registrazione dei soggetti che offrono servizi di intermediazione per la condivisione di dati tra imprese e interessati dietro un corrispettivo[362], ma si estende anche il novero delle basi giuridiche che legittimano la condivisione dei dati (ad esempio, una delle maggiori novità della proposta consiste nella previsione della possibilità di raccogliere e trattare i dati messi a disposizione per scopi altruistici da persone fisiche e giuridiche – c.d. *data altruism*)[363]. Accanto a questi tipi di interventi, al fine di aumentare i controlli e la sicurezza nel mercato unico dei dati, l'Atto di Governance sui Dati propone l'istituzione di misure dedicate a monitorare la sua osservanza e, se del caso, sanzionare eventuali trasgressori; in particolare, viene proposta la istituzione di un *European Data Innovation Board* (avente tra le varie funzioni quella di garantire la coerenza e uniformità nell'applicazione del regolamento in oggetto) e di un'Autorità di controllo sulle organizzazioni che ricorrono al *data altruism* (avente tra i vari ruoli quello di mantenere un registro di tali organizzazioni al fine di monitorarne le attività) e la previsione di un regime speciale di notifica per le imprese che vogliono fornire servizi di intermediazione dei dati, avente la finalità di consentire alle autorità designate dagli Stati membri di valutare la sussistenza di tutti i requisiti per l'esercizio di detta attività[364] e di monitorare il loro esercizio, applicando, in caso di trasgressioni, sanzioni pecuniarie dissuasive e/o misure impeditive alla fornitura del servizio.

Una seconda novità rilevante in tema di portabilità dei dati potrebbe indubbiamente derivare dall'adozione di altre due recenti proposte avanzate dalla Commissione europea nell'ambito del Digital Services Act Package[365]: il Digital Services Act[366] e il Digital Markets Act[367]. Tali proposte mirano a regolare e prevenire aspetti problematici riscontrati in tema di portabilità dei dati derivanti dalle condotte poste in essere dai prestatori di servizi di intermediazione online e, in particolare, dalle piattaforme online di grandi dimensioni, che, come già anticipato in tema di portabilità dei dati

362 E' in particolare prevista l'istituzione di nuovi fornitori di servizi di condivisione dei dati (intermediari dei dati) e di servizi di assistenza nell'esercizio della portabilità dei dati personali (c.d. *Personal data-sharing Intermediary*).

363 Per "*data altruism*" s'intende il consenso degli interessati al trattamento dei dati personali che li riguardano, o le autorizzazioni di altri *data holder* per consentire l'uso dei loro dati non personali senza chiedere una retribuzione, per scopi di interesse generale, come scopi di ricerca scientifica o migliorare i servizi pubblici. Tali scopi includerebbero l'assistenza sanitaria, la lotta al cambiamento climatico, il miglioramento della mobilità, l'agevolazione della creazione di statistiche ufficiali o il miglioramento della fornitura di servizi pubblici. Anche il sostegno alla ricerca scientifica, compresi, ad esempio, lo sviluppo tecnologico e la dimostrazione, la ricerca fondamentale, la ricerca applicata e la ricerca finanziata da privati, dovrebbero essere considerati scopi di interesse generale.

364 Tra i vari requisiti richiesti, a titolo esemplificativo e non esaustivo vi rientrano l'obbligo di rimanere neutrali rispetto i dati scambiati; la non utilizzabilità dei dati o metadati per scopi diversi; la previsione di una procedura di accesso al servizio equa, trasparente e non discriminatoria anche in relazione ai costi; la garanzia di armonizzazione rispetto standard internazionali o europei sui dati; la predisposizione di procedure che prevengano attività fraudolente o abusive; la garanzia di un elevato livello di sicurezza per l'archiviazione e trasmissione di dati non personali.

365 Tale pacchetto di iniziative legislative è stato proposto sulla scia della recente e già citata Comunicazione *Shaping Europe's digital future*, adottata a livello europeo il 19 Febbruary 2020, che annuncia l'adozione da parte dell'Unione di nuove regole di portata orizzontale in materia di responsabilità e obbligazione dei prestatori di servizi di intermediazione *online* e, in particolare, delle piattaforme *online*.

366 *Proposal for a Regulation on a Single Market For Digital Services* (Digital Services Act), Brussels, 15.12.2020 COM(2020) 825 final.

367 *Proposal for a Regulation on contestable and fair markets in the digital sector* (Digital Markets Act), Brussels, 15.12.2020 COM(2020) 842 final.

personali, attuano diverse pratiche anticoncorrenziali tra cui quelle di lock-in nei confronti dei propri utenti. Più precisamente, la prima proposta sembra affrontare l'ormai annoso tema della responsabilità dei prestatori di servizi di intermediazione online in merito alle attività condotte dai privati sulle proprie piattaforme (ad esempio, l'upload di contenuti illeciti) sotto una duplice prospettiva: per un verso, essa attua un nuovo bilanciamento delle responsabilità tra gli utenti e le piattaforme online, prevedendo nuove condizioni di esenzione dalla responsabilità delle piattaforme online a seconda del tipo di attività da quest'ultime esercitate (*mere conduit activities*, *caching activities* e *hosting services*)[368]; per altro verso, invece, prevede una serie di obblighi in capo ai prestatori di servizi di intermediazione online qualificati come *gatekeepers*[369] che si suddividono in obblighi aventi portata orizzontale, applicati indistintamente a tutti i prestatori di servizi, e in obblighi con portata verticale, che sono invece applicati solo ai prestatori di servizi appartenenti ad una predeterminata categoria (prestatore di servizi di intermediazione; prestatore di servizi di hosting; piattaforme online; piattaforme online di grandi dimensioni)[370]. Senza alcuna pretesa di esaustività, tra gli obblighi applicabili indistintamente a tutti i prestatori di servizi si annoverano, ad esempio: 1) l'obbligo di designare nello Stato membro in cui esercitano le proprie attività un punto di contatto ovvero, ove necessario, un legale rappresentante; 2) l'obbligo di designare un legale rappresentante nell'Unione nel caso in cui il prestatore di servizi non sia stabilito nel territorio dell'Unione; e 3) gli obblighi di comunicazione al fine di promuovere la trasparenza in relazione alle operazioni di rimozione o di disabilitazione di informazioni considerate illegali o contrarie ai termini e condizioni dei prestatori stessi.

In considerazione di quanto esposto, la proposta in esame sembra avere le caratteristiche per stimolare concretamente la portabilità dei dati nell'ambito del mercato interno, incentivando la sicurezza delle attività poste in essere dai prestatori di servizi di intermediazioni online e la loro trasparenza. A conferma di ciò, si deve osservare che detta normativa prevede inoltre un articolato sistema di *enforcement* di tutti gli obblighi in essa previsti, consistente, per un verso, nella istituzione di autorità nazionali di vigilanza e di un organismo centrale europeo di coordinamento (*European Board for Digital Services*) e, per altro verso, nella attribuzione in capo alla Commissione europea di poteri specifici di natura investigativa e sanzionatoria.

La seconda proposta è, invece, finalizzata a promuovere l'innovazione e ad incentivare la concorrenza dei servizi digitali nel mercato unico digitale contrastando tutte quelle condotte anticoncorrenziali adottate dai prestatori di servizi online di grande dimensione che, stante la scarsa efficacia delle tradizionali regole concorrenziali europee nel settore digitale, non sono state ad oggi efficacemente contrastate e sanzionate. Dette pratiche (consistenti, ad esempio, nella previsione di costi di *switching* troppo elevati per gli utenti, tali da disincentivarli a passare ad un altro fornitore) comportano infatti un impedimento alla dinamicità del mercato propria di un sistema concorrenziale equilibrato, sia per i nuovi operatori, che trovano barriere d'ingresso, sia per i piccoli e medi prestatori di servizi di intermediazione, che non hanno la possibilità

368 Articoli 3, 4 e 5 del *Digital Services Act*, op cit.

369 Come si dirà nel prosieguo, la definizione di *gatekeeper* è prevista dal *Digital Markets Act*.

370 Articoli 10- 37 del *Digital Services Act*, op cit.

di crescere e competere con le piattaforme online già affermate[371]. Partendo da questi dati, come si evince nel medesimo testo della proposta, la Commissione europea ha elaborato questa iniziativa legislativa optando per la seconda strategia avanzata in sede di consultazione[372], che richiamava la necessità di predisporre un quadro di designazione parzialmente flessibile dei prestatori di servizi di intermediazione soggetti alla nuova disciplina e un regime di obblighi in grado di essere aggiornato per stare al passo con le nuove innovazioni tecnologiche. Conseguentemente, la proposta in esame prevede, in primo luogo, una lista chiusa dei servizi oggetto del proprio ambito di applicazione (c.d. *core platform services*[373]) e stabilisce una serie di criteri quantitativi e qualitativi che devono sussistere in capo ai prestatori dei suddetti servizi per consentirne la qualificazione, ai sensi della medesima normativa, come "*gatekeepers*". In secondo luogo, con esclusiva applicazione nei confronti di prestatori qualificati come *gatekeeper*, la normativa prevede una serie di obblighi misti aventi natura concorrenziale che si suddividono in due categorie: obblighi fissi, espressamente previsti e direttamente applicabili a tutti i *gatekeepers*[374], e obblighi variabili, il cui contenuto e momento di applicazione è rimesso all'apprezzamento della Commissione europea in seguito alle attività dalla medesima svolte di *market investigation*[375].

Al pari della prima proposta, anche la proposta in esame sembra poter stimolare concretamente la portabilità dei dati, incentivando in tal caso la concorrenza tra i prestatori di servizi digitali, che avrebbero finalmente un testo normativo di riferimento che indichi le attività che possono e non possono fare e che regoli espressamente i loro rapporti in un'ottica concorrenziale[376].

Nell'ambito delle probabili novità in ambito concorrenziale non si può non accennare anche al New Competition Tool, che è stato oggetto di una autonoma consultazione pubblica (parallela a quella dedicata al Digital Services Act) e che è ancora in fase di discussione in sede europea. In breve, detto strumento consiste nell'attribuzione alla Commissione di determinati poteri di *enforcement* (aventi ad oggetto l'imposizione di specifici obblighi, comportamentali o strutturali) per affrontare i problemi strutturali del mercato derivanti dalle condotte anticoncorrenziali, senza tuttavia essere necessario il previo accertamento di una violazione del diritto della concorrenza. In tal senso, quindi, esso costituirebbe uno strumento concorrenziale sui generis che

371 Il mercato unico digitale è invero caratterizzato per basarsi sugli effetti network che, associati a determinati comportamenti delle imprese dominanti, determinano per quest'ultime la possibilità di dominare il mercato controllandone l'accesso (*gatekeeper*). Invero, il mercato unico digitale è anche descritto dagli esperti come un mercato in cui "*the winner takes it all*", ovverosia in cui l'impresa di più grandi dimensioni e che offre per prima un determinato servizio potrà agevolmente appropriarsi di una quota di mercato rilevante. Quanto detto trova conferma nei dati, che illustrano che su oltre 10.000 piattaforme online operanti nel territorio dell'Unione solo pochissime detengono una quota rilevante nel mercato, che è inoltre mantenuta nel tempo. Cfr. *Digital Services Act*, p. 1.

372 Le consultazioni pubbliche avviate dalla Commissione europea in tale tematica hanno avuto luogo tra il 2 giugno e l'8 settembre 2020. Per una sintesi dei risultati delle consultazioni si veda *Digital Market Act*, p. 2.

373 I *core platform services* individuati nel *Digital Market Act* sono: (i) *online intermediation services*; (ii) *social networking;* (iii) *video sharing platform services*; (iv) *operating systems;* (v) *cloud services*; (vi) *advertising services.* Cfr. *Digital Market Act,* p. 2.

374 Articolo 5 del *Digital Markets Act.*

375 Articolo 6 del *Digital Markets Act.*

376 Anche in tale ambito vi è l'attribuzione alla Commissione di poteri di natura investigativa e sanzionatoria. Si vedano gli Articoli 18 – 27 del *Digital Markets Act.*

offusca la tradizionale differenza tra regolamentazione *ex ante* e applicazione *ex post* delle regole concorrenziali e che, aggiungendosi alle regole *ex ante* previste dal Digital Services Act Package, avrebbe le potenzialità di contrastare in maniera più efficace e tempestiva le pratiche anticoncorrenziali poste in essere dalle piattaforme online.

Infine, un'ultima proposta da richiamare in tale sede è quella relativa al Regolamento e-privacy[377] che, qualora adottata, giocherà un ruolo di primo piano nel disciplinare alcuni aspetti della condivisione dei dati personali nella materia delle comunicazioni elettroniche. Essa riesamina la direttiva sulla vita privata elettronica del 2002 sulla scorta degli obiettivi fissati dalla strategia per il mercato unico digitale e la allinea alla nuova disciplina del GDPR, prevedendo, a titolo esemplificativo, nuove specifiche condizioni per i fornitori di servizi di comunicazione elettronica per il trattamento dei dati e dei metadati e stabilendo il generale obbligo, salvo casi specifici[378], della loro cancellazione o anonimizzazione dopo che il o i destinatari previsti abbiano ricevuto il contenuto della comunicazione elettronica oggetto di trattamento. In aggiunta a quanto detto, sempre a titolo esemplificativo, la proposta prevede un regime specifico di tutela delle informazioni raccolte dalle apparecchiature terminali degli utenti finali, un regime specifico del consenso, allineato a quello previsto nel GDPR, per il trattamento dei dati delle comunicazioni elettroniche, e, in linea di massima, un generale rafforzamento dei diritti di controllo degli utenti relativamente alle comunicazioni elettroniche, consentendogli di porre in essere una serie variegata di attività: bloccare, anche singolarmente, le chiamate provenienti anche da numeri sconosciuti o anonimi; impedire la presentazione dell'identificazione della linea chiamante per ogni singola chiamata; impedire la presentazione dell'identificazione della linea chiamante per le chiamate in entrata; la possibilità per l'utente finale chiamato di rifiutare le chiamate in entrata se la presentazione dell'identificazione della linea chiamante è stata bloccata dall'utente finale chiamante[379].

4.5 Conclusioni

Il GDPR e il Regolamento per la libera circolazione dei dati non personali pongono le basi per l'applicazione del principio della libera circolazione a tutti i dati (personali e non personali) nell'Unione, essenziale per il pieno sviluppo del mercato unico digitale e per la costruzione di un'economia dei dati europea altamente competitiva.

A tal fine, entrambi i regolamenti prevedono il diritto alla portabilità dei dati con lo scopo di agevolare il loro trasferimento da un ambiente IT ad un altro, producendo effetti concorrenziali rilevanti in termini di prevenzione delle pratiche di *lock-in* e di promozione e stimolo della concorrenza tra i fornitori di servizi. Tuttavia, come si è avuto modo di analizzare nel corso del presente intervento, l'angolazione da cui è affrontata la portabilità nei due regolamenti è opposta: mentre il GDPR disciplina

377 Proposta di regolamento relativa al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche, Bruxelles, 10.01.2017, COM (2017) 10 final.

378 Ovverosia nei casi di cui all'Articolo 6, paragrafo 1, lettera b) e All'articolo 6, paragrafo 3, lettere a) e b) della medesima proposta di regolamento.

379 Articolo 12 del Regolamento *e-privacy*.

espressamente il diritto alla portabilità dei dati personali con riferimento al rapporto tra interessato e titolare di trattamento, prevedendo una rigida disciplina dedicata, ancor prima che a stimolare la concorrenza, a rafforzare la protezione dei dati personali degli utenti/interessati; al contrario, il regolamento sulla libera circolazione dei dati non personali si allontana dal paradigma privacy-concorrenza, rivolgendosi esclusivamente agli utenti professionali ed incoraggiando un approccio di autoregolamentazione che tenga conto dei soli effetti concorrenziali prodotti dalla portabilità.

La differente prospettiva da cui è affrontato il diritto alla portabilità nelle due normative deriva dal tipo di dati oggetto della richiesta di portabilità e dall'impatto che la loro circolazione produce nei confronti dei differenti diritti e valori di volta in volta coinvolti. Questa duplice regolamentazione ha avuto l'effetto di instaurare un mercato unico dei dati nell'Unione, che riassume e bilancia detti diritti e valori con il principio della libera circolazione. Il percorso per la piena attuazione di tale obiettivo è, tuttavia, ancora in corso. Come visto, la Commissione europea ha recentemente adottato una strategia europea per i dati[380], che poggia le basi sull'istituto in esame e ha l'ambizione di implementarlo nei singoli settori strategici e ambiti di interesse pubblico, creando molteplici spazi comuni europei di dati[381]. Per far ciò, la Commissione europea è orientata, in prima istanza, a promuovere ingenti investimenti sulle infrastrutture e le capacità europee per l'*hosting*, l'elaborazione, l'utilizzo dei dati e l'interoperabilità[382]; in seconda istanza, ad adottare un quadro di governance intersettoriale per l'accesso ai dati e il loro utilizzo; e, infine, ad adottare ulteriori normative che disciplinino, nei rispettivi ambiti settoriali, determinati aspetti della portabilità dei dati e della loro condivisione.

Come si è avuto modo di analizzare, lo stesso regime orizzontale di portabilità dei dati instaurato dai due regolamenti deve ancora superare alcuni aspetti controversi nell'ambito dei quali il ricorso agli strumenti di *soft law* e all'autoregolamentazione sembrano ricoprire un ruolo cruciale: invero, tenuto conto che il mercato digitale investe spesso questioni puramente tecniche, per garantire e stimolare un equo flusso di dati (personali e non personali) nell'Unione, sembra inevitabile dover ricorrere ad interventi specifici da parte di gruppi di esperti (come, ad esempio, linee guida istituzionali) e alla elaborazione, da parte degli operatori di settore, di codici di condotta e buone prassi applicative.

Accanto a questi interventi, si auspica altresì l'adozione delle recenti iniziative legislative proposte dalla Commissione europea che, sulla scia dei due regolamenti suddetti, completano un mercato unico europeo dei dati ancora oggi inefficiente, prevedendo una serie di interventi mirati aventi l'obiettivo di promuovere la concorrenza tra i servizi digitali e tutelare la *privacy* e gli altri diritti fondamentali degli utenti. In particolare, detti interventi consentirebbero al mercato unico digitale di fare un balzo in avanti in tema di portabilità e condivisione dei dati, garantendo maggiore semplicità nella circolazione dei dati, regole più mirate e proporzionate per i servizi digitali e un

380 Commissione europea, Comunicazione "*Una strategia europea per i dati*", COM (2020) 66 final.

381 *Ibidem*, p. 24 ss.

382 *Ibidem*, p. 13 ss.n

ruolo poliedrico in capo alla Commissione europea, che accanto al tradizionale potere di iniziativa legislativa vedrebbe accrescere anche i propri poteri di natura investigativa e sanzionatoria.

5 Il diritto alla portabilità dei dati in materia di servizi di pagamento: punti di contatto, differenze e proposte

5.1 Introduzione

Con l'introduzione di un regime settoriale di accesso ai conti di pagamento (XS2A), la Direttiva 2366/2015 relativa ai servizi di pagamento nel mercato interno (PSD2) ha segnato un passo fondamentale verso lo scorporamento dei tradizionali servizi di pagamento a potenziale beneficio di nuovi operatori, che da ora in avanti godranno del diritto di richiedere l'accesso alle informazioni dei conti di pagamento della clientela senza la necessità di un previo accordo con il relativo gestore bancario[383]. In particolare, l'obiettivo della PSD2 è quello di far leva sulle soluzioni tecnologiche offerte dagli operatori FinTech per promuovere la concorrenza in un mercato, quale quello dei servizi bancari al dettaglio, tradizionalmente affetto da scarsa elasticità della domanda, inerzia dei consumatori e problemi di *lock-in*, e perciò favorevole alla possibilità che le banche estraggano profitti sovra-competitivi a scapito del *consumer welfare*[384].

I modelli di business tradizionali stanno, infatti, fronteggiando un sempre più serio rischio di sovvertimento derivante dall'emersione di imprese operanti nell'ambiente FinTech che, mediante lo sfruttamento di *mobile applications*, tecniche di identificazione digitale, *big data analytics*, intelligenza artificiale, e implementazioni basate su *blockchain*, forniscono innovativi servizi bancari e finanziari[385]. Le moderne tecniche di analisi di grandi quantità di dati permettono un'ampia gamma di nuove attività, tra cui la profilazione dei consumatori e l'identificazione di modelli di consumo volti alla prestazione di offerte personalizzate nonché attività di controllo e gestione del rischio

383 GU L 337/35 (2015), Articoli 36 e 64-68.

384 Oscar Borgogno e Giuseppe Colangelo, Data, Innovation and Competition in Finance: The Case of the Access to Account Rule, 31 European Business Law Review 573 (2020); Oscar Borgogno e Giuseppe Colangelo, Consumer inertia and competition-sensitive data governance: the case of Open Banking, 9 Journal of European Consumer and Market Law 143 (2020). Si vedano anche Australian Government Productivity Commission, Competition in the Australian Financial System, (2018) https://www.pc.gov.au/inquiries/completed/financial-system#report; UK Competition and Markets Authority, The Retail Banking Market Investigation Order 2017, (2017) https://assets.publishing.service.gov.uk/media/5893063bed915d06e1000000/retail-banking-market-investigation-order-2017.pdf; The Netherlands Authority for Consumers & Markets, Barriers to Entry into the Dutch Retail Banking Sector, (2014) https://www.acm.nl/en/publications/publication/13257/Barriers-to-entry-into-the-Dutch-retail-banking-sector.

385 Iris H.-Y. Chiu, *The Disruptive Implications of Fintech-Policy Themes for Financial Regulators*, 21 Journal of Technology Law & Policy 55 (2017); Dirk A. Zetzsche, Ross P. Buckley, Douglas W. Arner, Janos N. Barberis, *From* FinTech to TechFin: The Regulatory Challenges of Data-Driven Finance, EBI Working Paper Series No. 6 (2017), 11-12, https://www.law.ox.ac.uk/business-law-blog/blog/2017/05/fintech-techfin-regulatory-challenges-data-driven-finance.

finanziario[386]. Pertanto, nuovi operatori possono essere coinvolti nella catena del valore, sia nelle attività di gestione della clientela privata che nel *back-office* e nell'erogazione di servizi alla clientela[387].

Al fine di agevolare l'interazione tra operatori tradizionali e sviluppatori FinTech, numerose autorità di regolamentazione hanno istituito appositi centri in cui le imprese possono rapportarsi con gli organi di controllo per discutere di problematiche connesse al FinTech e chiarificare eventuali questioni circa la conformità dei propri modelli di business rispetto al quadro regolamentare e agli specifici requisiti legali per l'esercizio dell'attività[388]. Molti paesi hanno anche istituito *regulatory sandboxes* per imprese innovative, ossia spazi normativi circoscritti e temporalmente limitati nell'ambito dei quali gli operatori e le autorità di controllo possono testare prodotti e soluzioni innovative individuandone concreto funzionamento e peculiarità[389].

Tuttavia, per promuovere innovazione e concorrenza nel comparto bancario aprendo la strada agli operatori FinTech, è necessario fronteggiare un problema di *data bottleneck*[390]. Le informazioni sono, infatti, una risorsa essenziale per competere nei servizi finanziari: l'intero comparto è costruito sulle informazioni e sulla loro gestione[391], sicché il tipo di informazioni in possesso delle istituzioni finanziarie e le modalità con le quali esse le utilizzano è centrale per l'impatto futuro delle FinTech[392]. Quali custodi delle finanze dei clienti, le banche svolgono un ruolo di *gateway* cruciale per la fruibilità di molti modelli di business FinTech[393]. Laddove i nuovi entranti necessitino di avere accesso a tali informazioni essenziali per orientare i consumatori verso i propri servizi, gli *incumbents* non saranno ovviamente disposti a condividere il proprio tesoro informativo. Pertanto, a tal riguardo, la regola di accesso ai conti disposto dalla PSD2 è finalizzata ad abbattere una barriera all'entrata per i *newcomers*[394].

L'accesso ai conti disposto dalla PSD2 non soltanto aumenta il livello potenziale di concorrenza nell'industria dei servizi finanziari e bancari, ma rappresenta inol-

386 European Supervisory Authorities, *Joint Committee Discussion Paper on The Use of Big Data by Financial Institutions*, (2016) 8-10, https://www.esma.europa.eu/sites/default/files/library/jc-2016-86_discussion_paper_big_data.pdf.

387 European Banking Authority, Discussion Paper on the EBA's approach to financial technology (FinTech), (2017) https://www.eba.europa.eu/documents/10180/1919160/EBA+Discussion+Paper+on+Fintech+%28EBA-DP-2017-02%29.pdf.

388 Oscar Borgogno e Giuseppe Colangelo, Regulating FinTech: From Legal Marketing to the Pro-Competitive Paradigm, (2020) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3563447.

389 Commissione europea, FinTech Action plan: For *a more competitive and innovative European financial sector,* COM(2018) 109 final, 8.

390 Borgogno e Colangelo, *Data, Innovation and Competition in Finance: The Case of the Access to Account Rule,* cit..

391 Robert Hauswald e Robert Marquez, *Information Technology and Financial Services* 16 Review of Financial Studies 921 (2003).

392 Giorgio Barba Navaretti, Giacomo Calzolari, Alberto Pozzolo, *FinTech and Banking. Friends or Foes?* 2 European Economy 9 (2017).

393 European Commission, Towards an Integrated European Market for Card, Internet and Mobile Payments, COM(2011) 941 final, 11.

394 UK Competition and Markets Authority, Retail Banking Markets Investigation Report, (2016) 126, https://www.gov.uk/cma-cases/review-of-banking-for-small-and-medium-sized-businesses-smes-in-the-uk. Si segnala anche Financial Conduct Authority, Strategic Review of Retail Banking Business Models, (2018) 8, https://www.fca.org.uk/publications/multi-firm-reviews/strategic-review-retail-banking-business-models.

tre un tassello fondamentale nella transizione verso l'Open Banking. Con tale espressione viene generalmente intesa l'evoluzione dell'attività bancaria che, mediante l'uso di *application programming interfaces* (APIs), permette ai consumatori di condividere i dati e le funzionalità dei propri conti bancari con imprese terze rispetto alla banca che gestisce il conto stesso[395].

Più in generale, la PSD2 si inserisce nel quadro di interventi europei tesi a promuovere la condivisione dei dati conferendo agli utenti nuovi diritti e poteri di controllo sugli stessi. In tal senso, la regola XS2A si aggiunge al diritto alla portabilità dei dati personali[396], alla promozione della libera circolazione dei dati non personali nei rapporti *business-to-business*[397] e del riutilizzo delle informazioni del settore pubblico[398], nonché al sostegno all'attiva partecipazione dei consumatori nel mercato dell'energia elettrica tramite l'implementazione di sistemi di *smart metering*[399]. Nella recente Comunicazione sulla "European strategy for data", la Commissione europea ha inoltre annunciato una ulteriore misura legislativa (Data Act) per incentivare il *data sharing* tra settori industriali[400], che al momento si è tradotta nella proposta di Regolamento sulla "European data governance" presentata lo scorso novembre[401].

Tutti i menzionati interventi condividono la medesima *ratio* pro-competitiva, ossia quella di incoraggiare la concorrenza promuovendo l'accesso ai dati e facilitando la condivisione e la portabilità degli stessi. Del resto, l'accesso ai dati è considerato un fattore cruciale per liberare la concorrenza e, secondo la Commissione europea, non sarebbero attualmente disponibili abbastanza dati per riutilizzi innovativi, laddove invece "businesses need a framework that allows them to start up, scale up, pool and use data, to innovate and compete or cooperate on fair terms"[402]

Non si può, tuttavia, sottacere come un numero crescente di studi mettano in discussione l'efficacia della portabilità dei dati nel favorire la concorrenza. In particolare, diversi studiosi hanno segnalato gli effetti inattesi e involontari del Regolamento generale sulla protezione dei dati (GDPR), documentando come lo stesso abbia di fatto rafforzato il potere di mercato degli *incumbents*[403]. Medesime preoccupazioni sono

395 Oscar Borgogno e Giuseppe Colangelo, Data sharing and interoperability: Fostering innovation and competition through APIs, 35 Computer Law & Security Review 1 (2019).

396 Regolamento 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, GU L 119/1 (2016), Articolo 20.

397 Regolamento 2018/1807 relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea, GU L 303/59 (2018).

398 Direttiva 2019/1024 relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico, GU L 172/56 (2019).

399 Direttiva 2019/944 relativa a norme comuni per il mercato interno dell'energia elettrica, GU L 158/125 (2019).

400 COM(2020) 66 final, 13.

401 European Commission, 'Proposal for a Regulation on European data governance (Data Governance Act)', COM(2020) 767 final.

402 Commissione europea, Comunicazione 'Shaping Europe's digital future', COM(2020) 67 final, 1 e 6.

403 Michail Batikas, Stefan Bechtold, Tobias Kretschmer, and Christian Peukert, *European Privacy Law and Global Markets for Data*, (2020) CEPR Discussion Paper No. 14475, http://cepr.org/active/publications/discussion_papers/dp.php?dpno=14475; James Bessen, Stephen M Impink, Lydia Reichensperger, and Robert Seamans, *GDPR and the Importance of Data to AI Startups*, (2020) Boston University School of Law, Law & Economics Series Paper No. 20-13 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3576714; Michal Gal and Oshrit Aviv, *The Unintended Competitive Effects of the GDPR*, Journal of Competition Law and Economics (in corso di pubblicazione); Damien Geradin,

state sollevate riguardo l'ingresso delle piattaforme BigTech nel mercato dei servizi bancari al dettaglio a seguito della regola XS2A introdotta dalla PSD2[404]. Il timore che le BigTech, sfruttando l'enorme dotazione di dati generati dai loro networks, possano utilizzare la regola di accesso ai conti per monopolizzare il mercato dei servizi finanziari offrendo una combinazione di servizi e praticando il *self-preferencing*, ossia riconoscendo un trattamento preferenziale ai propri prodotti e servizi rispetto a quelli offerti dai concorrenti[405].

In questo senso, si segnala la particolare attenzione rivolta ai servizi di pagamento offerti dai *digital gatekeepers* nella recente proposta del Digital Markets Act[406]. Al considerando 14, la Commissione europea segnala, infatti, come "[a]s gatekeepers frequently provide the portfolio of their services as part of an integrated ecosystem to which third-party providers of such ancillary services do not have access, at least not subject to equal conditions, and can link the access to the core platform service to take-up of one or more ancillary services, the gatekeepers are likely to have an increased ability and incentive to leverage their gatekeeper power from their core platform services to these ancillary services [such as identification or payment services and technical services which support the provision of payment services], to the detriment of choice and contestability of these services". Date queste premesse, il successivo Articolo 6, nel dettagliare gli obblighi specifici in capo alle piattaforme *gatekeeper*, prevede alla lettera f) che queste ultime "shall allow business users and providers of ancillary services access to and interoperability with the same operating system, hardware or software features that are available or used in the provision by the gatekeeper of any ancillary services".

5.2 Il diritto alla portabilità dei dati nella PSD2: obiettivi e strumenti

Negli ultimi anni l'approccio adottato dall'Unione Europea nei confronti dell'industria dei sistemi di pagamento è mutato considerevolmente. Inizialmente, tra

Theano Karanikioti and Dimitrios Katsifis, *GDPR Myopia: How a Well-Intended Regulation ended up Favoring Google in Ad Tech*, (2020) TILEC Discussion Paper No. 12, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3598130; Garrett Johnson and Scott Shriver, *Privacy & market concentration: Intended & unintended consequences of the GDPR*, (2020) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3477686.

404 Oscar Borgogno e Giuseppe Colangelo, *The data sharing paradox: BigTechs in finance*, 16 European Competition Journal 492 (2020); Fabiana Di Porto e Gustavo Ghidini, "*I Access Your Data, You Access Mine*": *Requiring Data Reciprocity in Payment Services*, 51 IIC 307 (2020); Jon Frost, Leonardo Gambacorta, Yi Huang, Hyun Song Shin, e Pablo Zbinden, *BigTech and the changing structure of financial intermediation*, Economic policy (in corso di pubblicazione); Miguel de la Mano e Jorge Padilla, *Big Tech Banking*, 14 Journal of Competition Law and Economics 494 (2018); Xavier Vives, *Digital disruption in financial markets*, 11 Annual Review of Financial Economics 243 (2019).

405 Jacques Crémer, Yves-Alexandre de Montjoye, e Heike Schweitzer, *Competition policy for the digital era*', (2019) 33, https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf; Expert Group on Regulatory Obstacles to Financial Innovation, *Thirty Recommendations on Regulation, Innovation and Finance*, (2019) 79-80, https://ec.europa.eu/info/sites/info/files/business_economy_euro/banking_and_finance/documents/191113-report-expert-group-regulatory-obstacles-financial-innovation_en.pdf.

406 European Commission, 'Proposal for a Regulation on contestable and fair markets in the digital sector (Digital Markets Act)', COM(2020) 842 final.

l'entrata in vigore del Trattato di Roma e gli anni '90, il quadro regolamentare comunitario in materia di pagamenti ha coinvolto prevalentemente la disciplina delle movimentazioni trans-frontaliere mediante strumenti di *soft law* e *negative integration*[407]. Soltanto con l'introduzione dell'euro come moneta unica, il legislatore europeo ha orientato i propri sforzi verso il coordinamento della disciplina pubblica e dell'autoregolamentazione privata. A questo proposito, l'arena dei pagamenti al dettaglio è stata rinnovata dalla commistione tra la legislazione comunitaria e la standardizzazione normativa coordinata dal Consiglio Europeo per i Pagamenti che ha permesso l'istituzione dell'Area Unica dei Pagamenti in Euro (SEPA). Nella parte finale del proprio percorso evolutivo, un nuovo approccio, noto come *regulation for competition*, finalizzato ad assicurare un adeguato livello di concorrenza nei mercati dei servizi di pagamento, è divenuto il nuovo cardine della politica legislativa europea.

Sin dalle sue prime fasi di implementazione, il mercato unico europeo per i sistemi di pagamento si è fondato sull'ibridazione regolamentare pubblico-privata. Dal punto di vista legislativo, la Direttiva 2007/63/EC (PSD) ha rappresentato il primo tentativo di disegnare una chiara cornice normativa capace di ripartire in modo netto i rischi e le responsabilità tra i prestatori di servizi di pagamento e gli utenti così come i limiti di reversibilità delle transazioni[408]. Oltre all'ambizioso proposito di normare omogeneamente una vasta gamma di strumenti di pagamento mediante uno strumento di regolamentazione orizzontale, la PSD si era distinta per l'espresso obiettivo di incentivare la concorrenza nel mercato dei sistemi di pagamento[409]. Tale scopo è stato perseguito armonizzando i requisiti di accesso al mercato[410] e impostando una licenza unica per gli operatori del settore così come un primo meccanismo di accesso alle infrastrutture tecniche dei sistemi di pagamento adottate dalle imprese prestatrici[411].

A partire dall'entrata in vigore della PSD, l'industria dei pagamenti al dettaglio ha vissuto un significativo processo evolutivo culminato recentemente nell'innovazione FinTech, con una crescita esponenziale di nuovi servizi di pagamento tale da richiedere un incisivo aggiornamento della cornice regolamentare definita nel 2007[412]. In prima battuta, buona parte dei nuovi servizi di pagamento *front-end* emersa negli ultimi anni sono infatti risultati esenti dell'applicazione della PSD, rendendo estremamente difficile definire una chiara ripartizione di diritti e doveri circa i rapporti con la clientela, le banche e altri operatori finanziari. In particolare, i prestatori di servizi di disposizione di ordini di pagamento – che permettono ai pagatori di ordinare pagamenti attraverso la piattaforma di *online banking* del proprio istituto bancario - si stanno dimostrando efficienti e competitivi rispetto ai sistemi tradizionali, riducendo i costi di transazione per i consumatori. Analogamente, i prestatori di servizi di informazione sui conti hanno

407 Agnieszka Janczuk-Gorywoda, *Evolution of EU Retail Payments Law*, 40 European Law Review 858 (2015).

408 GU L 300/47 (2007).

409 Despina Mavromati, *The Law of Payment Services in the EU: The EC Directive on Payment Services in the Internal Market*, 2008, 199-200 e 213-214, Kluwer Law International, Alphen aan den Rijn.

410 PSD, Considerando 10, 17, e 42.

411 PSD, Considerando 16 e Articolo 28(1).

412 Commissione europea, *Towards an integrated European market*, cit., 7.

iniziato ad offrire agli utenti servizi di analisi aggregata delle movimentazioni realizzate sui rispettivi conti di pagamento[413]. La frammentazione dell'industria lungo i confini degli Stati Membri è rimasta infine un grave ostacolo allo sviluppo del Mercato Unico europeo anche per quanto concerne il settore dei servizi di pagamento.

Alla luce di tali esigenze, il legislatore europeo ha ritenuto appropriato predisporre una nuova cornice regolamentare con la PSD2, entrata in vigore il 13 gennaio 2018. In via di prima approssimazione, la suddetta direttiva affronta molti dei vuoti legislativi e di supervisione lasciati dalla PSD, tra cui la mancanza di sufficienti misure di tutela della clientela e ripartizione delle responsabilità lungo l'intero processo di pagamento[414]. La PSD2 riconosce inoltre la presenza dei nuovi operatori specializzati nell'offerta di servizi di disposizione di ordine di pagamento e di servizi di informazione sui conti riconducendoli ("indipendentemente dal modello commerciale da essi applicato")[415] sotto un'uniforme cornice regolamentare ricomprendente requisiti uniformi di sicurezza, licenza e supervisione in condizioni di parità rispetto agli altri prestatori di servizi di pagamento[416].

Offrendo servizi di radicamento del conto, gli istituti bancari ricoprono una funzione cruciale nell'ambito dell'ecosistema FinTech. Infatti, la possibilità di prestare un'ampia gamma di nuovi servizi è condizionata all'accesso delle piattaforme bancarie su cui sono ancorati i conti di pagamento degli utenti. Il modello di *business* di molte imprese FinTech richiede, oltre alla disposizione di ordini di pagamento e la raccolta di informazioni circa le movimentazioni di denaro, anche una celere conferma circa la disponibilità di fondi sui conti della clientela è spesso vitale

Ai sensi della PSD, gli istituti bancari potevano legittimamente rifiutare l'accesso o la condivisione di informazioni riservate con imprese terze per ragioni di sicurezza, tutela della proprietà intellettuale nonché per tutelarsi da rischi di responsabilità civile e reputazionale[417]. Per quanto astrattamente ragionevoli, è chiaro che tali motivazioni offrirebbero uno scudo agli *incumbents* per impedire ogni accesso alla propria clientela da parte di nuovi concorrenti. I gestori dei conti conservano infatti un incentivo economico a rifiutare qualsiasi forma di cooperazione con i fornitori esterni, nonostante l'esplicita richiesta dei propri clienti o quando nessuna valida giustificazione può essere rinvenuta[418]. Ne consegue, pertanto, che, in mancanza di un apposito quadro regolamentare, la stessa esistenza di mercati integrati fondati su conti di pagamento bancari rischia di essere seriamente compromessa. Per questa ragione, fin dai lavoratori preparatori alla redazione della PSD2, la Commissione Europea ha esaminato

413 Commissione europea, *Impact Assessment accompanying the Proposal for a directive on payment service in the internal market*, SWD(2013) 288 final, 25-26.

414 Commissione europea, *Impact Assessment*, cit., 16.

415 PSD2, Considerando 33.

416 PSD2, Considerando 27-33.

417 Commissione europea, *Impact Assessment*, cit., 137.

418 Commissione europea, *Towards an integrated European market*, cit., 11.

varie opzioni di intervento volte a prevenire il verificarsi di pratiche commerciali escludenti capaci di soffocare sul nascere l'innovazione FinTech nel mercato dei servizi di pagamento[419].

La Commissione europea ha infine optato per un approccio volto ad eliminare un ostacolo primario per l'accesso ai conti ed allo stesso tempo farsi carico del vuoto normativo circa l'attività dei prestatori di servizi di pagamento. Ai sensi delle disposizioni sul regime di accesso ai conti, prestatori di servizi di pagamento di radicamento del conto, come le banche, devono permettere a imprese terze di accedere in tempo reale ai dati relativi ai conti di pagamento oltre a garantire l'accesso a tali conti eseguendo ordini di pagamento disposti attraverso fornitori esterni, fermo restando il consenso dell'utente interessato e l'accessibilità online del conto di pagamento[420]. Inoltre, le banche sono soggette all'obbligo di garantire tale accesso a condizioni non-discriminatorie sia nei confronti dei prestatori di servizi di disposizione di ordine di pagamento[421] che dei prestatori di servizi di informazione sui conti[422]. In particolare, qualsiasi gestore di conto di pagamento ha l'onere di eseguire e processare ogni ordine di pagamento veicolato da un soggetto terzo come se fosse richiesto dall'utente stesso attraverso la piattaforma di pagamento della banca, senza alcun onere aggiuntivo in termini di tariffe, tempistiche e priorità[423]. Ciò nonostante, non è ancora del tutto chiaro se i gestori dei conti possano addebitare una commissione per l'accesso fornito agli operatori *front-end*. In effetti, i servizi di pagamento assicurati alla clientela bancaria non sono gratuiti *ex se* in quanto ricompresi nella tariffa complessiva applicata dalla banca per la gestione del conto[424]. Pertanto, potrebbe essere teoricamente possibile che una tale forma di accesso forzato sia compensata al pari di come avviene, *mutatis mutandis*, con i brevetti essenziali (*standard essential patents*) concessi in licenza a condizioni eque, ragionevoli e non discriminatorie (FRAND)[425].

Allo stesso tempo, sia i prestatori di servizi di disposizione di ordine di pagamento che i prestatori di servizi di informazione sui conti sono tenuti ad una previa registrazione secondo le procedure predisposte nello stato membro competente al fine di poter legittimamente esercitare la propria attività nel rispetto dei requisiti stabilità dall'Autorità Bancaria Europea (EBA)[426]. Inoltre, i prestatori terzi devono rispettare alti standards di sicurezza e rispettare la disciplina di tutela dei dati personali[427]. Ciò posto,

419 Commissione europea, *Impact Assessment*, cit., 63-64 e 222-223.

420 PSD2, Articoli 64-68.

421 PSD2, Articolo 66(4)(c).

422 PSD2, Articolo 67(3)(b).

423 PSD2, Articoli 66(4)(c) e 67(3)(b).

424 The Netherlands Authority for Consumers & Markets, *Fintechs in the payment system. The risk of foreclosure*, (2017) 35, https://www.acm.nl/sites/default/files/documents/2018-02/acm-study-fintechs-in-the-payment-market-the-risk-of-foreclosure.pdf.

425 Commissione europea, *FinTech Action plan*, cit., 7.

426 European Banking Authority, *Draft Regulatory Technical Standards on Strong Customer Authentication and common and secure communication under Article 98 of Directive 2015/2366 (PSD2)*, (2017) 5-11, https://www.eba.europa.eu/documents/10180/1761863/Final+draft+RTS+on+SCA+and+CSC+under+PSD2+(EBA-RTS-2017-02).pdf.

427 PSD2, Articolo 94. I dati relativi ai conti di pagamento rappresentano dati personali secondo l'ampia definizione fornita dall'Articolo 4 del Regolamento 2016/679 (GDPR), sicché è necessario chiarire come le due discipline vadano coordinate. L'Articolo 20 del GDPR ha, infatti, introdotto un nuovo diritto alla portabilità dei dati, alla luce del quale ogni

tali operatori, non dovendo custodire il denaro degli utenti, sono esenti dai più stringenti requisiti macroprudenziali cui sono soggette le imprese bancarie[428]. A questo proposito, ai prestatori di servizi di informazione sui conti è vietato lo sfruttamento, la raccolta e l'accesso di informazioni raccolte che trascendano quanto necessario per l'esecuzione dello specifico servizio fornito all'utente[429].

Con riferimento alla sicurezza delle movimentazioni di denaro, la PSD2 impone che le credenziali degli utenti non siano condivise con parti esterne al rapporto[430]. L'unico soggetto cui è permesso ottenere tali informazioni, oltre al cliente stesso ed al gestore del conto, è il beneficiario del pagamento, previo assenso del pagatore[431]. Da ultimo, i prestatori di servizi di pagamento sono tenuti ad identificarsi presso l'infrastruttura *online* del gestore del conto per ogni singola richiesta di accesso. Conseguentemente, ogni forma di comunicazione tra il gestore ed il prestatore terzo deve avvenire in modo sicuro e predefinito[432]. L'EBA è stata a tal fine incaricata di sviluppare cinque raccolte di linee guida e sei bozze di standard tecnici di regolamentazione (RTS) cui i prestatori di servizi di pagamento devono conformarsi per garantire non soltanto adeguati livelli di sicurezza, ma anche un regolare ed effettivo funzionamento del meccanismo di accesso ai conti[433]. In ultimo, è opinione unanime tra esperti ed operatori che le APIs rappresentino il più affidabile strumento per assicurare l'implementazione del nuovo regime regolamentare delineato dalla PSD2[434]. Ciò posto, va al pari rilevato che al momento manca ancora un ampio consenso sulle modalità attraverso cui tali APIs vadano adottate e, più in particolare, se sia nella piena libertà delle imprese adottare autonomamente o coordinarne lo sviluppo mediante apposite attività di standardizzazione.

persona ha il diritto di vedersi restituite le informazioni personali fornite ad un titolare del trattamento sulla base del proprio consenso o di un contratto e ha il diritto che i suddetti dati vengano trasmessi senza impedimenti da un titolare del trattamento all'altro, se tecnicamente fattibile. Pertanto, con riferimento ai dati sui conti di pagamento, nel momento in cui gli utenti rivendicano la portabilità dei propri dati dovranno necessariamente optare per uno dei due regimi (PSD2 o GDPR). A tal riguardo, come chiarito dall'Article 29 Working Party (*Guidelines on the right to data portability*, (2017) 8, nota 15, http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233), dal momento che la regola di accesso stabilita nella PSD2 è *sector-specific*, l'eventuale opzione esercitata dall'utente supera l'applicazione del principio generale di portabilità dei dati previsto nel GDPR.

428 PSD2, Considerando 34 e 35.

429 PSD2, Articoli 65(3) e 66(3)(e-f).

430 PSD2, Articolo 66(3)(b).

431 PSD2, Articoli 63(3)(d) e 98(1)(d).

432 PSD2, Articoli 66(4)(a) e 98(1)(d).

433 PSD2, Articolo 96(3) and (4).

434 Portuguese Competition Authority, *Technological Innovation and Competition in the Financial Sector in Portugal*, (2018) 23, http://www.concorrencia.pt/vEN/Estudos_e_Publicacoes/Estudos_Economicos/Banca_e_Seguros/Documents/2018%20-%20Issues%20Paper%20Technological%20Innovation%20and%20Competition%20in%20the%20Financial%20Sector%20in%20Portugal.pdf; Financial Conduct Authority and HM Treasury, *Expectations for the third party access provisions in Payment Services Directive II*, 2017, 2, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/630135/Expectations_for_the_third_party_access_provisions_in_PSDII.pdf; Markos Zachariadis e Pinar Ozcan, *The API Economy and Digital Transformation in Financial Services: the Case of Open Banking*, SWIFT Institute Working Paper No. 1 (2016), 6, https://swiftinstitute.org/wp-content/uploads/2017/07/SIWP-2016-001-Impact-Open-APIs-FINAL.pdf.

5.3 Banche e piattaforme: l'emergere del modello *Open Banking*

Le recenti innovazioni in ambito FinTech hanno reso possibile un'evoluzione dell'attività bancaria comunemente definita come Open Banking[435]. Con tale espressione si intende lo sviluppo del business tradizionale fondato sull'interoperabilità e moderne tecniche di elaborazione dati amplificate dal nuovo potere conferito ai consumatori di permettere a terze parti di valorizzare i propri dati.

L'Unione Europea ed il Regno Unito stanno accelerando il processo di transizione verso l'Open Banking mediante interventi di carattere regolamentare e misure volte a supportare e coordinare iniziative di standardizzazione[436]. Le autorità di regolamentazione stanno dirigendo tale mutamento permettendo ad operatori esterni rispetto alle banche di accedere ai conti di pagamento della clientela ed ai relativi dati, permettendo loro di offrire una vasta gamma di nuovi servizi. Come già notato, l'Unione Europea ha gettato le fondamenta per rendere possibile l'Open Banking con l'emanazione di una nuova cornice regolamentare definita nella PSD2. Dal canto suo, il Regno Unito ha deciso di rafforzare ulteriormente tale nuovo quadro regolamentare emanando misure aggiuntive volte ad implementare il livello di concorrenza e porsi all'avanguardia nello sviluppo dell'Open Banking.

In particolare, a valle di una *market investigation* lanciata nel 2014 e completata nell'agosto del 2016[437], la UK Competition and Market Authority (CMA) decise di emanare un pacchetto di rimedi complementare alla PSD2 e espressamente diretto ad accelerare l'implementazione della XS2A[438]. Gli obiettivi dichiarati erano quelli di favorire un maggiore coinvolgimento dei consumatori rendendo ad essi più agevole la possibilità di cambiare il fornitore di servizi bancari e di ridurre le barriere d'ingresso al mercato facilitando l'accesso a potenziali nuovi entranti. Al fine di supportare una effettiva condivisione e portabilità dei dati, la CMA ha così imposto ai nove principali istituti bancari di sviluppare un'unica e aperta API standardizzata, disponibile gratuitamente per l'intero comparto. In secondo luogo, al fine di rafforzare la fiducia dei consumatori nel meccanismo della XS2A, è stato introdotto un livello di protezione più elevato rispetto a quello definito dalla PSD2, imponendo alle banche di pubblicare informazioni affidabili ed oggettive sulla qualità dei propri servizi in una modalità tale da poter essere utilizzate da *comparison tools*, nonché di informare tempestivamente i consumatori su eventuali incrementi tariffari o chiusure di filiali locali e di predisporre meccanismi di indennizzo per risolvere le dispute.

435 Euro Banking Association, *Understanding the Business Relevance of Open APIs and Open Banking for Banks*, (2016) https://www.abe-eba.eu/media/azure/production/1522/business-relevance-of-open-apis-and-open-banking-for-banks.pdf; Euro Banking Association, *Open Banking: Advancing Customer-Centricity. Analysis and Overview*, (2017) https://www.abe-eba.eu/media/azure/production/1355/eba_open_banking_advancing_customer-centricity_march_2017.pdf; UK Open Banking Working Group, *Unlocking the potential of open banking to improve competition, efficiency and stimulate innovation,* (2016) http://dgen.net/1/The-Open-Banking-Standard.pdf.

436 Diana Milanesi, *A New Banking Paradigm: The State of Open Banking in Europe, the United Kingdom and the United States*, TTLF Working Papers n. 29 (2017), 50-105, https://law.stanford.edu/publications/a-new-banking-paradigm-the-state-of-open-banking-in-europe-the-united-kingdom-and-the-united-states/.

437 UK Competition and Markets Authority, *Retail Banking Markets Investigation Report*, cit..

438 UK Competition and Markets Authority, *The Retail Banking Market Investigation Order*, cit..

Sulla scia dell'Europa e del Regno Unito, numerose autorità hanno manifestato interesse nello sviluppo di un quadro regolamentare capace di consentire ai consumatori di gestire i propri *account data* attraverso APIs standardizzate. Nello specifico, l'Australian Government Productivity Commission ha raccomandato l'adozione di un regime di Open Banking[439] e, su queste basi, il recente *Australian Consumer Data Right* ha introdotto un ampio diritto di portabilità dei dati che verrà inizialmente applicato proprio al settore bancario[440]. Replicando l'esperienza britannica, l'Australian Competition and Consumer Commission ha imposto ai principali quattro istituti bancari di condividere dati di riferimento dei prodotti, quali tassi di interesse, tasse, tariffe, e requisiti per l'accesso a mutui e carte di credito. Sulla stessa falsariga, a partire dal 2018 in Messico la *Ley de Instituciones de Tecnología Financiera* ha imposto agli istituti finanziari di definire APIs che consentano, previo consenso degli utenti, l'accesso ad interfacce sviluppate o gestite da FinTech e altri operatori finanziari. In modo simile, il Canadian Competition Bureau ha sollecitato i *policymakers* ad adottare i passaggi necessari per favorire l'ingresso degli operatori FinTech attraverso la definizione di un regime aperto di accesso ai dati finanziari tramite API[441]. Come risultato, il Ministero delle Finanze ha istituito un apposito comitato con il compito di fornire indicazioni al Governo sull'adozione del regime di Open Banking[442]. Si segnala, inoltre, come nel 2017 in Giappone sia stato modificato il Banking Act al fine di promuovere una *open innovation* consentendo alle FinTech di accedere tramite API ai sistemi delle istituzioni bancarie. Nel 2018, la Hong Kong Monetary Authority ha lanciato l'*Open API Framework* fornendo specifiche linee guida per favorire la collaborazione tra banche e altri fornitori di servizi, e recentemente la Monetary Authority di Singapore ha pubblicato un *API Playbook* e predisposto un registro delle API per incoraggiare gli istituti bancari ad aprire i propri sistemi ai terzi. Infine, anche il Brasile si è dotato di una regolamentazione che introduca l'Open Banking a partire dalla fine del 2020.

Sebbene il quadro regolamentare europeo e britannico sia limitato ai servizi di pagamento, la ratio ed i principi sottostanti possono essere estesi ben al di là del comparto bancario consentendo ai consumatori di condividere i propri dati con diversi fornitori di servizi in una modalità standardizzata e sicura[443]. In questa direzione, il Regno Unito si è impegnato ad implementare tale approccio all'intero comparto dei servizi finanziari (mutui, assicurazioni, pensioni, risparmi ed investimenti) aprendo la strada alla *Open Finance*[444].

439 Australian Government Productivity Commission, *Competition in the Australian Financial System*, cit..

440 Australian Competition and Consumer Commission, *Competition and Consumer (Consumer Data Right) Rules 2020*, (2020) https://www.accc.gov.au/media-release/consumer-data-right-rules-made-by-accc.

441 Canadian Competition Bureau, *Technology-led innovation and emerging services*, (2017) https://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/04315.html.

442 Government of Canada, *Consumer-directed finance: the future of financial services*, (2019) https://www.canada.ca/en/department-finance/programs/consultations/2019/open-banking/report.html. Si veda anche Advisory Committee to the Open Banking Review, *A Review into the Merits of Open Banking*, (2019) https://www.canada.ca/en/department-finance/programs/consultations/2019/open-banking.html.

443 John Fingleton, *From Open Banking to Open Everything*, (2018) https://medium.com/fingleton/from-open-banking-to-open-everything-3072079b7c58.

444 See Financial Conduct Authority, *Call for Input: Open finance*, (2019) https://www.fca.org.uk/publication/call-for-input/call-for-input-open-finance.pdf.

Da un punto di vista concorrenziale, l'Open Banking presenta profili che meritano di essere indagati e pienamente compresi. È infatti evidente che tale evoluzione racchiude il potenziale di rafforzare la concorrenza all'interno dei mercati bancari e finanziari che sono tradizionalmente affetti da problemi di *lock-in* e alte barriere all'ingresso. Basti pensare, a questo riguardo, che il regime di accesso ai conti di pagamento può minare le rendite di posizione di cui hanno finora goduto gli *incumbents* nell'accedere alle informazioni circa le abitudini di spesa dei propri clienti e nel fornire loro servizi addizionali unitamente a quelli propriamente bancari. Analogamente, gli utenti ed i clienti professionali potranno beneficiare di un maggiore controllo in merito all'uso ed alla valorizzazione delle proprie risorse finanziarie, ad esempio attraverso lo sfruttamento delle possibilità offerte dalle più moderne tecniche di elaborazione dati (per esempio, manovrando più efficientemente le risorse detenute in conti detenuti presso diversi gestori mediante l'uso di un'unica piattaforma fornita da un operatore terzo).

Mediante l'apertura dell'infrastruttura di pagamento a soggetti terzi, il legislatore e le autorità di regolamentazione stanno predisponendo il mercato bancario per l'implementazione di modelli di business fondati su piattaforme. Parimenti gli istituti bancari hanno la possibilità di cogliere le opportunità competitive offerte da tale sviluppo e valorizzare a pieno il nuovo ruolo di intermediazione tra la clientela ed i nuovi operatori FinTech, tra cui in primo luogo i prestatori di servizi di pagamento.

In essenza, l'Open Banking sta rendendo possibile l'ascesa di nuovi mercati a più versanti fondati su piattaforme bancarie che svolgono attività di intermediazione tra gli utenti e gli operatori FinTech, generando ricadute positive per entrambi i versanti. In tali strutture di mercato, la piattaforma facilita le interazioni tra due o più gruppi di agenti che dipendono vicendevolmente l'uno dall'altro e che, senza la piattaforma, non potrebbero interagire generando reciproci benefici. In un ambiente Open Banking si generano effetti di rete indiretti capaci di bilanciare gli interessi degli operatori sui due versanti, internalizzando le esternalità di rete non altrimenti risolvibili mediante interazioni bilaterali: la piattaforma, pertanto, riveste un ruolo essenziale per i prestatori di servizi di disposizione di ordine di pagamento e di informazione sui conti. Date queste premesse, non stupisce che il ruolo di intermediazione svolto dai gestori dei conti di pagamento rivestirà con ogni probabilità una funzione cruciale nel permettere alle imprese FinTech di fornire i propri servizi, aumentando contemporaneamente il benessere complessivo dei consumatori. Gli istituti bancari si troverebbero, di conseguenza, di fronte alla necessità di raccogliere imprese ed individui da ambo i lati della piattaforma in modo da assicurarsi una massa critica sufficiente per alimentare gli effetti di rete indiretti, rendendo così la propria infrastruttura più attrattiva rispetto a quelle dei concorrenti.

In ragione della verosimile riduzione degli *switching costs* conseguente all'implementazione della PSD2, gli istituti bancari saranno immersi in un rinnovato ambiente competitivo molto più dinamico e contendibile rispetto al presente, in cui il pieno sfruttamento degli effetti di rete costituirà l'incentivo primario per innovare e offrire soluzioni più convenienti[445]. Al momento, i principali istituti bancari hanno già

445 Zachariadis e Ozcan, cit., 13.

avviato lo sviluppo di interfacce capaci di fornire agli sviluppatori esterni la possibilità di accedere alle proprie infrastrutture per offrire servizi aggiuntivi alla clientela. Analogamente alla strategia adottata da Apple nel permettere a sviluppatori esterni di operare sui propri sistemi operativi, le società finanziarie che intendono guadagnarsi (e mantenere) una posizione di forza in tale nuovo mercato dovranno attrezzarsi per offrire APIs opportunamente strutturate per agevolare l'attività e l'interazione con imprese esterne, che possano poi costruire nuovi prodotti per le piattaforme bancarie.

A tali nuove sfide gli istituti bancari potranno rispondere scegliendo tra una gamma variegata di approcci. Tra questi merita una speciale menzione il modello di mercato (*marketplace model*), grazie a cui la clientela potrà accedere sia ai servizi offerti da operatori terzi che ai prodotti della banca stessa[446]. In alternativa, i gestori dei conti potranno optare per l'adozione di un modello *plug-and-play* (simile a quello predisposto da Apple con la propria piattaforma chiusa). In questo scenario, la banca svilupperà e renderà disponibili una serie di APIs che ogni impresa interessata sarà libera di utilizzare per offrire servizi e prodotti sulla sua piattaforma. Con ogni probabilità, la strategia che le imprese bancarie adotteranno dipenderà fortemente dalle modalità con cui il regime di accesso ai conti di pagamento sarà implementato.

5.4 Conclusioni

L'emersione ed il crescente sviluppo del fenomeno FinTech ha azionato una corsa tra i policymakers a riformare il quadro regolatorio per supportare tale innovazione tecnologica. Di conseguenza, un ampio ventaglio di nuovi strumenti e approcci regolatori sono emersi negli ultimi anni. In tale contesto, l'intervento regolamentare implementato dall'Unione Europea con la PSD2 e, segnatamente, l'introduzione del regime di accesso ai conti di pagamento, rappresenta un convincente tentativo di rafforzare il livello di concorrenza nel mercato dei servizi finanziari e di pagamento al dettaglio. Inoltre, tale strumento normativo ha gettato le fondamenta per lo sviluppo dell'Open Banking predisponendo il mercato bancario all'implementazione di modelli di business fondati su piattaforme.

Da un punto di vista concorrenziale, la strategia adottata dal legislatore europeo e ulteriormente sviluppata da quello inglese si presenta come un interessante esperimento legislativo volto ad instaurare un regime di accesso ai dati su base non-discriminatoria a favore di nuovi potenziali operatori che altrimenti sarebbero nell'impossibilità di entrare sul mercato e competere alla pari con gli *incumbents*. I modelli di *business* di numerosi prestatori di servizi di pagamento innovativi si fondano, infatti, sulla disponibilità di informazioni affidabili e continuative circa la disponibilità di fondi sui conti di pagamento degli utenti. Pertanto, è di palese evidenza che per i prestatori di servizi di disposizione di ordini di pagamento e di informazione sui conti la possibilità di accedere agevolmente all'infrastruttura bancaria di gestione dei conti di pagamento è di cruciale importanza per l'esercizio della propria attività.

446 Milanesi, cit., 158.

Le autorità di concorrenza e di supervisione bancaria sono chiamate a vigilare sulla transizione verso l'Open Banking avviata dall'intervento regolamentare del legislatore europeo. Considerando i forti incentivi degli *incumbents* ad escludere dal mercato rilevante i nuovi operatori unitamente all'intrinseca difficoltà di implementazione del regime di accesso ai conti di pagamento, è opportuno che le autorità sorveglino con attenzione tale processo per evitare che pratiche anti-competitive siano poste in campo con lo scopo di neutralizzare il potenziale pro-competitivo della PSD2. Allo stesso tempo, l'ingresso delle piattaforme BigTech nel mercato dei servizi bancari al dettaglio impone un'attenta riflessione in ragione di una duplice prospettiva[447]: per un verso, il timore che tali piattaforme possano utilizzare la regola di accesso ai conti per monopolizzare il mercato dei servizi finanziari offrendo una combinazione di servizi e praticando il *self-preferencing*; per un altro verso, la possibilità che esse rappresentino, a differenza delle FinTech, l'unica vera minaccia competitiva agli attuali *incumbents* e che regole tese a limitarne l'ingresso nel settore finanziario possano paradossalmente favorire la difesa della posizione e delle rendite di questi ultimi.

447 Borgogno e Colangelo, *The data sharing paradox: BigTechs in finance*, cit..

La disintermediazione finanziaria. Flussi informativi e soggetti coinvolti

SECONDA PARTE

(con il coordinamento di S. Alvaro)

LE PIATTAFORME FINANZIARIE E LE AREE DI ARTICOLAZIONE DEL FINTECH

O. Borgogno, A. Manganelli, M. Manzi, C. Sertoli (*)

1 I nuovi soggetti di diritto. Funzioni, diritti e obblighi dei *Third Party Providers*

1.1 Premessa

Per comprendere il ruolo dei così detti *Third Party Providers*, e quindi la disciplina che è stata al riguardo prevista a livello europeo, è forse necessario partire dalla constatazione che oggi gran parte del valore dell'attività bancaria è nelle informazioni di cui la banca dispone.

La realtà economica e sociale è mutata: per un verso, la maggior parte del lavoro delle banche si riconduce all'elaborazione dei dati dei clienti, mentre, per altro verso, il processo di "dematerializzazione della moneta" ha raggiunto uno stadio di sviluppo assai maturo.

Sotto il primo riguardo, può osservarsi come, più in generale, siano proprio i dati a rivestire un ruolo centrale nel sistema economico, permettendo, per chi ne dispone, la conoscenza del mercato, delle sue tendenze e dei processi relativi ai consumi. Di qui, il loro cospicuo valore economico e la ragione per cui i nuovi protagonisti del *Fin-tech*[1] pongono alla base della loro attività proprio la raccolta e lo scambio dei dati stessi.

(*) Oscar Borgogno, dottorando Università di Torino (oscar.borgogno@unito.it);

Antonio Manganelli, Professore aggiunto in Competition Policy, Università di Siena; Coordinatore scientifico di Deep-In e Competition Policy Centre-ICPC (antonio.manganelli@unisi.it);

Mariachiara Manzi, dottoranda Università Europea e Innovation and Competition Policy Centre-ICPC (mariachiara.manzi@yahoo.it);

Cecilia Sertoli, Avv.; Eni S.p.A. (assistente al Presidente di Eni); dottoranda Università Europa e Innovation and Competition Policy Centre-ICPC (ceciliasertoli@gmail.com).

Sotto il secondo riguardo, si tenga presente come il processo di digitalizzazione dei rapporti economici ha coinvolto, e coinvolge, anche i sistemi di pagamento, donde, appunto, il fenomeno di "dematerializzazione" degli strumenti di pagamento.

In questo scenario si sono grandemente sviluppate nella prassi le attività di raccolta e di analisi dei dati personali: ci si riferisce al fenomeno che oggi è comunemente evocato con la locuzione *Big Data* e che è ormai al centro di un ricco dibattito dottrinale. L'attività delle banche di costituzione di *Big Data* si sostanzia essenzialmente nel momento della c.d. profilazione. Per tale si intende la raccolta e l'analisi di una cospicua mole di dati per ricostruire il "profilo" del cliente (gusti, interessi, preferenze, abitudini, stili, propensioni di consumo, ecc.) che viene realizzata, nel caso dei pagamenti digitali, tanto dalle banche quanto da altri soggetti (tra i quali appunto i *Third Party Providers*), al fine di poter creare un profilo personale di quella che è la situazione economica del singolo individuo così da consentire a tutti gli operatori economici potenzialmente interessati di disegnare una offerta *ad hoc* e anzi, diremmo, *ad personam*.

Ora, se da un lato sembrerebbe che la raccolta dei dati possa apportare benefici tanto all'impresa quanto ai consumatori, dall'altro occorre sottolineare come questa attività, che è in continua ed esponenziale crescita, può comportare anche pericoli e distorsioni per il mercato. Inoltre, a questo riguardo, è necessario prestare attenzione al problema, che ora si presenta come concreto ed attuale, della c.d. "de-patrimonializzazione dei dati"[2].

Se si muove da questi assunti – peraltro ormai ben poco originali – risulta allora evidente che la *Payment Services Directive 2* (d'ora in avanti anche solo "PSD2")[3] non ha rappresentato uno dei moltissimi atti normativi di natura tecnica, che a vari livelli gli ordinamenti nazionali e sovranazionali continuamente promulgano, quanto piuttosto il primo passo verso l'*open banking*[4]: con essa si è infatti inteso disciplinare le condizioni per rendere disponibili i dati dei clienti tra i diversi soggetti del mondo bancario (banche e altre soggetti operanti nel settore: appunto i *providers*)[5]. L'*open banking* presuppone infatti, per funzionare, la simultanea cura di due interessi: da un

1 Per una prima informazione si rinvia a AA.VV., *FinTech, Introduzione ai profili giuridici di un mercato unico tecnologico dei servizi finanziari,* Giappichelli, Torino, 2017, e R. LENER, G. CARRARO, G. FIORDIPONTI ET AL., *Fintech: Diritto, tecnologia e finanza*, in *Quaderni di Minerva Bancaria*, 2018/1, p. 29 ss.

2 Cfr. sul tema G. RESTA – V. ZENO ZENCOVICH, *Volontà e consenso nella fruizione dei servizi in rete*, in *Riv. trim. dir. proc. civ.*, 2018, p. 411 ss.

3 Direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio, del 25 novembre 2015 relativa ai servizi di pagamento nel mercato interno.

4 Il fenomeno di apertura del sistema bancario a soggetti diversi dalle banche, realizzato attraverso l'obbligo, rivolto alle banche, di mettere a disposizione e condividere con tali soggetti i dati bancari e finanziari degli utenti.

5 EURO BANKING ASSOCIATION, *Understanding the Business Relevance of Open APIs and Open Banking for Banks*, 2016, consultabile attraverso il *link: https://www.abe-eba.eu/media/azure/production/1522/business-relevance-of-open-apis-and-open-banking-for-banks.pdf*; EURO BANKING ASSOCIATION, Open Banking: Advicing Customer-Centricity. Analysis and Overview, 2017, https://www.abe-eba.eu/media/azure/production/1355/eba_open_banking_advancing_customer-centricity_march_2017.pdf; EUROPEAN BANKING AUTHORITHY, Discussion Paper on the EBA's approach to financial technology, *(Fintech), 2017, https://eba.europa.eu/sites/default/documents/files/documents/10180/1919160/7a1b9cda-10ad-4315-91ce-d798230ebd84/EBA%20Discussion%20Paper%20on%20Fintech%20%28EBA-DP-2017-02%29.pdf?retry=1.*

lato, garantire un sufficiente grado di sicurezza dei dati del cliente e, dall'altro, la possibilità per banche e *providers* di scambiarsi informazioni in modo tale che il cliente e il consumatore possano essere oggetto di migliore profilazione e, al contempo disporre, di un canale unico per i pagamenti digitali.

Ne consegue che la Direttiva ha rappresentato l'inizio di una vera e propria lotta concorrenziale nel settore dei servizi di pagamento: una competizione tra banche (e altri tradizionali protagonisti dei sistemi di pagamento già autorizzati ad operare) e nuovi soggetti interessati a entrare in quello stesso mercato. Come è stato scritto, si tratta di «*un modo di "fare banca" che presumibilmente sta già mettendo in discussione le vecchie logiche e gli equilibri più tradizionali*»[6].

La PSD2, con lo scopo ultimo di realizzare un mercato unico dei pagamenti elettronici in Europa, mira dunque a introdurre, da un lato, più innovazione e, dall'altro, più concorrenza, con la ulteriore conseguenza di segnare la inevitabile fine del monopolio delle banche nel controllo delle informazioni e dei dati relativi ai clienti e alle loro operazioni[7].

Questa premessa può allora dare ragione del modo con cui il presente contributo è articolato.

Anzitutto, si ripercorreranno più da vicino le ragioni che hanno portato alla approvazione di una nuova disciplina europea dei sistemi di pagamento e al contenuto generale della PSD2.

In secondo luogo, si analizzeranno nelle loro diverse varietà e specie, le figure (del tutto centrali) dei *Third Party Providers*.

Solo allora si potrà affrontare *ex professo* il tema più specificamente evocato dal titolo dello studio, quello cioè della specifica disciplina di questi nuovi soggetti.

Infine, l'ultima parte sarà espressamente dedicata a quello che, coerentemente con le premesse del discorso, appare il problema cruciale del rapporto tra *Third Party Providers*, banche e clienti: quello, appunto, relativo al regime di accesso e trattamento dei dati.

1.2 La seconda direttiva sui sistemi di pagamento (PSD2)

La seconda direttiva sui sistemi di pagamento, e cioè la già citata PSD2 (attuata in Italia con il d.lgs. 15 dicembre 2017, n. 218[8]), fu voluta per modificare in modo

6 Come si legge in I. D'Ambrosio, *La tutela del consumatore nei pagamenti elettronici e la nuova direttiva europea PSD2*, in *Notariato*, 2019, p. 685.

7 Così A. Brener, *Payment Service Directive II and Its Implications, in Disrupting Finance. Palgrave Studies in Digital Business & Enabling Technologies*, a cura di T. Lynn, J. Mooney, P. Rosati, M. Cummins, Palgrave Pivot, 2019, p. 104 (citando, a sua volta, V. Dombrovskis, *Payment services: Consumers to benefit from cheaper, safer and more innovative electronic payments*, disponibile su http://europa.eu/rapid/press-release_IP-18-141_en.htm2018).

8 Che ha tra l'altro inciso, modificandoli, sui seguenti decreti legislativi: 1° settembre 1993, n. 385 (Testo unico delle leggi in materia bancaria e creditizia); 27 gennaio 2010, n. 11; 18 agosto 2015, n. 135. Cfr. F. Marasà, *Servizi di pagamento e responsabilità degli intermediari*, Giuffrè, 2020, p. 36 ss.

significativo il previgente assetto normativo in tema di servizi di pagamento. Tale assetto era stato dettato, nel mercato interno, solo pochi anni prima dalla Prima direttiva in materia (la così detta *Payment Services Directive* o anche PSD)[9]. Ma quella prima direttiva sui servizi di pagamento aveva sostanzialmente mancato l'obbiettivo di sviluppare i sistemi di pagamento in una dimensione sovranazionale ed era ben lungi dal rappresentare una intelaiatura sulla quale realizzare il mercato unico digitale[10]. E, d'altra parte, la crescita esponenziale dell'attività bancaria mobile e a distanza (c.d. *mobile and internet banking*) evidenziava l'esigenza di una revisione integrale della disciplina a livello europeo.

In questo contesto le istituzioni euro-unitarie ritennero di cogliere l'occasione per incentivare l'introduzione e l'affermazione di nuovi servizi di pagamento, che potessero, in prospettiva, disintermediare i vecchi sistemi (sempre, ben si intende, di pagamento), quali ad esempio quelli rappresentati dalle tradizionali carte di credito; e ciò al dichiarato scopo di ridurre i costi dei pagamenti.

Di qui quel valore e quel significato della PSD2 di cui si è detto nelle premesse: per le banche e gli altri intermediari *incumbent*, di sfida; per i grandi *incomers*, di opportunità; per tutti, segnale di inizio delle "ostilità".

Più nel dettaglio, merita di essere ricordato come la PSD2 abbia modificato: *(i)* la Direttiva concernente la commercializzazione a distanza di servizi finanziari ai consumatori[11]; *(ii)* quella concernente l'avvio, l'esercizio e la vigilanza prudenziale dell'attività degli istituti di moneta elettronica[12]; *(iii)* quella sull'accesso all'attività degli enti creditizi e sulla vigilanza prudenziale sugli enti stessi e sulle imprese di investimento[13]; *(iv)* nonché il Regolamento istitutivo della *European Banking Authority* (EBA)[14]. Già questi semplici riferimenti rappresentano un'ottima riprova di come il quadro normativo relativo ai pagamenti digitali fosse assai frammentato e, soprattutto, come esso non arrivasse a comprendere le attività di quei nuovi soggetti che ormai erano entrati a far parte del mercato degli intermediari.

Attraverso questi interventi di dettaglio la PSD2 persegue – come si è accennato in premessa – la finalità di sviluppare un mercato unico digitale, così come d'altronde era stato in occasione della nascita della "Area Unica dei Pagamenti in Euro" (la

9 Direttiva 2007/64/CE del Parlamento europeo e del Consiglio del 13 novembre 2007, relativa ai servizi di pagamento nel mercato interno. Per una sintesi cfr. ora F. MARASÀ, *Servizi di pagamento e responsabilità degli intermediari*, cit., p. 21 ss.

10 Gli Stati Membri avevano applicato i principi e le regole della *Payment Services Directive*, quantomeno in relazione ad alcuni specifici servizi, in modo così eterogeneo da comportare: *(i)* arbitraggi normativi; *(ii)* un grado non tollerabile di incertezza giuridica; e soprattutto *(iii)* un livello non sufficiente di pari protezione dei consumatori. In questo senso si può con sicurezza affermare che il principale scopo dell'ultimo intervento normativo (e quindi appunto l'adozione della PSD2) è rappresentato dal superamento della differenza tra le discipline dei diversi Paesi.

11 Direttiva 2002/65/CE del Parlamento europeo e del Consiglio, del 23 settembre 2002, concernente la commercializzazione a distanza di servizi finanziari ai consumatori.

12 Direttiva 2009/110/CE del Parlamento europeo e del Consiglio, del 16 settembre 2009, concernente l'avvio, l'esercizio e la vigilanza prudenziale dell'attività degli istituti di moneta elettronica.

13 Direttiva 2013/36/UE del Parlamento europeo e del Consiglio, del 26 giugno 2013, sull'accesso all'attività degli enti creditizi e sulla vigilanza prudenziale sugli enti creditizi e sulle imprese di investimento.

14 Regolamento (UE) n. 1093/2010.

c.d. SEPA)[15], dettando precise disposizioni per disciplinare l'ingresso nel mercato dei nuovi intermediari e regolando i servizi da questi offerti[16]. In realtà, la instaurazione del mercato unico digitale è stata pensata e continua ad essere perseguita attraverso una serie di direttive accomunate, appunto, dallo scopo di rafforzare la integrazione europea realizzando un mercato unico, che promuova la concorrenza e la innovazione così da apportare migliori servizi per la clientela.

In altre parole, l'obbiettivo alla base della introduzione della PSD2 è stato quello di modernizzare il mercato dei sistemi di pagamento, rendendo i relativi strumenti più economici, efficienti e sicuri, e, allo stesso tempo, quello di garantire la libera concorrenza del mercato. Come si legge nella premessa del documento per la consultazione predisposto dalla Banca d'Italia, «la PSD2 mira a promuovere lo sviluppo di un mercato integrato dei pagamenti elettronici più sicuro, efficiente, competitivo e idoneo ad assicurare un elevato livello di protezione degli utenti, anche in termini di maggiore trasparenza delle informazioni relative alle operazioni e ai servizi di pagamento»[17].

Ne discendono una serie di novità volte ad omologare il quadro normativo in merito ai pagamenti digitali e a colmare le predette lacune. Tali novità sono numerose e una loro puntuale disamina esula dai limiti di questo studio. Qui è sufficiente richiamare le più significative, che ci paiono essenzialmente quattro.

In primo luogo, la PSD2 risulta più ampia nel suo ambito di applicazione rispetto alla PSD. Infatti, è previsto che questo debba essere esteso anche alle operazioni di pagamento che non sono nella valuta di uno Stato membro e, quindi, ricomprende operazioni di pagamento in tutte le valute (c.d. «*one leg*» *transaction*), purché si tratti di pagamenti (*a*) effettuati con carte di pagamento ossia, come è stato detto, di operazioni «*basate su carta*»[18] e (*b*) dove anche solo uno dei due prestatori di servizi di pagamento (e quindi l'*issuer o* l'*acquirer*) si trovi nel territorio dell'Unione Europea.

In secondo luogo, sono state considerate e regolate anche nuove soluzioni di pagamento, come, ad esempio, il credito telefonico, quella relativa a *fee* uniformi per i

15 L'Area unica dei pagamenti in euro è un progetto promosso dalla Banca Centrale Europea e dalla Commissione europea che facendo seguito all'introduzione dell'euro mira a estendere il processo d'integrazione europea ai pagamenti al dettaglio in euro effettuati con strumenti diversi al contante (bonifici, addebiti diretti e carte di pagamento). La realizzazione di una area unica dei pagamenti consente quindi ai cittadini europei di poter effettuare pagamenti in euro a favore di beneficiari situati in qualsiasi paese della SEPA con la stessa facilità e sicurezza su cui si può contare nel proprio contesto nazionale.

16 F. Marasà, *Il trattamento dei dati personali dell'utente dei servizi di pagamento tra PSD2 e GDPR*, in Rivista Orizzonti del diritto commerciale, 2020, p. 629 ss., spec. p. 633. Ead., Servizi di pagamento e responsabilità degli intermediari, cit., p. 25 ss.

17 Documento per la consultazione del luglio 2018, Modifiche alle disposizioni materia di "*trasparenza delle operazioni e dei servizi bancari e finanziari. Correttezza delle relazioni tra intermediari e clienti*".

18 cfr. R. Caravaglia, *Il nuovo regolamento europeo sulle interchange fee dei pagamenti con carta: capiamolo meglio*, pubblicato su pagamenti digitali l'11 giugno 2015 e consultabile sul sito https://www.pagamentidigitali.it/mobile-app/il-nuovo-regolamento-europeo-sulle-interchange-fee-dei-pagamenti-con-carta-capiamolo-meglio/, dove si legge che «per "operazioni di pagamento basate su carta" si debba intendere qualsiasi transazione a valere su carta (ossia basata sull'infrastruttura e le regole commerciali di uno schema di carte di pagamento), che venga effettuata o in presenza del titolare (transazione presso un esercizio commerciale tramite pos) o in sua assenza (**e-commerce**, prescindendo dalla tecnologia di supporto o adozione. In tal senso, rientrano nell'ambito di applicazione anche quei pagamenti che sono eseguiti mediante l'impiego di **mobile wallet** e **digital wallet**, a patto che il risultato sia un'operazione di pagamento tramite la carta in essi registrata). Il regolamento si applica altresì ai pagamenti effettuati con carte **contactless** e a tutte le transazioni di **mobile payment** che prevedano l'impiego di una carta».

pagamenti con carta in linea con la MIF[19] o come la rimodulazione delle esenzioni esistenti (i c.dd. *negative scope*)[20].

In terzo luogo, è stata introdotta la c.d. *strong costumer authentication*, e, quindi, l'autenticazione basata sull'uso di due o più elementi, di cui uno conosciuto solo dall'utente (*knowledge*) e uno posseduto sempre solo dall'utente (*possession*), indipendenti l'uno dall'altro tanto che la eventuale violazione di uno non compromette l'affidabilità dell'altro[21].

Ultima, ma non ultima per importanza (quantomeno ai fini dell'oggetto del presente studio), è la novità rappresentata dalla circostanza che per la prima volta sono, appunto, oggetto di disciplina anche i *Third Party Providers* (la PSD non li contemplava, finendo così per configurare una lacuna significativa)[22].

1.3 I *Third Party Providers*

Ma di cosa parliamo esattamente quando evochiamo i *Third Party Providers*?

Una spiegazione proviene dalla Commissione Europea: «*new services have emerged in the area of internet payments where so called third party providers offer e-merchants specific payment solutions which do not necessarily require customers to open accounts with the third party provider*»[23].

La novità quindi non risiede tanto nel riconoscimento dell'attività di prestazione di servizi di pagamento a soggetti diversi dalle banche, già oggetto della PSD; bensì nel fatto che tale attività non debba essere collegata all'esistenza di un conto di pagamento presso lo stesso soggetto che svolge il servizio richiesto: come sopra detto i *Third Party Providers* si interpongono nella relazione che intercorre tra la banca (o istituto presso cui è radicato il conto) e il consumatore o, per essere più precisi, quei soggetti che fanno da tramite tra il cliente e il suo conto di pagamento *on-line*[24]. Ne

19 Si tratta, infatti, di quelle commissioni extra legate alla utilizzazione delle carte negli acquisti *on-line* o al ricorso al del *POS*, commissione comunemente applicati anche per pagamenti di importi di esiguo valore.

20 Tra cui quelle relative agli agenti commerciali, alle operazioni di pagamento effettuate tramite un fornitore di reti o servizi di comunicazione elettronica per un abbonato alla rete, quelle relative alle reti a spendibilità limitata e quella relativa il servizio di prelievo del contante tramite sportelli automatici di prestatori indipendenti.

21 Cfr., sul punto, EBA, Discussion on RTS on *strong costumer authentication and secure communication under PSD2*, consultabile attraverso il *link*: https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/regulatory-technical-standards-on-strong-customer-authentication-and-secure-communication-under-psd2/-/regulatory-activity/discussion-paper.

22 La Direttiva, tuttavia, non ha elaborato una definizione di "servizio di pagamento" ma si è limitata ad aggiungere all'elenco delle attività considerate tali, già esistente nella PSD, il servizio di disposizione di pagamento e il servizio di informazione sui conti.

23 Cfr. Commissione Europea, *Commission Staff Working Document: Impact Assessment Accompanying the PSD2 and Interchange Fees Regulation proposal* (Bruxelles, 24.7.2013) disponibile su: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013SC0288&from=EN, spec. p. 137.

24 Come si legge nel considerando 27 della direttiva 2015/2366 *"successivamente all'adozione della direttiva 2007/64/CE si sono diffusi nuovi tipi di servizi di pagamento, specialmente nel settore dei pagamenti tramite Internet. In particolare, si sono evoluti i servizi di disposizione di ordine di pagamento nel settore del commercio elettronico. Tali servizi di pagamento svolgono un ruolo nei pagamenti in detto settore mediante un software che fa da ponte tra il sito web del commerciante e la piattaforma di online banking della banca del pagatore per disporre pagamenti via Internet sulla base di bonifici"*.

discende, che, prescindendo la prestazione del servizio dall'esistenza di un conto presso l'intermediario che lo rende, sorgono ulteriori margini di rischio, soprattutto in ordine alla gestione e alla sicurezza dei dati del cliente[25].

La PSD2, al fine di consentire un ordinato sviluppo del commercio elettronico ha considerato – lo si è accennato – come nuovi servizi di pagamento le attività di alcuni operatori professionali, già esistenti sul mercato, volte a soddisfare il bisogno del venditore di avere sicurezza del pagamento elettronico disposto dal cliente, prima di dare corso all'esecuzione della prestazione dovuta in forza del contratto sinallagmatico stipulato *on-line*.

Ne consegue che la PSD2 ha regolamentato una realtà economica e una prassi, già molto diffusa in anni recenti, in virtù della quale gli utenti che hanno un conto corrente *on-line* sono soliti effettuare i pagamenti e accedere alla loro rendicontazione bancaria attraverso *software* realizzati da parti terze.

Possiamo quindi concludere che i *Third Party Providers* sono, anzitutto, istituti di pagamento che si affiancano alle banche e agli istituti di moneta elettronica[26]; essi sono infatti qualificati come istituti di pagamento e in quanto tali possono operare solo previa autorizzazione della Banca d'Italia[27]. In particolare, tale autorizzazione viene rilasciata quando l'operatore soddisfa una serie di requisiti, che rappresentano un sottoinsieme di quelli richiesti per gli altri istituti di pagamento[28]. Per quanto i *Third Party Providers* debbano dunque essere autorizzati in via amministrativa come istituti di pagamento, essi soggiacciono a una disciplina parzialmente differenziata rispetto alla categoria generale degli intermediari e ciò in considerazione della specificità della loro attività[29].

Tuttavia, essi sono estranei alla custodia e alla gestione dei fondi in relazione ai quali il servizio viene eseguito[30]. A livello pratico, il *provider* è in grado (e così ad

25 V. F. Marasà, *Il trattamento dei dati personali dell'utente dei servizi di pagamento tra PSD2 e GDPR*, cit., p. 634.

26 In merito cfr. F. Ciraolo, *I servizi di pagamento nell'era Fin Tech*, in AA.VV., FinTech, *Introduzione ai profili giuridici di un mercato unico tecnologico dei servizi finanziari*, Giappichelli, Torino, 2017, spec. p. 188 ss.

27 Per quanto riguarda i PISP, al rilascio dell'autorizzazione consegue l'iscrizione in un apposito registro, liberamente consultabile on line e gestito dall'autorità competente di ogni singolo Stato (art. 14, par. 1 e 2, PSD2).

28 È opportuno sottolineare come, mentre per gli AISP non siano previsti requisiti patrimoniali minimi commisurati ai rischi assunti; per i PISP, viceversa, questi requisiti sono pari al capitale minimo iniziale fissato dalla Banca d'Italia. Sul punto v. B. Szego, *I nuovi prestatori autorizzati,* in *Innovazione e regole nei pagamenti digitali,* a cura di M.C. Paglietti e M.I. Vangelisti, RomaTrePress, Roma, 2020, spec. p. 164.

29 All'art. 14, par. 1, commi 1 e 2, la Direttiva prevede che il rilascio dell'autorizzazione per l'esecuzione dei servizi di disposizione d'ordine dà luogo, come per gli altri servizi di pagamento, all'iscrizione dell'istituto richiedente e dei relativi agenti in un pubblico registro liberamente consultabile, accessibile *on-line* e tempestivamente aggiornato, presso lo Stato membro di origine. L'European Banking Authority detiene inoltre un proprio registro elettronico centrale, di nuova istituzione, nel quale vengono concentrate tutte le informazioni iscritte nei rispettivi registri nazionali. Il registro dell'EBA, pubblicato sul sito *web* dell'Autorità e consultabile gratuitamente, deve consentire al cittadino facile accesso e agevole ricerca delle informazioni. In questo modo ogni consumatore ha la possibilità di verificare se il soggetto da autorizzare è presente nel registro: in questo modo si garantisce la certezza di fornire l'accesso ai propri dati bancari e alle operazioni di pagamento esclusivamente ad enti che siano certificati e che siano effettivamente stati approvati a livello normativo.

30 Cfr. F. Marasà, *Il trattamento dei dati personali dell'utente dei servizi di pagamento tra PSD2 e GDPR*, cit., p. 634.

esempio, come si vedrà meglio in seguito, nel caso del *Payment Initiation Service Provider*) di registrare l'identificativo del cliente e, conseguentemente, è altresì in condizione di accedere al conto di quest'ultimo e dare l'impulso di pagamento.

Tali istituti, proprio in ragione della loro attività così trasversale ed eterogenea, sono soggetti a preventiva autorizzazione, come si è visto, nonché a determinati obblighi e doveri e alle conseguenti responsabilità[31], su cui si avrà modo di soffermarsi nei prossimi paragrafi.

Siffatti servizi si caratterizzano per il fatto di operare su un conto di pagamento *on-line* e, in particolare, su un conto aperto presso un altro prestatore di servizi di pagamento al quale compete amministrare e gestire il conto per il medesimo cliente (*Account Servicing Payment Service Provider* o ASPSP)[32].

Ne deriva che si tratta di soggetti terzi rispetto al rapporto intercorrente tra l'utente e l'ASPSP; ma, la Direttiva si limita a descrivere le possibilità operative dei *Third Party Providers* senza però prevedere come necessaria l'esistenza di una specifica relazione tra i due tipi di prestatori, e cioè tra *Third Party Providers* e ASPSP.

La funzione chiave dei *Third Party Providers* pare dunque identificarsi nella possibilità di effettuare pagamenti *on-line* più rapidi, meno costosi, collegati allo sviluppo dell'*e-commerce* al quale, a loro volta, danno impulso.

Per quanto attiene, invece, alle prerogative di questi operatori esse si sostanziano essenzialmente nella possibilità di accedere ai dati e alle informazioni sui conti di pagamento che i privati intrattengono presso banche o altri istituti di radicamento del conto.

Per ciò che concerne invece gli obblighi dei *providers* la Direttiva ha previsto stringenti *standard* di sicurezza che i servizi di pagamento sono tenuti a osservare. Inoltre, si è disposto che i servizi di pagamento siano preventivamente autorizzati; i *providers* di servizi di pagamento dovranno essere abilitati all'accesso ai conti correnti *on-line* attraverso interfacce facilmente integrabili[33]. Queste disposizioni introdotte dalla Direttiva sono volte ad armonizzare e rafforzare il processo di "autenticazione" nel rispetto delle disposizioni BCE, cui si è già avuto modo di accennare e che si avrà modo di approfondire nel seguito della trattazione[34]. Si ricordi infatti come l'obbiettivo primario della Direttiva resti quello di assicurare maggiore sicurezza, sia per quanto attiene alle operazioni di pagamento sia per quanto riguarda la *privacy* degli utenti, nel

31 M. Pimpinella – G. Carrafiello, *L'evoluzione normativo regolamentare nel settore dei pagamenti*, MFC, Milano, 2016, p. 31.

32 È possibile svolgere detti servizi solo in relazione ai conti accessibili *on-line* e quindi non per eseguire operazioni o per dare informazioni con riferimento a conti di pagamento ad operatività tradizionale, non raggiungibili da remoto in maniera telematica, tenuto conto che essi vengono espletati esclusivamente in maniera telematica e si sostanziano proprio nella conoscenza o nella movimentazione digitale a distanza dei conti radicati presso un distinto intermediario. Come meglio illustrato al par. 5.

33 Il principio appartenente alla nuova cornice normativa rappresenta nel contempo una opportunità di mercato e un elemento di grande preoccupazione per le banche più tradizionali che rischiano una disintermediazione dalla loro clientela. Inoltre, si segnala che la Direttiva prevede anche che tutti gli intermediari debbono essere registrati presso appositi elenchi.

34 In particolare, ci si riferisce alla *Strong Costumer Authentication*, su cui *infra*, par. 5.

momento del c.d. "colloquio" tra *Third Party Providers* e banche (e cioè in sostanza quando questi due operatori si scambiano i dati degli utenti). La nuova disciplina si preoccupa di potenziare soprattutto i presidi di sicurezza informatica dei pagamenti elettronici e il monitoraggio delle frodi, attribuendo all'*European Banking Authority* (EBA) la competenza per la definizione di *standard* tecnici di comunicazione sicura tra i *Third Party Providers* e i prestatori di radicamento del conto, consentendone una revisione periodica con modalità più flessibili di implementazione e aggiornamento che permettono anche di tener conto della continua evoluzione tecnologica[35].

Tanto premesso in linea generale, deve ora aggiungersi che, nel disciplinare più in dettaglio i prestatori di servizi la Direttiva li distingue in due specie: da un lato, i prestatori di servizi di ordine di pagamento *Payment Initiation Service Providers* (d'ora in avanti anche solo PISP); e, dall'altro, i prestatori di servizi di informazione sui conti e cioè, gli *Account Information Services Providers* (d'ora in avanti anche solo AISP)[36].

1.3.1 I *Payment Initiation Service Providers*

I PISP, sono definiti come quelli che dispongono «l'ordine di pagamento su richiesta dell'utente di servizi di pagamento relativamente ad un conto di pagamento detenuto presso un altro prestatore di servizi di pagamento»[37]. In sostanza, i PISP si frappongono tra l'utente-pagatore e il soggetto presso cui è radicato il conto, che può essere un istituto bancario o un prestatore di servizi di pagamento di radicamento del conto, l'ASPSP, al fine di dare impulso al pagamento[38]. Questo significa che questi soggetti "bypassano" la catena tradizionale dei circuiti delle carte di credito, operando mediante un *software* ponte tra il sito *web* del commerciante e la piattaforma di *online banking* della banca del pagatore[39]. In pratica, si tratta di quello che è comunemente noto come il modello *PayPal*[40] e al quale oggi si stanno affacciando anche altri colossi, quali *Amazon*, *Apple*, *Facebook* e *Google*[41].

Orbene, la principale novità della PSD2 appare proprio quella di aver regolato questi servizi a tecnologia digitale che possono accedere ai conti di pagamento (anche al fine di verificare l'effettiva esistenza dei fondi necessari) e ordinare alla banca, per conto dell'utente, di eseguire il trasferimento di fondi a favore del beneficiario, nonostante non siano i soggetti presso cui è radicato il conto corrente *on-line*[42].

35 BANCA D'ITALIA, Le nuove frontiere dei servizi bancari e di pagamento tra PSD2, criptovalute e rivoluzione digitale, a cura di F. Maimeri e M. Mancini, in Quaderni giuridici, n. 87/2019, p. 53.

36 Cfr. in merito l'allegato 1 alla PSD2 che include entrambi i suddetti servizi tra i servizi di pagamento.

37 Cfr. art. 4, comma 15, della Direttiva stessa.

38 A. SCIARRONE ALIBRANDI, I*mpostazione sistematica della Direttiva PSD2*, in *Liber Amicorum Guido Alpa*, a cura di F. Capriglione, Cedam, Padova 2019, p. 16 ss.

39 In questo senso F. CASCINELLI - V. PISTONI, *La Direttiva (UE) 2015/2633 relativa ai servizi di pagamento nel mercato interno*, in *Riv. dir. banc* (www.dirittobancario.it), 2016.

40 Un modello che prevede che l'intermediario non entri mai in possesso dei fondi del cliente e che segna la differenza sostanziale con l'attività propria degli intermediari bancari.

41 V. A. ANTONUCCI, *Mercati dei pagamenti: le dimensioni del digitale*, in *Riv. dir. banc.*, (www.dirittobancario.it), 2018.

42 *S. VANINI, L'attuazione in Italia della seconda direttiva sui servizi di pagamento nel mercato interno: le innovazioni introdotte dal d.lgs. 15 dicembre 2017*, n. 18, in *Nuove leggi civ. comm.*, 2018, p. 839 ss.

I PISP hanno quindi un ruolo fondamentale nell'operazione di pagamento, nonostante si pongano come terza parte rispetto al fornitore del servizio di pagamento. Il ricorso ad un "*software* intermediario", e cioè un *software* ponte tra il sito *di e-commerce* e la piattaforma di *on-line banking*, se da un lato assicura una maggiore garanzia all'utente[43], dall'altro pone una serie di questioni relative al flusso dei dati personali che una simile operazione comporta e alle quali sarà dedicata specifica attenzione[44].

In merito poi all'operatività dei PISP giova sottolineare che questi non hanno un ruolo attivo in senso proprio in quanto, di fatto, non entrano mai in possesso dei fondi oggetto del trasferimento. Essi infatti non sono considerati operatori finanziari[45] e nemmeno possono controllare il flusso nella fase della scritturazione a debito e a credito, dal momento che tali funzioni restano strettamente riservate alle banche o agli altri intermediari, che dispongono delle somme dei propri correntisti in modalità esclusiva e in ordine ad un rapporto contrattuale. Viceversa, la prestazione dei servizi offerti dai PISP non è subordinata alla conclusione di un rapporto contrattuale tra questi e l'ASPSP (art. 5-*ter*, comma 1, d.lgs. n. 11/2010; art. 66, par. 5, dir. 2015/2366/UE).

Si tratta a questo punto di individuare con maggior precisione quali siano i benefici legati alla operatività caratteristica dei PISP; ad una attività, cioè, che non solo agevola lo scambio di informazioni commerciali fra pagatore e beneficiario, ma si sostituisce al primo nell'ordinare di eseguire l'operazione di pagamento[46].

Tali benefici possono allora essere riassunti come segue:

- per quanto concerne la categoria dei consumatori, il venir meno della necessità di disporre di un conto di pagamento per compiere acquisti *on-line*;
- per quanto riguarda, invece, i c.dd. "*merchant*", e cioè le imprese, la possibilità di risparmiare sulla commissione tipica delle operazioni effettuate con carte di credito[47].

1.3.2 Gli *Account Information Service Providers*

Gli AISP sono invece definiti come prestatori di «un servizio *online* che fornisce informazioni consolidate relativamente a uno o più conti di pagamento detenuti dall'utente di servizi di pagamento presso un altro prestatore di servizi di pagamento o presso più prestatori di servizi di pagamento»[48]. In sostanza, gli AISP forniscono un servizio *on-line* di consolidamento delle informazioni, e quindi dei movimenti bancari, permettendo al consumatore di ottenere (ovviamente sempre *on-line*) informazioni

43 Sul punto v. G. Aranguena - D. Jegerson, *I pagamenti elettronici. Dal baratto ai portafogli digitali*, goWare, 2016, p. 104 ss.

44 Cfr. *infra, sub* par. 6.

45 Tale divieto è disciplinato dall'art. 66, par. 3, lett. a, dir. 2015/2366/UE.

46 F. Marasà, Servizi di pagamento e responsabilità degli intermediari, cit., p. 82 ss.

47 Quindi andando, in sostanza, a configurare un'alternativa più economica della tradizionale transazione con carta di credito. Tuttavia, da ciò discende il delicato problema, sul quale si è sviluppato un ampio dibattito, della ripartizione delle commissioni tra *merchant* e *Third Party Providers*.

48 Cfr. art. 4, comma 16, della Direttiva stessa.

complete sui propri conti di pagamento. Il consumatore avrà quindi la possibilità di avere un quadro completo grazie ad un servizio di monitoraggio dei propri conti[49]. L'attività dei prestatori di servizi di informazione sui conti è dunque quella di aggregare le informazioni (*id est*: i dati) presenti su vari e diversi conti *on-line* per creare (o talvolta semplicemente restituire) una visione complessiva della situazione finanziaria[50].

Questo comporta che gli AISP sono nella condizione di utilizzare i dati del consumatore, ma sempre ed esclusivamente previo suo consenso, secondo un'articolata disciplina su cui si avrà modo di tornare segnatamente[51].

Le utilità che quindi discendono dall'attività propria di questi prestatori di servizi risiedono: da un lato, nel consentire a consumatori e clienti di poter accedere *on-line* alle informazioni relative ai propri conti in qualsiasi momento e senza necessariamente dover fare ricorso al sito *internet* del proprio intermediario finanziario (banca o altro che sia), e dall'altro nella possibilità per l'AISP di analizzare ed elaborare le abitudini di consumo dei clienti e, conseguentemente, offrire loro un ulteriore ventaglio di possibili servizi collegati[52]. L'idea alla base di tale servizio è proprio quella di migliorare la consapevolezza del consumatore riguardo alla propria situazione finanziaria e quindi, in concreto, rendere possibile o facilitare la programmazione di spesa. Anche in questo caso possono essere offerti servizi collaterali idonei a rendere il *software* o l'applicazione ancora più accattivanti sul piano commerciale. E, anzi, è plausibile ipotizzare che la competizione fra i diversi operatori sarà sempre più imperniata su quella che viene definita come *customer experience*.

Per quanto poi attiene agli specifici doveri e obblighi di questi operatori, è qui sufficiente ricordare che essi: *(i)* possono agire solo sulla base del consenso esplicito dell'utente; *(ii)* devono autenticarsi presso l'ASPSP del proprietario del conto e comunicare in sicurezza con tutti i soggetti coinvolti nell'operazione di pagamento; *(iii)* possono accedere alle sole informazioni sui conti di pagamento designati e sulle operazioni di pagamento effettuate a valere su tali conti; *(iv)* non possono richiedere dati sensibili relativi ai pagamenti; *(v)* non possono utilizzare nè conservare i dati del consumatore; *(vi)* devono effettuare l'accesso ai dati solo per i fini espressamente previsti dal servizio stesso. Tale accesso, in particolare, deve avvenire mediante interfacce *on-line* (c.d. *Application Programming Interface*) con gli ASPSP[53].

49 A. Burchi, S. Mezzacapo, P. Musile Tanzi, V. Troiano, *Financial Data Aggregation e Account Information Services*, in *Quaderni FinTech della Consob*, n. 4, marzo 2019, p. 33 ss.

50 Cfr. S. Vanini, *L'attuazione in Italia della seconda direttiva sui servizi di pagamento nel mercato interno*, cit., p. 860, secondo cui si tratta «di servizi digitali in base ai quali l'utente dispone di un'unica interfaccia grafica che sintetizza – o anche rielabora – le situazioni finanziarie esistenti presso le diverse banche che detengono i conti di pagamento intestati all'utente».

51 Cfr. *infra, sub* par.6.

52 F. Marasà, *Servizi di pagamento e responsabilità degli intermediari*, cit., p. 95 ss.

53 O. Borgogno - G. Colangelo, *Data Sharing and Interoperability Trough APIs: Insights from European Regulatory Strategy, European Union Law Working Paper,* Stanford – Vienna Transatlantic Technology Law Forum, 2018; Financial Conduct Authority and HM Treasury, *Expectations for the third party access provisions in Payment Services Directive II*, 2018, 2, in https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/630135/Expectations_for_the_third_party_access_provisions_in_PSDII.pdf.

1.4 Il rapporto tra i prestatori autorizzati e gli istituti di pagamento

Le banche e tutti gli altri "fornitori di servizi di pagamento di radicamento del conto" sono tenuti a consentire sia ai PISP che agli AISP di accedere alle informazioni sui conti di pagamento in loro possesso, ma solo qualora i clienti abbiano prestato il loro consenso all'accesso ai conti ai sensi della Direttiva.

In realtà il rapporto tra i prestatori di servizi, così come sopra identificati, e le banche (o istituti di pagamento che siano) può atteggiarsi sia in termini di concorrenza, come si è sottolineato nelle premesse, sia in termini di cooperazione[54].

Il fatto che le banche siano già in possesso dei dati del cliente permette loro di avere un ruolo privilegiato. Inoltre, gli istituti bancari possono giovarsi di un rapporto fiduciario con i propri clienti, dal momento che essi hanno un contatto diretto con questi (si pensi alla pluralità di servizi che non si risolvono nell'accesso da remoto)[55]. E tuttavia, sembra che, quantomeno in prospettiva, sia più probabile l'instaurarsi di un rapporto di collaborazione tra gli istituti bancari e i nuovi operatori, quantomeno nella misura in cui questi secondi possano fornire un più deciso contributo in termini di tecnologia ed innovazione.

Ma al di là di questi scenari, l'aspetto che resta decisivo dal punto di vista giuridico è rappresentato dalla disciplina relativa all'accesso e al trattamento dei dati.

La Direttiva, infatti, li definisce come prestatori di «un servizio di pagamento che fornisce e amministra un conto di pagamento per un pagatore»[56].Questo significa che gli ASPSP si interpongono nella gestione del conto risultando essere abilitati all'accesso ai dati e, soprattutto, alla loro utilizzazione; e ciò anche qualora non risulti legato da una relazione contrattuale[57].

È infatti la stessa Direttiva a prevedere l'obbligo per gli ASPSP di consentire l'accesso ai dati ogni qualvolta sia richiesto e i *Third Party Providers* sia stato autorizzato dal cliente titolare del conto *on-line* (che è il principio alla base dell'*Open banking*). Tale accesso avviene sia per quanto attiene all'aspetto dispositivo che riguarda i PISP, sia per quanto riguarda il profilo informativo che interessa gli AISP, il che ancora una volta riporta al tema della tutela della *privacy* dei consumatori e quindi al trattamento dei dati.

In capo all'ASPSP vi è dunque un vero e proprio obbligo di permettere ai *Third Party Providers* (che si tratti di un PISP o di un AISP) l'accesso al conto, con la precisazione che ciò costituisce una legittima pretesa che sussiste a prescindere dall'esistenza

54 In merito al rapporto tra le banche e questi nuovi soggetti, cfr. *Europe's lenders buckle up for open banking; Financials Regulation; EU's PSD2 directive will allow third parties such as retailers and rivals access to accounts*, in *Financial Times*, del 2 gennaio 2018; G. Barba Navaretti, G. Calzolari, A.F. Pozzolo, *Banche e fintech. Amici o nemici?*, in *Fintech*, a cura di F. Fimmanò e G. Falcone, ESI, Napoli 2019, p. 25 ss.

55 Per un'approfondita analisi dei pro e dei contro che rappresenta la PSD2 per i tradizionali istituti di pagamento, v. Aa.Vv., *The Payment Services Directive II and Competitiveness: The Perspective of European Fintech Companies*, in *European Research Studies Journal*, 11/1/2018, Vol. XXI (Issue 2), spec. pp. 9 e 10.

56 Cfr. art. 4, co. 17, della Direttiva stessa.

57 Invece per un approfondimento sui contratti informatici si veda: G. Finocchiaro, *Il contratto nell'era dell'intelligenza artificiale*, in *Riv. trim. dir. proc. civ.*, 2018, p. 441 ss.

di un rapporto contrattuale tra questi[58]. Tuttavia, per ottenere ciò è indispensabile che *(i)* gli ASPSP si dotino di infrastrutture adeguate a consentire una efficiente e sicura interazione con i *Third Party Providers*; *(ii)* alla base del rapporto vi sia una leale collaborazione; *(iii)* vi sia un'adeguata previsione relativa alla corretta e sicura gestione dei dati[59].

Con particolare riferimento a quelle che sono le infrastrutture adeguate a consentire una efficiente e sicura interazione tra i soggetti coinvolti, è opportuno richiamarsi ai sistemi informatici di dialogo tra ASPSP e *Third Party Providers*, e quindi all'*Application Programming Interface* sopra menzionata[60]. In questo contesto di rapporti e servizi completamente digitalizzati anche le informazioni assumono forma digitale. Tuttavia, la Direttiva non fa riferimento ad una specifica soluzione tecnologica, quanto piuttosto ad un nuovo paradigma tecnologico (successivo alla preesistente tecnologia dei *web-services*)[61], il che porta alla configurazione del rischio che la massima libertà di cui dispongono gli ASPSP nel predisporre la propria interfaccia si traduca nella necessità che andrebbe a ricadere sui *Third Party Providers* di dover predisporre tante interfacce digitali quanti siano gli interlocutori.

Un profilo che va necessariamente richiamato è poi quello della responsabilità dei *Third Party Providers* per la mancata, inesatta o tardiva esecuzione[62]. Secondo questa disciplina è il prestatore dei servizi di radicamento del conto che deve rimborsare al pagatore l'importo della operazione di pagamento non eseguita o non correttamente eseguita "e, se del caso, riporta il conto di pagamento addebitato nello stato in cui si sarebbe trovato se l'operazione non correttamente eseguita non avesse avuto luogo".

È opportuno che la responsabilità del prestatore di servizi di pagamento sia limitata alla 'esecuzione corretta della 'operazione di pagamento conformemente all'ordine di pagamento del PISP: l'esigenza di tutela del mercato e il perseguimento di finalità di interesse generale tendono pertanto a prevalere sull'interesse del singolo.

In conclusione, risulta evidente come, anche là dove la responsabilità per la mancata, inesatta o tardiva esecuzione dell'operazione possa identificarsi in capo al PISP, il destinatario della richiesta di rimborso o risarcimento rimane in capo alla banca, o comunque al soggetto presso cui è radicato il conto. Ne deriva che per il pagatore nulla cambia rimanendo l'individuazione della responsabilità per l'inadempimento dell'operazione destinata ad un secondo momento.

La Direttiva, infatti, si limita a disciplinare un rimedio a carattere restitutorio, che il cliente può far valere nei confronti dell'ASPSP, qualora si verifichino casi di addebiti non autorizzati, anche là dove questi siano avvenuti senza coinvolgimenti di altri operatori. Nel caso in cui l'ordine di pagamento non sia stato autorizzato dal cliente, questi ha diritto all'immediata restituzione, indipendentemente dalla provenienza

58 Cfr. S. Vanini, *L'attuazione in Italia della seconda direttiva sui servizi di pagamento nel mercato interno*, cit. p. 860.

59 In merito cfr. F. Ciraolo, *I servizi di pagamento nell'era Fin Tech*, cit., spec. p. 190, nt. 20.

60 Cfr. *supra sub* 3.2.

61 Tuttavia, deve ricordarsi che in Italia, il consorzio Cbi, in collaborazione con Nexi e con l'appoggio dell'Abi, ha progettato un modello unico di piattaforma digitale.

62 L'ipotesi di inadempimento del PISP è disciplinata nel nostro ordinamento all'art. 25-*bis* del d.lgs. 218/2017.

dell'ordine, che dunque in questo caso non assume alcun rilievo[63]. Viceversa, la provenienza dell'ordine da parte di un prestatore di servizi di pagamento assume rilevanza nei casi di inadempimento o di fatto illecito a carico dello stesso. Sempre sotto il profilo della responsabilità è opportuno sottolineare che l'*European Banking Authority* – nel dettare le regole in materia di *strong costumer authentication* e *standard* di comunicazione definendo ciò che gli ASPSP devono fornire per garantire ai *Third Party Providers* l'accesso ai dati del conto di pagamento dei propri clienti[64] – ha ritenuto che non sia necessario che gli ASPSP effettuino un controllo ulteriore in merito al consenso dell'utente prima di agevolare l'accesso ai dati.

1.5 Il diritto di accesso ai conti

Le modalità di accesso ai conti risultano dunque cruciali per non pregiudicare la sicurezza dei fondi e quella dei dati di pagamento e per prevenire le frodi informatiche. Per tale ragione la Direttiva si è preoccupata di disciplinarne le caratteristiche dettando misure alle quali devono attenersi tutti i soggetti coinvolti nell'operazione di pagamento: PISP e AISP, da un lato, e prestatori di radicamento del conto (e cioè banche e ASPSP) dall'altro. Essi, infatti, devono reciprocamente comunicare «in maniera sicura», conformemente a quanto dispone l'art. 98, par. 1, lett. d) della PSD2. Comunicare in maniera sicura significa farlo nel rispetto delle norme tecniche che sono state introdotte per garantire:

(i) un livello adeguato di sicurezza per gli utenti e i prestatori di servizi di pagamento mediante l'adozione di requisiti efficaci e basati sul rischio;

(ii) la sicurezza dei fondi e dei dati personali degli utenti;

(iii) a concorrenza equa tra i prestatori di servizi di pagamento;

(iv) la neutralità dei modelli tecnologici e commerciali;

(v) lo sviluppo di mezzi di pagamento accessibili, innovativi e di facile utilizzo.

Ne deriva che, come più volte detto, tra i problemi più rilevanti a proposito di *Third Party Providers*, si annoverano quello della tutela della *privacy* del consumatore (o meglio dell'utente) e quello della sicurezza digitale.

È importante sottolineare che i *Third Party Providers* non possono detenere in nessun momento e per nessuna ragione i fondi del cliente, e in tal senso vi sono particolari disposizioni. Nello svolgimento della loro attività sono invece abilitati a conoscere e utilizzare i dati considerati nella esclusiva disponibilità dell'utente e ciò è previsto, anche in consonanza con il diritto alla *portabilità*[65] dei dati, al fine di agevolare

63 Per un approfondimento cfr. M.C. Paglietti, Questioni in materia di prova nei casi di pagamenti non autorizzati, in Innovazione e regole nei pagamenti digitali, cit., p. 43 ss.; I.A. Caggiano, Pagamenti non autorizzati tra responsabilità e restituzioni. Una rilettura del d.lgs. 11/2010 e lo scenario delle nuove tecnologie, in Riv. dir. civ., 2016, p. 459 ss.

64 EBA, Discussion on RTS on strong costumer authentication and secure communication under PSD2, in: https://eba.europa.eu/sites/default/documents/files/documents/10180/1303936/13129941-7581-4473-a767-52ec002bd00a/EBA-DP-2015-03%20%28RTS%20on%20SCA%20and%20CSC%20under%20PSD2%29.pdf.

65 Su cui cfr. meglio *infra*, *sub* par. 6.

il trasferimento da un fornitore di servizi ad un altro e di incentivare così la creazione di nuovi servizi nell'ambito del mercato unico digitale.

In particolare, nel provvedimento italiano di attuazione della Direttiva, viene regolato, per quanto riguarda i PISP, l'accesso ai conti di pagamento. Il d.lgs. n. 218/2017 infatti prevede: da un lato, che in caso di servizi di ordine di pagamento l'utente ha il diritto di avvalersi di un prestatore di servizi di pagamento (qualora il suo conto sia accessibile *on-line*); e dall'altro, che tale prestazione non sia subordinata alla esistenza di un rapporto contrattuale tra i PISP e gli ASPSP[66], limitando la possibilità di questi ultimi di opporsi a fornire l'accesso ai dati in oggetto.

Viene inoltre stabilito che i PISP non possano richiedere dati diversi da quelli necessari per l'operazione in oggetto e, soprattutto, che essi non possano usare né, tanto meno, conservare i dati per fini differenti dalla prestazione propria della disposizione di ordine di pagamento.

Infine, si prevede che gli ASPSP non possano per alcuna ragione conservare i dati sensibili relativi ai pagamenti dell'utente[67].

Infatti, la PSD2, infatti, rispettivamente agli artt. 66 e 67, detta le condizioni che devono essere rispettate per accedere al conto del pagatore da parte dei PISP e degli AISP al fine di reperire le informazioni necessarie per l'erogazione del servizio e per l'avvio della transazione.

In particolare, per quanto concerne i PISP si dovrà assicurare che questi mettano a disposizione dell'utente tutte le informazioni circa il servizio offerto e i suoi dati personali, e questo nel rispetto del principio della trasparenza delle operazioni di pagamento. Le informazioni, in particolare, riguardano: *(i)* la conferma della trasmissione dell'ordine di pagamento, *(ii)* il riferimento che consente al pagatore e al beneficiario di individuare l'operazione di pagamento e, se opportuno, al beneficiario di identificare il pagatore e tutte le informazioni trasmesse con l'operazione di pagamento, *(iii)* l'importo dell'operazione, *(iv)* il tempo massimo di esecuzione e di tutte le spese pagabili ai PISP e relative all'operazione di pagamento effettuata, *(v)* il nome, l'indirizzo e i riferimenti del PISP[68]. Inoltre, all'art. 5-*ter* del d.lgs. 218/2017 viene disciplinato il comportamento che i PISP sono tenuti ad adottare in caso di servizi di disposizione di ordine di pagamento e viene regolato, in maniera puntuale, l'uso che questi possono fare dei dati di cui vengono a conoscenza. Al riguardo è previsto che i PISP non possono detenere in alcun momento i fondi del pagatore, come si è avuto modo di precisare, e debbono provvedere affinché *(i)* le credenziali di sicurezza personalizzate del pagatore non siano accessibili a terzi; *(ii)* qualunque altra informazione ottenuta nella prestazione del servizio sia a sola disposizione del beneficiario.

Per quanto invece riguarda gli AISP, l'art. 5-*quater* del d.lgs. 218/2017 regola in maniera puntuale le modalità di accesso alle informazioni sui conti di pagamento e alla loro utilizzazione. Gli AISP prestano il proprio servizio unicamente sulla base del

66 Cfr. art. 5-*ter*, comma 1, introdotto dal d.lgs. 218/2017.

67 V. art. 5-*ter* (introdotto dal d.lgs. 218/2017), comma 2, lett. *e*).

68 M. Pimpinella – G. Carrafiello, L'evoluzione normativo-regolamentare nel settore dei pagamenti, cit., p. 31.

consenso esplicito dell'utente e provvedono affinché le credenziali di sicurezza personalizzate dello stesso non possano essere accessibili ai terzi.

Più in generale l'art. 97, par. 1, della Direttiva prevede per i prestatori di servizi di pagamento l'obbligo di applicare l'autenticazione forte del cliente[69] quando il pagatore accede al suo conto *on-line*, ovvero quando dispone un'operazione di pagamento elettronico o effettua qualsiasi azione tramite un canale a distanza che possa comportare il rischio di frode o altri abusi nei pagamenti[70].

Si tratta della *strong costumer authentication*, e, cioè, l'autenticazione basata sull'uso di due o più elementi indipendenti l'uno dall'altro in modo che la eventuale violazione di uno non comprometta la affidabilità dell'altro.

Sul punto occorre richiamare il già citato documento dell'Autorità Bancaria Europea che detta appunto le norme tecniche (c.dd. *Regulatory Technical Standards* o RTS) per l'autenticazione forte dei clienti e per la comunicazione sicura, fondamentali per raggiungere l'obiettivo principe della PSD2 e, quindi, rafforzare la protezione dei consumatori, promuovere l'innovazione e migliorare la sicurezza dei servizi di pagamento in tutta l'Unione Europea[71].

1.6 Il trattamento dei dati

Nel paragrafo precedente si sono richiamate le modalità con le quali i *Third Party Providers* possono entrare nella disponibilità dei dati degli utenti, oltre a quelle che sono le limitazioni previste dalla PSD2 e dalle relative norme di attuazione a livello nazionale ai fini della utilizzazione e della conservazione di tali dati.

Tuttavia, negli ultimi anni, come si è visto e come è ben noto, i dati hanno assunto sempre maggior valore[72] e la cornice normativa non è stata in grado di stare al passo con i tempi, senza che perciò possa dirsi venuta meno (essendosi semmai rafforzata) l'esigenza di procedere comunque a un inquadramento normativo del fenomeno.

69 Che consente di verificare l'identità di un utente di servizi di pagamento o la validità dell'uso di uno specifico strumento di pagamento, utilizzando due o più elementi, classificati nelle categorie della conoscenza (qualcosa che solo l'utente conosce), del possesso (qualcosa che solo l'utente possiede) e dell'inerenza (qualcosa che caratterizza l'utente) che sono indipendenti, in quanto la violazione di uno non compromette l'affidabilità degli altri, e che è concepita in modo tale da tutelare la riservatezza dei dati di autenticazione (cfr. art. 4, par. 1, n. 30, PSD2).

70 In particolare, l'autenticazione dovrà avvenire attraverso la corretta combinazione di almeno due strumenti tra i seguenti: *(i) knowledge*, e cioè qualcosa che soltanto l'utente conosce (come nel caso di una password o di un PIN); *(ii) possession*, e cioè qualcosa che solo l'utente possiede (si pensi ad una chiavetta o *token*); *(iii) inherence*, e cioè qualcosa che è propria dell'utente può essere (per esempio l'impronta digitale). Per questi aspetti cfr. tra gli altri S. Balsamo Tagnani, *Il mercato europeo dei servizi di pagamento si rinnova con la PSD2*, in *Contratto e impresa/Europa*, 2018, spec. p. 619 ss.

71 EBA, *Discussion on RTS on strong costumer authentication*, cit. Per un approfondimento sul punto v. S. Hellmann, *Payment Service Directive 2. (Cyber) Security for Payment Service Provider*, Università di Leida, 2018 in: https://d1rkab7tlqy5f1.cloudfront.net/TBM/Over%20faculteit/Afdelingen/Engineering%20Systems%20and%20Services/People/Professors%20emeriti/Jan%20van%20den%20Berg/MasterPhdThesis/Thesis-Stephan-Hellmann-Final.pdf.

72 V. sul punto, anche per ulteriori riferimenti, Aa.Vv., *Informazione e Big Data tra innovazione e concorrenza*, a cura di V. Falce, G. Ghidini e G. Olivieri, Milano, Giuffrè, 2018; A. Ottolia, *Big Data e Innovazione computazionale*, in AIDA, 2017, p. 93 ss.

A tale riguardo può ricordarsi come il diritto alla protezione dei dati personali, a fronte del fatto che da tali dati si può risalire alle caratteristiche attinenti alla sfera giuridica di un soggetto[73], vada ascritto ai diritti fondamentali della persona. Sicché è superfluo aggiungere che esso necessiti di essere tutelato e attuato nel migliore dei modi nell'intero ambito dell'Unione europea[74].

Ad oggi la nozione di "dati personali" risulta poi assai ampliata, tanto che non ricopre più solamente la sfera della persona e le informazioni ad essa riferibili, ma anche tutti i fenomeni che siano pertinenti ad un individuo identificabile e che possano essere oggetto di analisi da parte di terzi.

Per inquadrare la questione è poi anche necessario richiamare, oltre alla nozione di dati personali, anche quella di "trattamento": e cioè «qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'inter-commissione, la limitazione, la cancellazione o la distruzione»[75].

È opportuno, dunque, interrogarsi sull'uso che i *Third Party Providers,* fanno, o meglio possono fare, dei dati dell'utente; ma prima ancora su quale sia la tipologia di dati oggetto di tali operazioni.

A tale riguardo la PSD2, nel disciplinare le loro attività, ha posto alcuni limiti in ordine alla categoria dei dati sensibili dell'utente[76]; viene specificato come i PISP non debbano conservare i dati sensibili relativi ai pagamenti dell'utente e come invece, gli AISP non siano nemmeno tenuti a richiedere dati sensibili relativi ai pagamenti.

Con riferimento specifico al trattamento dei dati di cui viene a conoscenza nel corso dell'operazione, i PISP: *(i)* non chiedono al pagatore dati diversi da quelli necessari per prestare il servizio di disposizione di ordine di pagamento; *(ii)* non usano e non conservano dati e non vi accedono per fini diversi dalla prestazione del servizio di disposizione di ordine di pagamento; *(iii)* non conservano dati sensibili relativi ai

73 Quali ad esempio la nazionalità, il domicilio, la localizzazione, ecc.

74 D'altronde è proprio questa una delle motivazioni che è alla base della, ormai prossima, introduzione del regolamento *ePrivacy* di cui al par. 6 di questo scritto. Non pare d'altronde un caso che la stessa Carta dei diritti fondamentali dell'Unione Europea senta l'esigenza di disciplinare (nel suo art. 8) proprio la protezione dei dati di carattere personale, stabilendo che «ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano; tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica; il rispetto di tali regole è soggetto al controllo di un'autorità indipendente». E può anche essere segnalato come il "principio di riservatezza" sia altresì riconosciuto, e conseguentemente ritenuto meritevole di tutela, dalla *Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali* del 1950, la quale prevede, infatti, il diritto al rispetto della vita privata e familiare, del domicilio e della corrispondenza.

75 È questa la definizione dettata dall'art. 4, par. 2, del Regolamento.

76 La Direttiva al considerando 32 specifica che debbono essere intesi per "dati sensibili relativi ai pagamenti" quei dati che «possono essere usati per commettere frodi, incluse le credenziali di sicurezza personalizzate. Per l'attività dei prestatori di servizi di disposizione di ordine di pagamento e dei prestatori di servizi di informazione sui conti, il nome del titolare del conto e il numero del conto non costituiscono dati sensibili relativi ai pagamenti».

pagamenti del pagatore. Ancora, la Direttiva prevede che i PISP siano tenuti a comunicare in maniera sicura e a fornire tutte le informazioni disponibili sull'ordine di pagamento[77].

Per quanto invece riguarda gli AISP questi *(i)* accedono soltanto alle informazioni sui conti di pagamento designati e sulle operazioni di pagamento effettuate a valere su tali conti, *(ii)* non richiedono dati sensibili relativi ai pagamenti; *(iii)* non usano, non conservano i dati né vi accedono per fini diversi dalla prestazione del servizio di informazione sui conti.

Dal diritto alla titolarità e alla protezione dei dati[78] discendono anche tutti quei diritti relativi all'aggiornamento (e quindi, ove necessario, anche alla loro correzione) e alla cancellazione dei dati (ove non sia più necessario disporne per l'operazione in funzione della quale erano stati forniti o generati).

Occorre ancora soffermarsi sull'effettivo "trattamento dei dati" da parte dei *Third Party Providers*, fermo restando che esso deve sempre essere attuato nel rispetto dei diritti del cliente-consumatore. In funzione di ciò è previsto che «le autorità di regolamentazione bancaria devono creare uno *standard* che definisce con precisione come le imprese bancarie debbano condividere e proteggere i dati. Per fare ciò devono cerare "interfacce di programmazione applicativa" o API, che consentano alle imprese tecnologiche di inserire i loro programmi nei sistemi di finanziatori»[79].

Tuttavia, la portata di simili previsioni generali va valutata alla luce della loro effettiva attuazione nel nostro ordinamento: il che ci porta a considerare come siano stati disciplinati i dati personali dal d.lgs. di recepimento in Italia della PSD2 (d.lgs. n. 218/2017). A questo riguardo si deve segnalare come la Direttiva, e in particolare il suo art. 94 dedicato appunto alla «protezione dei dati», si limiti infatti a richiamare la precedente (ma ormai superata) disciplina relativa al trattamento dei dati personali e alla libera circolazione degli stessi, di cui alla direttiva 95/46/CE. Disciplina ormai completamente sostituita dal Regolamento (UE) 2016/679 o *General Data Protection Regulation* (d'ora in avanti anche solo GDPR)[80].

In Italia, a seguito della promulgazione del GDPR, il legislatore ha modificato il Codice della *privacy*[81], il quale quindi tiene ora conto della (sovraordinata) regolamentazione europea. Si deve a questo punto rilevare come però il d.lgs. 218/2017 di

77 Cfr. Rabitti M., *Il riparto di competenze tra autorità amministrative indipendenti nella Direttiva sui sistemi di pagamento*, in *Innovazione e regole nei pagamenti digitali*, cit., p. 93.

78 Come è noto, le regole per la tutela dei dati personali sono state disciplinate per la prima volta, in Italia, dalla legge 31 dicembre 1996, n. 675, legge successivamente abrogata e sostituita dal Codice in materia di protezione di dati personali(Introdotto con il d.lgs. 30 giugno 2003, n. 196).

79 V. *Libro Bianco su Fintech e pagamenti digitali, STARTmagazine*, p. 25. Di cui è disponibile il formato pdf al *link*: https://www.startmag.it/wp-content/uploads/Fintech_Web-260218.pdf.

80 Il Regolamento (UE) 2016/679, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali e alla libera circolazione di tali dati, abroga la Direttiva 95/46/UE. È entrato in vigore il 24 maggio 2016 e si prevede che abbia applicazione diretta a partire dal 25 maggio 2018. introdotto con l'obbiettivo di fissare alcune regole generali sulla privacy, che fossero direttamente applicabili dagli Stati, e ciò al fine di superare la frammentazione dei regimi nazionali che rappresentava un problema.

81 Con il d.lgs. 10 agosto 2018, n. 101, recante appunto "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla

attuazione della PSD2 non faccia alcun riferimento al GDPR e alle conseguenti modifiche del Codice della Privacy.

Da questo mancato coordinamento discende, in misura più consistente, la esigenza di soffermarsi sul confronto tra le due discipline, anche in considerazione della circostanza che, da un lato, il GDPR, nel regolare la condivisione dei dati, accresce i diritti delle persone quando si tratta di proteggere i loro dati personali, e, dall'altro, la PSD2, finalizzata ad aumentare la condivisione dei dati, aumenta il flusso di dati personali e lo "legittima".

La suddetta interazione tra i due plessi regolamentari (GDPR e PSD2) solleva delicate questioni interpretative e complessi problemi di coordinamento; sicché risulta, anche sotto questo riguardo, particolarmente urgente la adozione di una disciplina volta a regolare le comunicazioni e i flussi di dati nella operatività *on-line*.

Ma tornando allo stato del diritto positivo è preliminarmente necessario sottolineare quale sia il perimetro di attuazione delle due discipline: il GDPR si applica a tutti gli Stati della Unione Europea e a coloro i quali trattano i dati di cittadini dell'UE[82], mentre la PSD2 si applica ai servizi di pagamento prestati nell'Unione.

In primo luogo, la Direttiva estende l'ambito di applicazione della disciplina in tema di trasparenza delle condizioni e di requisiti informativi anche nei confronti: *(i)* delle operazioni di pagamento in una valuta che non è quella di uno Stato membro, qualora il prestatore di servizi di pagamento del pagatore e il prestatore di servizi di pagamento del beneficiario siano entrambi situati nell'Unione; o l'unico prestatore di servizi di pagamento coinvolto nell'operazione di pagamento sia situato nell'Unione; *(ii)* delle operazioni di pagamento in tutte le valute, qualora solo uno dei prestatori di servizi di pagamento sia situato nell'Unione – "operazioni *one-leg*" – anche se relativamente e limitatamente ai soli segmenti delle operazioni di pagamento eseguiti all'interno dei confini dell'Unione[83].

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)".

82 L'art. 3 GDPR prevede: «1. Il presente regolamento si applica al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione.

2. Il presente regolamento si applica al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano: a) l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione.

3. Il presente regolamento si applica al trattamento dei dati personali effettuato da un titolare del trattamento che non è stabilito nell'Unione, ma in un luogo soggetto al diritto di uno Stato membro in virtù del diritto internazionale pubblico».

83 Cfr. art. 2 PSD2 che disciplina per l'appunto l'ambito di applicazione e, nello specifico, prevede che: «1. La presente direttiva si applica ai servizi di pagamento prestati nell'Unione.

2. I titoli III e IV si applicano alle operazioni di pagamento nella valuta di uno Stato membro laddove il prestatore di servizi di pagamento del pagatore e il prestatore di servizi di pagamento del beneficiario siano entrambi situati nell'Unione o l'unico prestatore di servizi di pagamento coinvolto nell'operazione di pagamento sia situato nell'Unione.

3. Il titolo III, salvo l'articolo 45, paragrafo 1, lettera b), l'articolo 52, paragrafo 2, lettera e), e l'articolo 56, lettera a), e il titolo IV, salvo gli articoli da 81 a 86, si applicano alle operazioni di pagamento in una valuta che non è quella di uno Stato membro laddove il prestatore di servizi di pagamento del pagatore e il prestatore di servizi di pagamento del

In secondo luogo, nel confronto tra le due discipline, assume particolare rilevanza il tema del consenso al trattamento dei dati. Da un lato, il GDPR impone che il consenso sia preventivo e inequivocabile nonché, là dove riguardi dati sensibili, esplicito[84]. Inoltre, sempre secondo il Regolamento, il cliente può revocare in ogni momento il consenso precedentemente dato, con il conseguente venire meno del fondamento giuridico, per le banche e i *Third Party Providers*, del trattamento e della elaborazione dei dati di pagamento[85]. Dall'altro lato, la PSD2, proprio al precitato art. 94, prevede che i prestatori di servizi di pagamento possano avere accesso ai dati solo previo ottenimento di un consenso dell'utente di tali servizi di pagamento; il quale consenso deve essere sempre esplicito, pur non riguardando dati sensibili[86]. Ma, anche ai sensi del GDPR, i responsabili del trattamento dei dati (e quindi, nella nostra prospettiva, anzitutto banche, ASPSP e *Third Party Providers*) devono disporre di una "base legale" (come con inelegante anglismo si esprime il Regolamento per fare riferimento al fondamento o presupposto giuridico) per elaborare i dati personali del cliente. E però il "consenso" è solo una di tali possibili "basi legali" (e probabilmente non la più praticabile): infatti, è permesso il trattamento di dati personali (senza consenso) al ricorrere di presupposti alternativi (come, ad esempio, quando il trattamento è necessario per eseguire un contratto o per l'adempimento di un obbligo legale). In pratica, se un cliente desidera effettuare una transazione di pagamento con un *Third Party Provider*, questo ha bisogno di accedere ai dati dell'*account* di pagamento per eseguire la prestazione, ed essendovi un contratto che disciplina il rapporto tra l'operatore e l'utente, ne deriva che per eseguire il pagamento la relativa elaborazione dei dati associati non abbisogna di un ulteriore consenso dell'utente.

In definitiva, risulta come la PSD2 imponga uno *standard* di protezione rafforzato rispetto al GDPR, dal momento che, come si è visto, la prima impone sempre il consenso esplicito, mentre la seconda prevede una serie di ipotesi in cui esso può essere omesso (pur mantenendosi il diritto al trattamento dei dati).

Per quanto poi riguarda il diritto alla cancellazione dei dati personali, esso opera in modo analogo tanto nel GDPR quanto nella PSD2. I clienti o utenti possono infatti richiedere la cancellazione dei propri dati personali[87] in qualsiasi momento[88];

beneficiario siano entrambi situati nell'Unione, o l'unico prestatore di servizi di pagamento coinvolto nell'operazione di pagamento sia situato nell'Unione, per ciò che riguarda le parti dell'operazione di pagamento effettuate nell'Unione.

4. Il titolo III, salvo l'articolo 45, paragrafo 1, lettera b), l'articolo 52, paragrafo 2, lettera e), l'articolo 52, paragrafo 5, lettera g), e l'articolo 56, lettera a), e il titolo IV, salvo l'articolo 62, paragrafi 2 e 4, gli articoli 76, 77 e 81, l'articolo 83, paragrafo 1, e gli articoli 89 e 92, si applicano alle operazioni di pagamento in tutte le valute laddove soltanto uno dei prestatori di servizi di pagamento sia situato nell'Unione, per ciò che riguarda le parti dell'operazione di pagamento effettuate nell'Unione.

5. Gli Stati membri possono derogare all'applicazione della totalità o di una parte delle disposizioni della presente direttiva con riferimento agli enti di cui ai punti da (4) a (23) dell'articolo 2, paragrafo 5, della direttiva 2013/36/UE».

84 V. art. 9, comma 1, *a*), PSD2 la quale norma disciplina per l'appunto il "Trattamento di categorie particolari di dati personali".

85 V. artt. 13, 14 e 17 GDPR.

86 In particolare, le banche devono consentire ai *Third Party Providers* di accedere ai dati del conto di pagamento dei clienti solo se i *Third Party Providers* hanno il "consenso esplicito" del cliente: cfr. artt. 67 e 94 PSD2.

87 Sulla cancellazione dei dati personali sia ai sensi del GDPR che della PSD2.

88 Detto anche (impropriamente) diritto all'oblio, che consente di ottenere la rimozione dei dati quando venga meno l'interesse.

con la conseguenza che banche e *Third Party Providers* potrebbero trovarsi di fronte all'obbligo di cancellare i dati di pagamento di costoro. E tuttavia, pur nella uniformità delle due discipline, proprio questo diritto (e correlativo obbligo) di cancellazione dei dati solleva all'atto pratico, quantomeno nella prospettiva di banche, ASPSP e *Third Party Providers*, significative incertezze applicative, soprattutto alla luce della disciplina interna che reca norme aggiuntive e diverse sui diritti delle persone.

Occorre ora soffermarsi sul diritto alla *data portability*. Il diritto alla portabilità dei dati, come accennato, permette all'utente di trasferire i propri dati personali da un titolare di trattamento all'altro ed è il principio cardine su cui si basa la Direttiva nel prevedere, per l'appunto, il flusso di dati tra le banche (o gli intermediari finanziari) e i *Third Party Providers*. Anche l'art. 20 del GDPR disciplina tale diritto e, in particolare, prevede che l'interessato abbia il diritto di ricevere i dati personali che lo riguardano che sono stati forniti ad un titolare del trattamento e trasmetterli ad altro titolare senza che vi siano impedimenti da parte del primo. Questo principio comporta però che vi sia, a monte, un adeguamento delle politiche interne per quanto riguarda la mappatura dei dati e dei flussi di dati che sono stati trattati da parte del titolare del trattamento; e, allo stesso tempo, la necessità che venga garantito un maggior controllo in riferimento a quali debbano essere i dati che devono essere effettivamente trasmessi in modo da evitare la divulgazione di notizie ulteriori a quelle strettamente necessarie[89].

Infine, deve essere richiamato il principio dell'*accountability*, principio che si sostanzia nella responsabilizzazione degli stessi titolari del trattamento, e che comporta l'adozione da parte loro di comportamenti proattivi volti a dimostrare la concreta adozione delle misure finalizzate ad assicurare l'applicazione del Regolamento[90]. Questo principio fonda le sue ragioni nella necessità di evitare il rischio che si possano verificare dei trattamenti non autorizzati, o addirittura illeciti, nonché la perdita o la distruzione di dati personali e delle attrezzature impiegate per il trattamento.

Per quanto attiene alla PSD2, occorre sottolineare come i dati che sono richiesti dai *Third Party Provider*, come si è già avuto modo di anticipare nel par. 4, siano soggetti alla titolarità da parte delle banche e, di conseguenza, al fine del rispetto del principio dell'*accountability*, queste debbano necessariamente garantirne la sicurezza in un'ottica di protezione dell'interessato. Tale principio si traduce nell'adozione di misure tecniche e di modelli organizzativi atti a garantire che la gestione e la conservazione dei dati avvenga in maniera conforme ai principi di protezione dei dati personali.

89 Qualora la Banca sia l'unico titolare del trattamento (questo avviene quando è la stessa banca che elabora i dati dei clienti) dovrà essere nominato il c.d. *responsabile del trattamento* con indicazione specifica: *(i)* della natura; *(ii)* della durata; *(iii)* delle finalità del trattamento (o dei trattamenti assegnati); *(iv)* delle categorie di dati oggetto di trattamento; *(v)* delle misure tecniche e organizzative adeguate a consentire il rispetto delle istruzioni impartite dal titolare; *(vi)* delle disposizioni contenute nel regolamento, anche ai fini dell'adempimento degli obblighi in caso di *data breach* e della cancellazione dei dati al termine della fornitura dei servizi.

Qualora, invece, la banca sia co-titolare del trattamento dei dati, e quindi vi sia una collaborazione con la società di gestione dei sistemi informativi, sarà necessario che sia definito *ex ante* il rispettivo ambito di responsabilità e, di conseguenza, quelli che sono i rispettivi compiti con riferimento all'esercizio dei diritti dei clienti. Rimane tuttavia la responsabilità solidale dei co-titolari nei confronti di coloro che sono gli interessati di tale trattamento di dati e questo indipendentemente dalla ripartizione dei compiti e degli obblighi che venga fatta *ex ante*.

90 Cfr. capo IV, in particolare artt. da 23 a 25 del GDPR.

Il titolare del trattamento sarà tenuto a svolgere un'analisi preventiva dell'impatto, la c.d. *Data Privacy Impact Assessment* (DPIA), che consente di individuare e applicare le misure correttive che si rivelano opportune per la prevenzione del rischio sin dalla progettazione del servizio o prodotto.

In conclusione, il trattamento dei dati personali del beneficiario da parte dei *Third Party Providers* deve ritenersi, in linea di principio, consentito: in particolare, dal combinato disposto delle norme del GDPR e della PSD2 si ricava, da un lato, che l'operazione di pagamento è circostanza sufficiente a giustificare il trattamento, nonostante tra l'intermediario del pagatore e il beneficiario non vi si alcun rapporto diretto, d'altro lato, che quest'ultimo è tutelato tramite la delimitazione dell'area di legittimità del trattamento al solo utilizzo che egli potrebbe ragionevolmente aspettarsi.

Tuttavia, risulta evidente come la non coincidenza e la mancanza di richiami tra GDPR e PSD2 creino discrasie nell'interpretazione da parte degli operatori del diritto[91], e quindi relativamente a quelli che sono, da un lato, i diritti e, dall'altro, gli obblighi dei *Third Party Providers*. Ad esempio, le banche si astengono dal fornire ai *Third Party Providers* l'accesso ai dati di pagamento dei clienti per timore di violare i diritti alla *privacy* dei loro clienti ai sensi del GDPR, dal momento che le autorità di concorrenza potrebbero considerare tale rifiuto non tanto legittimo ai sensi dei dettami del Regolamento, quanto più, invece, una violazione della normativa sulla concorrenza.

1.7 Conclusioni

Come è noto, «l'esperienza contemporanea attesta che larga parte dei pagamenti di debiti pecuniari è operata attraverso moneta bancaria o scritturale, vale a dire, per semplicità, con strumenti e operazioni che impongono l'intervento istituzionale di prestatori di servizi di pagamento»[92]. La possibilità di acquistare prodotti e servizi *online* è sempre più apprezzata e ciò comporta un incremento significativo delle negoziazioni che genericamente compongono il vasto settore dell'*e-commerce*; da ultimo questa tendenza risulta accentuata a causa delle restrizioni imposte dalla emergenza pandemica.

91 Il quadro normativo costituito dalla Direttiva *E-Commerce*, sebbene oggetto di molteplici interventi della Corte di Giustizia, è rimasto invariato nel corso di vent'anni e non è più in grado di essere un baluardo regolatorio sufficiente. Ben consapevoli che la pura e semplice regolamentazione del mercato non è sufficiente a garantire la piena attenzione verso i diritti fondamentali in gioco, la Commissione sta vagliando due iniziative legislative, entrambe parte della "*European Digital Strategy, Shaping Europe's Digital Future*": il *Digital Services Act* e il *Digital Single Market Act*. Sebbene entrambe abbiano delle finalità in comune, facendo correre su binari paralleli tanto la realizzazione di uno spazio rispettoso delle libertà individuali quanto la promozione di un contesto di crescita rivolta verso innovazione e competitività, il raggio di azione dei due atti sarà essenzialmente diverso. Rimandando la spiegazione sul DSA ai paragrafi che seguono, il *Digital Market Act* rappresenterà un nuovo strumento per bloccare condotte manipolatorie del mercato supportando la partecipazione di piccole e medie imprese in un contesto ove i costi di entrata sono esageratamente alti e gestiti dai *gatekeepers*, i giganti del Web. Il *Digital Services Act* è un pacchetto di riforme che la Commissione Europa ha lanciato il 15 dicembre 2020 allo scopo di disciplinare i servizi digitali. Un concetto ad ombrello nel quale possiamo ricomprendere, tra gli altri, "i servizi di intermediari online, sia di contenuti, prodotti e servizi, messi a disposizione di terzi". Come si legge in apertura della proposta, con riferimento alle ragioni ed agli obiettivi, la riforma segue le fila di un necessario emendamento di quanto era stato previsto dalla richiamata Direttiva *E-Commerce*. In merito cfr. https://www.iusinitinere.it/il-digital-services-act-verso-una-nuova-governance-di-internet-34071.

92 M. Rossi, *Pagamenti intermediati e disciplina con*corsuale, Cedam, Milano, 2020, p. 1.

Ciò nonostante, rispetto ad altri Paesi e ad altre economie, in Italia l'*e-commerce* risulta ancora in proporzione assai poco sviluppato: persiste diffidenza a inserire o comunicare i propri dati, bancari e personali, *on-line* e la stessa diffusione delle tecnologie, che rappresentano il presupposto per la conclusione di contratti e per la relativa esecuzione di operazioni di pagamento sulla rete, appare ancora tutto sommato limitata.

In questo senso la PSD2, che ha fatto della sicurezza e della trasparenza nei pagamenti *on-line* il suo scopo principe, gioverà all'evoluzione dell'*e-commerce* dato che fiducia e sicurezza sono i presupposti necessari delle vendite e degli altri contratti *on-line*. D'ora in avanti, si assisterà ad un ampliamento del campo di applicazione della PSD2, e si considereranno l'uso, l'accesso e la condivisione dei dati in un contesto più ampio e non solo in relazione ai servizi finanziari.

2 I costitutori delle banche dati e i titolari dei software

2.1 *Intangible rich economy, Fintech, Techfin* e *Big Data* nel settore bancario: un nuovo paradigma digitale

La crescente digitalizzazione ha significatamene modificato il contesto in cui operano i tradizionali *incumbents*, richiedendo nuove modalità di dialogo e interazione con i clienti. Si assiste, in sostanza, al proliferare di una serie di fenomeni esogeni ed endogeni che interessano il settore bancario, alimentando, di rimando, la necessità di operare un'attenta riflessione sulle potenziali linee di sviluppo cui dovranno attenersi le Autorità di controllo e le istituzioni finanziarie, in ragione del consistente impatto che tale nuova tendenza ha sull'ecosistema in cui esse operano. La profonda fase di trasformazione che interessa l'attività bancaria coinvolge nuovi attori quali aziende Fintech e Big Tech, rimodellando l'economia in una nuova prospettiva di "*intangible rich economy*", ove gli *asset* intangibili (R&S, *software*, *database*, processi aziendali, *etc.*, nonché diritti di proprietà intellettuale) prevalgono su quelli tangibili. Il progressivo passaggio a un'economia caratterizzata da investimenti in capitale intangibile rappresenta un punto cruciale per il sistema bancario, data l'introduzione di una significativa modifica tanto dal lato della domanda quanto dell'offerta dei servizi finanziari[93]. A ciò si aggiunga che tale capitalizzazione contribuisce a mutare le dinamiche competitive e, in alcuni casi, gli stessi "confini tipici del settore bancario"[94], contribuendo fattivamente alla diffusione del paradigma dell'*Open Innovation*[95].

93 Ambrosetti, Le banche del futuro, The European House Ambrosetti, 2020, pp. 58 ss., disponibile al sito internet: http://www.astrid-online.it/static/upload/ambr/ambrosetti_le-banche-del-futuro-2020.pdf; Lanzilotta D., Sul filo dell'innovazione. Visioni e soluzioni per le PMI che sfidano il futuro, Goware, 2017, pp. 30 ss.

94 Ambrosetti, op. cit., p. 74.

95 H.W. Chesbrough, Open Innovation, the new imperative for creating and profiting from technology, Harvard Business School Press, Boston, Massachussetts, 2006, p. XX; per un ulteriore approfondimento sul punto si veda H.W. Chesbrough, Everything you need to know about open innovation, Forbes, 2011, disponibile al sito Internet: https://www.forbes.com/sites/henrychesbrough/2011/03/21/everything-you-need-to-know-about-open-innovation/#4e96537075f4; D. Binci, Innovazione e Cambiamento, Struttura, tecnologia, competenze e leadership tra innovazione tradizionale e innovazione aperta, Franco Angeli, 2016, p. 17; G. Santoro, Open Innovation, aspetti teorici ed

La *digital revolution* ha cambiato profondamente il settore dei servizi finanziari e di pagamento, aprendo le porte alle imprese Fintech. Esse elaborano e adottano modelli particolarmente efficienti di *business solutions,* che consentono loro di pianificare efficaci strategie imprenditoriali atte a rinnovare e/o semplificare i processi produttivi interni, nonché implementare la digitalizzazione negli scambi e nell'offerta di servizi sempre più rispondenti alle esigenze dei singoli. A queste ultime si affiancano i *new entrants*, spesso soggetti *leader* nel settore digitale e dell'informazione, che traggono vantaggio competitivo e profitto dallo sfruttamento della grande mole di dati cui hanno accesso e che, a differenza dei predetti istituti finanziari, pur non avendo a propria disposizione una tradizionale rete di filiali, godono di una consolidata base di clientela, a fronte della loro notorietà. Le Big Tech, ovverosia le grandi aziende tecnologiche – in tale ambito si sottolinea la presenza di GAFA in U.S.A. (Google, Apple, Facebook e Amazon) e BAT in Asia (Baidu, Alibaba e Tencent) – forti della complementarietà tra varie tecnologie[96], volgono il proprio interesse alle "*revenues* delle parti più profittevoli della catena di valore"[97], cominciando a offrire servizi di carattere finanziario come pagamenti, gestione del *wallet,* pacchetti assicurativi e prestiti, servendosi dell'analisi dei dati, dell'intelligenza artificiale e del *machine learning*. Il punto di forza di queste ultime risiede nell'offrire ai consumatori un peculiare modello di *business*, frutto del binomio tra effetti di *network* (generati, a esempio, da piattaforme *e-commerce*, *search engines*, *etc.*) e dalla tecnologia da esse impiegata. Accanto alle Fintech, dunque, cominciano ad affermarsi imprese che operavano *ab origine* in un contesto totalmente distinto – e, più nello specifico, nel settore tecnologico o nel canale distributivo – e che risultano molto più temibili e competitive rispetto agli intermediari finanziari vigilati (IFv) e alle Fintech stesse[98].

Il complesso di conoscenze derivanti dall'ecosistema digitale e dalla *data driven economy*[99] collocano la suddetta transizione tra le sfide che interessano la *leadership* bancaria. Le banche, infatti, possono accedere e raccogliere dati spesso limitati e circoscritti alla storia del cliente, forniti dallo stesso ovvero acquisiti in ragione di un sottostante rapporto contrattuale[100], dai quali astrarre valore e supportare le decisioni finanziarie. È chiaro come, anche in tale settore, la *Big data analytics*[101] svolga un ruolo

evidenze empiriche, Giappichelli Editore, 2017, p. 50; T. Felin, T.R. Zenger, Closed or open innovation? Problem solving and the governance choice in Research Policy, Policy Management, and economic studies of science. technology and innovation, A. Bergek, A. Coad *et al.*, Elsevier, 2005, pp. 914 ss.; L. Serio, L. Quarantino, L'innovazione aperta, la prospettiva dell'innovazione aperta e le nuove logiche organizzative manageriali, Sviluppo&Organizzazione, 2009, pp. 64 ss.

96 J. Padilla, M. De la Mano, Big Tech Banking, 2018, disponibile al sito Internet: SRN: https://ssrn.com/abstract=3294723.

97 M. Panebianco, Il possibile impatto in economia e finanza dei GAFA, PWC, 2018, disponibile al sito Internet: https://www.pwc.com/it/it/industries/asset-management/assets/docs/impatto-economico-finanziario-gafa.pdf.

98 M. Maggiolino, M. Scopsi, op. cit., p. 186; D.A. Zetzsche, R.P. Buckley, D.W. Arner, J.N. Barberis, From Fintech to Techfin: The Regulatory Challenges of Data-Driven Finance, European Banking Institute, Working Paper Series, n. 6, 2017, p. 11-17; C. Schena, A. Tanda, C. Arlotta, G. Potenza, Lo sviluppo del Fintech, opportunità e rischi per l'industria finanziaria nell'era digitale, Consob, 2018, p. 11.

99 Commissione Europea, Towards a thriving data-driven economy, Bruxelles, 2014, COM (2014) 442 final, p. 4; M.A. Rossi, Il ruolo delle piattaforme nell'economie dei Big Data, in op. cit., p. 75.

100 M. Maggiolino, M. Scopsi, op. cit., p. 187.

101 M.M. Najafabadi *et al.,* Deep learning applications and challenges in big data analytics, in Journal of Big data, Springer, 2015, p. 7; G. Colangelo, M. Maggiolino, Big Data as Misleading Facilities, in European Competition Journal, 2017,

di rilievo, correlato alla natura stessa delle informazioni, "elemento chiave" per la concorrenza[102]. Ne deriva che la conseguente utilità economica non dipende dai dati in quanto tali ma dal complesso di risorse materiali e intellettuali investite nello sviluppo di sistemi di analisi idonei a trarre interferenze affidabili[103].

Gli intermediari finanziari, dunque, si trovano innanzi a un bivio per il quale o la progressiva disintermediazione[104] spingerà gli stessi ai margini del sistema oppure, se sceglieranno di attrezzarsi adeguatamente, competeranno in maniera efficiente nel mercato.

2.2 Il duplice livello di tutela delle banche dati: accesso, proprietà e regolamentazione

Se da una parte l'implementazione di nuove tecnologie di gestione, processamento e archiviazione apporta significativi vantaggi e contribuisce alla crescita del capitale intangibile interno del sistema bancario[105], dall'altra si pongono importanti quesiti in termini di accesso. In tale scenario – e al fine di favorire l'ascesa del Fintech – sarà opportuno sfruttare la mole di dati al fine di elaborare accurati modelli finanziari, che contribuiscano a sostenere il settore di riferimento e la gestione dei potenziali rischi.

La proprietà intellettuale non interessa i dati in quanto tali ma le strutture che li contengono, ovverosia i *database*[106]. Per banca dati «si intende, ai fini della Direttiva, una raccolta di opere, dati o altri elementi indipendenti, sistematicamente o metodicamente disposti e individualmente accessibili grazie a processi elettronici o in

disponibile al sito Internet: https://ssrn.com/abstract=2978465; F. Ponte, I big data come common goods, in Cyberspezio e Diritto, 2017, pp. 34-38; A. Preta, M. Maggiolino, L'economia dei dati, 2018, pp. 93-96, disponibile al sito Internet: http://www.itmedia-consulting.com/DOCUMENTI/economiadeidati.pdf; H.G. Miller, P. Mork, From data to decisions: a value chain for Big Data, in IT Professional 15, 2013, pp. 2-4, disponibile al sito Internet: https://www.researchgate.net/profile/H_Miller5/publication/260305818_From_Data_to_Decisions_A_Value_Chain_for_Big_Data/links/5620110708ae93a5c9243a66/From-Data-to-Decisions-A-Value-Chain-for-Big-Data.pdf?origin=publication_detail.

102 G. Pitruzzella, Fintech e nuovi scenari competitivi, in Fintech: diritti, concorrenza, regole. Le operazioni di finanziamento tecnologico, a cura di V. Falce, G. Finocchiaro, Zannichelli Editore, 2019, p. 14; è bene puntualizzare che, accanto alla Big Data Analytics, si sta sviluppando la c.d. *predictive analysis*, la quale prevede l'applicazione di algoritmi statistici e di apprendimento automatico ai dati c.d. storici. Ciò consentirà di effettuare previsioni future, individuando nuove possibili opportunità. Sul punto si veda: M.M. Najafabadi *et al.*, art. cit., pp. 6-7; M.A. Waller, S.E. Fawcett, Data science, predictive analytics, and big data: a revolution that will transform supply chain design and management, in Journal of Business Logistics, vol 34 [2], 2013, pp. 2-15; F.L.F. Almedia, Benefits, challenges and tools of big data management, in Journal of Systems Integration, 2017, p. 16; B.M. Balachandran, S. Prasad, Challenges and Benefits of Deploying Big Data Analytics in the Cloud for Business Intelligence, International Conference on Knowledge Based and Intelligent Information and Engineering Systems, 2017, in Procedia Computer Science, vol. 112, Elsevier, pp. 1118-1119, disponibile al sito Internet: https://doi.org/10.1016/j.procs.2017.08.13.

103 G. Colangelo, M. Maggiolino, Big Data as Misleading Facilities. European Competition Journal, Forthcoming, Bocconi Legal Studies Research Paper No. 2978465, 2017, pp. 15 ss., disponibile al sito Internet: https://ssrn.com/abstract=2978465.

104 V. Meli, Opportunità e sfide per la concorrenza nella disciplina dei servizi di pagamento, RomaTrePress, 2020, disponibile al sito Internet: http://romatrepress.uniroma3.it/wp-content/uploads/2020/03/Opportunit%C3%A0-e-sfide-per-la-concorrenza.pdf.

105 S. Aliprandi, Il fenomeno open data, indicazione e norme per un mondo di dati aperti, Ledizioni, 2014, pp. 25 ss.

106 Art. 3, co. 2, Dir. 96/9/CE.

altro modo, quali processi di tipo elettromagnetico, elettronico o di natura analoga»[107].A livello europeo è accordato un duplice livello di protezione: la tutela autoriale e quella *sui generis*; il *discrimen*, in questo caso, viene individuato nella presenza o meno del carattere creativo. Il diritto *sui generis* interessa le banche dati non creative e riconosce un diritto esclusivo in ragione dei rilevanti investimenti sostenuti per la sua costituzione, sia dal punto di vista quantitativo che qualitativo[108]. La *ratio* è quella di proteggere "l'interesse economico dell'imprenditore"[109], prospettando, in tal senso, una sorta di "iper-tutela degli investimenti"[110]. Sarà, dunque, vietata qualsiasi indebita appropriazione dei risultati ottenuti, al fine di tutelare quest'ultimo da eventuali gravi conseguenze economiche e tecniche, nonché da un pregiudizio sostanziale all'investimento, di carattere finanziario e professionale, sopportato. Titolare del diritto è il costitutore, il quale è definito, ai sensi del 41° considerando della Direttiva 96/9/CE, come colui che prende l'iniziativa e assume su di sé il rischio di effettuare i dovuti investimenti. Egli, dunque, potrà vietare *erga omnes* operazioni di estrazione[111] e/o reimpiego[112] della suddetta banca dati, nella sua totalità ovvero in una sua parte sostanziale. I diritti a lui riconosciuti sono indipendenti dalla protezione offerta e non pregiudicano, in alcun modo, quelli che vertono sul contenuto o su di una sua parte. Ne deriva che sarà lecito prelevare e riutilizzare una piccola porzione del *database* ovvero una singola informazione[113]. Il diritto di vietare e di autorizzare sorgono al suo completamento e si estinguono una volta decorsi quindici anni dal primo gennaio dell'anno successivo alla data della sua ultimazione (art. 102 *bis,* co. 6, l.d.a.). Viceversa, ove si tratti di banca dati messa a disposizione del pubblico, in qualunque modalità,

107 V.M. De Sanctis, M. Fabiani, I Contratti di Diritto d'Autore, Giuffrè Editore, 2007, p. 81; Il considerando 17 della Dir. 96/9/CE statuisce che con il termine «banca di dati» si intende «definire una raccolta di opere, siano esse letterarie, artistiche, musicali o di altro genere, oppure di materiale quali testi, suoni, immagini, numeri, fatti e dati; che deve trattarsi di raccolte di opere, di dati o di altri elementi indipendenti, disposti in maniera sistematica o metodica e individualmente accessibili; che di conseguenza la definizione di un'opera audiovisiva, cinematografica, letteraria o musicale in quanto tale non rientra nel campo d'applicazione della presente direttiva»; M. Della Torre, Diritto e informatica, Giuffrè Editore, p. 33; C. Grassetti, Statistica per la pubblica amministrazione, libreriauniversitaria.it, 2008, p. 134: «per banche dati si intendono vasti sistemi di informazioni gestiti da appositi software».

108 F. Faini, S. Pietropaoli, Scienza giuridica e tecnologie informatiche, Giappichelli editore, 2017, p. 222; F. Auletiano, La rilevanza delle banche dati nel sistema di "*cyberlaw*", in I Contratti, fasc. 10, 1999, pp. 925 ss. A parere dell'autore la protezione garantita dal diritto *sui generis* si inquadrata tra i principi del diritto alla concorrenza, dal momento che persegue quale obiettivo quello di alimentare lo sviluppo del settore e, contestualmente, prevenire qualsiasi atto di concorrenza sleale.

109 L. Chimenti, Lineamenti del nuovo diritto d'autore, Giuffrè, 2006, p. 74; G. Guglielmetti, La tutela delle banche dati con diritto *sui generis* nella direttiva 96/6/CE, in Contratto e impresa Europa, 1997, pp. 177 ss.; A. Sirotti Gaudenzi, Il nuovo diritto d'autore, la tutela della proprietà intellettuale nella società dell'informazione, Maggioli Editore, 2018, pp. 321-322.

110 V. Falce, L'insostenibile leggerezza delle regole sulle banche dati nell'unione dell'innovazione, in Rivista di Diritto Industriale, fasc. 4-5. 2018, p. 389; il diritto *sui generis* andrebbe riconosciuto esclusivamente alla raccolta di materiale preesistente, si veda sul punto C. Manavello, Prima decisione della Corte di Giustizia sulla protezione delle banche dati, in Il Diritto Industriale, 2005, fasc. 4, pp. 422-423.

111 Art. 102 *bis,* co. 1, lett. a), L. 633/1941: «il trasferimento permanente o temporaneo della totalità o di una parte sostanziale del contenuto di una banca di dati su un altro supporto con qualsiasi mezzo o in qualsivoglia forma. L'attività di prestito dei soggetti di cui all'articolo 69, comma 1, non costituisce atto di estrazione».

112 Art. 102 *bis,* co. 1, lett. a), L. 633/1941: «qualsivoglia forma di messa a disposizione del pubblico della totalità o di una parte sostanziale del contenuto della banca di dati mediante distribuzione di copie, noleggio, trasmissione effettuata con qualsiasi mezzo e in qualsiasi forma. L'attività di prestito dei soggetti di cui all'articolo 69, comma 1, non costituisce atto di reimpiego».

113 V. Falce, Tech-Fin databases in the open banking system. An out-of-the-box competition law perspective, p. 2.

prima dello scadere del periodo di cui sopra, la durata della tutela si estinguerà trascorsi quindici anni dal primo gennaio dell'anno successivo alla data in cui la stessa è stata resa disponibile per la prima volta (art. 102 *bis*, co. 7, l.d.a.). Detto in altri termini, il vantaggio accordato consiste nel protrarre la durata di protezione a ogni nuova integrazione ovvero modifica sostanziale, che sarà valutata, sotto il profilo qualitativo e quantitativo, prospettando un autonomo termine di durata di tutela, pari a quello delineato dai commi summenzionati.

L'anello di congiunzione tra la tutela giuridica riconosciuta alle banche dati e il diritto di accesso è stato oggetto di un'importante pronuncia da parte della Corte di Giustizia nella causa C-46/02, la quale ha statuito che tale diritto concerne unicamente le operazioni sovra menzionate, non interessando quelle di mera consultazione[114]. Il costitutore, in tal senso, potrà scegliere se prevedere un diritto di accesso esclusivo, riservarlo a soggetti individuati ovvero subordinarlo al concretizzarsi di determinate condizioni. Al terzo che abbia ottenuto specifica autorizzazione, dunque, sarà assicurata la consultazione, la quale non potrà essere inibita dal diritto *sui generis,* salvo che, a tale operazione, segua un trasferimento di tipo permanente ovvero temporaneo, della totalità o di una parte sostanziale del contenuto verso altro supporto[115]. Ne deriva che la disponibilità di accesso potrà essere garantita anche a seguito della sottoscrizione di un contratto e dietro pagamento di corrispettivo. Il prelievo di elementi da una banca dati sottoposta a tutela e il loro successivo inserimento all'interno di un'altra (a seguito della consultazione della prima su schermo e alla valutazione individuale degli elementi in essa contenuti), potrà configurare "estrazione" ai sensi dell'art. 7 Dir. 96/9/CE, a condizione che tale operazione consista nel trasferimento di una sua parte sostanziale, valutata qualitativamente e quantitativamente, ovvero al trasferimento di parti non sostanziali che, per il loro carattere ripetuto e sistematico, siano state in grado di ricostruire una parte rilevante del suo contenuto[116]. Ove, tuttavia, all'operazione di consultazione non corrisponda il trasferimento di dati verso altro supporto, non avrà luogo alcuna lesione del diritto *sui generis*. Ciò comporta la piena salvaguardia del diritto di accesso all'informazione, escludendo ipotesi di monopoli ovvero abuso di posizione dominante[117]. A tal proposito è utile sottolineare come la Direttiva non pregiudichi quanto previsto dalla disciplina sulle intese e sulla concorrenza sleale. Più nello specifico, nel 47esimo considerando il Legislatore comunitario ha avuto un occhio di riguardo nel preservare la concorrenza, puntualizzando come tale diritto non debba essere in alcun modo esercitato per facilitare l'abuso di posizione dominante. A tale principio è stato, poi, attribuito valore normativo attraverso il disposto di cui all'art. 13, il quale afferma che le disposizioni ivi contenute lasciano intatta l'applicazione delle norme che regolano la concorrenza, indipendentemente dalla loro natura comunitaria ovvero nazionale. Proprio in tale ottica, l'art. 16 dispone che la Commissione debba

114 Corte di Giustizia, Sentenza 9/11/2004, Causa C-46/02, Fixtures Marketing Ltd vs. Oy Veikkaus Ab.

115 Corte di Giustizia, Sentenza 9/10/2008, Causa C-304/07, Directmedia Publishing GmbH vs. Albert-Ludwigs-Universität Freiburg.

116 *idem*.

117 P. Sammarco, Nota Corte di Giustizia 9 ottobre 2008, n. 96/9/CE, in Diritto e Informatica, 2008, p. 785.

redigere, periodicamente, una relazione sulla scorta delle informazioni fornite da ciascun Stato Membro, al fine di verificare se l'applicazione del summenzionato diritto abbia, di fatto, determinato un pregiudizio alla libera concorrenza.

La focalizzazione sul valore della tecnologia come alternativa efficiente ed economica, veloce ed elastica, ha portato i *leader* bancari all'implementazione di servizi di *cloud computing*[118] e, in particolar modo, a quelli di tipo flessibile ovvero ibrido[119]. Questi ultimi apportano notevoli vantaggi in termini di flessibilità, scalabilità e riduzione dei costi, consentendo, al contempo, di rispondere in maniera puntuale alla crescente necessità di sicurezza dei dati, nonché al miglioramento delle prestazioni aziendali e dei rendimenti degli azionisti[120]. La combinazione tra la flessibilità propria del *cloud* pubblico e la sicurezza di quello privato costituisce, dunque, la soluzione ottimale per operare in un mercato fortemente regolamentato, che presenta in sé crescenti livelli di *compliance*. A ciò si aggiunga che il ricorso alla tecnologia *blockchain* contribuisce a rivoluzionare le modalità di gestione e distribuzione dei dati, in virtù della decentralizzazione delle informazioni registrate sui nodi della medesima rete. La stessa, infatti, potrebbe apportare considerevoli benefici anche nell'ambito del *trading* di azioni, obbligazioni e titoli. Questo perché, da una parte, beneficia della dematerializzazione mediante gli *smart contracts* e, dall'altra, consente una maggiore tracciabilità e trasparenza delle operazioni. Ne deriva che ogni qual volta viene immesso all'interno del sistema un ordine di acquisto ovvero di vendita, tale tecnologia ne consente l'esecuzione una volta verificata l'esistenza dei requisiti in capo alle parti[121].

Al fine di consolidare la *leadership* europea in tema di dati e di creare un ecosistema digitale omogeneo e aperto è stato avviato il progetto franco-tedesco denominato "Gaia-X", il quale mira a creare una comune infrastruttura *cloud* "federata"

118 E.M. Tripodi, Dig.ital r.evolution, 5 lezioni per la riqualificazione delle imprese italiane, youcanprint, Tricase, 2016, p. 13; Commissione Europea, Comunicazione del 27 settembre 2012, Sfruttare il potenziale del cloud computing in Europa, COM (2012) 529 final; A. Salam, Z. Gilani, S. Ul Haq, Deploying and managing a cloud infrastructure, Sybex, 2015, pp. 62 ss.; G. Neri, L'impresa nell'era digitale, tecnologie informatiche e rivoluzione digitale al servizio dell'impresa, GuaraldiLAB, 2015, pp. 240 ss.; Garante della Protezione dei dati personali, Cloud Computing: indicazioni per l'utilizzo consapevoli dei servizi, schede di documentazione, pp. 6-7, disponibile al sito Internet: www.garateprivacy.it; L.M. Vaquero, L. Merino-Rodero, J. Caceres, M. Lindner, A break in the clouds: towards a cloud definition, ACM SIGCOMM Computer Communication Review, Volume 39, Number 1, 2019, pp. 50-53; G. Reese, Cloud Computing. Architettura, infrastrutture, applicazioni, Tecniche Nuove, 2010, p. 8; M. Bertani, Internet e la "amministrativizzazione" della proprietà intellettuale, in il Regolamento AGCOM sul diritto d'autore a cura di L.C. Umbertazzi, Giappichelli Editore, 2014, p. 12.

119 The Economist Intelligent Unit, The distruption of banking, Report, 2015, p. 12, disponibile al sito Internet: http://www.fintech-ecosystem.com/assets/the-disruption-of-banking---the-economist--10-29-15.pdf. I principali vantaggi di un cloud ibrido includono una netta riduzione dei costi, una maggiore efficienza operativa e una maggiore innovazione.

120 E. Martini, Banche in cloud, grandi vantaggi e forti rischi normativi: il quadro, Agenda Digitale, 2018, disponibile al sito Internet: https://www.agendadigitale.eu/infrastrutture/banche-in-cloud-grandi-vantaggi-e-forti-rischi-normativi-il-quadro/.

121 M. Bellezza, Blockchain, in Fintech: introduzione a profili giuridici di un mercato unico tecnologico dei servizi finanziari, a cura di M. Paracampo, Giappichelli Editore, 2017, pp. 2018 ss.; H. Atlam, A. Alenzi, M.O. Alassafi, G.B. Wills, Blockchain with internet of things: benefits, challenges, and future directions, in I.J. Intelligent Systems and Applications, Modern Education and Computer Science (Mecs) Press, 2018, pp. 40-46; M. Pilkinton, Blockchain technology: principles and applications, 2015, Research Handbook on Digital Transformations, edited by F.X. Olleros, M. Zhegu, Edward Elgar, 2016, pp. 4-39, disponibile al sito Internet: https://ssrn.com/abstract=2662660; P. Boucher, S. Nascimento, M. Kritikos, Come la tecnologia blockchain può cambiarci la vita, Servizio di Ricerca del Parlamento Europeo, 2017, p. 5.

europea[122], atta a conservare e gestire il flusso costante dei dati conformemente ai valori e alle normative europee in materia; il tutto puntando su valori quali sicurezza, innovazione, *open source* e trasparenza[123]. Collegando le varie infrastrutture centralizzate e decentralizzate, esso mira a trasformare queste ultime in un unico sistema omogeneo di facile impiego, favorendo l'interoperabilità tra i vari fornitori di servizi *cloud*.

2.3 Banche dati e ipotesi di abuso dei diritti: le prospettive anticoncorrenziali

Il Fintech ha rivoluzionato il modo in cui i fornitori di servizi finanziari operano e interagiscono con i propri utenti, cambiando radicalmente i tradizionali paradigmi e rappresentando una priorità per le Istituzioni Europee. A fronte dei considerevoli benefici emergono, tuttavia, potenziali rischi anticoncorrenziali, che pongono nuove sfide rispetto l'applicazione dei consueti modelli utilizzati in concorrenza[124]. La combinazione dell'utilizzo di piattaforme digitali e la modalità con cui i singoli utenti accedono e si avvalgono della tecnologia Fintech prospetta criticità in termini di "interoperabilità" e "standardizzazione". Una delle maggiori problematiche risiede nella distribuzione del potere di mercato dei dati che, allo stato attuale, tende a concentrarsi nella disponibilità di pochi operatori: i Big Tech[125]. Questi ultimi riescono ad attingere da varie risorse complementari, contribuendo alla creazione di un ampio "*cluster* dinamico e interattivo" costantemente integrato: le abitudini di acquisto e le preferenze dei consumatori, combinati con i dati afferenti al conto e a quelli di pagamento, per-

122 Gaia-X: Pan European GAIA-X Summit, GAIA-X will give birth to the new generation of data ecosystem, available at: https://www.data-infrastructure.eu/GAIAX/Redaktion/EN/Downloads/gaia-x-press-release-20201118.pdf?__blob=publicationFile&v=2; a ciò si aggiunga che è proprio la "forma federata" che potenzierà la capacità di accedere e condividere i dati in maniera affidabile.

123 FASI (Fundingn Aid Strategies Investments, Gaia-X: 28 imprese italiane aderiscono al cloud europeo, 2020, disponibile al sito Internet: https://www.fasi.biz/it/notizie/strategie/22869-gaia-x-cloud-europeo.html; si veda anche Pisano P., Intervento del Ministro per l'Innovazione tecnologica e la digitalizzazione Paola Pisano al Gaia-X Summit, 19 novembre 2020.

124 F. Divetta, Fintech fra dati e concentrazioni, in Fintech: diritti, concorrenza, regole. Le operazioni di finanziamento tecnologico, a cura di F. Falce, G. Finocchiaro, Zanichelli Editore, 2019, p. 143.

125 R. Romano, Intelligenza artificiale: decisioni e responsabilità in Fintech: diritti, concorrenza, regole. Le operazioni di finanziamento tecnologico, a cura di F. Falce, G. Finocchiaro, Zanichelli Editore, 2019, p. 321; D.A. Zetzsche, R.P. Buckley, D.W. Arner, J.N. Barbieri, From Fintech to Techfin: The Regulatory Challenges of Data-Driven Finance, European Banking Institute Working Paper Series 2017- No. 6, University of Hong Kong Faculty of Law Research Paper No. 2017/007, University of Luxembourg Law Working Paper No. 2017-001, disponibile al sito Internet: https://ssrn.com/abstract=2959925 or http://dx.doi.org/10.2139/ssrn.2959925.

metterebbero di ricavare informazioni circa l'inclinazione al risparmio e, più in generale, di delineare il "profilo finanziario" del consumatore[126], creando prodotti e servizi difficilmente replicabili dagli *incumbents*[127].

Negli ultimi anni il drammatico mutamento nell'ampiezza e nella portata dell'accumulo dei dati e la crescente capacità delle imprese di analizzarli mediante moderne potenze di calcolo, hanno posto i Big data sotto la lente d'ingrandimento dell'Antitrust.

Il non corretto funzionamento del mercato per ragioni strutturali potrebbe costituire una causa di mancanza di concorrenza. Si pensi all'ipotesi in cui i tradizionali operatori, in virtù del potere di mercato conferito dai dati, limitino l'accesso di terzi alle informazioni dei propri clienti, sia mettendo questi ultimi nella difficile posizione di dover decidere se prestare il proprio consenso ai TPP a condizioni particolarmente svantaggiose sia introducendo ostacoli alla portabilità dei dati da un servizio a un altro, mediante restrizioni poste all'interoperabilità[128]. Tra le ulteriori possibili condotte anticompetitive si menzionano: l'ingiustificato rifiuto di accesso alle piattaforme e alle loro funzionalità;[129] la limitazione o l'indebito diniego della portabilità dei dati[130] e, infine, il rifiuto di adottare adeguate soluzioni di interoperabilità[131].

La crescente frequenza dei fenomeni abusivi nel contesto del mercato unico digitale ha spinto le Autorità Antitrust a mutare il proprio approccio. Per tale motivo e al fine di ovviare all'incertezza del quadro normativo in un'ottica di progressiva armonizzazione delle forme regolatorie, la Commissione Europea ha dato avvio a una ambiziosa strategia digitale, che si inserisce nel solco della Digital Single Market Strategy[132].

126 In un'ottica di "dimensione sociale" dei dati rilevano anche le c.d. *leaked information exernalities*. Esse rappresentano il complesso di esternalità positive a carattere "informativo" che consentono alle grandi piattaforme di poter analizzare, contemporaneamente, i dati di più individui. Delineando un profilo "tipizzato" del consumatore, sarà, infatti, possibile anticipare le preferenze e gli interessi prima ancora che questi siano rivelati. Non a caso, la forte posizione economica delle Big Tech consente loro di esercitare un impatto significativo sul mercato interno. Ne deriva che il fatto di riuscire a collegare la grande base di utenti a un ingente numero di imprese, garantisce loro una "forte posizione di intermediazione"; A. Burchi, S. Mezzacapo, P. Musile Tanzi, V. Troiano, Financial Data Aggregation e Account Information Services, Questioni regolamentari e profili di business, Quaderni Fintech, Consob, 2019, p. 4.

127 European Commission, Expert Group on Regulatory Obstacles to Financial Innovation (ROFIEG): 30 recomedations on regulation, innovation and finance, 2019, p. 77; A. Burchi *et al.*, *loc. ult. cit.*

128 European Parliament, Competition Issues in the Area of Financial Technology (Fintech), 2018, pp. 87 ss., disponibile al sito Internet: https://www.europarl.europa.eu/RegData/etudes/STUD/2018/619027/IPOL_STU(2018)619027_EN.pdf.

129 Si pensi all'eventuale diniego di accesso ai servizi di pagamento offerti dalle piattaforme stesse.

130 Come pure il reimpiego dei dati mediante servizi diversi al fine di ostacolare ovvero disincentivare l'utente ad abbandonare la piattaforma.

131 M.R. Carbone, Digital Markets Act, così l'Europa limita il potere delle Big Tech, 2020, disponibile al sito internet: https://www.agendadigitale.eu/mercati-digitali/digital-markets-act-come-si-sta-disegnando-il-futuro-dellecono-mia-digitale-europea/.

132 European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A Digital Single Market Strategy for Europe, COM/2015/0192 final.

È stato presentato un pacchetto di iniziative legislative ricomprendente il Digital Markets Act (DMA)[133] e il Digital Services Act (DSA)[134], quale risposta unitaria all'operato delle Big Tech. L'accelerazione del processo di digitalizzazione, tanto delle imprese quanto dell'economia, ha determinato il consolidamento del potere delle grandi piattaforme (LoP), le quali, in qualità di *gatekeeper,* beneficiano di importanti effetti di rete e detengono il controllo dell'accesso al mercato digitale, al punto di ergersi, con sempre più frequenza, a legislatori privati. Il Regolamento sui mercati digitali, quale strumento *ex ante*[135], è volto a contrastare il regime anticoncorrenziale e monopolistico in cui si trovano a operare le imprese che abbiano assunto crescente rilevanza sistemica[136]. Le stesse soggiaceranno a un complesso di obblighi direttamente proporzionali alla dimensione dei servizi digitali offerti e al loro impatto, al fine di prevenire forme di concorrenza sleale tra i vari operatori. Per tali ragioni la Commissione Europea propone di abbracciare una visione prospettica, dal momento che la migliore applicazione della concorrenza è quella combinata con la regolamentazione. L'obiettivo è quello di replicare l'approccio adottato in altri settori – come in quello bancario, delle telecomunicazioni o dell'energia – così da fornire un "*set* completo di strumenti" che consentano alle Autorità di lavorare, di pari passo, con la regolazione[137]. Viceversa, il DSA si offre di disciplinare il settore delle piattaforme online, assicurando vantaggi ai consumatori, incentivando gli scambi transfrontalieri dentro e fuori l'UE e offrendo nuove prospettive a un'ampia gamma di aziende e di operatori commerciali europei. Ciò sarà possibile mediante la revisione del precedente quadro normativo comunitario sui servizi digitali (Direttiva 2000/31/CE), oramai "anacronistico", data l'evoluzione e l'assetto dei mercati

133 European Commission, Proposal for a regulation of the European Parliament and of the council on contestable and fair markets in the digital sector (Digital Markets Act), 2020, COM (2020) 842 final.

134 European Commission, The Digital Services Act package, Shaping Europe's digital future, Policy, 2020, disponibile al sito Internet: https://ec.europa.eu/digital-single-market/en/digital-services-act-package.

135 Sebbene il ricorso a uno strumento normativo *ex ante* consenta un controllo e un'applicazione a priori tali da favorire il tempestivo intervento delle Autorità, è pur vero che imporre a priori obblighi di accesso a infrastrutture immateriali potrebbe costituire un limite al diritto di chi materialmente ha sostenuto ingenti investimenti, prospettando il classico "*trade-off*" tra efficienza statica e dinamica e spingendo a porre un'elevata attenzione nei confronti dell'obbligo di accesso, il quale andrebbe accordato al ricorrere di particolari condizioni. Si veda sul punto A. Preta, Big Tech e Digital Services Act, tutti i nodi da sciogliere. Scrive Preta, 2020, disponibile al sito Internet: https://formiche.net/2020/12/digital-services-act/. A parere di alcuni l'adozione di una normativa *ex ante* potrebbe non riuscire a rispondere in maniera compiuta alle esigenze del mercato digitale, proprio in ragione della sua scarsa adattabilità e flessibilità ai settori in evoluzione. D'altro canto, la mancanza di compiute evidenze empiriche sottolinea come tale regolamentazione tecnologica difficilmente riesca a perseguire gli obiettivi europei di "sovranità tecnologica" e competitività globale. Con particolare riferimento al DSA, le principali preoccupazioni emergono in relazione a tre aspetti rilevanti: la scarsa chiarezza della definizione e dell'applicazione del quadro normativo; i rischi di sovrapposizione normativa; la riduzione dei benefici per le LoP. Per un ulteriore approfondimento sul punto si veda M. Broadbent, The Digital Services Act, the Digital Markets Act, anche the New Competition Tool, European Initiatives to Hobble U.S. Tech Companies, 2020, disponibile al sito Internet: https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/201109_Broadbent_Digital_Services_Act_Digital_Markets_Acts.pdf.

136 Si tratta, in sostanza, di piattaforme che esercitano un impatto significativo sul mercato interno e che rappresentano un importante punto di accesso. L'eventuale posizione consolidata e durevole potrebbe sia attribuire loro il potere di agire quali legislatori privati sia rappresentare una "strozzatura" nel rapporto tra imprese e consumatori. Così Commissione Europea, Un'Europa pronta per l'era digitale: proposta della Commissione di nuove norme per le piattaforme digitali, 2020, Comunicato Stampa, disponibile al sito Internet: https://ec.europa.eu/commission/presscorner/detail/it/ip_20_2347.

137 Confindustria, DSA e DMA: semaforo e cassetta degli attrezzi per gli OTT, 2020, disponibile al sito Internet: https://confindustriaradiotv.it/dsa-e-dma-semaforo-e-cassetta-degli-attrezzi-per-gli-ott/.

online[138]. La legge sui servizi digitali[139] persegue quale obiettivo quello di riequilibrare le responsabilità all'interno dell'ecosistema digitale, mediante un *corpus* normativo comune, orizzontale e armonizzato, che troverà applicazione, nel pieno rispetto dei diritti fondamentali, in tutto il mercato unico digitale.

Con riferimento all'abuso di posizione dominante, il possesso di ampi *dataset* consente alle imprese di ottenere un consistente vantaggio competitivo e di acquisire, nel tempo, ampie quote di mercato. Tuttavia, non è ben chiaro se, di fatto, possa prospettare abuso di posizione dominante l'ipotesi in cui un'impresa – che abbia sviluppato un sofisticato sistema di raccolta e analisi[140] – precluda l'entrata nel medesimo mercato ad altri *competitors*[141]. L'eventuale rifiuto ovvero l'incapacità di condividere dati con i nuovi operatori potrebbe, infatti, costituire un limite per l'innovazione e per la stessa concorrenza.

La disciplina generale prevede che il rifiuto di accesso costituisca, a tutti gli effetti, un comportamento anticoncorrenziale solamente al ricorrere di "strutture essenziali" ovvero prodotti e/o servizi che risultino indispensabili. Ora, i dati, in relazione alla loro particolare natura e alle eterogenee modalità di raccolta e fonti di accesso, non costituiscono un'infrastruttura fondamentale[142]. A ciò si aggiunga che la mancanza dei presupposti per l'applicazione della *Essential Facility Docrine* non consente di rilevare, in un tale rifiuto, un'ipotesi di abuso di posizione dominante[143]. La giurisprudenza ritiene più plausibile l'applicazione della disciplina dell'abuso di dipendenza economica, ex. art. 9, L. 192/1998, la quale, alla luce della particolare natura "transtipica", rappresenterebbe la fattispecie ideale in virtù del rapporto asimmetrico creatosi in ragione dell'ampio potere di mercato acquisito grazie al possesso di ampi *dataset*[144]. L'esigenza di accedere ai dati ivi contenuti da parte delle imprese di piccole dimensioni, le quali avrebbero difficoltà a sostenere ingenti costi di R&S, prospetterebbe l'elemento sintomatico di un eccessivo squilibrio di diritti e obblighi. E, infatti, a differenza

138 Direttiva 2000/31/CE del Parlamento europeo e del Consiglio dell'8 giugno 2000 relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno («Direttiva sul commercio elettronico»).

139 Per servizio digitale, stante alla definizione fornita dalla Dir. (UE) 2015/1535, si intende qualsiasi tipo di servizio che viene fornito, normalmente, mediante compenso per via telematica e su richiesta individuale di un destinatario di servizi. Di tale ampio *genus*, il Digital Services Act individua regole specifiche che interessano gli intermediari e le piattaforme (a titolo di esempio: *online marketplaces, social networks,* piattaforme adibite alla condivisione dei contenuti, *app store*, piattaforme per la prenotazione online di viaggi e pernottamenti).

140 È pacifico come difficilmente «un'impresa che abbia costruito il proprio *know-how* sulla base di tecniche di raccolta ed analisi di dati, sia disposta poi a condividerlo con le altre imprese concorrenti» ma al contrario scoraggerebbe ulteriori investimenti nel settore del R&S nell'ambino dei Big data, così E. Palmerini *et al.*, op. cit. p. 36.

141 V. Meli, op. cit., pp. 139-140.

142 F. Vessia, 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, pp. 81 ss; OECD, Big data: bringing competition policy to digital era, 2016, disponibile al sito Internet: http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DAF/COMP/M%282016%292/ANN4/FINAL&docLanguage=En.

143 Il Parlamento Europeo ha invitato la Commissione a riesaminare sia il concetto di "abuso di posizione dominante" sia la dottrina inerente alle "infrastrutture essenziali", al fine di garantire piena conformità con lo scopo perseguito nell'era digitale. Sarà, inoltre, necessario operare un'analisi più estesa del potere di mercato in relazione agli effetti tanto dei "conglomerati" quanto dei "gatekeepers", per impedire il verificarsi di situazioni di abuso di posizione dominante da parte dei principali operatori e la mancanza di interoperabilità. Si veda sul punto Parlamento Europeo, Risoluzione del Parlamento europeo del 18 giugno 2020 sulla politica di concorrenza – relazione annuale 2019 (2019/2131(INI)).

144 Cass., S.U., 25/11/2011, Ordinanza n. 24906.

dell'abuso di posizione dominante – laddove è necessario provare il carattere insostituibile dell'*asset* – nella fattispecie sovra menzionata il rifiuto di vendere ovvero concedere in licenza la risorsa detenuta sarà considerato abusivo solamente ove si dimostri che non vi sia possibilità di reperire, sul mercato, un'alternativa apprezzabile. Ne deriva che, qualora al costitutore «a cui venga richiesto il rilascio di una licenza non sia l'unico a possedere quei dati, ma i suoi *dataset* siano notoriamente i più vasti, aggiornati e completi presenti sul mercato, questo potrà essere sufficiente a ritenere *insoddisfacenti* le altre *alternative* reperibili sul mercato»[145].L'abuso di dipendenza economica, inoltre, potrebbe essere utile tanto nel valutare le ipotesi in cui un'impresa preveda un accesso discriminatorio ai dati personali in suo possesso (applicando condizioni dissimili e favorendo talune imprese a scapito di altre), quanto nel porre in essere pratiche leganti (c.d. *tying contracts*), che impongano l'acquisto dei propri dati in abbinamento a servizi, a esempio, di *data analytics*[146].

Ci si chiede se l'ipotesi di *closed-loop network,* di proprietà e nella gestione delle Big Tech, possa prospettare problematiche antitrust. Tali imprese, in genere, ricoprono posizioni dominanti sul mercato, che potrebbero diventare lesive della concorrenza ove l'offerta di servizi venga estesa anche ad altri settori. I maggiori rischi figurerebbero nella possibilità di sfruttare le economie di scala legate agli effetti di rete, nell'offrire *bundling* di servizi diversificati al fine di conquistare grandi fette di mercato e, da ultimo, nell'eccessiva archiviazione e analisi dei dati raccolti. Per tali ragioni e al fine di garantire un effettivo *level playing field* a favore dei tradizionali *incumbents,* sarebbe opportuno che, in piena conformità con un'ottica di "*reverse*", venga garantito il diritto di accesso ai dati nella disponibilità delle Big Tech anche agli istituti finanziari, per ovviare a particolari asimmetrie di rete e garantire la concorrenza anche all'interno delle grandi piattaforme.

La progressiva integrazione e collaborazione tra *start-up* e istituti di credito, quale chiave di successo nel settore del *financial services*[147], prospetta criticità in termini di controllo delle concentrazioni. Non a caso, la concentrazione del potere di mercato nelle mani di pochi operatori e il conseguente rischio che talune imprese acquisiscano una posizione di dominanza tale da porre in essere condotte escludenti[148], prospettano barriere atte a precludere l'ingresso a nuovi concorrenti (c.d. *foreclosure effects*). Analogamente, la continua cessione di dati personali da parte degli utenti alle grandi imprese contribuirebbe ad accrescere il divario esistente tra queste ultime e quelle emergenti, sia in termini di qualità di servizi offerti sia di quote di mercato detenute[149]. Una delle principali conseguenze derivanti dalle concentrazioni consiste

145 F. Vessia, Big data e profili di concorrenza, in Fintech, Introduzione a profili giuridici di un mercato unico tecnologico dei servizi finanziari, a cura di M. Paracampo, Giappichelli Editore, 2017, pp. 95 ss.

146 *Idem.*

147 Capgemini, World Fintech Report, 2018, pp. 10 ss., disponibile al sito Internet: https://www.capgemini.com/wp-content/uploads/2018/02/world-fintech-report-wftr-2018.pdf.

148 Si pensi, a titolo di esempio, al diniego di accesso per ragioni di sicurezza a un sistema di pagamento considerato struttura essenziale. In questo specifico caso, si prospetterebbe una pratica escludente dove l'unico rimedio riconosciuto a tutela del soggetto non bancario, quale forma di garanzia dell'effettivo principio di non discriminazione, è l'intervento dell'Autorità Antitrust.

149 M. Malaguti, op. cit., p. 80.

nella creazione di *database* integrati nei quali confluiscono tutti i dati in possesso degli operatori che vi hanno preso parte. E dunque, se all'operazione di "integrazione" corrisponde un'incorporazione dei *database*, è evidente come il controllo di una determinata concentrazione non possa prescindere dall'esaminare la rilevanza che Big data e servizi di *analytics* ricoprono nell'operazione stessa[150]. Benché, ad atto pratico, tali operazioni suscitino particolari preoccupazioni in seno alle Autorità Antitrust nazionali, la Commissione Europea ha finora dato il suo benestare a tutte le concentrazioni Fintech sottoposte al suo vaglio[151], lasciando deliberatamente aperta la definizione di mercato rilevante[152]. La ragione sottesa potrebbe essere ricollegata all'utilizzo dei tradizionali schemi operativi basati sul *test* di dominanza e incentrati prettamente sul valore delle quote di mercato; aspetti che risultano inadatti a valutare l'incidenza che l'incremento del *set* di dati aziendali ha sull'attività di un una data impresa. Il sistema di valutazione, infatti, manca di focalizzarsi sull'elemento dinamico della questione e, dunque, «sugli effetti che una concentrazione, e il connesso aumento della disponibilità di dati in capo ad un'impresa, può avere sulla struttura del mercato»[153]. Numerose operazioni, seppur apparentemente risultino irrilevanti in termini di soglie di fatturato, potrebbero in realtà rivestire particolare natura strategica nell'ottica del controllo dei dati[154]. Sul punto la Commissione ha accolto con favore l'impegno di attuare la revisione della "Comunicazione sulla definizione del mercato"[155], quale parte di un più generale processo di aggiornamento e riforma del diritto della concorrenza, per riflettere prontamente gli sviluppi giurisprudenziali, l'attuale assetto dei mercati, il fenomeno della globalizzazione, nonché lo sviluppo tecnologico ed economico. Sebbene la definizione del mercato continui a rappresentare lo strumento principale mediante il quale definire l'ambito in cui le imprese sono in reciproca concorrenza, al contempo è opportuno che le recenti tendenze e gli sviluppi che hanno influito sull'applicazione della Comunicazione vengano debitamente tenuti in considerazione e riflessi all'interno di una guida aggiornata. Nei mercati digitali e in rapida espansione, infatti, la pressione competitiva

150 F. Divetta, op. cit., pp. 149-150; V. Falce, Big Data, Dataset e diritti esclusivi, Liasons dangereuses tra innovazione e mercato, in V. Falce, G. Ghidini, G. Olivieri, Informazione e Big data tra innovazione e concorrenza, Giuffrè, pp. 113 ss.; European Pasrliament, Competition issues in the Area of Financial Technology, a cura di A. Fraile Carmona, A. González-Quel Lombardo, R. Rivera Pastor, C. Tarín Quirós, J. P. Villar García, D. Ramos Muñoz, L. Castejón Martín, 2018, disponibile al sito Internet: https://www. europarl.europa.eu/RegData/etudes/STUD/2018/619027/IPOLSTU (2018) 619027_EN.pdf; I. Vandenborre, C. Janssens, S.D. Levi, Fintech and access to data, in Banking and Big Data, in Concurrences, a cura di Marianne Verdier *et al.,* 2019, pp. 22 ss.; Parlamento Europeo, Questioni relative alla concorrenza nel settore della tecnologia finanziaria (Fintech), sintesi a cura di D. Ramos Muños, J.P. Villar García *et al.,* 2019, disponibile al sito Internet: https://www.europarl.europa.eu/RegData/etudes/STUD/2018/619027/IPOL_STU(2018)619027(SUM01)_IT.pdf.

151 Case No COMP/M.6314 – Telefónica UK/ Vodafone UK/ Everything Everywhere/ JV; Case No COMP/M.6956 - TELEFONICA/ CAIXABANK/ BANCO SANTANDER / JV.

152 Divetta F., op. cit., p.143.

153 E. Palmerini *et al.,* op. cit., p. 19.

154 F. Divetta, op. cit., p. 156: «Il fatto che un'impresa offra anche servizi di *analytics* sui dati ben può rappresentare un indizio dell'importanza che i dati hanno nel *business* dell'impresa. Infatti, è solo osservando il funzionamento del mercato dei servizi di analisi dei dati, che si percepisce il valore strategico (e commerciale) che i Big Data possono assumere».

155 Commissione Europea, Comunicazione della Commissione sulla definizione del mercato rilevante ai fini dell'applicazione del diritto comunitario in materia di concorrenza, C 372 del 09/12/1997. Tale Comunicazione fornisce orientamenti sulle modalità con cui la CE dà applicazione alla nozione di mercato rilevante, del prodotto e geografico, in piena attuazione del diritto europeo della concorrenza.

può essere esercitata da vari fattori, quali: prodotti, servizi, nonché modelli di *business* complementari e non sostitutivi. La valutazione della sostituibilità sul versante della domanda dovrebbe, dunque, strutturarsi sul criterio di "intercambiabilità funzionale" dei prodotti, piuttosto che sul loro prezzo e questo poiché, sempre più spesso, numerosi servizi digitali sono offerti in modo solo apparentemente gratuito[156]. D'altro canto, l'accesso ai dati che consente l'espansione dei grandi operatori in nuovi mercati dovrebbe essere valutato sia con riferimento alla sostituibilità sul lato dell'offerta sia, andando oltre la definizione propria del mercato, rispetto alla valutazione della stessa concorrenza potenziale. Quest'ultima – che non viene direttamente presa in considerazione al momento della definizione dei mercati ma solamente in una fase successiva dell'analisi – assume particolare rilievo nei mercati caratterizzati da dinamicità. In ragione di ciò, la stessa non dovrebbe essere esclusa nella fase di delineazione del mercato. Ulteriore aspetto che andrà preso in considerazione è la modalità con cui la sostituzione sul versante della domanda può essere misurata nei *tipping markets*, nei mercati a prezzo zero e, infine, nei *multi side markets*[157]. Con particolare riferimento ai mercati della piattaforma sarà, inoltre, necessario che la Commissione fornisca adeguati orientamenti rispetto la possibile definizione di più mercati rilevanti (uno per ciascun lato della piattaforma) ovvero di un unico mercato rilevante omnicomprensivo[158].

Le attuali dinamiche competitive basate sull'innovazione, i partenariati nonché i processi di esternalizzazione, contribuiscono attivamente ad alimentare una rivoluzione nel panorama finanziario, richiedendo una grande attenzione da parte delle Autorità Garanti nell'assicurare parità di trattamento tra i vari operatori[159].

Sebbene i soli strumenti tradizionali di concorrenza non siano formalmente idonei a risolvere le problematiche connesse ai dati digitali, ove opportunamente integrati con la disciplina della tutela dei dati personali potrebbero essere in grado di rivestire un ruolo determinante «nel promuovere una concezione armonica tra le ragioni del mercato e le esigenze di protezione dei consumatori, soprattutto in un contesto complesso quale quello della finanza digitale»[160]. A ciò si aggiunga che l'applicazione della suddetta normativa, unitamente a quella inerente alla tutela dei consumatori[161],

156 Per tale motivo, a parere di alcuni intervistati, sarà opportuno individuare modelli diversi dal classico SNIPP test quali, a titolo esemplificativo, il ricorso a modelli che facciano riferimento al tempo impiegato, all'attenzione dell'utente, a parametri di qualità (SSNQ) ovvero ai costi (SSNIC).

157 European Commission, Summary of the stakeholder consultation to the Evaluation of the Market Definition Notice, 2020, disponibile al sito Internet: https://ec.europa.eu/competition/consultations/2020_market_definition_notice/index_en.html; Dla Piper, Market Definition Notice, 2020, disponibile al sito Internet: https://www.dlapiper.com/it/italy/insights/publications/2020/12/antitrust-matters---special-edition/market-definition-notice/.

158 Per un ulteriore approfondimento sulla questione si veda OECD, Market definition in multi-sided markets - Note by Sebastian Wismer & Arno Rasek Hearing on Re-thinking the use of traditional antitrust enforcement tools in multi-sided markets, 2017, disponibile al sito Internet: http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DAF/COMP/WD%282017%2933/FINAL&docLanguage=En.

159 M.T. Paracampo, Fintech e il mercato unico tecnologico dei servizi finanziari, in Fintech, introduzione ai profili giuridici di un mercato unico tecnologico dei servizi finanziari, a cura di M.T. Paracampo, Giappichelli Editore, p. 7.

160 E. Palmerini *et al.,* op. cit., p. 39; M. Maggiolino, I big data e il diritto antitrust, Egea, 2018, pp. 30 ss.

161 Tra le recenti risposte normative in termini di esigenze di tutela del consumatore si menzionano: Commissione Europea, Comunicazione Della Commissione Al Parlamento Europeo, Al Consiglio, Al Comitato Economico E Sociale Europeo E Al Comitato Delle Regioni, Un approccio globale per stimolare il commercio elettronico transfrontaliero per i cittadini e le imprese in Europa, Bruxelles, 2016, COM (2016) 320 final; Pacchetto di misure denominate "New Deal for

potrebbe contribuire fattivamente alla riduzione delle asimmetrie informative, garantendo la piena consapevolezza circa lo scopo e l'utilizzo dei dati. La ragione è chiara: man mano che cresce l'utilizzazione dei servizi di *online banking* da parte dei consumatori sarà necessario capire in che modo il cambiamento tecnologico influisca sul loro comportamento finanziario e sulla loro vulnerabilità. Tali accorgimenti costituiscono una precauzione essenziale nello sviluppo di tecnologie, nel pieno rispetto dei diritti collettivi e individuali. È necessario, dunque, che le rispettive Autorità Antitrust nazionali e di vigilanza bancaria coordinino il processo di trasformazione avviato dal Legislatore europeo, al fine di prevenire e impedire il perpetrarsi di pratiche sleali che minino la portata pro-competitiva della PSD2[162]. Sul punto è interessante, inoltre, notare come, a seguito dell'approvazione del GDPR, si sia assistito a un progressivo mutamento del paradigma: le tradizionali categorie della responsabilità civilistica stanno progressivamente scivolando verso una forma di "responsabilizzazione", in virtù della quale le imprese saranno oggetto di valutazione solamente a seguito dell'adozione di tutte le misure necessarie atte a prevenire eventuali rischi.

Alla luce di quanto finora esposto, compito delle Autorità sarà quello di trovare il giusto equilibrio tra concorrenza, cooperazione e standardizzazione, aspetti che risultano particolarmente rilevanti per lo sviluppo del settore dei servizi digitali nell'area unica europea.

2.4 TPPs e nuovi servizi di accesso i conti: software e profili giuridici di tutela

La Direttiva 2015/2366/UE (c.d. PSD2) persegue lo scopo di promuovere l'innovazione e la creazione di un mercato interno dei servizi di pagamento che risulti valido, sicuro e competitivo, riformando i classici metodi di pagamento e consentendo l'ingresso di nuovi *players*. Questi ultimi, i *Third Party Providers* (TPP) includono in sé i *Payment Initiation Services Providers* (PISP, che dispongono gli ordini di pagamento) e gli *Account Information Service Providers* (AISP, i quali forniscono servizi di aggregazione di informazioni che provengono dai conti dei clienti)[163]. I tradizionali *incumbents* sono, dunque, obbligati ad aprire le proprie *Application Programming Interface* (API) a società Fintech ovvero ad altre aziende che si occupano di erogare servizi e prodotti finanziari, previa autorizzazione espressa da parte del cliente. In altri termini, al consumatore, unico e solo titolare, è riconosciuta la possibilità di condividere i propri dati e le funzionalità connesse ai conti bancari, nonché disporre pagamenti per il tramite di

Consumers, consultabile al sito: https://ec.europa.eu/info/law/law-topic/consumers/review-eu-consumer-law-new-deal-consumers_en.

162 Colangelo G., op. cit., p. 131.

163 Non a caso, il servizio di informazione sui conti (c.d. *account information services*) consente all'utente di poter prendere visione del quadro generale della propria situazione economico-finanziaria, mediante accesso a informazioni online aggregate inerenti a conti correnti allocati presso uno o più prestatori di servizi di pagamento (si veda sul punto la Direttiva 2366/2015, art. 4 definizione n. 16 e punto 8 dell'Allegato 1); S. Vezzoso, Fintech, accesso to data, and the role of competition policy, 2018, in V. Bagnoli (Ed.), Competition and Innovation, São Paulo: Scortecci, 2018, disponibile al sito Internet: https://ssrn.com/abstract=3106594 or http://dx.doi.org/10.2139/ssrn.3106594: Dietro espresso consenso del cliente, gli AISP potranno a loro volta condividere i dati raccolti con altre aziende, come, a titolo di esempio, siti web che attuano un confronto dei prezzi e che offrono servizi aggiuntivi di cui il cliente può beneficiare.

app di terze parti[164]. Il consolidamento della rete informativa – dovuto in *primis* al cospicuo giacimento di dati presente nei sistemi bancari – e la corrispondenza tra tecnologia, AI e connettività, traccia un nuovo e interessante quadro nel quale il cliente, in qualità di erogatore e fruitore, diventa egli stesso oggetto di confronto, fornendo informazioni e condividendole con terzi. È bene puntualizzare che le API non sono una novità nel panorama informatico, sebbene solamente nell'ultimo decennio la riscoperta della loro potenza innovativa ha spinto gli operatori, in una prospettiva di "API *as a Product*" (AaaP), a rivalutarne la componente strategica nella *business transformation*[165]. Esse costituiscono un insieme di procedure che attuano lo scambio di informazioni tra componenti *software,* mediante l'ausilio di un linguaggio univoco tra le diverse applicazioni, che consente di estendere e/o migliorare le funzionalità proprie di una piattaforma o programma, impiegando risorse provenienti da altri sistemi. Più in generale, nel settore bancario le *open standard* API rappresentano un ponte di raccordo tra vari *database,* un intermediario *software* che contribuisce alla circolazione e fruizione delle informazioni finanziarie sui conti dei clienti[166], abilitando l'*Open banking*[167] e assicurando agli utenti l'utilizzazione dei propri dispositivi mobili in qualità di soluzioni di pagamento ovvero di consultazione del conto. Su tali dati, a loro volta, i TPP elaboreranno prodotti e servizi, caratterizzati da una sempre maggiore digitalizzazione, disintermediazione e decentralizzazione. Sebbene il Legislatore europeo propenda per la progressiva "standardizzazione" delle misure di accesso ai conti, a oggi non vi è, tra gli operatori del settore,consenso unanime circa l'adozione di API "aperte e uniformi" ovvero lo sviluppo di interfacce proprie[168]. È pur vero, tuttavia, che tale uniformazione costituisce uno *step* fondamentale per ridurre frodi, facilitare l'interoperabilità e la scalabilità, nonché velocizzare l'accesso al mercato.

Per quanto concerne i profili di tutela, queste ultime, analogamente ai linguaggi di programmazione[169] e alle funzionalità proprie di un programma, non sono tutelabili dal diritto d'autore e questo poiché le caratteristiche funzionali di un *software* non sono oggetto di tutela autoriale. Il predetto assunto prende le mosse da una

164 G. Colangelo, Open Banking, in Fintech: diritti, concorrenza e regole, a cura di G. Finocchiaro, V. Falce, Zanichelli Editore, 2019, p. 119.

165 D. Milanesi, A New Banking Paradigm: The State of Open Banking in Europe, the United Kingdom, and the United States, TTLF Working Papers, Stanford-Vienna Transatlantic Technology Law Forum, 2017, p. 41, disponibile al sito Internet: http://ttlf.stanford.edu.

166 S. Pearlman, What is an API?, 2016, disponibile al sito Internet: https://blogs.mulesoft.com/biz/tech-ramblings-biz/what-are-apis-how-do-apis-work/: «an API is the messenger that delivers your request to the provider that you're requesting it from and then delivers the response back to you (...) When developers create code, they don't often start from scratch. APIs enable developers can make repetitive yet complex processes highly reusable with a little bit of code. The speed that APIs enable developers to build out apps is crucial to the current pace of application development.».

167 L. Brodsky, L. Oakes, Data sharing and open banking, 2017, MickKinsey&Company, disponibile al sito Internet: https://www.mckinsey.com/~/media/McKinsey/Industries/Financial%20Services/Our%20Insights/Data%20sharing%20and%20open%20banking/Data-sharing-and-open-banking.pdf.

168 G. Colangelo, op. cit., p. 119.

169 Per un ulteriore approfondimento sul punto si veda M. Della Puppa, C++, manuale di programmazione orientata agli oggetti, Hoepli, 2006, p. 11; G. Candilio, Elementi di informatica generale, Franco Angeli, 2006, p. 79; M. Gabrielli, S. Martini, Linguaggi di programmazione: principi e paradigmi, McGraw-Hill, 2011, p. 5; S. Crespi Reghizzi, L. Breveglieri, A. Morzenti, Linguaggi formali e compilazione, Esculapio, 2015, p. 6; D. Harel, Y. Feldman Y., Algoritmi, lo spirito dell'informatica, Springer, 2008, p. 64.

pronuncia della Corte di Giustizia dell'Unione Europea[170], la quale ha statuito che, a chiunque abbia lecitamente acquistato una licenza, è riconosciuta la possibilità di decompilare il programma (c.d. *reverse engineering*). Saranno considerate, in ogni caso, nulle le clausole eventualmente poste dagli sviluppatori ovvero dalle *software house* che vietino tale attività. La *ratio* è chiara: preservare il progresso tecnologico e lo sviluppo industriale a scapito di un'eccessiva monopolizzazione.

Tale sentenza fa eco a una controversia decennale che ha tenuto vivo, negli Stati Uniti, il dibattito sulla possibile protezione delle API alla luce del *copyright*. Nel caso di specie oggetto della *quaestio* era il riconoscimento della suddetta tutela alle interfacce di programmazione delle applicazioni del linguaggio Java, di proprietà di Oracle e implementate da Google all'interno del sistema Android. Se in prime cure i giudici avevano riconosciuto a favore di Google l'applicazione della *fair use doctrine*, la pronuncia in secondo grado aveva ribaltato quella precedente dal momento che, pur essendo Android un sistema *open source*, in realtà era venuta meno, con il tempo, l'originaria natura non lucrativa del progetto. A inizio 2019, Google aveva avviato una petizione, accolta e discussa innanzi la *Supreme Court*. A parere dello stesso l'eventuale riconferma della decisione avrebbe rappresentato una battuta d'arresto per lo sviluppo, l'innovazione e l'interoperabilità; aspetti che risultano fondamentali per il progresso tecnologico e che finirebbero per essere sottoposti al diritto di veto da parte dei detentori dei diritti[171]. Nell'aprile 2021, la Corte Suprema si è definitivamente pronunciata sul punto, ritenendo legittimo l'operato del colosso di *Mountain View*, poiché le API costituiscono, a tutti gli effetti, un "metodo operativo essenziale", in grado di consentire lo sviluppo di un nuovo programma. Detto in altre parole, il principio statuito è stato quello secondo il quale, ove si utilizzino linee di codice di proprietà di terzi a cui si apporti un significato contributo creativo da cui ha origine un prodotto nuovo e originale, non si incorre in alcuna violazione dei diritti[172].

Nonostante la portata epocale di tale giudizio, è indubbio come sia stata lasciata volutamente aperta la questione inerente allo *status* legale delle interfacce, riguardo alla possibilità o meno di far ricadere le stesse sotto l'egida del *copyright*. A tale proposito, sarà necessario attentere i futuri orientamenti giurisprudenziali in materia, per vedere se, nel settore delle *software house*, il principio del *fair use* si riconfemi regola e non anche eccezione[173].

170 Corte Europea di Giustizia, 2/5/2012, C-406/10, SAS Institute Inc, vs. World Programming Ltd.

171 M.R. Mazzella III, R.H. Dilday, Oracle America, Inc. V. Google Inc.: Copyrightability Of Application Programming Interfaces and a fair use defense, GLTR Staff Member; Georgetown Law, 2018, University of Arizona, 2015, disponibile al sito Internet: https://georgetownlawtechreview.org/wp-content/uploads/2017/01/Mazzella-and-Dilday-1-Geo.-Tech.-L.-Rev.-62-2016.pdf; S. Parker, J. Rosenberg, Oracle v. Google Proves Again Why Fair Use Is So Troublesome, 2018, Alston&Bird, disponibile al sito Internet: https://www.alston.com/-/media/files/insights/publications/2018/04/183156-oracle-v-google-proves-again-why-fair-use-i.pdf.

172 Supreme Court of United States, Google LLC v. Oracle America, Inc., 5 aprile 2021, no. 18-956, disponibile al sito Internet: https://www.supremecourt.gov/opinions/20pdf/18-956_d18f.pdf.

173 Berti R., Zumerle F., Google vince su Oracle, tutelato il software libero ma non le piccole aziende, 2021, disponibile al sito Internet: https://www.agendadigitale.eu/mercati-digitali/google-vince-su-oracle-gli-impatti-sul-futuro-del-software-libero/.

Nella mera eventualità teorica in cui le API soggiacciano alla protezione offerta dai diritti di proprietà intellettuale, sarebbe, tuttavia, opportuno prospettare soluzioni che prevedano, comunque, la concessione di licenze gratuite[174].

2.5 *"Banking as a platform"* e prospettive di condivisione dei dati

Le API aperte e l'*open platform banking* rappresentano lo strumento in grado di cambiare radicalmente la fisionomia dei servizi finanziari. Le banche, infatti, stanno progressivamente diventando piattaforma per altri servizi, all'insegna del paradigma del "*banking as a platform*" (BaaP)[175]. Agendo in qualità di "piattaforme di intermediazione", esse metteranno in contatto i propri clienti con le Fintech o, comunque, con quelle imprese che manifestino l'interesse di ampliare i propri *dataset*, ricorrendo al diritto alla portabilità dei dati personali disciplinato dall'art. 20, Reg. n. 2016/679[176]. Tuttavia, è opportuno puntualizzare che, benché tale diritto attribuisca ai singoli il potere di esercitare un maggiore controllo, dal punto di vista concreto la portabilità dei dati, in senso strettamente giuridico, non è ancora utilizzata dai consumatori nel contesto dell'economia digitale[177]. Le numerose criticità legate all'accesso ai dati[178] e la carenza di standardizzazione[179] delle API contribuiscono fattivamente alla frammentazione del mercato dei servizi, rendendo difficile l'offerta scalabile a livello europeo[180]. Tali problematiche, tuttavia, potrebbero essere risolte sostenendo un complesso di notevoli sforzi come: fornire orientamenti puntuali rispetto le modalità con cui facilitare tale mobilità; interpretare, in senso lato, il diritto di portabilità dei dati, ricomprendendo, oltre a quelli volontariamente ceduti, anche i c.d. "*observed data*"[181]; incenti-

174 V. Torti, Norme tecniche, concorrenza e innovazione, in Fintech: diritti, concorrenza e regole, a cura di G. Finocchiaro, V. Falce, Zanichelli Editore, 2019, p. 113.

175 R. Bansode, Banking as a platform, it's time for banks to open-up and integrate!, Synechron, pp. 2 ss., disponibile al sito Internet: https://www.synechron.com/sites/default/files/white-paper/Banking-as-a-platform.pdf; M. Kitsing, Internet banking as a platform for e-government, 2017, Conference: Annual International Conference on Innovation and Entrepreneurship, pp. 1 ss.; A. Omarini, The Retail Bank of Tomorrow: A Platform for Interactions and Financial Services. Conceptual and Managerial Challenges, Research in Economics and management, Vol. 3, No. 2, 2018, disponibile al sito Internet: www.scholink.org/ojs/index.php/rem, pp. 112 ss.

176 M. Maggiolino, M. Scopsi, Prospettiva antitrust sulle Big Data Companies, in op. cit., p. 203.

177 Questo è dovuto, in particolare, per due principali ragioni: in *primis* la mancanza di sufficienti studi empirici sull'argomento; in *secundis*, poiché numerosi servizi digitali non garantiscono, a livello tecnico, la possibilità di importare i dati.

178 Sebbene la PSD2 abbia espresso in maniera chiara il principio di non discriminazione e di *open access* ai sistemi di pagamento da parte di operatori non bancari, persistono, tuttavia, ostacoli alla creazione di un mercato competitivo e di un adeguato *level playing field*. Più nello specifico, si fa richiamo alla facoltà riconosciuta in capo al gestore del circuito di pagamento di negare l'accesso al sistema per ragioni di sicurezza (benché debba trovare applicazione l'ulteriore criterio previsto dalla direttiva, ovverosia quello di non discriminazione) e l'ipotesi dei sistemi individuati dalla stessa direttiva che sono espressamente esentati dall'applicazione della disciplina sull'accesso aperto.

179 È bene puntualizzare che, tuttavia, piccoli passi si stanno effettuando nella direzione di una graduale standardizzazione delle API, come segnalato dall'iniziativa NextGenPSD2 del Gruppo di Berlino, disponibile al sito Internet: https://www.berlin-group.org/nextgenpsd2-downloads.

180 G. Nucci, M. Balducci *et al.*, La PSD2 è l'inizio della nuova era degli open data, 2020, disponibile al sito Internet: https://www.riskcompliance.it/news/la-psd2-e-linizio-della-nuova-era-degli-open-data/.

181 In base alla formulazione originaria dell'art. 20 GDPR solamente i dati forniti direttamente dall'utente rilevano ai fini della portabilità. Con il termine *observed data* si riferimento ai dati ottenuti mediante l'utilizzo di dispositivi digitali, siti *web* ovvero servizi digitali (in essi andranno ricompresi anche i *clickstream* e i dati di tracciamento). Sul punto si

vare politiche di dialogo e cooperazione tra imprese ad alta intensità di dati e le rispettive Autorità di regolamentazione; garantire il consenso esplicito da parte dei consumatori, anche nell'ipotesi di richieste di portabilità avviate da soggetti terzi; prevedere API standardizzate che, facendo eco alle politiche britanniche e australiane[182], garantiscano la "portabilità continua dei dati", al fine di stimolare l'innovazione e la concorrenza nel contesto dei mercati digitali; ricorrere ai *Personal Management Information Systems* (PMIS), che per loro natura sono in grado di consentire agli utenti un maggiore controllo dei propri dati personali[183].

La condivisione dei dati relativi ai pagamenti riveste un ruolo cruciale nell'attuale ecosistema finanziario, riservando a ciascun singolo attore una posizione di rilievo e promuovendo al contempo l'apertura e il consolidamento delle interazioni tra banche e soggetti esterni. I continui scambi, infatti, facilitano le interazioni dal lato dell'offerta e della domanda, amplificando gli effetti di rete[184] e intensificando le dinamiche concorrenziali[185]. In tale prospettiva i dati di pagamento non saranno più nella disponibilità esclusiva dei tradizionali *incumbents* ma sottoposti a condizioni di accesso giuste, non discriminatorie e proporzionate allo scopo che si intende perseguire: se da una parte i fornitori di servizi non strettamente bancari saranno soggetti a forme regolatorie e di vigilanza, dall'altra vi sarà un obbligo in capo alle banche di concedere l'accesso alle proprie interfacce, garantendo la portabilità delle informazioni ivi contenute. D'altro canto, l'attività di condivisione non si limita ai dati di pagamento ma prospetta l'inizio di un nuovo *trend* innovativo che punta a uno sviluppo molto più ampio. Si parla, a tal proposito, di *Open Data economy,* la quale contribuirà a garantire dati più aperti, integrati e *value accretive*[186]. Come accennato poc'anzi, il diritto di accesso ai conti prospettato e difeso dalla Direttiva, quale "forma settoriale" di portabilità dei dati[187], da un lato spinge gli istituti di credito verso un modello bancario più aperto e, dall'altro, accentua ulteriormente le dinamiche competitive nel mercato dei servizi finanziari e

veda European Commission, Guidelines of article 29 Data Protection Working Party on the right to data portability, 2017, disponibile al sito Internet: https://ec.europa.eu/newsroom/article29/itemdetail.cfm?item_id=611233.

182 Open Banking, Open Banking 2019 Review, 2019, disponibile al sito Internet: https://www.openbanking.org.uk/wp-content/uploads/2019-Highlights.pd; Furman J., Coyle D., Fletcher A., McAuley D., Marsden P., Unlocking digital competition: Report of the digital competition expert panel. Government of the United Kingdom.https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/un locking_digital_competition_furman_review_web.pdf; Australian Government, Consumer Data Right Overview, 2019, disponibile al sito Internet: https://treasury.gov.au/sites/default/files/2019-09/190904_cdr_booklet.pdf; Australian Government, Open Banking customer choice convenience confidence, 2017, disponibile al sito Internet: https://treasury.gov.au/sites/default/files/2019-03/Review-into-Open-Banking-_For-web-1.pdf.

183 Per un ulteriore approfondimento si veda J. Kraemer, Personal Data Portability In The Platform Economy: Economic Implications And Policy Recommendations, Journal of Competition Law & Economics, 2020, disponibile al sito Internet: https://ssrn.com/abstract=3742771.

184 A. McIntyre et. al., A new era open platform banking, Accenture, 2018, p. 3, disponibile al sito Internet: https://www.accenture.com/_acnmedia/pdf-79/accenture-open-platform-banking-new-era.pdf. Le API aperte, in genere, forniscono all'ecosistema i dati bancari fondamentali (a titolo di esempio, informazioni inerenti al conto, operazioni di pagamento, *etc.*). Per tale ragione le banche devono dotarsi di sufficienti mezzi e capacità informatiche che siano in grado di assicurare la sicurezza e consolidare la fiducia.

185 M. Zachariadis, P. Ozcan, The API Economy and Digital Transformation in Financial Services: The Case of Open Banking, 2017, SWIFT Institute Working Paper No. 2016-001, disponibile al sito Internet: https://ssrn.com/abstract=2975199.

186 Acta Fintech Srl, Blockchain Banking, definizioni, applicazioni e case study, 2020, disponibile al sito Internet: https://www.opengateitalia.com/wp-content/uploads/2020/07/Acta-Fintech-Blockchain-Banking.pdf.

187 G. Colangelo, op. cit., p. 131.

bancari. Un sano ambiente competitivo, infatti, consente agli istituti di credito di godere dei giusti incentivi per adattare la propria attività e i propri servizi alle dinamiche di mercato.

Nel contesto europeo, tra i primi pilastri della nuova strategia digitale promossa dalla Commissione si menzionano il Libro bianco sull'intelligenza artificiale[188] e la *Strategy for data*. Quest'ultima, in particolar modo, mira a creare un mercato unico per i Big data, finalizzato a garantire la competitività globale e la *leadership* mondiale dell'Europea nel campo della *data economy*. Insomma, uno spazio comune di dati europei, personali e non personali, accessibili in piena sicurezza a imprese, consumatori, processi di cooperazione industriale e servizi pubblici. Tale iniziativa consentirà, inoltre, la contestuale attuazione di misure pratiche, eque e chiare in materia di *governance*, accesso e riutilizzo, nel pieno rispetto dei valori fondamentali e delle normative europee[189].

In sintesi, per sfruttare appieno il complesso di opportunità offerte dalla condivisione dei dati all'interno dell'ecosistema finanziario è opportuno che vengano soddisfatte tre distinte condizioni. In primo luogo, l'industria finanziaria dovrebbe garantire un accesso standardizzato ai dati da parte di terzi. In secondo luogo, il Legislatore nonché le rispettive Autorità pubbliche e di regolamentazione coinvolte dovrebbero incentivare la cooperazione trasversale e il dialogo *ex ante* nella formulazione di leggi e regolamenti a lungo termine, ovviando a possibili contrasti – in tema di *privacy*, frode e sicurezza – e perseguendo obiettivi politici. Da ultimo, è necessario salvaguardare la fiducia dei consumatori nel controllo dei propri dati e nel semplificare la prestazione del consenso.

La proposta di Regolamento in materia di *data governance* (c.d. *Data Governance Act*)[190] – anch'essa nel novero delle misure europee preannunciate all'interno della Strategia Europea per i dati[191] – persegue lo scopo di uniformare l'azione dei singoli Stati Membri mediante la creazione di un *European Data Space*, che consenta il loro libero scambio, in modo sicuro e a costi contenuti, tanto nel settore pubblico quanto in quello privato, così da incentivare lo sviluppo di nuovi prodotti e servizi basati sui Big data. In tale ottica è importante incrementare la fiducia nei vari intermediari e consolidare i processi di condivisione in tutto il territorio dell'Unione, a beneficio di imprese, consumatori e, più in generale, dell'intera società.

188 Commissione Europea, Libro Bianco sull'intelligenza artificiale – Un approccio europeo all'eccellenza e alla fiducia, Bruxelles, 2020, COM (2020) 65 final.

189 European Commission, A European Strategy for Data, Shaping Europe's digital future, Policy, 2020, disponibile al sito Internet: https://ec.europa.eu/digital-single-market/en/policies/building-european-data-economy.

190 Commissione Europea, Proposal for a Regulation on European data governance (Data Governance Act), Shaping Europe's digital future, 2020, disponibile al sito Internet: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0767&from=EN.

191 Commissione Europea, Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, 2020, COM (2020) 66 final.

Sebbene in principio le banche percepissero come *distruptive* l'ingresso di nuovi operatori, in una prospettiva a lungo termine l'adozione di una politica di collaborazione e cooperazione duratura[192] consentirà alle due entità di completarsi a vicenda, senza, tuttavia, pregiudicare una sana competizione. Si è innanzi alla terza fase del Fintech, la c.d. *Fintegration,* che, da un lato, accorda alle banche la possibilità di diventare sempre più digitali mediante l'integrazione con *start-up* e Fintech *companies* e, dall'altro, consente a questi ultimi l'accesso ad ampi *cluster* di dati[193].

2.6 Approcci strategici in merito all'impiego delle *Smart Technologies* nello scenario dell'*open banking*

La *digital transformation*[194] nel settore finanziario incarna la sfida su cui si gioca la capacità delle banche di lavorare con efficacia e in modo competitivo nei prossimi anni. Gli investimenti nelle infrastrutture di rete e in R&S, il potenziamento di schemi produttivi e distributivi e la riduzione dei costi di connessione sono soltanto alcuni degli elementi che, autoalimentandosi, contribuiscono a mantenere un vantaggio competitivo sui concorrenti e a offrire prodotti e servizi sempre più rispondenti alle esigenze dei singoli[195]. I settori maggiormente interessati sono il credito (*crowdfunding* e trasferimenti *peer-to-peer landing*), i servizi di pagamento (*instant payment*), la valuta virtuale, la consulenza automatizzata (*robo-advisory*), le tecnologie di registrazione e validazione delle transazioni (*Blockchain*), la *predictive analytics* (AI e *machine learning*), le strategie e gli strumenti basati sulla raccolta, l'analisi e l'archiviazione dei

192 Mediante partnership, joint venture, esternalizzazioni, etc.

193 Capgemini, *loc. ult. cit.*

194 A. Strømmen-Bakhtiar, Introduction to Digital Transformation and its impact on society, Informing Science Press, 2020, pp. 67 ss.; T.U. Daim, Digital transformation, evaluating emerging technologies, World Scientific, 2020, pp. 25 ss.; G. Pitruzzella, Audizione del Presidente dell'Autorità Garante della concorrenza e del Mercato, in merito a Indagine conoscitiva sulle tematiche relative all'impatto della tecnologia finanziaria sul settore finanziario, creditizio e assicurativo, 2017, pp. 1 ss., disponibile al sito Internet: https://www.agcm.it/dotcmsDOC/audizioni-parlamentari/Audizione-20171122.pdf.

195 Per un ulteriore approfondimento si veda P. Gomber, C. Parker, R.J. Kauffman, B.W. Weber, On the fintech revolution: interpreting the forces of innovation, disruption, and transformation in financial services, journal of management information systems, 2018, pp. 10 ss.

dati (*Big data analytics*[196] e *cloud computing*)[197] La diffusione capillare dei dispositivi digitali ha radicalmente mutato le abitudini dei consumatori in una prospettiva di ubiquità tecnologica, che ha eliminato il vincolo fisico e temporale tipico degli sportelli fisici bancari, erogando prodotti e servizi in maniera sempre più diretta. Si assiste, in sostanza, al passaggio dalle interazioni fisiche al coinvolgimento digitale[198]. In una fase caratterizzata da una particolare razionalizzazione del numero delle filiali, investire nell'innovazione tecnologica sarà la chiave che permetterà di presidiare la relazione con il cliente in modo ottimale, grazie a un ascolto continuativo e sistematico fortemente centrato sulle sue esigenze, attuali ovvero potenziali[199]. La crescente domanda, infatti, è ricollegata a una chiara esigenza di immediatezza, trasparenza e semplicità, aspetti che, oggi, hanno spinto più di un terzo delle organizzazioni a estendere un approccio di tipo "*digital first*" a processi di *business* e al rapporto con i clienti[200]. Le variabili impiegate nella segmentazione della clientela sono state oggetto, nel corso del tempo, di profonda trasformazione: si è passati da un concetto prettamente qualitativo di *customer satisfaction* a quello di *customer experience*, abbracciando il paradigma di *customer centricity* in un'ottica di "*customer first*" [201]. Nella valutazione degli enti finanziari gli analisti sono passati da campioni universali ed essenzialmente basati sul prodotto a quelli sulla segmentazione della clientela per tenore di ricchezza, fino ad arrivare a modelli incentrati sulla propensione all'investimento e a modelli c.d. "multi variabili", nei quali la digitalizzazione riveste un ruolo significativo[202].

196 Le T.M., Liaw S., Effects of Pros and Cons of Applying Big Data Analytics to Consumers' Responses in an E-Commerce Context, in Sustainability, 2017, pp. 3-4; B.M. Balachandran, S. Prasad, Challenges and Benefits of Deploying Big Data Analytics in the Cloud for Business Intelligence, International Conference on Knowledge Based and Intelligent Information and Engineering Systems, 2017, in Procedia Computer Science, vol. 112, Elsevier, pp. 1118-1119, disponibile al sito Internet: https://doi.org/10.1016/j.procs.2017.08.138; M.A. Waller, S.E. Fawcett, Data science, predictive analytics, and big data: a revolution that will transform supply chain design and management, in Journal of Business Logistics, 2013, pp. 2-15; F.L.F. Almedia, Benefits, challenges and tools of big data management, in Journal of Systems Integration, 2017, p. 16; PWC, Le aziende del Fintech in Italia 2017, Analisi condotta da Net Consultin e Pwc, disponibile al sito Internet: https://www.pwc.com/it/it/industries/fintech/docs/2017-fintech-report.pdf; Si fa, inoltre, espresso rinvio a un interessante Report condotto dall'EBA, inerente alle recenti tendenze del settore, rispetto l'impiego di sistemi di Big Data e Advance Analytics (BD&AA), compreso il Machine Learning. Questi ultimi prospettano sfide per Istituzioni, Autorità di vigilanza e di regolamentazione, con la conseguente esigenza di garanzie a supporto della neutralità tecnologica. Per un ulteriore approfondimento: European Banking Authority, EBA Report on Big Data and Advanced Analytics, 2020, disponibile al sito Internet: https://eba.europa.eu/sites/default/documents/files/document_library//Final%20Report%20on%20Big%20Data%20and%20Advanced%20Analytics.pdf.

197 C. Barbagallo, Fintech and the future of financial services, Director General for Financial Supervision and Regulation Bank of Italy, 2018, disponibile al sito Internet: https://www.bancaditalia.it/pubblicazioni/interventi-vari/int-var-2018/barbagallo-20180723.pdf.

198 J. Marous, 2018 Retail BankingTrends & Predictions,Digital Banking Report, 2017.

199 Banca D'Italia, Fintech in Italia, Indagine conoscitiva sull'adozione delle innovazioni tecnologiche applicate ai servizi finanziari, 2017, p. 11; F. Panetta, L'innovazione digitale nell'industria finanziaria italiana, Intervento del Vicedirettore Generale della Banca d'Italia, 2017, p. 3, disponibile al sito Internet: https://www.bancaditalia.it/pubblicazioni/interventi-direttorio/int-dir-2017/Panetta_26092017.pdf.

200 IDG, State of Digital Business Transformation, Executive Summary, 2018, p. 2, disponibile al sito Internet: https://cdn2.hubspot.net/hubfs/1624046/Digital%20Business%20Executive%20Summary_FINAL.pdf.

201 B. Nicoletti, The future of Fintech: Integrating Finance and Technology in Financial Services, Palgrave Macmillan, Switzerland, 2017, p. 166; PWC, Costumers in the spotlight, how fintech is reshaping banking, global fintech survey 2016, disponibile al sito Internet: https://www.pwc.com/jg/en/publications/fin-tech-banking-2016.pdf.

202 A. Di Mascio, Wealth Managemt e Fintech, le nuove sfide tra private banker e Robo Advisor, Egea, 2018, p. 71.

Alla luce delle considerazioni finora espresse si prospetta un futuro all'insegna della crescita economica e tecnologica, ove lo sviluppo delle competenze e l'alfabetizzazione finanziaria digitale costituiranno il motore immobile e l'elemento chiave nell'allocazione del capitale umano, sempre più formato in termini di conoscenze specialistiche e "complementari"[203]. In quest'ottica un'opzione da caldeggiare consiste nell'adozione di un sistema armonizzato di "*data protection standards*", che consenta di sfruttare al massimo le potenzialità del diritto alla portabilità dei dati, sia come leva per incrementare la concorrenza sia come strumento essenziale in capo ai consumatori per evitare effetti di *lock in*[204]. Sebbene il legislatore abbia posto un primo tassello nella regolamentazione del Fintech sarà opportuno, in questo orizzonte, aggiustare il tiro e convogliare il complesso di opportunità e sfide poste dall'era digitale all'interno di "binari giuridico-regolamentari certi"[205], che consentano di tenere vivo il dibattito sulla complessità e multidimensionalità di tale fenomeno globale e intersettoriale[206].

3 Il nuovo scenario competitivo: open banking e piattaforme BigTech

3.1 Premessa

Il termine BigTech è comunemente impiegato per indicare grandi società tecnologiche il cui business è incardinato su di una piattaforma che permette loro di interagire con una vasta platea di utenti, generando significativi effetti di rete (*network effects*). Esempi di tale categoria di imprese sono Uber, Google, Facebook, Amazon e Apple. In base alla definizione fornitane dal Comitato di Basilea per la Vigilanza Bancaria, le BigTech operanti a livello globale si distinguono per un significativo vantaggio competitivo con riferimento allo sfruttamento sistematico e su larga scala di informazioni (*big data analytics*) permesso dall'innovazione tecnologica[207]. Tali operatori forniscono solitamente servizi via internet al pubblico (motori di ricerca, servizi di *e-commerce*, *social network*, ecc.) e gestiscono infrastrutture digitali di elevata capacità di *storage* e *processing* tramite cui altre imprese o individui possono fornire a loro volta servizi o prodotti. Tali piattaforme tecnologiche possono entrare in contatto con i mercati finanziari con due modalità principali[208]. In primo luogo, possono operare come fornitori terzi di istituzioni finanziarie. Un esempio di tale categoria è costituito dai servizi di *cloud* offerti da Amazon, Microsoft ed altre imprese tecnologiche oppure la condivisione di flussi di dati utili per l'elaborazione di modelli di rischio. In secondo

203 M.T. Paracampo, op. cit., p. XVI.

204 E. Palmerini *et al.*, op. cit., p. 43.

205 V. Falce, G. Finocchiaro, La digital evolution nel settore finanziario. Una nota di metodo, nota di metodo, (doi: 10.1433/94558) Analisi Giuridica dell'Economia (ISSN 1720-951X), Fascicolo 1, 2019, p. 315.

206 Consob, Comunicato Stampa Del 23 Marzo 2018: "Fintech: Consob Pubblica Il Primo Volume Della Collana Dedicata All'impatto Della Digitalizzazione Sui Servizi Finanziari. Un Progetto In Collaborazione Con Le Università", 2018, disponibile al sito Internet: http://www.consob.it/documents/46180/46181/comunicato_20180323.pdf/2a445758-11c1-49a3-a1c6-f51b975ba2a4.

207 Bank of International Settlements (2019), 15.

208 Zetzsche, Buckley, Arner, Barberis (2018).

luogo, le BigTech hanno la possibilità di entrare gradualmente nel sistema finanziario fornendo inizialmente canali di collegamento tra istituzioni finanziarie e potenziali consumatori per poi erogare in via diretta servizi di natura finanziaria direttamente ai propri utenti.

Dal un punto di vista sistematico, le BigTech nel campo dei servizi finanziari possono essere qualificati come una sottocategoria particolare della più ampia sfera degli operatori che impiegano la c.d. Financial Technology (c.d. FinTech). Con tale concetto vengono usualmente intese le imprese che sfruttano le più recenti innovazioni tecnologiche per la distribuzione o lo sviluppo di nuovi servizi finanziari[209]. L'elemento che distingue le BigTech dai restanti operatori FinTech consiste nella capacità di scalare in tempi brevi il mercato in cui operano sfruttando le peculiarità del proprio metodo di *business* insieme alla propria forza economico-finanziaria[210]. Tra questi, in particolare, vi sono il grande bacino di utenti che fanno uso delle loro piattaforme, l'ampio riconoscimento sul mercato, la mole di informazioni accumulate circa i comportamenti e le preferenze dei propri utenti e la possibilità di accesso alle più avanzate tecnologie in campo di raccolta ed analisi dati. In alcuni stati, la penetrazione delle BigTech nel mercato dei servizi finanziari è stata rapida. È questo il caso della Cina e di altre nazioni del sud est asiatico, dell'Africa orientale e dell'America Latina dove i servizi di pagamento sono stati in poco tempo presidiati da grandi piattaforme tecnologiche[211]. Grazie alla possibilità di interagire direttamente con la moltitudine dei propri utenti giornalieri, ad esempio, Alipay è riuscita a diffondere esponenzialmente in oltre dodici giurisdizioni del sud-est asiatico l'offerta dei propri servizi di pagamento. Non deve dunque sorprendere che la capitalizzazione di mercato delle BigTech operanti nel settore finanziario cinese sia comparabile a quella delle più grandi istituzioni finanziarie a livello mondiale. Alla luce di tali caratteristiche, l'ingresso delle BigTech può avere ripercussioni di carattere competitivo su numerosi settori del sistema finanziario.

I servizi di pagamento sono tra i primi servizi ad essere stati offerti dalle BigTech, per aumentare la l'affidabilità delle piattaforme di e-commerce nonché la fiducia tra consumatori e venditori. È appena il caso di notare, a questo proposito, che gli acquirenti richiedono affidabilità circa la consegna dei prodotti, mentre i venditori necessitano di avere la garanzia del pagamento prima di spedire la merce. Alipay e PayPal hanno risposto a queste esigenze offrendo servizi di regolamento dei pagamenti alla consegna insieme alla possibilità di riottenere le somme corrisposte dagli acquirenti in caso di inadempimento. Non a caso, tali attività si sono sviluppate con riferimento alle principali piattaforme di vendita elettronica, come PayPal per eBay ed Alibaba per Alipay.

Col passare del tempo, nel sud-est asiatico ed in numerosi stati africani[212] tale tipologia di servizi si è diffusa al punto da superare i tradizionali canali bancari ed i sistemi di carte di credito. In Cina, ad esempio, i servizi di pagamento veicolati tramite

209 Per un'analisi aggiornata dello sviluppo FinTech, si veda: Financial Stability Board (2019a); Financial Stability Board (2017).

210 Vives (2019).

211 Bank of International Settlements (2019).

212 In Africa M-Pesa si è affermata come fornitore di servizi di pagamento veicolari mediante la rete telefonica mobile.

smartphone hanno raggiunto l'equivalente del 16% del PI[213]. In tali paesi l'innovazione tecnologica ha permesso lo sviluppo di una rete di pagamenti autonoma ed indipendente dagli operatori bancari tradizionali. Viceversa, nei paesi con economie avanzate ed una più solida rete finanziaria, i servizi FinTech di pagamento si limitano ad offrire una sovrastruttura ancorata sui sistemi di pagamento al dettaglio già esistenti (Google Pay, PayPal, Apple Pay). Da tali evidenze si può ricavare come la penetrazione dei BigTech nel sistema finanziario sia stata sinora più rapida e dirompente nelle economie dove il livello di inclusione bancaria della popolazione è ridotto[214]. Analogamente, Facebook ha investito su una nuova moneta digitale (Libra) e sta contemporaneamente mettendo a punto un nuovo *brand* di pagamenti digitali integrati con i propri servizi di comunicazione (Messenger e WhatsApp). Del pari, Uber ha annunciato l'istituzione di Uber Money per mettere a disposizione dei propri utenti un portafoglio digitale nonché un autonomo servizio di carte prepagate[215].

Parallelamente ai servizi di pagamento, alcune grandi società che gestiscono piattaforme digitali hanno iniziato ad erogare credito ai propri utenti. In particolare, si tratta di prestiti e linee di credito messe a disposizione dei venditori e delle piccole e medie imprese che fanno uso di una determinata piattaforma. Un caso esemplare di tale strategia è quella implementata da Amazon sin dal 2012 con il servizio Amazon Lending ed ulteriormente migliorata con gli apporti del c.d. Internet of Things (tra cui, in particolare, l'assistenza digitale domestica)[216]. Le BigTech possono infatti trarre particolari vantaggi competitivi rispetto agli operatori bancari tradizionali. Sfruttando la grande mole di dati relativi ai propri utenti nonché le proprie capacità di analisi incrociata, le BigTech hanno la possibilità di allocare prodotti finanziari in modo efficiente e personalizzato, senza al contempo dover sostenere i costi operativi degli operatori bancari tradizionali (succursali locali, risorse umane, ecc.). L'analisi incrociata delle informazioni già accumulate nel corso degli anni con riguardo ai propri utenti permettere loro di effettuare report di meritevolezza del credito più accurati e rapidi. Come già dimostrato da studi empirici focalizzati sul mercato nord-americano, l'analisi sistematica del *digital footprint* degli utenti (l'insieme delle informazioni a disposizione di alcune piattaforme di *social network* o *e-commerce* che gli utenti hanno disperso online nel corso del tempo) permette alle stesse di fornire servizi e prodotti personalizzati sui bisogni e la disponibilità di spesa di ciascun utente, aumentando significativamente i margini di profittabilità del servizio[217]. Analogamente ai prodotti di pagamento, il volume di credito sinora erogato dalle BigTech varia considerevolmente in base alle aree geografiche. Ad esempio, l'ammontare di credito generato da operatori FinTech (ivi comprese le BigTech) risulta essere maggiore in Cina dove ampie sacche di popolazione e di imprenditoria, soprattutto in zone rurali e poco urbanizzate, non hanno accesso ai servizi bancari tradizionali[218]. Ciò nonostante, il livello di credito generato dalle

213 Financial Stability Board (2019), 5.

214 Bank of International Settlements (2019), 58.

215 McGee (2019).

216 Megaw (2019) evidenzia come dai resoconti finanziari della società risulta che lo sviluppo di Amazon Lending ha riscontrato un significativo rallentamento negli ultimi tre anni.

217 Seru (2019).

218 Financial Stability Board (2019), 8.

BigTech costituisce una percentuale minima del totale a livello mondiale. Anche in Cina, se confrontato con i dati complessivi, il credito erogato tramite canali FinTech rappresenta soltanto l'1.5% del totale. Tale fenomeno può essere spiegato col fatto che l'attività di erogazione del credito è regolamentata rigidamente nella maggior parti dei paesi in considerazione delle implicazioni di stabilità finanziaria che la stessa comporta. Per esempio, in numerosi stati membri dell'Unione Europea (Francia, Germania, Italia, ecc.) tale attività, anche quando non combinata con la raccolta del risparmio tramite depositi bancari, è sottoposta a supervisione prudenziale equivalente a quella bancaria, che si traduce in significative barriere all'ingresso e costi di transazione per gli operatori[219].

Parallelamente al mercato del credito, le BigTech possono sfruttare i propri *assets* e la loro ampia riconoscibilità per offrire prodotti assicurativi e fondi comuni monetari (*money market funds*) attraverso le proprie piattaforme. Anche in questo caso si tratterebbe di un passo naturalmente successivo all'erogazione di servizi di pagamento, volto ad affermare la piattaforma come un'*one-stop-shop* alternativo ai tradizionali canali bancari e assicurativi. Gli utenti dei servizi di pagamento, infatti, conservano sui propri conti di pagamento delle somme di denaro. La piattaforma potrebbe permettere a tali utenti di impiegare tali somme tramite investimenti di breve periodo in fondi di mercato monetario, gestiti direttamente dalla piattaforma oppure da istituzioni finanziarie convenzionate. Questo permetterebbe alle BigTech di disintermediare gli operatori tradizionali, impadronendosi dell'interfaccia diretta con l'utente. Uno scenario simile si è verificato nel mercato cinese, dove i fondi promossi dalle piattaforme che offrono servizi di pagamento sono cresciuti sensibilmente negli ultimi cinque anni: per esempio, il fondo "Yu'ebao" promosso da Alipay è ora uno dei più capitalizzati al mondo con un patrimonio pari a circa $150 miliardi ed oltre 350 milioni di partecipanti[220]. Non va tuttavia dimenticato che tale crescita è parzialmente dovuta anche a cause esogene rispetto alle peculiarità delle piattaforme. In particolare, il tasso degli interessi interbancari degli ultimi sette anni è stato superiore a quello dei depositi bancari ed ha permesso ai fondi di offrire alla clientela condizioni più vantaggiose[221]. Del pari, le piattaforme rappresentano un canale privilegiato per l'erogazione di prodotti assicurativi a persone fisiche grazie alle proprie abilità di *marketing*, analisi del rischio e di *price discrimination*.

Le BigTech sono inoltre accomunate dal grande bacino di utenti che sono riuscite a consolidare rapidamente grazie al proprio metodo di *business*. A tale riguardo, l'influenza dei *social network* sui mercati finanziari è stata rimarcata durante i primi mesi del 2021 negli Stati Uniti dalla vicenda che ha interessato i titoli azionari di GameStop[222]. Al netto degli aspetti giuridici relativi alle pratiche di vendite allo scoperto e all'affidabilità delle informazioni finanziarie condivise *online* da investitori *retail*, tale episodio ha palesato alcune conseguenze inattese dell'integrazione digitale, connesse

219 Gola et al. (2019); European Banking Authority (2017).

220 Bank of International Settlements (2019), 59-60.

221 Del pari, nel 2011 PayPal ha chiuso il proprio fondo in quanto i tassi negli Stati Uniti si erano quasi azzerati.

222 Ventoruzzo (2021).

alla sostanziale diminuzione dei costi di transazione e alla relativa facilità di coordinamento tra investitori dispersi[223]. Una piattaforma digitale, Reddit, ha giocato un ruolo chiave nel permettere ad una miriade di piccoli investitori di scambiarsi informazioni e coordinare le proprie strategie di compra-vendita con pesanti ripercussioni sulla volatilità di strumenti finanziari quotati in borsa. Per quanto d'interesse ai fini del presente lavoro, la vicenda ha dimostrato come l'interazione del sistema finanziario con piattaforme digitali che vantano una significativa base di utenti ponga importanti rischi non solo di carattere competitivo, ma anche di gestione dell'informazione e di influenza della condotta individuale degli investitori[224].

Nell'ambito di tale contesto, il presente contributo analizza, da un punto di vista economico e regolatorio, l'ingresso delle BigTech nel mercato dei servizi finanziari. La seconda sezione tratta delle caratteristiche economiche intrinseche che possono permettere alle grandi piattaforme digitali potenzialmente di offrire servizi e prodotti più competitivi rispetto sia a quelli degli *incumbent* che a quelli delle *start-up* in campo FinTech. La terza sezione si sofferma sullo scenario regolamentare pro-competitivo che ha creato i presupposti per l'ingresso di nuovi operatori FinTech e BigTech nel mercato dei servizi finanziari. La quarta sezione offre un'analisi critica delle nuove proposte di regolazione del settore emerse nello scenario europeo. La quinta sezione conclude con alcune raccomandazioni critiche *de iure condendo*.

3.2 Piattaforme e mercato dei servizi finanziari: il nuovo contesto competitivo

L'ingresso di grandi piattaforme tecnologiche nel mercato dei servizi finanziari amplifica sia i benefici che i rischi competitivi generati dallo sviluppo del FinTech[225]. Da un lato, le BigTech possono sfruttare il bagaglio di informazioni accumulate dalle interazioni dei propri utenti per offrire prodotti e servizi più competitivi degli operatori bancari tradizionali. Tale fenomeno spingerà inevitabilmente questi ultimi ad aggiornare le proprie strategie nonché i propri metodi di *business* per far fronte alla nuova sfida competitiva. Ciò beneficerà di conseguenza i consumatori, che potranno godere di migliore qualità, prezzi inferiori nonché di più elevati tassi di inclusione finanziaria.

D'altro canto, non si possono sottovalutare i radicali impatti innovativi che l'ingresso delle BigTech ha notoriamente comportato in altre industrie. Simili mutamenti nel settore finanziario potrebbero causare instabilità finanziaria ed innescare ripercussioni negative per il tessuto economico. Le banche tradizionali, infatti, vedrebbero inesorabilmente ridotti i propri margini di profittabilità con conseguente aumento del rischio di dissesti e insolvenze. Allo stesso tempo, i medesimi elementi che hanno determinato gli elevati tassi di concentrazioni dei mercati digitali (effetti di rete e costi di transazione quasi assenti) potrebbero esacerbare il tradizionale problema del "too-

223 ESMA (2021).

224 Oudin, Valbuena (2021).

225 Financial Stability Board (2019), 13.

big-to-fail" che affligge i mercati finanziari a livello mondiale. Qualora infatti le piattaforme tecnologiche dovessero penetrare tanto a fondo nel mercato dei servizi finanziari da legare inestricabilmente le proprie sorti alla stabilità complessiva del sistema, autorità di vigilanza e *policy makers* sarebbero costretti a considerarle al pari di operatori significativi ed essenziali per il mercato. Al momento, tuttavia, le BigTech non sono sottoposte agli stringenti vincoli normativi e prudenziali previsti per gli operatori bancari e finanziari. Tale circostanza ha spinto alcuni commentatori a denunciare l'esistenza di un arbitraggio regolamentare a favore delle piattaforme che dovessero decidere di penetrare nel mercato della distribuzione di prodotti finanziari, senza tuttavia svolgere le attività riservate tipicamente alle banche (raccolta del risparmio tramite depositi e fondi rimborsabili)[226]. Un ulteriore rischio è legato alla possibilità che le BigTech raggiungano uno status di too-connected-to-fail (TCTF) nel sistema finanziario[227]. Il mercato odierno è infatti già basato su infrastrutture digitali che contribuiscono in modo significativo ad innalzare il livello di rischio sistemico.

Infine, da un punto di vista della tutela dei consumatori e delle parti contrattualmente più deboli, l'impiego sistematico delle piattaforme digitali per la distribuzione di servizi finanziari pone rischi più elevati in termini di discriminazione e iniquità contrattuale. Gli operatori bancari tradizionali non detengono più interamente l'infrastruttura su cui sono immagazzinati i dati e le informazioni inerenti alla propria clientela ed alle proprie registrazioni contabili. Le imprese tecnologiche che forniscono tali servizi non sono di per sé sottoposte a vigilanza prudenziale o ad appositi meccanismi di risanamento e risoluzione in caso di crisi al pari delle istituzioni bancarie. Tale scenario non pone soltanto problemi sotto il profilo del rischio operativo e delle continuità delle attività in caso di *shock*, ma solleva importanti dubbi sula resilienza complissiva della struttura del mercato ed il suo livello di competitività. Al netto dei rischi operativi che tale situazione comporta, le banche tradizionali potrebbero trovarsi in una situazione di dipendenza economica nei confronti di fornitori esterni di servizi informatici (che spesso coincidono con le BigTech, come nel caso di Amazon)[228].

Oltre ai rischi per la stabilità finanziaria e la tutela degli utenti, l'ingresso delle BigTech nel mercato dei servizi finanziari solleva delicati problemi di carattere concorrenziale. In primo luogo, la presenza di effetti di rete indiretti (*indirect network effects*), forti economie di scala e di diversificazione resi possibili dall'analisi sistematica dei dati accumulati continuamente dalle piattaforme tecnologiche rischia di esporre ad una rapida concentrazione il mercato della distribuzione dei servizi finanziari. In secondo luogo, le piattaforme digitali sono nella posizione di sfruttare tale proprio vantaggio informativo trasversalmente a più mercati così da costituire nuovi conglomerati economici rafforzati da dinamiche di portafoglio e relativa distribuzione del rischio complessivo (*portfolio effects*)[229].

226 de la Mano, Padilla (2018).

227 Buckley, Arner, Zetzsche, Selga (2019), 12.

228 Arner, Barberis, Buckley, Zetzsche (2017).

229 Bank of International Settlements (2019).

Da questo punto di vista, l'ingresso delle BigTech nel mercato dei servizi finanziari permette di essere analizzato ricorrendo all'analisi antitrust delle piattaforme e dei mercati a più versanti. Con tale ultimo concetto si intende fondamentalmente un mercato caratterizzato dai seguenti tratti distintivi: il necessario intervento di un intermediario per eliminare le frizioni che altrimenti ostacolerebbero l'incontro delle parti, pertanto originando valore per gli utenti di almeno uno dei versanti interessati; la presenza di esternalità di rete indirette che non possono essere internalizzate attraverso semplici relazioni bilaterali (*membership* e *usage externalities*); la non neutralità dei sistemi di fissazione dei prezzi da parte del gestore della piattaforma a seconda dell'elasticità della domanda di ciascun versante, praticando prezzi asimmetrici (*skewed pricing*) indipendentemente dal costo del servizio offerto; la presenza di un rapporto di interdipendenza necessario tra i gruppi che interagiscono attraverso la piattaforma al fine di portare "*both sides on board*" (ossia attrarre un adeguato numero di utenti su entrambi i versanti per poter garantire una massa critica utile a sostenere gli effetti di rete indiretti)[230]. Il funzionamento dei mercati a due versanti si fonda sulla teoria delle esternalità di rete e l'analisi coasiana del rapporto tra contrattazione privata e rilevanza dei costi di transazione.

Tali peculiarità incidono sulla valutazione delle condotte antitrust e delle strategie di applicazione dei prezzi, oltre a rivelarsi utili nella definizione di una possibile *theory of harm*[231]. Essendo i gruppi di utenti coinvolti sui due versanti interdipendenti, il loro benessere deriva necessariamente dall'interazione veicolata dalla piattaforma. L'operatore di quest'ultima può adoperarsi agevolmente per attirare e mantenere una domanda sostenuta e costante su entrambi i lati. Di conseguenza, il tradizionale approccio focalizzato su un solo mercato rilevante risulta inadeguato nel cogliere le dinamiche competitive tra gestori di piattaforme nonché nel valutare efficacemente l'impatto delle relative condotte.

Sfruttando tali dinamiche economiche, le imprese BigTech possono fare leva sul proprio bagaglio di strumenti algoritmici e conoscenze in materia di analisi dei dati per processare e incrociare le grandi moli di informazioni a loro disposizione al fine di offrire prodotti e servizi personalizzati agli utenti già presenti sui loro versanti tradizionali (*social networks*, motori di ricerca, servizi di e-commerce, ecc.). In particolare, come illustrato nella prossima sezione, le BigTech possono ora impiegare nuovi meccanismi regolamentari di accesso ai dati conservati da soggetti terzi per consolidare il proprio potere di mercato. È difficile pensare che tali operatori non tenteranno di replicare le strategie anti-competitive già sperimentate con successo in altri mercati al fine di conquistare rapidamente quote del mercato finanziario ora detenute da operatori tradizionali. In particolare, è possibile ipotizzare che mettano in atto condotte di c.d. *self-preferencing*, tying e bundling di prodotti tradizionali legati al proprio brand (accesso a servizi multimediali, e-commerce, etc.) con prodotti finanziari propri od of-

230 Borgogno, Colangelo (2019).

231 Colangelo, Maggiolino (2018); Auer, Petit (2015).

ferti per conto terzi discriminando gli altri operatori tradizionali. Tali strategie di commercializzazione potrebbero erodere in poco tempo il vantaggio tradizionalmente goduto dalle imprese bancarie in termini di interfaccia diretta ed accesso alla clientela.

Ciò detto, è probabile che l'aumento del livello di concorrenza nel mercato determinato dall'ingresso delle BigTech sia destinato a scomparire nel lungo periodo[232]. Come già verificatosi in altri comparti industriali caratterizzati da catene del valore sviluppate verticalmente su più livelli, è possibile che i gestori di piattaforme tecnologiche possano sfruttare i propri vantaggi competitivi per estendere il proprio potere di mercato in altri settori collegati (come ad esempio il mercato dei servizi di pagamento o della distribuzione di prodotti bancari). Un simile scenario potrebbe essere agevolmente reso possibile attraverso l'integrazione verticale combinata con strategie volte a privilegiare sulle proprie piattaforme i propri prodotti e servizi a discapito di quelli della concorrenza[233]. È pertanto possibile che le banche, gli intermediari finanziari tradizionali e la autorità di vigilanza dovranno presto fronteggiare il rischio di un rapido tentativo di posizionamento delle piattaforme tecnologiche nei gangli strategici della distribuzione di servizi finanziari e di accesso alla clientela. Qualora un tale scenario dovesse realizzarsi, le banche e società finanziarie rischierebbero di perdere il monopolio sulle informazioni della propria clientela che da sempre costituisce il vantaggio indiretto di cui hanno tradizionalmente goduto per lo svolgimento della trasformazione del credito e l'offerta di servizi connessi.

3.3 BigTech e regolazione pro-competitiva

Il quadro normativo che trova applicazione all'operatività del FinTech riveste un'importanza preminente per le dinamiche competitive delle BigTech nel settore finanziario. A questo proposito, la disciplina pro-competitiva recentemente introdotta in Unione Europea con riferimento all'accesso dei dati dei conti di pagamento offre un chiaro esempio del *trade-off* esistente tra competitività, stabilità finanziaria e rischio di monopolizzazione del mercato.

Nel corso dell'ultimo decennio si è affermata la tesi secondo cui le *start-up* FinTech non hanno potuto svilupparsi e competere nel mercato finanziario in quanto danneggiate da un doppio vantaggio competitivo degli operatori bancari tradizionali che avrebbe eliminato ogni concreta possibilità di *contestability*[234]. In primo luogo, gli operatori bancari godono di un posizionamento privilegiato dovuto all'implicita protezione assicurata dai meccanismi di risanamento e risoluzione in caso di dissesto economico. In secondo luogo, per quanto concerne l'accessibilità dei dati essenziali di nuovi servizi (comparazione, budgeting personalizzato, consigli d'investimento, etc.), le banche e tutti gli istituti che forniscono conti di pagamento hanno la possibilità di impedire ogni accesso a tali informazioni, indipendentemente dalla volontà del titolare del conto. Alla luce di tali ostacoli, il legislatore europeo ha compreso che l'imposizione

232 de la Mano, Padilla (2018), 498; Vives (2019), 259.

233 Borgogno, Colangelo (2020a).

234 Commissione Europea (2018); Borgogno, Colangelo (2019b).

ai nuovi operatori FinTech di un quadro regolamentare equivalente a quello degli *incumbent* bancari avrebbe paralizzato l'innovazione tecnologica nel mercato finanziario. Viceversa, l'imposizione di nuovi obblighi di condivisione dei dati avrebbe potuto ridurre in chiave pro-competitiva le barriere all'ingresso ed agevolare l'ingresso di nuove imprese FinTech a beneficio della concorrenza e dei consumatori[235].

Secondo tale prospettiva, l'accesso contingentato alle informazioni inerenti i conti di deposito e di pagamento dei consumatori costituirebbe una vera e propria barriera all'ingresso[236]. Lo sviluppo di qualsiasi nuovo servizio o prodotto reso possibile dall'innovazione tecnologica incontrerebbe un vincolo costituito dall'indisponibilità dei custodi alla condivisione di tali informazioni. Da un lato, infatti, gli *incumbent* non sono incentivati a condividere risorse con potenziali concorrenti. Dall'altro, ragioni di carattere reputazionale nonché di sicurezza dei dati e di tutela della privacy impediscono alle stesse banche di cimentarsi autonomamente in attività di condivisione col rischio di enormi effetti negativi sulla propria attività d'impresa. Del resto, ai sensi della Direttiva 2007/63/EC (PSD), gli istituti bancari avevano il diritto di negare l'accesso ad informazioni riservate nei confronti di imprese terze per ragioni di tutela della proprietà intellettuale, sicurezza, nonché per tutelarsi da rischi di responsabilità civile. Per quanto astrattamente ragionevoli, è chiaro che tali motivazioni avrebbero offerto la possibilità agli operatori bancari di reprimere sul nascere ogni minaccia competitiva[237].

Al fine di superare tale *data bottlneck*, sono state da più parti avanzate proposte di nuovi schemi regolamentari volti ad imporre obblighi di condivisione di alcune categorie di dati tra imprese finanziarie[238]. In particolare, la Direttiva UE 2366/2015 relativa ai servizi di pagamento nel mercato interno (PSD2) ha segnato un passaggio fondamentale per alleviare tale problematica. Introducendo la regola di accesso ai conti di pagamento, la PSD2 ha imposto ai prestatori di servizi di pagamento di radicamento del conto, come le banche, di concedere l'accesso in tempo reale ai dati riguardanti i conti di pagamento dei propri clienti[239]. Inoltre, tale accesso deve essere garantito a condizioni non-discriminatorie sia nei confronti dei prestatori di servizi di informazione sui conti[240] che dei prestatori di servizi di disposizione di ordine di pagamento, ossia le due categorie di nuovi operatori operanti nell'ambito dei pagamenti identificati nella Direttiva[241].

In particolare, introducendo il regime di accesso ai conti di pagamento, la PSD2 segna un passaggio importante verso l'apertura del mercato dei servizi bancari al dettaglio a favore di prestatori terzi di servizi che, da ora in avanti, avranno il diritto di

235 Philippon (2018).

236 Hauswald and Marquez (2003).

237 Commissione Europea (2011), 11.

238 Padilla e Pagano (2000).

239 PSD2, Articoli 64-68. Inoltre, il regime di accesso ai conti di pagamento è volto anche a permettere la trasmissione di ordini di pagamento attraverso l'interfaccia prestata da operatori terzi, fermo restando il consenso dell'utente interessato e l'accessibilità online del conto di pagamento.

240 PSD2, Articolo 67(3)(b).

241 PSD2, Articolo 66(4)(c).

ottenere informazioni sui conti di pagamento senza il previo consenso degli istituti bancari.

Tale meccanismo regolamentare mira non solo a rafforzare il potere contrattuale del consumatore, attribuendogli un maggior controllo sui propri dati, ma anche a rinvigorire il livello di concorrenza nel mercato dei servizi di pagamento. Siccome i servizi finanziari sono intrinsecamente connessi all'impiego massivo di informazioni, una regola che ne agevola la circolazione offre la possibilità agli operatori di offrire nuovi servizi nonché di competere in modo più dinamico e orizzontale con l'identificazione di modelli comportamentali, la personalizzazione di prodotti e servizi, fino al miglioramento delle strategie di compliance e supervisione[242].

In seconda battuta, il regime di accesso ai conti di pagamento ha gettato le fondamenta per lo sviluppo del c.d. "Open Banking". Tale espressione indica un'evoluzione del *business* bancario che, mediante il sistematico impiego di API, permette ai consumatori di condividere in sicurezza i propri dati e le funzionalità dei propri conti di pagamento con prestatori di servizi terzi. Tuttavia, come nel caso del diritto alla portabilità dei dati personali introdotto all'articolo 20 del Regolamento UE 679/2016 del 27 aprile 2016 (GDPR), le modalità di implementazione di tale meccanismo regolamentare saranno cruciali nel sancirne il successo e l'effettivo impiego su larga scala da parte degli operatori del mercato[243].

È importante infatti notare come anche il diritto alla portabilità dei dati personali rifletta un chiaro obiettivo pro-competitivo del legislatore che andrà ad integrarsi con quello delineato nella PSD2[244]. Rafforzando il controllo sui propri dati personali da parte degli utenti, il legislatore europeo ha inteso rinvigorire la concorrenza nei mercati digitali fondati sull'uso e processamento di informazioni.[245] Di converso, la portabilità dei dati personali non va letta come un nuovo, ardito tentativo di ampliare le categorie civilistiche proprietarie ai dati[246].

Al momento, tale diritto presenta tuttavia numerose criticità che rendono particolarmente ostico assicurarne l'effettiva implementazione. L'articolo 20(1) del GDPR, infatti, non fornisce una guida dettagliata su come assicurare e coordinare meccanismi di portabilità tra diversi soggetti privati e pubblici. La disposizione si limita a predisporre un generale requisito circa la definizione dei dati trasmessi, che devono essere "in un formato strutturato, di uso comune e leggibile da dispositivo automatico". Inoltre, qualsiasi tentativo di rendere obbligatoria l'adozione di *standards* di interoperabilità viene escluso in quanto il Considerando 68 si limita ad incoraggiarne l'uso. Tale mancanza di disposizioni vincolanti o guida dettagliata a copertura dell'implementazione della portabilità dei dati genera serie preoccupazioni in termini di certezza del

242 European Supervisory Authorities (2016), 8-10.

243 Borgogno, Colangelo (2020).

244 Helgadottir (2020).

245 Lynskey (2017).

246 A ben vedere, un diritto proprietario offrirebbe la possibilità al titolare di escludere qualsiasi terzo dall'uso dei dati: tale facoltà non è concessa dal diritto alla portabilità dei dati personali introdotto nel GDPR. Analogamente, il diritto all'oblio (Articolo 17) non può certo essere inteso come parte di un nuovo diritto di proprietà in ragione dei suoi limiti applicativi.

diritto e di effettività della previsione in oggetto. L'interoperabilità e la portabilità devono essere rese tecnicamente funzionanti per non rischiare di restare lettera morta. L'Article 29 Working Group ha inoltre suggerito l'adozione di API per implementare la portabilità dei dati con un approccio settoriale calibrato alle specificità di ogni industria[247]. Nulla viene aggiunto circa la struttura delle API (aperta o chiusa), le eventuali iniziative di standardizzazione o i termini e le condizioni di licenza delle stesse[248].

Il principale rischio derivante da un approccio regolamentare di così alto livello risiede nell'incoerente sviluppo della portabilità dei dati nel mercato che potrebbe in ultimo ostacolare la nascita di uno spazio comune europeo dei dati. Infatti, anche se alcuni settori sono già ad uno stadio avanzato nella predisposizione di applicazione per il trasferimento dei dati, molti operatori di altri mercati potrebbero avere difficoltà nel tenere il passo con gli ultimi sviluppi tecnologici anche a causa della mancanza di API standardizzate, aperte e liberamente utilizzabili[249]. Inoltre, lasciare gli operatori privati completamente liberi di adottare API poco sicure o difettose amplifica il rischio di sistematiche violazioni dei dati personali nonché l'esposizione ad attacchi cibernetici, come recentemente messo in evidenza dallo scandalo riguardante Cambridge Analytica[250].

Al fine di evitare simili problematiche nel settore finanziario, la Commissione Europea ha iniziato ad incoraggiare lo sviluppo di *standards* aperti che possano aumentare la pressione competitiva, consolidando i livelli di interoperabilità e semplificando lo scambio e la condivisione di dati tra gli operatori[251]. Inoltre, il Parlamento Europeo ha espresso la propria preferenza per la creazione di un insieme di API standardizzate che le imprese possano utilizzare come interfaccia comune capace di garantire un livello di interoperabilità adeguato per lo sviluppo di applicazioni FinTech[252]. Sulla scorta di tali premesse, hanno preso vita le prime iniziative di standardizzazione delle API. Per esempio, il "Berlin Group" ha guadagnato attenzione tra i *policy-makers* come una tra le più promettenti iniziative pan-europee di standardizzazione delle API capace di radunare istituti bancari, associazioni di settore, rappresentanti dei nuovi prestatori di servizi FinTech e gestori di circuiti di carte di pagamento con l'obiettivo di fissare *standard* aperti e comuni all'ambiente finanziario. Un apposito gruppo di lavoro è stato istituito con l'obiettivo di definire API standardizzate liberamente accessibili e specificamente ideate per agevolare il funzionamento del regime di accesso ai conti predisposto ai sensi della PSD2. Allo stesso tempo, la Consumer and Market Authority del Regno Unito unitamente all'UK Government Open Banking Working Group stanno aprendo la strada all'Open Banking mediante l'adozione di una strategia ancora più ambiziosa degli obiettivi della PSD2[253]. Inoltre, la complessità ed i rischi derivanti dalle

247 Article 29 Data Protection Working Party, 17.

248 L'Article 29 Data Protection Working Party ha evidenziato che i formati vincolati da restrizioni di carattere proprietario non possono essere ritenuti adatti allo scopo.

249 Lynskey (2017), 803.

250 Polański, (2018), 141.

251 Commissione Europea (2018), 7-8.

252 Parlamento Europeo (2017), 13.

253 Milanesi (2017), 75-78.

incongruenze tra le diversi possibili modalità di implementazione del regime di accesso ai conti di pagamento ha spinto l'Autorità Bancaria Europea a pubblicare un parere ufficiale per coordinare ad aiutare le numerose iniziative di standardizzazione attualmente operanti in Unione Europea[254].

Nonostante il processo di implementazione del regime di accesso ai conti di pagamento sia soltanto agli albori, vi sono crescenti preoccupazioni che gli operatori bancari tradizionali siano svantaggiato nei confronti dei BigTech nel nuovo scenario competitivo. In particolare, i meccanismi regolamentari di accesso alle informazioni finanziarie si traducono in ingenti costi di *compliance*, sopportati interamente dalle banche e dai prestatori di conti di pagamento. Come evidenziato, sono infatti tali soggetti che hanno il compito di aggiornare la propria infrastruttura digitale per assicurare il flusso di dati verso operatori FinTech e BigTech. Di conseguenza, i costi operazionali (tra cui quelli connessi alla cybersecurity) lieviteranno ulteriormente per tali soggetti[255]. Viceversa, i secondi possono beneficiare di tale accesso standardizzato per offrire servizi interoperabili su larga scala senza dover fronte agli ingenti costi regolamentari delle banche.

Oltre alla disciplina inerente all'accesso e la condivisione delle informazioni nel contesto dei servizi di pagamento, vi sono inoltre significative differenze di carattere regolamentare tra operatori bancari e BigTech. I secondi, infatti, non sono soggetti al complesso quadro di regolamentazione prudenziale previsto per le istituzioni finanziarie[256]. Per esempio, a differenza delle banche commerciali, non devono rispettare rigorosi requisiti di fondi propri né tantomeno sono soggetti all'obbligo di costituire riserve di bilancio per evitare il rischio di crisi di liquidità. Alla luce di ciò gli *incumbents* rischiano di essere vittima di uno scompenso competitivo artificiale imposto dal nuovo quadro regolamentare, eccessivamente sbilanciato in favore delle BigTech[257].

3.4 Verso nuove asimmetrie regolatorie?

Al fine di evitare il rischio che le piattaforme possano approfittare dei meccanismi originariamente pensati per agevolare l'ingresso nel mercato finanziario di nuove start-up FinTech, sta prendendo piede la proposta di introdurre regole appositamente volte ad attenuare le differenze nei rapporti di forza tra *incumbent* e piattaforme. Ciò si tradurrebbe, dal punto di vista legislativo, nella definizione di nuove condotte anti-competitive imputabili soltanto in capo ai BigTech nel settore finanziario.

È stata da più parti sostenuta, ad esempio, la proposta di introdurre regole di condivisione dei dati detenuti dalle BigTech a favore delle banche in modo da controbilanciare le conseguenze della regola di accesso ai dati prevista dalla PSD2[258]. Tale proposta riecheggia del resto l'odierna strategia della Commissione Europea in merito

254 European Banking Authority (2018), 3.

255 Institute of International Finance, 2018.

256 Armour et al. (2016), 439.

257 de la Mano, Padilla (2018), 504.

258 Di Porto, Ghidini (2020).

all'introduzione di una cornice regolatoria ex-ante volta a disciplinare la condotta dei detentori di piattaforme tecnologiche in aggiunta ad un nuovo strumento di tutela antitrust, culminata di recente con la proposta di regolamento europeo "*on contestable and fair markets in the digital sector*" (c.d. Digital Market Act)[259]. Il *policy maker* europeo intende, così, colpire in modo più efficace di quanto non sia avvenuto passato le condotte più discusse messe in atto da molte piattaforme tecnologiche negli ultimi anni (*self-preferencing*, *killer acquisitions*, presidio esclusivo dell'accesso all'interfaccia con la clientela, ecc.).

Tali proposte, tuttavia, presentano ancora significativi coni d'ombra che rendono difficile potersi esprimere sulla loro congruità. Ad esempio, non è ancora stato raggiunto un consenso su criteri univoci ed oggettivi per individuare le imprese che andrebbero soggette ad obblighi aggiuntivi di condotta. Quelli proposti sinora (dimensioni della base degli utenti, intensità degli effetti di rete, la capacità di impiegare i propri dati in modo trasversale per estendere il proprio potere di mercato) non rappresentano parametri sufficientemente oggettivi per garantire la certezza del diritto[260]. Il modello ispiratore di queste possibili riforme fa riferimento al sistema regolamentare adottato nell'ambito della disciplina europea delle comunicazioni elettroniche, incentrato su tre condizioni per individuare gli operatori con un significativo posizione di dominanza[261]. Trattasi, in particolare, di una struttura del mercato che non permette sufficienti livelli di concorrenza, stabili e rilevanti barriere all'ingresso e l'insufficienza del diritto della concorrenza ordinario per far fronte ai conseguenti fallimenti di mercato[262]. Non è chiaro, inoltre, come la Commissione deciderà di circoscrivere quei mercati più esposti al rischio di saturazione e concentrazione: non è ancora stata operata la necessaria sistematizzazione complessiva dei possibili criteri qualitativi (possibilità di *multi-homing*, inerzia dei consumatori ed effetti di rete) e quantitativi (presenza di operatori con funzioni essenziali di controllo dell'accesso al mercato). Occorre infine domandarsi come tali strumenti potranno interagire con la disciplina pro-concorrenziale e settoriale del mercato dei servizi di pagamento già in vigore ed analizzate nella precedente sezione (diritto alla portabilità dei dati e regola di accesso ai conti di pagamento).

Infine, va evidenziato come l'inserimento di una clausola di reciprocità all'accesso dei dati ponga un doppio ordine di problemi[263]. In primo luogo, è estremamente difficile circoscrivere con chiarezza il perimetro dei dati che le BigTech avrebbero l'onere di condividere: non trattandosi, infatti, di dati economicamente indispensabili ed essenziali per l'erogazione di servizi finanziari, la norma si presterebbe a facili abusi da parte delle banche interessate ad ostacolare l'ingresso di nuovi concorrenti nonché a difficoltà applicative di carattere tecnico. A ciò va aggiunto che, al momento, l'ingresso delle BigTech nel mondo dei servizi finanziari non ha ancora raggiunto livelli tali

259 Commissione Europea (2020a).

260 Commissione Europea (2020).

261 Commissione Europea (2020); UK Digital Competition Expert Panel (2019), 81.

262 Direttiva (EU) 2018/1972, che istituisce il codice europeo delle comunicazioni elettroniche, [2018] OJ L 321/36, Articoli 63 and 67.

263 Borgogno, Colangelo (2020).

da far temere il rischio di una monopolizzazione del mercato con effetti irreparabili. Come è stato notato, i tentativi di ingresso nel mercato compiuti sinora hanno carattere settoriale e strettamente complementare ai servizi *core* delle rispettive piattaforme. Non possono, dunque, considerarsi una minaccia immediata per i grandi conglomerati finanziari di gravità tale per il pubblico interesse da comportare un intervento del legislatore[264].

In secondo luogo, l'introduzione di un tale obbligo risulterebbe probabilmente prematuro e contro-producente rispetto agli obiettivi pro-competitivi perseguiti dal legislatore europeo con la PSD2. Potrebbe, infatti, reprimere sul nascere l'unica effettiva spinta concorrenziale portata dal FinTech, ossia quella rappresentata dalle BigTech. Come è stato recentemente notato, le piccole start-up FinTech presentano un'intrinseca debolezza economica rispetto agli operatori bancari tradizionali che le porterebbe naturalmente a cooperare con questi ultimi (sia tramite acquisizioni o con accordi di *partnership*)[265]. Verrebbe così meno, dal punto di vista delle dinamiche competitive, l'unica forma di pressione che possa essere esercitata nei confronti dei tradizionali operatori bancari a livello europeo.

È opportuno infatti rimarcare che, per quanto concerne il mercato dei servizi di pagamento e finanziari, gli operatori che al momento continuano a godere di una posizione di vantaggio circa la gestione dei dati della clientela sono le banche tradizionali e non le piattaforme tecnologiche. Nell'ambito della gestione delle informazioni connesse ai conti di pagamento e dell'accesso alla clientela, gli enti creditizi rivestono una posizione strategica per l'evoluzione del mercato stesso. Qualora, infatti, tali operatori avessero la possibilità di ostacolare l'ingresso di potenziali concorrenti e al contempo godere degli strumenti di accesso ai dati per consolidare ulteriormente il proprio potere di mercato ai danni di consumatori e piccole banche concorrenti, la concorrenza in campo finanziario rischierebbe di subire pesanti ripercussioni negative.

La principale preoccupazione derivante da tale situazione è che gli *incumbents* cerchino di adeguarsi al nuovo panorama regolamentare adoperandosi surrettiziamente per ostacolare un omogeneo flusso di dati all'interno del Mercato Unico. A questo proposito, non bisogna dimenticare che la prestazione e l'esecuzione di servizi *data-enabled* richiede la cooperazione e interazione tra differenti operatori lungo la catena del valore. È dunque evidente che uno spazio europeo di condivisione dei dati in campo finanziario non raggiungerà mai il suo pieno potenziale senza l'impiego sistematico di APIs aperte e standardizzate che assicurino sufficienti livelli di interoperabilità e semplifichino lo scambio e accesso ai dati tra operatori. Finora, la Commissione Europea ha incoraggiato le imprese in tutto il Mercato Unico ad impiegare sistematicamente API aperte, standardizzate e ben documentate (rendendo le stesse leggibili da dispositivi automatici)[266]. Tuttavia, gli operatori privati sono fondamentalmente liberi di sviluppare le API ed i supporti tecnici per la portabilità dei dati che più preferiscono per adeguarsi agli obblighi regolamentari, anche se gli stessi rischiano di

264 Megaw (2019), in cui si evidenzia come il tasso di crescita dei finanziamenti generati da Amazon Lending sia diminuito negli ultimi tre anni.

265 Cole, Douglas, Taylor (2019); Financial Stability Board (2019); Bo̎mer and Hannes (2018).

266 Commissione Europea (2018), 9.

generare effetti inattesi, se non controproducenti, per il legislatore. In particolare, siccome i titolari dei dati conservano un forte interesse a non condividere i dati e l'attuazione dei regimi di accesso è intrinsecamente complesso, vi è il forte rischio che gli *incumbents* o titolari di *datasets* adottino espedienti tecnici e pratiche non cooperative per sabotare il libero flusso di dati[267]. In proposito, sussiste il rischio che le riforme attualmente prese in considerazione dalla Commissione Europea in materia di regolazione ex ante delle piattaforme tecnologiche possano paralizzare *tout court* l'apporto pro-competitivo della PSD2[268]. In tale prospettiva, l'intervento regolatorio in oggetto evidenzia l'interconnessione tra benessere dei consumatori, concorrenza e innovazione. L'impatto su tali *trade-off* derivante dal prossimo intervento regolatorio della Commissione Europea andrà monitorato con attenzione da parte di studiosi, regolatori e *policy makers*.

3.5 Riflessioni conclusive

L'ingresso dei BigTech nel mercato dei servizi finanziari rappresenta uno dei risvolti più interessanti del FinTech dal punto di vista dell'organizzazione industriale e della politica del diritto antitrust. A differenza dei piccoli operatori e delle *start-up*, le grandi società tecnologiche che hanno acquisito posizione di dominanza nel mercato dei *social network*, della pubblicità *online*, dell'*e-commerce* grazie al proprio *business* a piattaforma rappresentano un serio rischio competitivo per gli *incumbent* del mondo bancario. In particolare, il meccanismo regolamentare recentemente introdotto con la PSD2 volto a consentire l'accesso ai conti di pagamento da parte di imprese terze interessate a fornire servizi di pagamento ed analisi delle relative informazioni, pone numerose questioni di indubbio interesse economico e regolatorio.

In particolare, sta maturando la preoccupazione tra *policy makers* e commentatori che tale regime di accesso ai conti di pagamento possa generare ripercussioni economiche inizialmente non previste. La regola di accesso ai conti era stata pensata per agevolare l'ingresso sul mercato di nuovi operatori FinTech nonché per aumentare il livello di concorrenza nel mondo dei servizi bancari alla clientela a beneficio dei consumatori. In considerazione dell'evoluzione del mercato è tuttavia probabile che l'unica possibile pressione concorrenziale nei confronti delle banche possa essere posta dai BigTech, e non dalle piccole *start-up*. La forza finanziaria accumulata da tali imprese combinata con le capacità analitiche e di analisi dati già in loro possesso, potrebbero loro permettere di entrare nel mercato dei servizi finanziari con nuovi servizi e modalità distributive.

Il presente contributo ha offerto una prima panoramica delle caratteristiche economiche che potrebbero permettere alle BigTech di disintermediare ed innovare il tradizionale settore finanziario B2C mediante lo sfruttamento di effetti di rete, discriminazione di prezzo e disintermediazione degli operatori tradizionali. Tali fenomeni richiedono di essere attentamente valutati da regolatori e *policy makers* al fine di evitare

267 Milanesi (2017).

268 Borgogno, Colangelo (2020).

che eventuali pratiche anti-competitive finora poco conosciute nel mondo dei servizi finanziari possano generare effetti negativi per la stabilità del sistema finanziario ed il benessere dei consumatori.

Parallelamente, stanno emergendo nuove proposte regolatorie volte a prevenire in radice le potenziali problematiche competitive poste dalle BigTech mediante l'introduzione di nuovi meccanismi di accesso reciproco alle informazioni degli utenti. Tra gli interventi che, al momento, appaiono godere di maggiore sostegno in dottrina vi sono l'introduzione di codici di disciplina appositi per le piattaforme volti a vietare condotte di *self-preferencing* e di una clausola di reciprocità da accompagnare alla regola di accesso alle informazioni dei conti di pagamento[269].

Il presente contributo ha evidenziato, in chiave critica, come l'ingresso delle BigTech nei mercati finanziari è ancora un processo *in itinere* e simili interventi rischiano di frustrare l'obiettivo pro-competitivo della PSD2. Gravare gli operatori BigTech di nuovi oneri regolamentari mai sperimentati in precedenza genererebbe un implicito ostacolo al loro ingresso sul mercato dei servizi finanziari in termini di costi legati all'incertezza applicativa di tali nuovi istituti e potenziali danni reputazionali in caso di controversie e problemi applicativi. Inoltre, come è stato notato, tali riflessioni rischiano di essere premature in quanto il mercato sta affrontando una fase ancora preliminare dove i profili di anti-competitività delle BigTech nei mercati finanziari non sono ancora emersi nella loro concretezza. Non deve infine essere dimenticato che le grandi piattaforme esercitano in potenza l'unica effettiva pressione competitiva capace di disciplinare la condotta degli *incumbent* e spronarli a fare pieno uso delle opportunità offerte dall'innovazione tecnologica in campo finanziario per offrire servizi migliori a prezzi più competitivi per la clientela.

269 Expert Group on Regulatory Obstacles to Financial Innovation (2019), 79-80

A. Colaruotolo, M. Siragusa (*)

4 Responsabilità dei nuovi soggetti e delle piattaforme sul piano civilistico. L'insostenibile leggerezza della responsabilità civile degli Internet service provider

4.1 Introduzione

La quarta rivoluzione industriale[270] ha sollevato vari spunti di riflessione per gli interpreti poiché ha avuto un impatto dirompente cd. *disruptive* con modifiche di sistema a tutti i livelli dalla configurazione del mercato fino all'evoluzione delle relazioni economiche e sociali. In questo contesto, la digitalizzazione è un elemento di discontinuità che ha aperto scenari prima inediti e inimmaginabili con diverse occasioni di approfondimento, atteso che i dati ridefiniranno il modo di vivere, produrre e consumare. Secondo una recente analisi[271], il volume dei dati prodotti a livello mondiale passerà dai 33 zettabyte del 2018 ai 175 zettabyte del 2025 con enormi vantaggi per le imprese.

Quanto detto è il risultato dell'uso pervasivo dell'ICT (*Information Communication Technology*) e dell'IOT *(Internet of Things*) che permeano la gran parte delle attività quotidiane. Nello sviluppo tecnologico, l'industria finanziaria si è posta all'avanguardia, essendo stata tra le prime a cogliere le opportunità di progresso offerte dalla rivoluzione digitale[272]. Dalla sinergia tra trasformazione digitale e mercati finanziari è così sorto il FinTech che consiste nell'applicazione della tecnologia alla finanza[273]. Per

(*) Andrea Colaruotolo, dottorando e Team member Jean Monnet Chair in EU Innovation Policy, Università Europea di Roma (andrea.colaruotolo@unier.it);

Matteo Siragusa, Avv. e Post-Doc Researcher, Università Europea di Roma (matteo.siragusa@studiogambino.it).

270 V. Falce – G. Ghidini – G. Olivieri, *Informazione e Big Data tra innovazione e concorrenza*, Milano, 2018; A. Cipriani - A. Gramolati - G. Mari (a cura di), *Il lavoro 4.0. La Quarta Rivoluzione industriale e le trasformazioni delle attività lavorative,* Firenze, 2018

271 D. Reinsel – J. Gantz – J. Rydning, *The Digitization of the World From Edge to Core*, in IDC White Paper, 2018, disponibile al seguente link: https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf

272 P. Ciocca, *Dati e finanza: nuove opportunità e nuove vulnerabilità. La necessità di cambiare paradigma,* disponibile al seguente link: https://www.consob.it/documents/46180/46181/intervento_ciocca_20201118.pdf/d1d29034-5180-420a-adb2-a2f2248f4a8f

273 F. Di Ciommo – M. Rubino De Ritis – G. Cassano, Banche, intermediari e Fintech. I nuovi strumenti digitali in ambito finanziario, Milano, 2020; V. Falce – G. Finocchiaro (a cura di), Fintech: diritti, concorrenza e regole, Torino, 2019; R. Lener (a cura di), Fintech: diritto, tecnologia e finanza, Milano, 2018; R. Ferrari, L'era del Fintech. La rivoluzione digitale nei servizi finanziari, Milano, 2016

l'effetto, il settore finanziario ha mutato fisionomia sotto il profilo dei soggetti (Tech-Fin), dei prodotti e servizi (unbundled), dei mercati (disintermediati), dei modelli (market place model) e dei rapporti (decentrati)[274].

Secondo la Commissione Europea, il processo in parola può divenire "un importante motore della trasformazione digitale dell'economia e della società"[275]. Ciò si ricollega al fatto che il Fintech è un fenomeno pervasivo e intersettoriale che ricomprende un ampio novero di attività[276], contraddistinte da disintermediazione, decentralizzazione e digitalizzazione. Come osservato[277], si assiste pertanto alla frantumazione della catena del valore con l'affermazione di operatori e di servizi orientati solo su specifici segmenti della filiera a seguito del cd. *unbundling* della banca.

In termini generali, la *fintegration* ha così dato luogo ad una nuova economia *data driven*, le cui implicazioni dipendono dall'aggregazione attuale o potenziale dei dati tramite l'impiego di metodi computazionali estremamente avanzati[278]. In particolare, l'ecosistema in analisi è governato dalla formazione, circolazione ed elaborazione dei dati in combinazione con l'uso dell'intelligenza artificiale che congiuntamente hanno generato una nuova morfologia dei mercati finanziari. Ne è derivato un ridimensionamento del sistema bancocentrico che ha finito per assumere con il processo di trasformazione digitale frontiere mobili ed elastiche[279]. In altri termini, sono intervenuti nuovi attori nei mercati finanziari che hanno determinato un cambiamento dei paradigmi nei rapporti tra B2B e B2C tramite l'offerta di nuovi prodotti e servizi personalizzati a favore degli operatori. Questo si è tradotto in una maggiore efficienza operativa e in un'ottimizzazione delle risorse.

Fermo quanto sopra, è diventata impellente la necessità di dotarsi di un quadro normativo che comprenda la digitalizzazione e l'innovazione tecnologica entro una cornice in cui prodotti e soluzioni Fintech possano diffondersi rapidamente in tutta l'UE a vantaggio di economie di scala del mercato unico, salvaguardando però la stabilità finanziaria e la protezione dei consumatori.

274 C. Schena – A. Tanda – C. Arlotta – G. Potenza, Lo *sviluppo del Fintech – Opportunità e rischi per l'Industria finanziaria nell'Era Digitale*, in Quaderni Fintech - Consob, 2018 disponibile online al seguente link: https://www.consob.it/documents/46180/46181/FinTech_1.pdf/35712ee6-1ae5-4fbc-b4ca-e45b7bf80963

275 Comunicazione della Commissione al Parlamento Europeo, al Consiglio, alla Banca Centrale Europea, al Comitato Economico e Sociale e al Comitato delle regioni, Piano d'azione per le tecnologie finanziarie: per un settore finanziario europeo più competitivo e innovativo, 8-3-2018, 1 e ss, disponibile al seguente link: https://eur-lex.europa.eu/resource.html?uri=cellar:6793c578-22e6-11e8-ac73-01aa75ed71a1.0017.02/DOC_1&format=PDF

276 https://www.iosco.org/library/pubdocs/pdf/IOSCOPD554.pdf Secondo il rapporto IOSCO sul Fintech sarebbero identificabili almeno otto macroaree: 1) pagamenti; 2) assicurazioni; 3) pianificazione finanziaria; 4) lending & crowdinvesting; 5) trading; 6) catene di blocchi cd. blockchain;7) analisi delle informazioni; 8) sicurezza delle operazioni

277 G. Pitruzzella, Fintech e nuovi scenari competitivi, in V. Falce – G. Finocchiaro (a cura di), Fintech: diritti, concorrenza e regole, cit., 2

278 J. Cavanillas – E. Curry – W. Wahlster, New Horizons for a Data-Driven Economy A Roadmap for Usage and Exploitation of Big Data in Europe, 2016, disponibile al seguente link: https://link.springer.com/content/pdf/10.1007%2F978-3-319-21569-3.pdf

279 EBA, *Final Report on EBA Guidelines on outsourcing arrangements*, 25-02-2019, disponibile al seguente link: https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA%20revised%20Guidelines%20on%20outsourcing%20arrangements.pdf

Ciò premesso, si osserva che il cammino del progresso scientifico tecnologico risulta caratterizzato da una rapidità e complessità sempre crescenti cui si accompagna il declino delle tradizionali categorie e l'elaborazione di nuovi paradigmi[280]. Nel presente, difficilmente misurabili appaiono gli sviluppi in atto. Invero, le previsioni future indicano un'ulteriore accelerazione e pervasività delle soluzioni tecnologiche. In questo scenario, il legislatore spesso fatica a seguire la parabola evolutiva dei processi innovativi con il progressivo ampliamento della distanza tra il dato legale e quello reale parallelamente al decorso degli anni. Senza un'inversione di tendenza, scaturiranno prevedibilmente conseguenze negative per la generalità dei consociati a causa dell'affermazione di nuove forme di sfruttamento e di minaccia di diritti. Si tratta di una sfida regolamentare particolarmente accentuata nel settore finanziario, vista la stretta coesistenza tra rischi e opportunità, vantaggi e svantaggi[281].

Perno della odierna trasformazione digitale sono le piattaforme telematiche che forniscono le infrastrutture e i servizi necessari per il funzionamento della rete. Queste si pongono, infatti, quali principali motori della disintermediazione e della decentralizzazione nell'offerta di beni e servizi, tanto che oggi si suole parlare più propriamente di "*platform economy*". Mettendo in contatto utenti finali, produttori e aziende, le piattaforme on line assicurano una condivisione massiva e *real time* di informazioni, dando vita ad un modello di business *technology-enabled* inevitabilmente destinato a creare valore su larga scala.

A tal riguardo, è possibile individuare alcune tipologie principali di piattaforme fra cui: (i) *Matchmaker* digitali, ossia piattaforme transazionali e *marketplace*, deputate a far incontrare domanda e offerta di beni e servizi creando nuove occasioni di business (i.e. Amazon ed eBay, sul lato offerta di beni; Uber e Airbnb sul lato offerta di servizi); (ii) Piattaforme di pagamenti, che operano soprattutto nei micropagamenti e nei trasferimenti in denaro Peer-to-Peer (i.e.PayPal); (iii) Marketplace d'investimento, attive soprattutto nel settore dei servizi finanziari, si caratterizzano per la predisposizione di spazi all'interno dei quali il risparmio viene raccolto ed investito all'interno di circuiti più o meno tradizionali (si pensi al fenomeno dell'*equity crowdfunding* o del *marketplace lending*).

Tutti questi modelli ritrovano nella figura degli Internet Service Provider un antenato comune, che nel presente scritto si cercherà di analizzare, al fine di verificare se la normativa dettata per disciplinarlo e regolarlo, possa essere applicata, *mutatis mutandis,* anche a questi nuovi ecosistemi tecnologici, che si trovano, ancora oggi, sprovvisti di una regolamentazione adeguata e diretta ad evitare pericolosi vuoti di tutela.

In particolare, gli Internet Service Provider (cd. ISP o prestatori della società dell'informazione) veicolano lo scambio delle informazioni e l'interazione tra gli utenti

280 G. Alpa, *Fintech un laboratorio per i giuristi*, in Contr. e Impr., 2019, 2, 377 e ss.

281 E. Palmerini, G. Aiello, V. Cappelli - G. Morgante - N. Amore - G. Di Vetta - G. Fiorinelli - M. Galli, *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*, in Quderni FinTech – Consob, 2018

della rete attraverso la raccolta, l'elaborazione e la circolazione dei dati[282]. Così operando, le piattaforme online contribuiscono all'esercizio di diritti primari e di libertà fondamentali da parte degli utenti, atteggiandosi come manifestazioni della cd. "partecipatory culture" e della "sharing economy"[283].

La premessa di cui sopra offre lo spunto per procedere all'analisi della responsabilità civile degli ISP a seguito della commissione di illeciti da parte dei fruitori dei servizi di intermediazione online[284]. Sotto il profilo giuridico, invero, la definizione della *governance* di Internet e il trattamento giuridico degli intermediari online rappresentano al momento una delle questioni più critiche in relazione all'ecosistema digitale in considerazione della crescente proliferazione di attività illecite in rete[285]. Il tema esige particolare attenzione, stante la sussistenza di uno stretto binomio tra mercati virtuali e prestatori di servizi Internet con la conseguenza per cui risulterebbe impossibile immaginare i primi senza i secondi e viceversa[286]. Per l'effetto, pare opportuno sottolineare da subito che qualsiasi approccio di riforma in ordine alla disciplina degli Internet provider dovrebbe essere guidato da cautele e da accortezze.

La mancanza di regole cagiona irrimediabili vuoti di responsabilità che inficiano la fiducia dei fruitori dei servizi di intermediazione online, risolvendosi spesso in situazioni di incontrollato sovvertimento della stabilità del sistema finanziario realizzate proprio in quegli interstizi in cui l'assenza di una regolamentazione chiara e uniforme ha determinato la nascita di realtà pienamente sviluppate ancorché non regolate. Chiarita la necessità di una disciplina della materia, appare dunque necessario interrogarsi su quale sia la strategia migliore per attuarla, predisponendo un apparato normativo *ad hoc* oppure sfruttando plessi normativi già esistenti, là ove sia possibile adeguare il dato normativo a questi nuovi ecosistemi.

282 OECD, *An Introduction to Online Platforms and Their Role in the Digital Transformation*, Parigi, 2019, disponibile al seguente link: https://doi.org/10.1787/53e5f593-en

283 J. C. Plantin -C. Lagoze - P. N. Edwards - C. Sandvig, *Infrastructure studies meet platform studies in the age of Google and Facebook,* in New Media & Society online first, 2018, 20, 293 e ss.

A. Sundararajan, *The Sharing Economy: The End of Employment and the Rise of Crowd-Based Capitalism*, Cambridge, 2017.

284 Sulla responsabilità degli ISP cfr. *ex multis*: M. Tescaro, *Una proposta ricostruttiva contrastante con il diritto vivente in tema di responsabilità civile dell'internet provider nel diritto italiano tra direttiva 200/31/CE, Regolamento Ue 2016/679 e Direttiva Ue 2019/790*, in Juscivile, 2020, 1, 62 e ss; A. M. Gambino – A. Stazi – D. Mula, *Diritto dell'informatica e della comunicazione*, Torino, 2019, 241 e ss.; AA.VV, *Diritto dell'Informazione e dei media*, Torino, 2019, 333 e ss.; A. Maietta, *Il diritto della multimedialità*, Torino, 2018, 19 e ss.; S. Scuderi, *La responsabilità dell'internet service provider alla luce della giurisprudenza della Corte di Giustizia Europea* (causa c-610/15, 14 giugno 2017), in DIMT, 30-07-2018, 4 e ss., disponibile al seguente link: https://www.dimt.it/wp-content/uploads/2018/07/images_pdf_SimonaScuderi.pdf ; F. Piraino, *Spunti per una rilettura della disciplina giuridica degli Internet service provider*, in AIDA, 2017, XXVI, 468 e ss; R. Bocchini, La responsabilità extracontrattuale del provider, in D. Valentino (a cura di), *Manuale di diritto dell'informatica* Napoli, 2016, 540 e ss.; E. Tosi, Responsabilità civile per fatto illecito degli internet service provider, in Dig. disc. priv., sez. civ., X agg., 2016; F. Bravo, La responsabilità civile degli Internet Service Providers, in G. Alpa – G. Conte (a cura di), La responsabilità d'impresa, Milano, 2015, 688 e ss.

285 G. Frosio, *Why keep a dog and bark yourself? From intermediary liability to responsibility,* in International Journal of Law and Information Technology, 2018, 26, 1 e ss.

286 E. Tosi, *Responsabilità civile per fatto illecito degli internet service provider*, cit., § 3.

4.2 Profili generali sulla responsabilità degli ISP

In tema di intermediari online, la principale fonte normativa è ad oggi la Direttiva sul commercio elettronico 2000/31/CE del Parlamento europeo e del Consiglio dell'8 giugno 2000 relativa a taluni aspetti giuridici dei servizi della società dell'informazione nel mercato interno che ha armonizzato le condizioni alle quali gli Internet provider beneficiano della deroga in materia di responsabilità per le attività illegali in rete, poste in essere dai fruitori dei servizi di intermediazione online (cd. *third-party content*)[287]. La novella normativa ha avuto il merito di porre fine negli Stati membri all'incertezza relativa all'inquadramento giuridico dell'operato degli intermediari online[288]. Nell'ordinamento italiano, la Direttiva 2000/31/CE è stata recepita con il d.lgs. 9 aprile 2003 n. 70 che ne ha riprodotto il contenuto con alcune peculiarità, espressione del margine di discrezionalità devoluto agli Stati membri[289,290].

In particolare, il legislatore sovranazionale ha inteso perseguire almeno quattro finalità: *i)* realizzare un ambiente digitale sicuro tramite la condivisione di tale compito tra tutti gli attori coinvolti; *ii)* stimolare la crescita dei prestatori dei servizi della società dell'informazione e del commercio elettronico; *iii)* raggiungere un bilanciamento equo tra i diritti fondamentali in campo; *iv)* costruire il mercato unico digitale[291]. A livello di Unione Europea, quindi, l'intenzione è stata quella di evitare carichi

287 Direttiva 2000/31/CE del Parlamento europeo e del Consiglio dell'8 giugno 2000 relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno («Direttiva sul commercio elettronico»)

288 Prima della Dir. 2000/31/CE, il trattamento giuridico dell'attività dei prestatori dei servizi della società dell'informazione ha conosciuto in ambito nazionale e sovranazionale varie ricostruzioni esegetiche. Tuttavia, il progresso tecnologico e l'evoluzione della rete rendevano evidente l'inadeguatezza dell'applicazione dei tradizionali meccanismi della responsabilità aquiliana all'attività degli ISP per la risoluzione delle controversie relative alla società dell'informazione. Peraltro, la disciplina giuridica in materia appariva all'epoca connotata da una forte frammentazione di approcci, variabili a seconda del Paese di riferimento. Su questi temi, cfr. M. De Cata, *La responsabilità civile dell'internet service provider*, Milano, 2010, 89 e ss.; A. Contaldo - G. Cassano, *La natura giuridica e la responsabilità civile degli Internet Service Provider (ISP): il punto sulla giurisprudenza*, in Corr. Giur., 2009, 1206 e ss; U. Ruffolo, *Nuove tecnologie, questioni antiche e nuove tutele*, in Aa.Vv., *La tutela del navigatore in Internet*, 2002, Milano, 289 e ss; G. Poggio, *La responsabilità dell'internet provider*, *ivi*, 193 e ss.; E. Tosi, *Le responsabilità civili*, in E. Tosi (a cura di), *I problemi giuridici di internet* Milano, 1999, 233 e ss.

289 Decreto legislativo 9 aprile 2003, n. 70 Attuazione della direttiva 2000/31/CE relativa a taluni aspetti giuridici dei servizi della società dell'informazione nel mercato interno, con particolare riferimento al commercio elettronico.

290 In ordine alle peculiarità della normativa nazionale rispetto a quella sovranazionale, si osserva che il citato Decreto legislativo ha subordinato la rimozione delle informazioni e la disabilitazione dell'accesso da parte dell'hosting provider alla "comunicazione delle Autorità" a differenza della fonte sovranazionale, ove è assente una simile condizione. Ed ancora, le due proposizioni a) e b) dell'art. 14 Dir. 2000/31/CE sono legate con la disgiuntiva "o" mentre quelle corrispondenti dell'art. 16 d.lgs. 70/2003 non sono connesse da alcun inciso. Non si tratta di un rilievo meramente lessicale, giacchè la Direttiva consente un intervento in autotutela spontaneo da parte del provider a seguito della ricezione di una segnalazione stragiudiziale circa la presenza di contenuti illeciti rispetto al predetto Decreto legislativo che richiede invece un ordine formale per la cancellazione di materiale illecito, sebbene poi sostanzialmente nella prassi se ne faccia spesso a meno. Da ultimo, la mancanza di una precisa corrispondenza con l'articolato della normativa eurounitaria si coglie nella disposizione di cui all'art. 17 d.lgs. 70/2003 che prevede la responsabilità civile del prestatore se, una volta sollecitato dalle Autorità pubbliche, omette di impedire l'accesso ai contenuti illeciti o di informare le Autorità, ove venuto a conoscenza dell'illiceità di certi contenuti.

291 C. Ullrich, Standards for Duty of Care? Debating Intermediary Liability from a Sectoral Perspective, in JIPITEC, 2017, 8, 2, 111 e ss.

eccessivi in capo agli ISP solo in quanto destinatari più visibili e aggredibili nel caso di contenuti illeciti messi in rete dagli utenti[292].

Ciò premesso, la Direttiva sul commercio elettronico ha consacrato per gli ISP un sistema di esenzioni (cd. *safe harbor*) dalla responsabilità di tipo "orizzontale" e "funzionale"[293] che viene meno a seguito della mancata tempestiva rimozione dei contenuti illeciti pubblicati dagli utenti ovvero dall'omessa attenuazione delle relative conseguenze dannose successivamente alla conoscenza dei contenuti illegali presenti in rete[294]. Per l'effetto, è stata rigettata l'alternativa previsione di una forma di responsabilità *ex ante* degli ISP, risultante dal mancato controllo preventivo e generale su tutte le informazioni trattate e i contenuti immessi in rete[295].

Accanto alla responsabilità secondaria che è si innesta sul fatto illecito già compiuto dai fruitori del servizio internet[296], non si esclude comunque una responsabilità primaria dei prestatori della società dell'informazione per fatto proprio colpevole, risultante tanto dal diretto compimento di attività illecite a prescindere dal comportamento dei fruitori dei servizi internet quanto dal concorso con l'utente nel compimento di atti illeciti in rete, cui si ricollega l'applicazione sul piano interno delle tradizionali norme sulla responsabilità aquiliana.

Giova brevemente sottolineare che la normativa eurounitaria ha distinto nell'ambito dei servizi di intermediazione online tre attività: mero trasporto (cd. *mere*

292 P. Van Eecke, *Online Service Providers and Liability: A Plea for a Balanced Approach*, in Common Market Law Review, 2011, 48, 1457 e ss.

293 P. Valcke -A. Kuczerawy – P. J. Ombelet, *Did the Romans geti t right? What Delfi, google, Ebay, and UPC TeleKabel Wien have in common*, in L. Floridi – M. Taddeo (a cura di), *The responsibilities of Online Service Providers*, Oxford, 2017, 102 e ss. Per esenzione dalla responsabilità cd. orizzontale, si fa riferimento al fatto che l'operatività del *safe harbour* prescinde dal tipo di illecito perpetrato dagli utenti. Per esenzione dalla responsabilità cd. funzionale, viceversa, si allude al fatto che l'esonero vale solo in relazione agli specifici servizi di intermediazione online esercitati dagli operatori di settore e non a predeterminate categorie soggettive di provider. In giurisprudenza, Corte di Giust Ue, 20-12-2017, C-434/15 caso Asociación Profesional Élite Taxi c. Uber Spain e Corte di Giust. Ue, 10-04-2015, C-320/16 caso Uber France. In particolare, i Giudici di Lussemburgo hanno concluso sulla base degli elementi in atti che il servizio di intermediazione offerto da Uber oggetto di causa doveva essere considerato come parte integrante di un servizio complessivo di cui l'elemento principale era un servizio di trasporto ai sensi della direttiva 2006/123 e non come un servizio della società dell'informazione ai sensi della dir. 2000/31.

294 S. Scuderi, *La responsabilità dell'internet service provider alla luce della giurisprudenza della Corte di Giustizia Europea* (causa c-610/15, 14 giugno 2017), in DIMT, cit., 5 e ss.

295 B. Panattoni, *Il sistema di controllo successivo: obbligo di rimozione dell'ISP e meccanismi di notice and take down*, in Dir. pen. contemp., 2018, 5, 250 e ss. Con riferimento alla responsabilità ex ante dell'ISP, l'Autrice afferma che "Essa infatti richiederebbe interventi tecnicamente impraticabili nonché eccessivamente onerosi agli ISP, e confliggerebbe con l'espresso divieto contenuto nell'art. 15 della Direttiva sull'e-commerce (recepito dall'art. 17 D.lgs. n. 70/2003), il quale proibisce agli Stati membri l'imposizione a carico degli ISP di un generale e preventivo obbligo di sorveglianza sulle informazioni che trasmettono o memorizzano".

296 G. Sartor, *Providers liability: from the ecommerce Directive to the future,* Directorate General for Internal Policies – Economic and Scientific policy, 2017, 9 e ss. secondo cui "The intermediary does not initiate the wrongful activity that triggers sanction, but rather provides the context of infrastructure that enables and facilitates the user's illegal behavior, or magnifies its impacts...". A. De Streel - M. Buiten – M. Peitz, *Liability of online hosting platforms should exceptionalism end?,* cit, 37 e ss.; R. Bocchini, *La responsabilità di Facebook per la mancata rimozione di contenuti illeciti*, in Giur. it, 2017, 3, 642 e ss; G.B. Dinwoodie, *A Comparative Analysis of the Secondary Liability of Online Service Providers*, Springer, 2017, 1 e ss.; R. Petruso, *Responsabilità degli intermediari di internet e nuovi obblighi di conformazione: robo take down, policy of termination, notice and take steps*, cit., 451 e ss.

conduit)[297]; memorizzazione temporanea (cd. *caching*)[298] e memorizzazione duratura (cd. *hosting*)[299], graduando la responsabilità degli Internet provider per gli illeciti commessi dagli utenti a seconda della diversa natura e delle particolarità del servizio di intermediazione online[300]. Ed ancora, si rileva che il legislatore eurounitario ha espressamente escluso un obbligo generale di monitoraggio in ordine alle informazioni trasmesse e di controllo attivo in capo agli intermediari della società dell'informazione circa le eventuali attività illecite realizzate dai fruitori dei servizi[301].

Secondo una certa opinione[302], quindi, la Direttiva E-commerce non ha delineato autonome fattispecie di responsabilità connotate da propri elementi strutturali e riferibili a predeterminate categorie soggettive, bensì sfere di liceità d'azione che precludono contestazioni in capo agli ISP per l'attività di intermediazione svolta ovvero per gli illeciti commessi in rete dai fruitori dei relativi servizi.

Dall'analisi del quadro normativo, emergono forti analogie tra la Direttiva sul commercio elettronico e il modello americano del "Digital Millenium Copyright Act" del 1998 (DMCA), incentrato sul sistema delle cd. "exemptions" di cui al § 512 che esonera della responsabilità gli Internet provider in ordine alle informazioni trattate e alle operazioni compiute dagli utenti destinatari del servizio[303].

Da quanto sopra, quindi, traspare una logica di favore per i prestatori della società dell'informazione, stante la predeterminazione per gli ISP di coordinate di condotta, la cui osservanza scongiura in radice addebiti di responsabilità rispetto all'applicazione delle comuni regole civilistiche[304]. Invero, il legislatore europeo ha operato direttamente a monte un bilanciamento tra i vari interessi coinvolti nella rete, dando maggiore risalto alla libertà di manifestazione del pensiero, all'accesso alle informazioni e all'esercizio dell'attività di impresa degli intermediari rispetto ai diritti personali e patrimoniali degli utenti.

297 Art. 12 Dir. 2000/31/CE

298 Art. 13 Dir. 2000/31/CE

299 Art. 14 Dir. 2000/31/CE

300 R. Bocchini, *La responsabilità extracontrattuale del provider*, cit., 540 e ss.; E. Tosi, *Responsabilità civile per fatto illecito degli internet service provider*, cit., § 4.

301 Art. 15 Dir. 2000/31/CE

302 F. Piraino, *Spunti per una rilettura della disciplina giuridica degli Internet service provider*, cit., 478 e ss; A. Montanari, *Prime impressioni sul caso* SABAM c. Netlog NV: gli *Internet Service Provider e la tutela del diritto d'autore online*, in Dir. comm. int., 2012, 4, 1085 e ss., il quale puntualizza che la normativa sugli ISP si incentra non sulla definizione del soggetto in sé quanto piuttosto sulla definizione del regime di attività esercitata dall'intermediario.

303 R. Petruso, *Responsabilità delle piattaforme online, oscuramento di siiti web e libertà di espressione nella giurisprudenza della corte Europea dei diritti dell'uomo*, in Dir. inf e inf., 2018, 3, 511 e ss.

304 F. Piraino, *Spunti per una rilettura della disciplina giuridica degli Internet service provider*, cit., 472 e ss.; D. Mula, *La responsabilità e gli obblighi degli Internet provider per la violazione del diritto d'autore*, in Riv. Dir. Ind., 2010, 3, 252 e ss.

4.3 Sulla questione della conoscenza effettiva dei contenuti illeciti

Ai fini della valutazione della responsabilità dei prestatori dei servizi della società dell'informazione per le violazioni commesse dagli utenti, risulta centrale l'analisi del profilo relativo alla conoscenza in capo all'Internet provider dell'illecito perpetrato dai fruitori dei propri servizi di intermediazione online.

Come suesposto, la previsione di cui all'art. 14 Dir. 2000/31/CE ha subordinato l'esonero dalla responsabilità dell'*hosting provider* alla duplice condizione che "a) non sia effettivamente al corrente del fatto che l'attività o l'informazione è illecita e, per quanto attiene ad azioni risarcitorie, non sia al corrente di fatti o di circostanze che rendono manifesta l'illegalità dell'attività o dell'informazione, o b) non appena al corrente di tali fatti, agisca immediatamente per rimuovere le informazioni o per disabilitarne l'accesso". Prima dell'effettiva conoscenza dell'illecito commesso dagli utenti, quindi, non è predicabile di regola alcuna responsabilità dell'ISP[305].

All'interno della normativa comunitaria, tuttavia, non è ravvisabile alcuna nozione di diritto positivo che specifichi il contenuto e il coefficiente di consapevolezza richiesto in capo al provider ai fini dell'insorgenza dell'obbligo di rimozione dei contenuti illeciti caricati dagli utenti in rete[306]. Sul punto, è intervenuta la Corte di Giustizia dell'Unione Europea che ha interpretato l'accezione di effettiva conoscenza in termini estensivi, ricomprendendovi ogni forma di consapevolezza dell'illiceità da parte dell'intermediario "in qualsiasi modo" ottenuta secondo quanto è lecito attendersi da un operatore economico professionalmente diligente[307]. Conformemente alle elaborazioni della CGUE, la giurisprudenza nazionale più recente ha ritenuto sussistente il requisito della conoscenza effettiva in capo al prestatore anche in presenza di una segnalazione proveniente dal soggetto danneggiato dai contenuti immessi in rete, indipendentemente da una comunicazione dell'Autorità rivolta al provider a pena di una responsabilità dell'ISP[308]. Invero, la diffida dell'avente diritto determinerebbe il venir meno

305 V. Vozza, *La responsabilità civile degli internet service provider tra interpretazione giurisprudenziale e dettato normativo*, in Danno e resp., 2018, 1, 101 e ss.

306 E. Tosi, *Contrasti giurisprudenziali in materia di responsabilità civile degli hosting provider – passivi e attivi – tra tipizzazione normativa e interpretazione evolutiva applicata alle nuove figure soggettive dei motori di ricerca, social network e aggregatori di contenuti*, in Riv. dir. ind., 2017, 1, 56 e ss.

307 Corte di Giust. Ue, 12-07-11, C-342/09 caso L'Oreal c. eBay, punto 121, ove si afferma che "*inoltre, affinché non siano private del loro effetto utile, le norme enunciate all'art. 14, n. 1, lett. a), della direttiva 2000/31 devono essere interpretate nel senso che riguardano qualsiasi situazione nella quale il prestatore considerato viene ad essere, in qualunque modo, al corrente di tali fatti o circostanze*".

308 Cass., civ., sez. I, 19-03-2019, n. 7708 con nota di F. Di Ciommo, *Oltre la direttiva 2000/31/Cee, o forse no. La responsabilità dei provider di Internet nell'incerta giurisprudenza europea*, in Foro it., 2019, 2072 e ss; Corte d'App. Roma, 29-04-2017 con nota di G. Cassano, *Nozione di provider e delimitazione della responsabilità: la giurisprudenza prende una direzione*, in Dir. ind., 2018, 2, 183 e ss.; Trib. Roma, 27-04-2016, n. 8437 con nota G. Cassano, *Sulla responsabilità del provider per la diffusione abusiva in rete di opere audiovisive*, in Dir. Ind., 2016, 5, 460 e ss.; E. Bassoli, *Il diritto d'autore e la responsabilità del provider: evoluzioni tecniche e giurisprudenziali nell'appello Yahoo vs. RTI*, in Corr. Giur., 2016, 6, 811 e ss; Trib. Napoli, 3-11-2016 con nota di R. Bocchini, *La responsabilità di Facebook per la mancata rimozione di contenuti illeciti*, cit., 638 e ss. A sostegno della tesi circa la sufficienza della segnalazione stragiudiziale adottata dal Giudicante, l'Autore ha individuato cinque argomenti: *i)* secondo un ragionamento a contrario sarebbe stata inutile la previsione di un'autonoma fattispecie di irresponsabilità connessa alla non effettiva conoscenza dell'illecito così come la previsione di un obbligo di rimozione dei contenuti solo a seguito di un ordine dell'autorità; *ii)* se l'obbligo di attivazione nasce solo a seguito di un ordine dell'autorità non si comprende la necessità di un divieto di ricerca attiva di fatti o circostanze illecite; *iii)* il divieto di ricerca attiva degli illeciti non preclude una loro conoscenza passiva a seguito di segnalazioni; *iv)* la conoscenza dell'illecito può provenire anche dall'esterno oltre che dall'Autorità, con conseguente

dell'astratta neutralità del provider cui si ricollega ai sensi dei considerando 46 e 48 Dir. 2000/31/CE il corrispondente obbligo di adottare tutte quelle regole di diligenza professionale ragionevolmente esigibili nel contrasto alle attività illecite commesse online dai fruitori dei propri servizi di intermediazione online[309].

Ai fini dell'integrazione degli estremi della responsabilità dell'*hosting provider*, occorre accanto al profilo conoscitivo l'illiceità manifesta del contenuto segnalato e l'omessa rimozione tempestiva del materiale dalla rete. Per la Cassazione, la manifesta illiceità deve intendersi come quella che "sarebbe possibile riscontrare senza difficoltà alla stregua dell'esperienza e delle conoscenze tipiche dell'operatore di settore" e che sarebbe desumibile secondo il canone della diligenza professionale[310]. In caso di illiceità non manifesta ma potenziale, l'Internet provider è viceversa tenuto a segnalare senza indugio il contenuto alle Autorità competenti ai sensi dell'art. 17 d.lgs. 70/2003.

Il profilo dell'effettiva conoscenza, poi, si intreccia con gli interrogativi relativi ai requisiti della diffida stragiudiziale proveniente dal soggetto leso a determinare l'insorgenza dell'obbligo di attivazione in capo all'intermediario online ai fini della rimozione dei contenuti illeciti messi in rete dagli utenti. A riguardo, si sono confrontati in passato due opposti orientamenti interpretativi circa la menzione dell'URL del materiale illecito all'interno della segnalazione dell'utente danneggiato rivolta al prestatore: uno restrittivo[311] che richiedeva necessariamente l'URL per innescare l'obbligo di pronta rimozione in capo al provider dei contenuti illeciti segnalati e un altro estensivo[312] che escludeva l'indicazione dell'URL per l'insorgenza del predetto obbligo.

ingiustificabilità di un comportamento inerte a fronte della consapevolezza dell'illecito; *v)* occorre poi una comparazione degli interessi coinvolti. Nel caso di lesione di diritti personalità, infatti, le tempistiche necessarie per l'emanazione di un ordine dell'Autorità finirebbero per pregiudicare irrimediabilmente gli interessi del danneggiato, non suscettibili più di reintegrazione.

309 Trib. Roma, 20-01-2019, n. 693 con nota di E. BASSOLI, I*l caso RTI vs Vimeo e la responsabilità civile dell'hosting provider attivo: sentenza n. 693/2019 del Tribunale di Roma*, in Nuov. Dir. civ., 2019, 2, 131 e ss.; R. PANETTA, *La responsabilità civile degli Internet service provider e la tutela del diritto d'autore*, in Dir. Ind., 2017, 1, 61 e ss.

310 Cass., civ., sez. I, 19-03-2019, n. 7708 con nota di L. TORMEN, *La linea dura della Cassazione in materia di responsabilità dell'hosting provider attivo e passivo*, in Nuov. Giur. Civ., 2019, 5, 1044 e ss. In sostanza, l'aggettivo manifesta delimita la responsabilità del prestatore esclusivamente alle fattispecie di colpa grave e di dolo. Trattandosi di concetti di origine psicologica, deve ritenersi che la conoscenza effettiva in capo al prestatore dell'illecito sorga con la comunicazione del danneggiato.

311 Trib. Torino, 7-04-2017, n. 1928 con nota di V. VOZZA, *La responsabilità civile degli internet service provider tra interpretazione giurisprudenziale e dettato normativo*, cit., 102 e ss.; Corte d'App. Milano, 7-01-2015, n. 29 con nota di G. CASCELLA, *Dieci decisi no ad una scomposta sentenza della Corte d'Appello di Milano, ed una via di uscita - A proposito di Corte d'Appello di Milano il 7 gennaio 2015, n. 29*, in Vita not., 2015, 2, 1 ss.; Trib. Roma, 16-06-2011 con nota di L. GIOVE - A. COMELLI, *Responsabilità del provider per mancata rimozione di link a materiale illecito*, cit., 75 e ss. Per questo indirizzo esegetico, il contenuto della diffida doveva essere particolarmente specifico e dettagliato, occorrendo a tal uopo l'indicazione degli URL del materiale illecito di cui il danneggiato chiede la cancellazione. Diversamente, si escludeva l'attitudine della mera segnalazione contenente solo i titoli commerciali delle opere audiovisive contraffatte ad attivare in capo al provider l'obbligo di pronta rimozione dei contenuti illeciti sull'assunto della necessità di una conoscenza qualificata dell'esistenza dei contenuti illeciti messi in rete dagli utenti.

312 Trib. Roma, 12-07-2019, 14760; Trib. Roma, 12-07-2019, n. 14757; Trib. Roma, 20-01-2019, n. 693 con nota di E. BASSOLI, *Il caso RTI vs Vimeo e la responsabilità civile dell'hosting provider attivo: sentenza n. 693/2019 del Tribunale di Roma*, cit., 132 e ss.; Corte d'App. Roma, 29-04-2017 con nota di G. CASSANO, *Nozione di provider e delimitazione della responsabilità: la giurisprudenza prende una direzione*, cit., 181 e ss.; Trib. Roma, 27-04-2016, n. 8437 con nota di M. SIMONI, *La responsabilità degli hosting provider quali prestatori "tecnici, automatici e passivi" della società dell'informazione*, in Dir. Ind, 2017, 5, 455 e ss. G. CASSANO, *Sulla responsabilità del provider per la diffusione abusiva in rete di opere audiovisive*, cit., 460 e ss.; E. BASSOLI, *Il diritto d'autore e la responsabilità del provider: evoluzioni tecniche e giurisprudenziali nell'appello Yahoo vs. RTI*, cit., 811 e ss.; ID, *Giurisprudenza italiana e comunitaria sulla responsabilità*

Dinanzi al citato contrasto interpretativo, la Cassazione ha avallato la tesi per cui occorre una valutazione caso per caso circa l'adeguatezza della segnalazione dell'avente diritto a rendere edotto l'intermediario della presenza di contenuti illeciti, indipendentemente dalla presentazione di una diffida in senso tecnico e dalla comunicazione degli "URL", tenendo conto della specificità dell'avviso e delle risorse tecnologiche a disposizione del prestatore al momento della segnalazione[313]. In tale contesto, il danneggiato può provare la conoscenza effettiva dell'illecito in capo all'intermediario online, dimostrando l'avvenuto recapito della comunicazione all'indirizzo del prestatore. L'intermediario poi può superare la presunzione *iuris tantum* di conoscenza tramite la dimostrazione in concreto della mancanza di cognizione effettiva dell'illecito per un fattore estraneo alla sua volontà.

4.4 L'avvento dell'*hosting provider* cd. attivo

Secondo l'opinione prevalente[314], l'impianto della normativa eurounitaria sugli ISP è stato modellato attorno alla figura del cd. *hosting provider* cd. passivo. A sostegno di questa tesi, si è osservato che il considerando 42 Direttiva sul commercio elettronico fa leva sullo svolgimento da parte dell'Internet provider online di un'attività di carattere "neutro, passivo e automatico", estranea all'operato dei fruitori dei servizi di intermediazione online.

Tuttavia, il recente progresso tecnologico ha portato ad un mutamento nella natura e nella tipologia dei servizi offerti dagli intermediari online agli utenti onde fornire un'esperienza multimediale più efficiente. Si è sostanzialmente verificata una transizione da una fase in cui i servizi di *hosting* facevano capo ad una pluralità di siti

civile del service provider e la sentenza della Corte d'Appello di Milano nel caso Yahoo vs. RTI, cit., 230 e ss. Per questo indirizzo ermeneutico, era sufficiente una segnalazione che menzionasse chiaramente i contenuti audiovisivi o i materiali illeciti, indipendentemente dall'indicazione dei corrispondenti URL che non avrebbe nessuna copertura normativa. La ratio di tale prospettiva si coglieva alla luce del fatto che lo stato attuale della tecnica della società dell'informazione consente l'individuazione specifica e mirata da parte del provider dei contenuti illeciti segnalati indipendentemente dall'URL.

313 Cass., civ., sez. I, 19-03-2019, n. 7708 con nota di F. Di Ciommo, *Oltre la direttiva 2000/31/Cee, o forse no. La responsabilità dei provider di Internet nell'incerta giurisprudenza europea*, cit., 2072 e ss. Per la Suprema Corte, "La comunicazione al prestatore del servizio deve essere idonea a consentire al destinatario la comprensione e l'identificazione dei contenuti illeciti: a tal fine, deve allora aversi riguardo ai profili tecnico-informatici per valutare se, nell'ipotesi di trasmissione di prodotti video in violazione dell'altrui diritto di autore, questi siano identificabili mediante la mera indicazione del nome della trasmissione da cui sono tratti e simili elementi descrittivi, oppure occorra anche la precisa indicazione del cd. indirizzo "url" (uniform resource locator), quale sequenza di caratteri identificativa dell'indirizzo cercato; ciò, trattandosi di responsabilità aquiliana sorta al momento della condotta omissiva, alla stregua dello sviluppo tecnologico dell'epoca dei fatti...Resta affidato al giudice di merito l'accertamento in fatto se, sotto il profilo tecnico-informatico, l'identificazione di video, diffusi in violazione dell'altrui diritto, sia possibile mediante l'indicazione del solo nome o titolo della trasmissione da cui sono trattai, od, invece, sia indispensabile, a tal fine, la comunicazione dell'indirizzo "url", alla stregua delle condizioni esistenti all'epoca dei fatti".

314 G. D'Alfonso, *Anonimato in rete e responsabilità civile dell'hosting provider nella prospettiva de jure condendo*, in DIMT, 10-09-2019, 23 e ss. disponibile al seguente link: https://www.dimt.it/wp-content/uploads/2019/09/DAlfonso-Oblio_privacy-completo.pdf ; G. Cassano, *Nozione di provider e delimitazione della responsabilità: la giurisprudenza prende una direzione*, cit., 181 e ss; S. Scapin, *La responsabilità dell'internet service provider per omesso controllo dei contenuti illeciti immessi dagli utenti della rete*, in Dir. ind., 2018, 3, 264 e ss ; V. Vozza, *La responsabilità civile degli internet service provider tra interpretazione giurisprudenziale e dettato normativo*, cit., 99 e ss.; S. Scuderi, *La responsabilità dell'internet service provider alla luce della giurisprudenza della Corte di Giustizia Europea* (causa c-610/15, 14 giugno 2017), cit., 7 e ss.

di piccole dimensioni monofunzionali ad un'altra fase in cui l'ospitalità dei contenuti caricati in rete dagli utenti è gestita da un oligopolio di BigTech polifunzionali che offrono ai propri utenti una molteplicità contestuale di servizi accessori alla mera ospitalità dei contenuti: indicizzazione, condivisione, gestione, modifica, vendita, pubblicizzazione, manipolazione e trasformazione dei contenuti multimediali[315].

Quanto sopra ha sollevato interrogativi e perplessità tra gli interpreti in ordine all'inquadramento di tali nuove figure di Internet provider all'interno della previsione di cui all'art. 14 Dir. 2000/31/CE. Per superare i predetti inconvenienti, è stata così coniata in via pretoria la discussa figura dell'*hosting provider* cd. attivo per indicare quell'intermediario online che interviene in vario modo sui contenuti caricati dai fruitori del servizio di intermediazione online[316].

A tale ultima categoria di Internet provider, non si applica il regime di limitazione della responsabilità previsto dal citato art. 14 Dir. 2000/31/CE e dal corrispondente art. 16 d.lgs. 70/2003 con conseguente assoggettamento alle comuni regole di responsabilità, poiché l'intermediario online non si limita a svolgere un'attività meramente tecnica[317]. Tuttavia, non vi è uniformità di vedute sull'individuazione di quelle attività che qualificano un *hosting provider* come attivo.

A dirimere eventuali contrasti interpretativi sul punto, è intervenuta la Cassazione che ha delineato una serie di "indici di interferenza" ulteriori all'erogazione del mero servizio di ospitalità, seppur a titolo esemplificativo e non cumulativi[318]. Nondi-

315 L. Bugiolacchi, *Ascesa e declino della figura del provider "attivo"? Riflessioni in tema di fondamento e limiti del regime privilegiato di responsabilità dell'hosting provider*, in Resp. civ. 2015, 4, 1261 e ss.

316 Corte di Giust. Ue, 7-08-2018, C-521/17 caso Cooperatieve Vereniging SNB-REACT U.A. c. Deepak Mehta, punto 47 ove i giudici europei hanno collegato la nozione di *"hosting provider attivo"* a tutti quei casi che esulano da un'*"attività dei prestatori di servizi della società dell'informazione* [che] *sia di ordine meramente tecnico, automatico e passivo, con la conseguenza che detti prestatori non conoscono né controllano le informazioni trasmesse o memorizzate dalle persone alle quali forniscono i loro servizi"* mentre *"per contro, tali limitazioni di responsabilità non sono applicabili nel caso in cui prestatore di servizi della società dell'informazione svolga un ruolo attivo"* Trib. Roma, sent., 10-01-2019, n. 693 con nota di E. Bassoli, *Il caso RTI vs Vimeo e la responsabilità civile dell'hosting provider attivo: sentenza n. 693/2019 del Tribunale di Roma*, cit., 128 e ss. In particolare, il Giudicante ha considerato la piattaforma americana VIMEO come un *hosting provider* attivo in quanto *i)* offriva un servizio video on demand, in cui i contenuti audiovisivi venivano precisamente catalogati, indicizzati e messi in correlazione dal provider; *ii)* suddivideva la clientela; *iii)* associava ai contenuti annunci e collegamenti pubblicitari; *iv)* forniva un servizio di ricerca dei contenuti immessi nel portale; *v)* si riservava il diritto di modifica, distribuzione, adattamento e riorganizzazione dei contenuti caricati dagli utenti; *vi)* sottoponeva ai suoi utenti un contratto che prevedeva una licenza non esclusiva per l'esercizio dei diritti di riproduzione e adattamento dei video caricati dagli stessi; Trib. Milano, 13-06-2017 con nota di S. Scapin, *La responsabilità dell'internet service provider per omesso controllo dei contenuti illeciti immessi dagli utenti della rete*, cit., 264 e ss.; Corte d'App. Milano, 7-01-2015, n. 29 con nota di E. Bassoli, *Il diritto d'autore e la responsabilità del provider: evoluzioni tecniche e giurisprudenziali nell'appello Yahoo vs. RTI*, in Corr. Giur., 2016, 6, 811 e ss; Trib. Milano, sez. impresa, ord., 9-09-2011, n. 10893 con nota di S. Saraceno, *Note in tema di violazioni del diritto d'autore tramite internet: la responsabilità egli Internet Service Provider*, in Dir. ind., 2011, 6, 375 e ss.

317 Trib. Roma, 20-01-2019, n. 693 con nota di E. Bassoli, *Il caso RTI vs Vimeo e la responsabilità civile dell'hosting provider attivo: sentenza n. 693/2019 del Tribunale di Roma*, cit., 131 e ss.; Corte d'App., 29-04-2017 con nota di G. Cassano, *Nozione di provider e delimitazione della responsabilità: la giurisprudenza prende una direzione*, cit., 183 e ss;

318 Cass., civ., sez. I, 19-03-2019, n. 7708 con nota di F. Di Ciommo, *Oltre la direttiva 2000/31/Cee, o forse no. La responsabilità dei provider di Internet nell'incerta giurisprudenza europea*, cit., 2072 e ss; Per la Cassazione, "gli elementi idonei a delineare la figura [dell'hosting provider attivo]... sono le attività di filtro, selezione, indicizzazione, organizzazione, catalogazione, aggregazione, valutazione, uso, modifica, estrazione o promozione dei contenuti, operate mediante una gestione imprenditoriale del servizio, come pure l'adozione di una tecnica di valutazione comportamentale degli utenti

meno, l'arresto dei giudici di legittimità ha destato non pochi dubbi tra i primi commentatori, perché non ha specificato "quali" e "quanti" dei cd. indici di interferenza devono sussistere affinché il provider possa essere definito attivo, oltre alla forzatura del dato legislativo di matrice pretoria[319]. Ed ancora, una parte della dottrina ha manifestato perplessità sulla stessa ammissibilità di siffatta categoria di Internet provider in ragione dell'impossibilità di individuare precise situazioni tipo all'interno della rete[320]. Pertanto, si ritiene che il baricentro tra *hosting provider* attivo o passivo debba piuttosto essere individuato nella manipolazione dei contenuti memorizzati o nella trasformazione della natura del servizio. Ne deriva che l'organizzazione e l'indicizzazione dei materiali immessi in rete dagli utenti non escludono la neutralità dell'operatore, poiché non modificano i contenuti ma contribuiscono solo ad un migliore utilizzazione degli stessi[321].

Fermo quanto sopra, si evidenzia che l'inquadramento giuridico del provider costituisce comunque esplicazione di un apprezzamento di fatto ad opera del giudice di merito, insindacabile in sede di legittimità.

In conclusione, si osserva che sulla base degli ultimi orientamenti della Cassazione l'obbligo di intervento del provider per la rimozione e disabilitazione dell'accesso al materiale illecito scatta a partire dalla conoscibilità della sua manifesta illiceità, indipendentemente da una qualsiasi comunicazione del danneggiato e delle Autorità competenti nonchè dalla natura del provider, stante il dovere per gli ISP di agire secondo il canone della diligenza professionale[322].

4.5 Verso una maggiore responsabilizzazione degli Internet Service Providers fra interventi di *soft* e di *hard law*

Come suesposto, si riteneva originariamente che le questioni concernenti la responsabilità degli ISP potessero trovare un assetto definitivo con l'adozione della Di-

per aumentarne la fidelizzazione: condotte che abbiano, in sostanza, l'effetto di completare e arricchire in modo non passivo la fruizione dei contenuti da parte di utenti indeterminati"

319 Cass., civ., sez. I, 19-03-2019, n. 7708 con nota di F. Di Ciommo, *Oltre la direttiva 2000/31/Cee, o forse no. La responsabilità dei provider di Internet nell'incerta giurisprudenza europea*, cit., 2081 e ss.

320 M. Tescaro, *Una proposta ricostruttiva contrastante con il diritto vivente in tema di responsabilità civile dell'internet provider nel diritto italiano tra direttiva 200/31/CE, Regolamento Ue 2016/679 e Direttiva Ue 2019/790,* cit., 78 e ss.; L. Tormen, *La linea dura della Cassazione in materia di responsabilità dell'hosting provider attivo e passivo*, cit., 1047 e ss. Nell'opinione dell'Autore, sono ravvisabili alcuni ostacoli non trascurabili alla configurazione dell'hosting provider attivo: i) la mancanza di appigli normativi; ii) la diffusa interpretatio abrogans della Dir. 2000/31/CE giacchè oggi la quasi totalità di internet provider ricorre a sistemi di organizzazione, indicizzazione e processamento dei contenuti immessi in rete dagli utenti; iii) il regime di favore della Dir. sul commercio elettronico non fa leva su una determinata tipologia di provider bensì sulla natura dei servizi offerti dagli intermediari online.

321 Corte di Giust. UE, 23-03-2010, C-236/08 a C-238/08 caso Google France sarl e Google Inc. c. Louis Vuitton Malletier SA, punto 116; Corte di Giust. Ue, 12-07-2011, C-324/09 caso L'Oreal c. eBay, punto 115

322 Cass., civ., sez. I, 19-03-2019, n. 7708 con nota di L. Tormen, *La linea dura della Cassazione in materia di responsabilità dell'hosting provider attivo e passivo*, cit., 1043 e ss.; Trib. Roma, 20-01-2019, n. 693 con nota di E. Bassoli, *Il caso RTI vs Vimeo e la responsabilità civile dell'hosting provider attivo: sentenza n. 693/2019 del Tribunale di Roma*, cit., 131 e ss.; Corte d'App. Milano, 7-01-2015, n. 29 con nota di M. Iaselli, *Caso Yahoo! Video: la Corte di Appello di Milano non vede responsabilità nell'operato dell'Internet Provider*, in Riv. dir. ind., 2016, 2, 166 e ss.

rettiva E-commerce attraverso l'elaborazione di un sistema di esenzioni dalla responsabilità uniforme in tutti gli Stati membri. Tuttavia, il progresso tecnologico degli ultimi due decenni e la proliferazione di attività illecite online hanno messo in luce l'incompletezza della normativa attuale cui fa da sfondo un'attenzione in misura sempre crescente circa le problematiche legate al governo della circolazione dei contenuti in rete[323].

A sostegno di un irrigidimento della responsabilità degli ISP, si è posto l'accento : i) sull'obsolescenza della normativa eurounitaria e sulla sua incapacità di soddisfare la domanda di tutela delle vittime di illeciti online[324]; ii) sull'affermazione di nuove figure di intermediari online che esorbitano dalla rigida tripartizione (*mere conduit - caching - hosting provider*) della Direttiva sul commercio elettronico; iii) sulla capacità degli ISP di contrastare efficacemente ed efficientemente la diffusione di contenuti illeciti sulla rete grazie alle più moderne tecnologie di filtraggio, selezione e gestione dei contenuti online[325]; iv) sull'omesso aggiornamento periodico dell'impianto della Direttiva sul commercio elettronico, sebbene esplicitamente previsto[326].

A ciò, si è aggiunta anche una dilagante retorica secondo cui le piattaforme digitali sarebbero divenute "*the new online governors*"[327] e potrebbero "*grow so large and become so deeply entrenched in world economies that they could effectively make their own laws*"[328]. Come illustrato in un recente articolo apparso sulla Rivista "The Economist"[329], sarebbe sostanzialmente proprio il successo delle piattaforme online a spingere verso un irrigidimento della loro regolamentazione.

Accanto alle suesposte spinte riformistiche, si evidenziano nella direzione di un ripensamento della normativa in tema di responsabilità dei prestatori della società dell'informazione le molteplici questioni interpretative legate tanto al testo della Direttiva 2000/31/CE e al suo recepimento negli ordinamenti nazionali quanto alla fram-

323 S. SCUDERI, L*a responsabilità dell'internet service provider alla luce della giurisprudenza della Corte di Giustizia Europea* (causa c-610/15, 14 giugno 2017), cit., 4 e ss.; K. ERICKSON – M. KRETSCHMER, *Empirical, Approaches to Intermediary Liability,* in CREATe Working Paper, 2019, 6, 2 e ss.

324 A. DE STREEL - M. BUITEN – M. PEITZ, *Liability of online hosting platforms should exceptionalism end?,* cit., 21 e ss.

325 J. D. LIPTON, *Law of the Intermediated Information Exchange*, in Florida Law Review, 2012, 64, 5, 1337 e ss.

326 Art. 21, 2 comma, Dir. 2000/31/CE

327 K. KLONICK, The New Governors: *The People, Rules, and Processes Governing Online Speech*, in Harward Law Review, 2018, 131, 1598 e ss.; S. DENNING, *The Fight For Europe's Future: Digital Innovation Or Resistance*, Forbes, 20-05-2018, https://www.forbes.com/sites/stevedenning/2018/05/20/the-fight-for-europes-future-digital-innovation-or-resistance/#722f906948c0; R. B. REICH, *Big Tech Has Become Way Too Powerful*, N.Y. Times, 18-09-2015, https://www.nytimes.com/2015/09/20/opinion/is-big-tech-too-powerful-ask-google.html. In particolare, si registra in Europa l'emergere di spinte sovraniste e di sentimenti nazionalisti contrari all'egemonia dei giganti americani del web che sono stati etichettati come i cd. "Frightful Five" – Apple, Amazon, Facebook, Microsoft and Alphabet (Google) – poiché la loro forza economica sarebbe divenuta superiore a quella di interi Stati

328 F. Manjoo, *Why the World Is Drawing Battle Lines Against American Tech Giants*, New York Times, 1 giugno 2016, https://www.nytimes.com/2016/06/02/technology/why-the-world-is-drawing-battle-lines-against-american-tech-giants.html.

329 The Economist, *Internet firms' legal immunity is under threat*, 11 febbraio 2017, disponibile al seguente link:

https://www.economist.com/business/2017/02/11/internet-firms-legal-immunity-is-under-threat. Nella parte conclusiva dell'articolo, si legge "giving platforms a free pass is increasingly difficult for regulators and courts: they simply have become too important for the economy and society more generally. Successful online platforms, in other words, carry the seeds of their own regulation".

mentazione delle procedure di *notice and takedown* tra gli Stati membri e all'affermazione della figura dell'*hosting provider* cd. attivo[330]. Nella stessa direzione, pare deporre anche la più recente giurisprudenza della Corte di Giustizia dell'Unione Europea[331] e della Corte dei diritti dell'Uomo[332], le cui elaborazioni sembrano propendere per un irrigidimento della responsabilità degli ISP.

In altri termini, pare registrarsi nel regime di responsabilità degli ISP un cambio di paradigma segnato dalla transizione dall'approccio utilitaristico ad uno moralistico[333] e dal piano del risarcimento a quello della prevenzione degli eventi dannosi[334].

Da quanto sopra, si fa discendere la necessità di una rilettura in chiave moderna del ruolo dei prestatori della società dell'informazione, poiché le piattaforme online si avvantaggiano economicamente dei contenuti immessi in rete dagli utenti ma evitano di prendersi la responsabilità per il materiale diffuso tramite i propri servizi di intermediazione online. Per un certo indirizzo, quindi, l'erogazione di un servizio di intermediazione online comporterebbe implicitamente l'esercizio di un dovere di controllo sulle attività compiute dagli utenti e sui contenuti immessi in rete[335].

Di seguito, si passeranno in rassegna alcuni tra i principali interventi normativi di *soft e hard law* a livello eurounitario che hanno aperto la strada ad un regime di responsabilità rinforzato delle piattaforme online, animando il dibattito sulla necessità di una revisione anche della Direttiva sul commercio elettronico[336].

330 P. Van Eecke, *Online Service Providers and Liability: A Plea for a Balanced Approach*, cit., 1455 e ss.

331 Corte di Giust. Ue, 3-10-2019, C-18/18 caso Glawischnig c. Facebook; Corte di Giust. Ue, 7-08-2018, C-161/17 caso Land Nordrhein-Westfalen c. Dirk Renchoff; Corte di Giust. Ue, 7-08-2018, n. C-521/17 caso Coöperatieve Vereniging SNB-REACT U.A. c. Deepak Mehta; Corte di Giust. Ue, 15-09-2016, C-484/14 caso Tobias Mc Fadden c. Sony Music Entertainment Germany GmbH; Corte di Giust. Ue, 26-04-2017, C-527/15 caso Stichting Brein c. Jack Frederik Wullems; Corte di Giust. Ue, 11-11-2014 C-291/13 caso Sotiris Papasavvas v. O Fileleftheros Dimosia Etairia Ltd; Corte di Giust. Ue, 27-03-2014, C-314/12 caso UPC Telekabel Wien GmbH v. Constantin Film Verleih GmbH.

332 Corte Edu, 16-06-2015, n. 65469/09 caso Delfi AS v. Estonia; Corte Edu, 2-02-2016, n. 22947/13 caso Magyar Tartalomszolgaltatok Egyesülete and Index.hu ZRT v. Hungary.

333 G. Frosio, *Why keep a dog and bark yourself? From intermediary liability to responsibility*, cit., 4 e ss. secondo cui "the policy discourse is shifting from intermediary liability to intermediary responsibility. Policy approaches might be returning to implement moral theories of intermediary liability, rather than utilitarian or welfare theories. In this case, justification for policy intervention would be based on responsibility for the actions of users as opposed to efficiency or balance innovation vs harm. This is apparent form the enforcement of miscellaneous policy strategies— that will be detailed in the next few pages—and an overall move toward incentivizing intermediaries private ordering online".

334 M. Gambini, Intelligenza artificiale e diritto – algoritmi e sicurezza, cit., 1670 e ss.

335 S. Scuderi, *La responsabilità dell'internet service provider alla luce della giurisprudenza della Corte di Giustizia Europea* (causa c-610/15, 14 giugno 2017), cit., 14 e ss.; Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e sociale Europeo e al Comitato delle Regioni, Lotta ai contenuti illeciti online. Verso una maggiore responsabilizzazione delle piattaforme online, 2 e ss. ove si legge "Le piattaforme online che gran parte degli utenti di Internet consultano per accedere ai contenuti hanno la pesante responsabilità, nei confronti della società, di proteggere gli utenti e il pubblico in generale nonché prevenire lo sfruttamento dei loro servizi da parte di criminali e altri soggetti coinvolti in attività illegali online… Le piattaforme online dovrebbero intensificare con fermezza le loro azioni per affrontare tale problema, come parte della responsabilità derivante dal loro ruolo centrale nella società.

336 R. M. Hilty - A. Bauer, *Use of Protected Content on Online Platforms*, in Modernisation of the EU Copyright Rules (a cura di R.M. Hilty – V. Moscon), 2017, Position Statement of the Max Planck Institute for Innovation and Competition, Max Planck Institute for Innovation and Competition Research Paper, 17, 12, 99 e ss.

Sul piano degli interventi di *soft law*, bisogna avere anzitutto riguardo alla Comunicazione del 2017[337] e alla Raccomandazione del 2018[338] della Commissione Europea in merito alla lotta ai contenuti illeciti online che costituiscono un indice sintomatico della suddetta esigenza di ripensamento della responsabilità degli Internet Service Provider[339]. Invero, le citate fonti normative hanno esercitato un impatto significativo sull'attività degli intermediari online indipendentemente dalla loro fisionomia, giacchè contengono una serie di orientamenti volti ad intensificare il contrasto a tutte le forme di contenuti illeciti in rete tramite una cooperazione con Stati membri, Autorità di controllo e utenti.

Attraverso le due citate fonti normative, la Commissione Europea ha incoraggiato l'adozione di un doppio canale di misure, tanto *ex ante* quanto *ex post*, di contrasto agli illeciti dei fruitori dei servizi di intermediazione online[340], sollecitando il ricorso a strumenti automatizzati e a filtri per l'*upload*. Nell'ottica della Commissione europea, però, tali misure di intervento dovrebbero essere accompagnate da meccanismi di salvaguardia, controllo e revisione di tipo umano. Con riferimento alle procedure di *notice and take down*, è stata incoraggiata l'adozione di meccanismi sufficientemente effettivi e accurati nonché adeguatamente circostanziati. Allo stesso modo, è stata raccomandata la previsione di procedure di "*counter notices*" da parte dei titolari dei contenuti immessi in rete a fronte della segnalazione di un illecito dal soggetto danneggiato attraverso una dialettica e composizione delle controversie per via stragiudiziale. Ed ancora, la Commissione ha incentivato le piattaforme online ad adottare politiche trasparenti in relazione al trattamento dei contenuti immessi in rete dagli utenti, anche attraverso una comunicazione regolare alle Autorità di regolamentazione al fine di valutare l'efficacia dei risultati ottenuti.

In sostanza, i predetti interventi di *soft law* traggono le mosse dal fatto che non si ravvisa all'interno dell'Unione un metodo armonizzato e coerente nella rimozione dei contenuti illegali, bensì una molteplicità di soluzioni variabili a seconda dello Stato membro, della categoria di contenuto o del tipo di piattaforma. Nell'ottica comunitaria, quindi, una maggiore omogeneità degli approcci consentirebbe una più efficace lotta contro i contenuti illegali in rete ed un più celere sviluppo del mercato unico digitale, riducendo il costo economico per le piattaforme relativo alla conformazione alle singole leggi nazionali.

Nonostante alcuni dubbi di reale effettività derivanti dall'assenza di carattere vincolante ai sensi dell'art. 288 TFUE dei due citati interventi normativi, i provvedimenti della Commissione finiscono comunque per promuovere tanto una sensibilizzazione dal

337 Comunicazione (UE) 2017/555 della Commissione del 28 settembre 2017 al Parlamento Europeo, al Consiglio, al Comitato Economico e sociale Europeo e al Comitato delle Regioni Lotta ai contenuti illeciti online. Verso una maggiore responsabilizzazione delle piattaforme online

338 Raccomandazione (UE) 2018/334 della Commissione del 1 marzo 2018 sulle misure per contrastare efficacemente i contenuti illegali online

339 M. MAZZONETTO, *Il problema dei contenuti illegali on-line: la risposta della Commissione Europea*, 29-03-2018, in www.dirittodellinformatica.it

340 G. CODIGLIONE, *La nuova legge tedesca per l'enforcement dei diritti sui social network*, in Dir. inf. e inf., 2017, 734 e ss.

basso dell'attività degli Internet provider nel contrasto dei contenuti illeciti in rete tramite una sorta di "responsabilità sociale di impresa"[341] quanto un effetto cd. *moral suasion* in capo agli Stati membri con l'intento di indurli ad emanare provvedimenti legislativi conformi alle linee guida della Commissione.

4.5.1 La Direttiva sui servizi audio media visivi

Sul piano degli interventi di *hard law*, va posta in prima battuta l'attenzione alla Direttiva 2018/1808[342] che ha modificato la Direttiva 2010/13/UE[343] sui servizi audio media visivi ed ha inciso anche sull'attività dei prestatori dei servizi della società dell'informazione, là ove siano piattaforme di condivisione video[344].

La *ratio* della novella legislativa si rinviene nel mutato scenario del mercato audio media visivo che ha conosciuto l'affermazione di nuovi operatori come le piattaforme video a richiesta (cd. *on demand*). Invero, il progresso della tecnica ha reso possibile l'erogazione di nuovi tipi di servizi e di esperienze multimediali per gli utenti, fondate sulla convergenza tra media tradizionali ed Internet. Questo nuovo connubio ha però spinto le Istituzioni comunitarie ad intervenire tramite un aggiornamento della regolamentazione sui media a livello sovranazionale in un'ottica di protezione delle categorie più deboli e vulnerabili[345].

Ai fini della presente trattazione, occorre fare particolare riferimento alla disposizione di cui all'art. 28 ter Dir. sui servizi audio media visivi che impone ai provider di adottare misure adeguate alla salvaguardia dei minori e del grande pubblico da programmi - contenuti generati dagli utenti – comunicazioni commerciali che possano nuocere alla loro integrità psico fisica. Nella conformazione dei suddetti strumenti richiesti ai provider, bisogna tener conto tramite un bilanciamento di tutti gli interessi in gioco della specifica tipologia di contenuto multimediale e della corrispondente natura del danno che i materiali audiovisivi possono causare al pubblico nonchè delle caratteristiche dei soggetti da tutelare. Ciò nondimeno, le richiamate misure devono essere praticabili e proporzionate in considerazione delle dimensioni della piattaforma per la condivisione di video e della natura del servizio offerto.

All'interno della Direttiva, si legge che tali misure devono consistere nella predisposizione a favore degli utenti delle piattaforme di meccanismi trasparenti, facili e accessibili per la segnalazione della presenza di contenuti nocivi. Parimenti, è richiesta la previsione di sistemi di controllo parentale per evitare la fruizione di materiale audio

341 G. D'Alfonso, *Anonimato in rete e responsabilità civile dell'hosting provider nella prospettiva de jure condendo*, cit., 47.

342 Direttiva 2018/1808/UE del Parlamento europeo e del Consiglio del 14 novembre 2018 recante modifica della direttiva 2010/13/UE, relativa al coordinamento di determinate disposizioni legislative, regolamentari e amministrative degli Stati membri concernenti la fornitura di servizi di media audiovisivi (direttiva sui servizi di media audiovisivi), in considerazione dell'evoluzione delle realtà del mercato

343 Direttiva 2010/13/UE del Parlamento europeo e del Consiglio del 10 marzo 2010 relativa al coordinamento di determinate disposizioni legislative, regolamentari e amministrative degli Stati membri concernenti la fornitura di servizi di media audiovisivi (direttiva sui servizi di media audiovisivi)

344 Considerando 44 Dir. 2018/1808

345 F. Donati, *La tutela dei minori nella direttiva 2018/1808*, in Medialaws – Riv. dir. media, 2019, 1, 60 e ss.

video potenzialmente dannoso per i minori nonché procedure di gestione dei reclami. Ed ancora, è consigliato alle piattaforme di predisporre misure e strumenti efficaci di alfabetizzazione mediatica degli utenti in merito all'utilizzo di siffatti meccanismi. Tutto ciò deve trovare rispondenza anche nella sezione dedicata ai "termini d'uso" dei servizi offerti dal fornitore di contenuti digitali.

In sostanza, pare essere stata positivizzata una responsabilità di tipo gestionale in capo ai fornitori di servizi audio media visivi in relazione all'organizzazione dei contenuti caricati, prodotti e offerti al pubblico. Ciò nondimeno, si esclude una responsabilità di tipo editoriale per la mera presenza all'interno della piattaforma di contenuti illeciti ai sensi del combinato disposto dei considerando 47 e 48 della Dir. 2018/1808/UE.

Fermo quanto sopra, l'intervento normativo in esame solleva non trascurabili aspetti critici legati alla compatibilità con l'impianto della Direttiva sul commercio elettronico, stante il divieto di un obbligo generale di sorveglianza sui contenuti caricati dai fruitori dei servizi di intermediazione online e di ricerca attiva dei contenuti illeciti in rete. Ulteriori difficoltà di coordinamento emergono anche tra l'organizzazione dei contenuti ospitati nella piattaforma di condivisione video e l'insorgenza del requisito della conoscenza in capo all'Internet provider dell'illecito perpetrato dai fruitori dei propri servizi di intermediazione online che innesca l'obbligo di rimozione dei contenuti illegali immessi dagli utenti senza contare la genericità della locuzione "misure appropriate". Da ultimo, controverso è il carattere esemplificativo o tassativo degli strumenti elencati dall'art. 28 ter, 3 comma, Dir. servizi audio media visivi.

4.5.2 Il Regolamento sull'equità e trasparenza per gli utenti commerciali dei servizi di intermediazione online

In data 20 giugno 2019, è stato adottato il Regolamento 2019/1150/EU che promuove l'equità e la trasparenza per gli utenti commerciali dei servizi di intermediazione online, entrato in vigore a decorrere dal 12 luglio 2020 e direttamente applicabile in ciascuno degli Stati membri[346].

La finalità della novella normativa è stata quella di delineare un ecosistema competitivo, equo e sostenibile nell'ambito delle transazioni economiche via web in relazione al fatto che la rete è diventata un driver cruciale per lo sviluppo di nuovi modelli di business e un vettore indispensabile per raggiungere la platea dei consumatori con corrispondente successo commerciale delle aziende.

In particolare, Internet ha permesso in ragione del suo carattere transfrontaliero l'avvio e l'affermazione di nuove forme di imprenditorialità, non immaginabili prima dell'avvento della rete. Tale mutamento di paradigmi ha accentuato l'importanza del ruolo degli intermediari online e dei motori di ricerca nell'offrire alle imprese i vantaggi del mercato online. Accanto alle maggiori possibilità di scelta di beni e servizi per

346 Regolamento UE 2019/1150 del Parlamento Europeo e del Consiglio del 20 giugno 2019 che promuove equità e trasparenza per gli utenti commerciali dei servizi di intermediazione online https://eur-lex.europa.eu/legal-content/IT/ALL/?uri=CELEX%3A32019R1150

i consumatori, emergono però anche alcuni rischi che il presente Regolamento si è riproposto di affrontare mediante un apparato di norme vincolanti armonizzate in tutto il territorio dell'Unione, volte a creare un contesto commerciale sostenibile.

Sotto il profilo soggettivo, la novella normativa si rivolge agli intermediari online, motori di ricerca e agli utenti commerciali[347]. Ai fini dell'applicazione del Regolamento in esame non occorre che i fornitori dei servizi di intermediazione online abbiano la sede in uno Stato membro, mentre è necessario che gli utenti commerciali o i titolari di siti web aziendali siano stabiliti all'interno dell'Unione Europea ed offrano servizi a consumatori situati nell'Unione Europea almeno per parte della transazione[348]. Per converso, si esclude l'applicazione della novella normativa in esame tanto ai servizi di intermediazione online peer-to-peer e B2B quanto ai servizi di pagamento e di pubblicità online che non implicano relazioni contrattuali con consumatori. Inoltre, il presente Regolamento non pregiudica il diritto nazionale in materia di pratiche commerciali scorrette, validità, formazione, effetti, conclusione e risoluzione del rapporto contrattuale in ordine a quegli aspetti non esplicitamente contemplati dall'intervento normativo.

Per garantire una equilibrata relazione contrattuale tra intermediari online e utenti commerciali, i primi sono tenuti a delineare i termini e le condizioni di utilizzo dei servizi di intermediazione online con un linguaggio chiaro, semplice e accessibile, dovendosi intendere come tale quello che consente ai secondi di comprendere con un ragionevole grado di prevedibilità gli aspetti più importanti della relazione contrattuale. Ed ancora, le piattaforme online devono esplicitare in modo chiaro e trasparente le condizioni che determinano l'utilizzo, la sospensione e la cessazione dei servizi di intermediazione online. Eventuali modifiche unilaterali del contratto devono essere comunicate agli utenti commerciali con un preavviso almeno di 15 giorni, eccetto quando siano imposte da normative nazionali o sovranazionali. A tutela della trasparenza, è previsto che le piattaforme debbano consentire l'accesso ai termini e condizioni di utilizzo del servizio di intermediazione online a tutti i livelli del rapporto. Innovativamente, si stabilisce che le disposizioni dei termini e condizioni di utilizzo non conformi all'art. 3, par. 1 e 2, sono nulle, ferma restando la responsabilità risarcitoria della piattaforma online in caso di comportamenti abusivi.

In conformità ai principi di buona fede e leale collaborazione, le piattaforme sono tenute a comunicare con preavviso le motivazioni sottostanti alla decisione di sospendere o cessare l'erogazione dei servizi di intermediazione online nonché a predisporre un sistema interno di gestione dei reclami che consenta agli utenti commerciali di far valere in modo effettivo le loro ragioni. A tutela degli stessi principi summenzionati, le piattaforme non possono introdurre modifiche retroattive dei termini e delle condizioni di utilizzo dei servizi di intermediazione online, eccetto quando la modifica è imposta da un obbligo normativo, regolamentare o quando è vantaggiosa per gli utenti commerciali.

347 Art. 1 Regolamento UE 2019/1150

348 Per il soddisfacimento di tali ultimi due requisiti cumulativi, si rinvia alla pertinente giurisprudenza della CGUE sull'articolo 17, par. 1, lett. c), Regolamento 2012/1215/UE e sull'art. 6, par. 1, lett. b), Regolamento 593/2008/593/UE.

Ed ancora, gli intermediari online devono delineare preventivamente i parametri principali che influiscono sul posizionamento dei siti web e fornire agli utenti commerciali una chiara descrizione di portata, natura e condizioni del loro accesso a determinate categorie di dati e del loro utilizzo.

Da ultimo, la Commissione incoraggia i fornitori di servizi di intermediazione online a prevedere meccanismi di risoluzione stragiudiziale delle controversie con gli utenti commerciali nonché a predisporre con questi ultimi e le associazioni di categoria codici di condotta.

Sebbene il presente Regolamento non incida direttamente sulla responsabilità degli intermediari online, la novella normativa finisce comunque per interferire con l'attività delle piattaforme online nei confronti degli utenti commerciali, giacchè implica una conformazione delle condizioni e termini di utilizzo dei servizi di intermediazione online ai principi di buona fede, leale collaborazione e trasparenza. Il merito del Regolamento è stato, quindi, quello di aver intercettato il rischio di sperequazioni contrattuali tra intermediari online, motori di ricerca e utenti commerciali e di aver ricondotto in modo uniforme tra tutti gli Stati membri tali relazioni contrattuali nell'alveo di un contesto commerciale governato da regole certe. Per il corretto funzionamento del mercato interno dell'Unione, è infatti essenziale la fiducia dei consumatori in un ecosistema digitale che sia competitivo, equo e sostenibile in cui tutti gli attori in campo agiscono in modo responsabile.

4.5.3 La Direttiva sul diritto d'autore e sui diritti connessi nel mercato unico digitale

Nell'ambito dei recenti interventi normativi di *hard law*, quello più significativo sull'attività degli ISP è probabilmente rappresentato dall'approvazione all'esito di un lungo percorso evolutivo della Direttiva 790/2019 sul diritto d'autore e sui diritti connessi nel mercato unico digitale che modifica le Direttive 96/9/CE[349] e 29/2001/CE[350].

La *ratio* della novella normativa è da rinvenirsi nel fatto che l'evoluzione tecnologica degli ultimi decenni avrebbe determinato un cambio di paradigma attraverso cui i materiali protetti da diritto d'autore sono creati, prodotti e distribuiti. Invero, l'ambiente digitale ha dato luogo a nuove opportunità di accesso e di sfruttamento delle opere coperte da diritti d'autore[351].

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

350 Direttiva 2001/29/CE del Parlamento europeo e del Consiglio, del 22 maggio 2001 sull'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione

351 G. COLANGELO, "Digital Single Market strategy", *diritto d'autore e responsabilità delle piattaforme online*, cit., 614 e ss.; M. HUSOVEC, *Accountable, Not Liable: Injunctions Against Intermediaries*, in TILEC Discussion Paper, 2016, 12, 3 e ss.

Nel processo di riforma del diritto d'autore nel mercato digitale, centrale è stata la considerazione del cd. *value gap*[352] per cui il "*safe harbor*" di cui alla Direttiva sul commercio elettronico avrebbe consentito agli ISP di riconoscere *royalties* poco remunerative agli autori dei contenuti immessi in rete[353].

Per esigenze di economia di trattazione, si limita il presente campo di indagine al combinato disposto di cui agli artt. 15 e 17 che maggiormente impattano sull'attività degli ISP.

Con la prima previsione, la Direttiva in esame ha richiesto agli Stati membri di riconoscere agli editori di giornali i diritti di cui agli artt. 2 e 3, par. 2, Dir. 2001/29/CE per l'utilizzo online delle loro pubblicazioni di carattere giornalistico da parte dei prestatori della società dell'informazione. Tale prescrizione non opera con riferimento agli utilizzi privati e non commerciali così come ai collegamenti ipertestuali e agli estratti molto brevi di pubblicazioni.

Con la seconda, viceversa, si stabilisce esplicitamente che l'intermediario online effettua un "atto di comunicazione al pubblico" con disapplicazione del regime di cui all'art. 14 Dir. E-commerce, allorquando concede l'accesso al pubblico a opere protette da diritto d'autore messe in rete dai propri utenti. Per evitare di essere ritenuto direttamente responsabile per l'ospitalità di materiale protetto da diritti d'autore, l'intermediario online deve aver compito i massimi sforzi: a) per ottenere un'autorizzazione dai titolari dei diritti volta a rendere disponibili i contenuti protetti in rete; b) per evitare secondo un canone di diligenza professionale la disponibilità di opere protette in rete per le quali abbia ricevuto informazioni pertinenti e necessarie dai rispettivi titolari; c) per agire tempestivamente ai fini della disabilitazione dell'accesso e della rimozione del materiale illecito dopo aver ricevuto una segnalazione motivata da parte dei titolari dei diritti d'autore[354].

352 V. FALCE, *Direttiva Copyright 2019: fair use ed eccezioni al copyright tra esigenze di "apertura" e necessità di indirizzo*, in Filodiritto online su https://www.filodiritto.com/direttiva-copyright-2019-fair-use-ed-eccezioni-al-copyright-tra-esigenze-di-apertura-e-necessita-di-indirizzo , 22-07-2019; IFPI, "Rewarding creativity - fixing the value gap", http://www.ifpi.org/value_gap.php. AA.VV., *Automated anti-piracy systems as copyright enforcement mechanism: a need to consider cultural diversity*, in European Intellectual Property Review, 2018, 40, 4, 223 e ss. G. GHIDINI – F. BANTERLE, *A critical view on the European Commission's Proposal for a Directive on copyright in the Digital Single Market*, in Giuris. comm., 2018, 6, 921 e ss. Per value gap, si fa riferimento al divario tra i ricavi ottenuti dalle piattaforme online e i benefici guadagnati dai titolari dei diritti d'autore per lo sfruttamento delle opere dell'ingegno in rete.

353 *Contra* alcuni interpreti hanno osservato come ogniqualvolta un prodotto o servizio basato su contenuti protetti entri nel mercato sorgono quasi sempre discussioni circa la necessità di creare nuovi diritti o di estendere quelli esistenti anche a queste nuove realtà cfr. G. COLANGELO – M. MAGGIOLINO, *ISPs' copyright liability in the EU digital single market strategy*, in International Journal of Law and Information Technology, 2018, 26, 2, 156 e ss.; J. P. QUINTAIS – J. POORT, *A Brief History of Value Gaps: Pre-Internet Copyright Protection and Exploitation Models*, in P.BERNT HUGENHOLTZ (a cura di), *Copyright Reconstructed: Rethinking Copyright's Economic Rights in a Time of Highly Dynamic Technological and Economic Change*, Wolters Kluwer, 2018, 57 e ss.G. COLANGELO, *"Digital Single Market strategy", diritto d'autore e responsabilità delle piattaforme online*, in Analisi giur. Econ., 2017, 2, 633 e ss. Per le evidenze empiriche, si veda ad esempio il settore musicale dove i dati mostrano un incremento dei profitti per l'industria musicale negli Usa e in Europa proprio grazie allo sfruttamento online tramite piattaforme di streaming. A sostegno, cfr. IFPI, Global Music Report 2019, disponibile al seguente link: https://www.ifpi.org/media/downloads/GMR2019-en.pdf; CISAC, Global Collection Report 2018, disponibile al seguente link: https://www.cisac.org/CISAC-University/Library/Global-Collections-Reports/Global-Collections-Report-2018.

354 Art. 17, 4 comma, Dir. 2019/790

Per stabilire la conformazione della piattaforma alle predette condizioni di esonero dalla responsabilità, occorrerà avere riguardo alla tipologia dell'intermediario, al pubblico di riferimento, alla dimensione del servizio e alla natura dei materiali caricati dagli utenti nonché alla disponibilità di strumenti adeguati e al relativo costo per i prestatori dei servizi. La norma poi dispone una ragionevole attenuazione del regime di responsabilità a favore degli intermediari di piccole dimensioni.

Dal contenuto della Direttiva sul diritto d'autore nel mercato unico digitale, si evince quindi la previsione di un canale di tutela rafforzato per i cd. *copyright infringiments* rispetto agli altri illeciti online tramite il riconoscimento di una responsabilità diretta per i prestatori dei servizi della società dell'informazione in relazione alle attività illecite poste in essere dai fruitori dei servizi di intermediazione, le cui prime manifestazioni rinviano alle note pronunce della Corte di Giustizia dell'Unione Europea *Filmspeler*[355] e *PirateBay*[356] [357]. Con la novella normativa, quindi, l'Unione Europea ha inteso sollecitare le piattaforme online a collaborare con i titolari dei diritti d'autore attraverso la minaccia di una responsabilità diretta per le condotte degli utenti.

Sebbene la previsione di cui all'art. 17 Direttiva 790/2019 stabilisca che l'esecuzione dei citati adempimenti per la piattaforma online non comporti alcun obbligo generale di sorveglianza, sembrano sorgere evidenti difficoltà di coordinamento con l'impianto della direttiva sul commercio elettronico, specialmente con il combinato disposto di cui agli artt. 14 e 15 Dir. 2000/31/CE[358]. Invero, la piattaforma sarà inevitabilmente gravata da obblighi di filtraggio e monitoraggio in ordine alla costante conformità dei contenuti caricati dagli utenti alla normativa sul diritto d'autore per evitare di essere ritenuta responsabile di illeciti. Tali misure finiscono poi per essere generalizzate e continue là ove l'intermediario tratti principalmente opere protette da diritto d'autore.

Inoltre, si rileva che la linea di distinzione tra obbligo generale (non ammesso) e particolare (ammesso) di ricerca attiva di contenuti illeciti sembra sfumare in presenza di elevati quantitativi di materiale audio media visivo immesso in rete dagli utenti.

Allo stesso modo, pare problematica l'effettiva capacità selettiva dei meccanismi di filtraggio di distinguere tra eccezioni lecite al diritto d'autore, come utilizzi a scopo di critica o di parodia, rispetto ad ipotesi illecite di caricamento di opere protette[359]. A riguardo, si enfatizza il fatto che l'obbligo di misure proattive a carico degli

355 Corte di Giust. UE, sez. II, 26-04-2017, C-527/15 caso Stichting Brein c. Jack Frederik Wullems cd. Filmspeler

356 Corte di Giust. UE, sez. II, 14-06-2017, C-610/15 caso Stiching Brein c. Ziggo BV, XS4ALL Internet BV cd. Pirate Bay

357 S. Scalzini, "*Hyperlinking" e violazione del diritto d'autore nell'evoluzione giurisprudenziale europea*, in Analisi giur. Econ., 2017, 2, 657 e ss.

358 B. Saetta, *La nuova responsabilità degli intermediari in Europa*, 30-07-2017 disponibile al seguente link: https://bruno-saetta.it/responsabilita-provider/nuova-responsabilita-intermediari-in-europa.html

359 M. Lillà Montagnani – A. Tropova, *Safe harbours in deep waters: a new emerging liability regime for Internet intermediaries in the Digital Single Market*, in International Journal of Law and Information Technology, 2018, 26, 304. Per le Autrici, "It is highly doubtful that any filtering system currently in use, expensive or cheap, is sophisticated enough to draw the line sufficiently adequately between for instance a parody and an infringing use or any of the other exceptions provided in Article 5 of Directive 2001/29/EC and in the diverse Member States' copyright laws. What in fact exacerbates the issue is the lack of EU level harmonisation in relation to copyright exception and limitations, which

intermediari non risulta bilanciato da alcun strumento volto a salvaguardare nuovi usi legittimi di materiali coperti da diritto d'autore a causa dell'assenza di parametri certi e oggettivi su cui conformare i meccanismi di filtraggio[360].

Ed ancora, dubbi emergono con riferimento: i) alla traduzione nazionale del concetto di "*best effort*" di cui all'art. 17 Dir. 2019/790/CE[361]; ii) alla sostenibilità economica dell'utilizzo e dell'aggiornamento continuo dei meccanismi di filtraggio, giacchè vengono in rilievo valutazioni di mera opportunità economica demandate all'autonomia privata dei singoli intermediari online[362]; iii) all'individuazione dei parametri attraverso i quali valutare il rispetto degli "elevati standard di diligenza professionale di settore" e il carattere "sufficientemente motivato" delle segnalazioni dei titolari dei diritti, trattandosi di criteri potenzialmente variabili a seconda dello Stato membro di riferimento; iv) agli aggregatori automatici di contenuti e ai sistemi di intelligenza artificiale di autoapprendimento[363]; v) al pericolo di disparità di trattamento tra illeciti online a causa della previsione di una responsabilità differenziata degli ISP diversa a seconda del tipo di lesione[364].

Conclusivamente, si rileva che originariamente era compito dei titolari dei diritti individuare, segnalare e richiedere agli intermediari online la rimozione di materiale online pubblicato senza autorizzazione. Oggi, viceversa, la regolamentazione pare dirigersi verso un paradigma che pone a carico delle piattaforme online la salvaguardia dei diritti d'autore online, imponendo loro un obbligo di prevenzione di contenuti illeciti rispetto all'impostazione pregressa che subordinava l'intervento all'attualità della conoscenza degli stessi[365].

requires that, for filtering systems to be effective, they should ascertain on a case by case basis the infringing nature of a content in a geographically sound manner, i.e. taking into account the diverse existing national exception regimes".

360) M. Gambini, *Intelligenza artificiale e diritto – algoritmi e sicurezza*, cit., 1663 e ss.

361 M. Bixio, *La Direttiva Copyright tra proporzionalità e best effort. I nodi da sciogliere in sede di recepimento*, in DIMT disponibile al seguente link https://www.dimt.it/news/la-direttiva-copyright-tra-proporzionalita-e-best-effort-i-nodi-da-sciogliere-in-sede-di-recepimento/ Secondo l'opinione di autorevoli studiosi, il concetto dovrebbe essere tradotto con la dicitura di "massimi sforzi", "migliori sforzi" o "ogni ragionevole sforzo". Non è una questione meramente lessicale, giacchè la traduzione del concetto finisce per impattare a monte sull'interpretazione giuridica nelle corti giudiziarie e a valle sui diritti dei cittadini. Ciò nondimeno, pare inevitabile che l'effettivo compimento di massimi sforzi da parte del provider andrà valutato in concreto in combinazione con, tenendo conto dei principi di proporzionalità, di ragionevolezza, dei vari interessi in gioco e di tutte le specificità del caso.

362 C. Angelopoulos – L. Bently – S. van Gompel – M. Husovec – M. Kretschmer – M. Senftleben – S. Stalla-Bourdillon, *The Copyright Directive: Misinformation and Independent Enqudeeiry*, 29 giugno 2018, disponibile al seguente link: https://www.create.ac.uk/wp-content/uploads/2018/06/Academic_Statement_Copyright_Directive_29_06_2018.pdf.

363 S. Scalzini, "*Hyperlinking" e violazione del diritto d'autore nell'evoluzione giurisprudenziale europea*, cit., 660 e ss ; F. Banterle, *Linking a contenuti protetti da diritto d'autore nella giurisprudenza della Corte di Giustizia. Atto terzo*, Gs Media, in Riv. Dir. ind., 2017, 3, 475 e ss.

364 M. Lillà Montagnani – A. Tropova, *Safe harbours in deep waters: a new emerging liability regime for Internet intermediaries in the Digital Single Market,* cit., 310.

365 K. Erickson – M. Kretschmer, *Empirical, Approaches to Intermediary Liability*, cit., 3 e ss.

4.5.4 La proposta di Regolamento sui servizi digitali cd. Digital Service Act

In data 15 dicembre 2020, la Commissione Europea ha adottato all'esito di consultazioni pubbliche e discussioni tra vari attori a tutti i livelli una proposta di Regolamento, destinata a polarizzare l'attenzione degli interpreti nel prossimo periodo per le sue inevitabili ricadute applicative sulla responsabilità degli Internet Service Provider[366]. Si tratta del Digital Service Act (cd. DSA)[367], la cui bozza già solleva diversi spunti di riflessione ed occasioni di approfondimento per il suo impatto dirompente sulla disciplina del commercio elettronico.

Invero, l'iniziativa legislativa in esame costituisce la rilettura in chiave moderna della Direttiva sul commercio elettronico alla luce dei cambiamenti e sviluppi che hanno caratterizzato l'ecosistema digitale all'indomani del secondo millennio. Come già evidenziato nei precedenti paragrafi, l'originaria direttrice politica dell'Unione Europea era stata quella di incentivare quanto più possibile con la Direttiva 2000/31/CE la crescita e lo sviluppo dei mercati digitali mediante la predisposizione di una cornice normativa minima. Con il progredire degli anni, si è però registrata l'affermazione dei cd. giganti del web, la preponderanza dei *social networks* nella diffusione delle informazioni, la nascita della "*data driven economy*", la digitalizzazione di molti aspetti della vita quotidiana, la sistematica intermediazione delle piattaforme online nell'esercizio di attività economiche e nell'erogazione di servizi in rete, la proliferazione di contenuti digitali illegali e la disseminazione di *fake news*.

Accanto ai molteplici benefici introdotti dall'avvento della rete, sono quindi sorti nuovi rischi e insidiose criticità che richiedono un intervento risolutore da parte del legislatore comunitario al fine di offrire una risposta omogenea su tutto il territorio dell'Unione Europea.

In questo contesto, la proposta di Regolamento della Commissione Europea rappresenta un momento di svolta, mirando a costituire un passo in avanti nella disciplina delle attività online. In particolare, si intendono perseguire due obiettivi[368]. Da un lato, l'ambizione è quella di creare uno spazio digitale più sicuro, dove tutti i diritti e le libertà fondamentali degli utenti siano protetti. Dall'altro, il fine è quello di delineare un *level playing field* che favorisca all'interno dell'Unione Europea l'innovazione, la crescita e la concorrenza tra le piattaforme online all'insegna della costruzione di un mercato unico digitale cd. Digital Single Market.

Nell'ambito delle numerose novità contenute nel Digital Service Act[369], pare opportuno soffermarsi ai fini del presente campo di indagine sulla riproposizione della

366 A. GAMBINO – D. TUZZOLINO, *Il Digital Service Act tra responsabilità e governance. Commento alla proposta di Regolamento*, disponibile al seguente link https://www.dimt.it/news/il-digital-services-act-tra-responsabilita-e-governance-commento-alla-proposta-di-regolamento/

367 Proposal for a Regulation of the European Parliament and of the Council on a single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0825&qid=1610031765022&from=EN

368 https://ec.europa.eu/digital-single-market/en/digital-services-act-package

369 https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en

tripartizione (*mere conduit*, *caching* e *hosting provider*) degli Internet Service Provider, nonostante le spinte verso la codificazione di nuove figure di intermediari online. Allo stesso modo, si riconferma il *safe harbour* proprio della Direttiva sul commercio elettronico per cui l'intermediario non è responsabile là ove: 1) non abbia conoscenza di attività illecite o presunte tali commesse dai propri utenti; o 2) abbia rimosso tempestivamente i contenuti illeciti immessi in rete successivamente all'acquisizione della conoscenza degli stessi. Fortemente innovativa si atteggia l'esplicita esenzione di responsabilità a favore delle piattaforme online per l'adozione di misure proattive finalizzate al contrasto di contenuti illegali in rete sulla falsariga della "*Good samaritan clause*" del modello americano. In linea con l'art. 15 Dir. 2000/31/CE, viene riconfermato il divieto di obblighi generali di monitoraggio sulle informazioni trattate e di ricerca attiva di contenuti illeciti.

Non trascurabile è poi la previsione di obblighi di *due diligence* a carico delle piattaforme online che si snodano secondo una logica progressiva e cumulativa in considerazione del fatto che la loro pregnanza aumenta parallelamente alle dimensioni dell'intermediario. All'interno dell'Unione Europea, gli ISP dovranno nominare un rappresentante legale e avere un "*punto di contatto*", onde favorire le comunicazioni con il pubblico, le autorità nazionali ed organi sovranazionali.

Con accentuata enfasi, la proposta di Regolamento sollecita: i) la chiara definizione da parte delle piattaforme dei termini di utilizzo dei loro servizi online; ii) la pubblicazione di un report dettagliato e comprensibile su ogni attività intrapresa nel trattamento dei contenuti almeno una volta l'anno, ivi compresi gli ordini di rimozione provenienti dalle autorità competenti e le segnalazioni ricevute dagli utenti; iii) l'istituzione di meccanismi di *notice and action,* volti a consentire agli utenti di segnalare la presenza di contenuti illeciti in rete[370]; iv) l'introduzione di sistemi di *internal complaint-handling system* e di obblighi motivazionali sottesi alla disabilitazione di certi contenuti; vi) l'elaborazione di meccanismi stragiudiziali per la risoluzione delle controversie.

Per le piattaforme di maggiori dimensioni (cd. *very large online platform*), il DSA impone la realizzazione di procedure di *risk assessment,* l'adozione di misure di mitigazione dei rischi, la sottoposizione al controllo di organismi di *audit* terzi e indipendenti, l'illustrazione all'interno della sezione dei termini di utilizzo dei servizi online del funzionamento dei cd. *recommender system* e dei meccanismi pubblicitari. A tutela della trasparenza, è poi prevista la *disclosure* dei dati a favore di autorità nazionali di controllo, la pubblicazione di report periodici relativi ad attività criminali, l'adozione di codici di condotta. A determinate condizioni, è contemplata la condivisione dei dati da parte delle piattaforme online con le autorità competenti nazionali e sovranazionali nonché con i cd. *vetted researchers*. Ed ancora, la proposta di Regolamento sollecita la

370 In merito, va osservato che si registra per la prima volta una disciplina dettagliata della procedura di comunicazione stragiudiziale da parte dei fruitori dei servizi di intermediazione online a cominciare dall'indicazione delle ragioni dell'asserita illiceità del contenuto e dell'URL del materiale in questione fino alle generalità e alla buona fede dell'istante. Ed ancora, l'ISP deve informare l'istante dell'avvenuta ricezione della segnalazione e delle relative azioni intraprese. La bozza di Regolamento evidenzia che la comunicazione stragiudiziale è idonea a determinare nell'intermediario quella conoscenza manifesta o consapevolezza che innescano l'obbligo di tempestiva rimozione dei contenuti illeciti.

nomina di un *compliance officer* con compiti di monitoraggio e sorveglianza dall'interno. A livello di *governance*, si stabilisce l'istituzione del *Digital Service Coordinator*[371] e l'*European Board for Digital Service*[372]. Nel nuovo quadro normativo, la Commissione si riserva ampi poteri tanto di controllo quanto di sanzione.

A prima impressione, la bozza del Digital Service Act pare rievocare l'architettura del recente GDPR non solo per l'identità dello strumento normativo prescelto in sede comunitaria ma anche per la centralità conferita ai principi di *accountability, due diligence* e *compliance*. In questo senso, evidente è l'inversione di tendenza rispetto al *lasseiz faire* devoluto dalla Direttiva sul commercio elettronico ai prestatori dei servizi della società dell'informazione in ordine ai meccanismi di funzionamento, gestione e organizzazione della piattaforma online. Per contro, il Digital Service Act riconferma la struttura della Direttiva 2000/31/CE sotto vari aspetti a partire dalla riproposizione della tripartizione degli ISP, dalla responsabilità colposa degli intermediari online fino al divieto di un obbligo generalizzato di monitoraggio di tutte le informazioni trattate e dei contenuti immessi in rete dagli utenti. Evidente è l'intento di un adeguamento e aggiornamento piuttosto che di uno smantellamento della Direttiva sul commercio elettronico.

Tra le varie novità, positiva è l'esenzione dalla responsabilità per le *voluntary own-initiative investigations and legal compliance*, la trasparente preventiva definizione delle condizioni e termini di utilizzo dei servizi di intermediazione online, nonché la chiara predeterminazione dei sistemi di *notice and action*. Suscita invece dubbi e perplessità la previsione di alcuni obblighi trasversali particolarmente pregnanti per tutti gli intermediari che rischiano di danneggiare le piccole e medie imprese con costi organizzativi di rilievo, finendo così per impedire loro l'accesso al mercato. Il pensiero va all'istituzione per tutti gli ISP di un "punto di contatto" e alla nomina di un rappresentante legale all'interno del territorio europeo. Condivisibile è invece l'approccio differenziato e graduato per l'adozione di alcuni meccanismi di *due diligence*, variabili a seconda della dimensione della piattaforma online. In sostanza, encomiabile è il fatto che la bozza normativa abbia recepito molte istanze provenienti dagli studiosi a partire dall'armonizzazione delle regole di esenzione dalla responsabilità nonché degli obblighi di *due diligence* e *due process* nel segno di un rinnovato quadro normativo omogeneo in tutta l'Unione Europea. Tuttavia, bisogna attendere la conclusione dell'iter legislativo all'esito della dialettica tra Parlamento Europeo e Consiglio per esprimere un giudizio finale sull'effettività del Digital Service Act.

371 Si tratta di un'autorità scelta dai vari Stati membri con il compito di vigilare sull'applicazione del Regolamento attraverso la titolarità di vari poteri, chiamata a coordinarsi con i propri omologhi degli altri Paesi, European Board e con le altre competenti autorità nazionali

372 E' un advisory group, formato da alcuni DSC con l'incarico di monitorare l'attuazione del Regolamento e di informare la Commissione sulle varie questioni emergenti relative all'applicazione del DSA

4.6 Sull'adozione di misure proattive e meccanismi di filtraggio dei contenuti caricati in rete

Dagli interventi normativi passati in rassegna, emerge l'odierna tendenza trasversale a favore dell'adozione di misure proattive di filtraggio da parte dei prestatori[373]. La ragione giustificativa riposerebbe nell'asserito interesse complessivo della società a veder rimuovere i contenuti illegali il più rapidamente possibile, prima ancora della loro stessa messa a disposizione in rete. Si tratta di un radicale cambio di rotta rispetto al caposaldo della Direttiva E-commerce relativo al divieto di un obbligo generale di rimozione *ex ante* dei contenuti caricati online dagli utenti. Tale percorso intrapreso dalle Istituzioni Europee sembra però condurre all'affermazione di un sistema cd. "*automated or algorithmic enforcement*", cui si ricollegherebbe la creazione di un "*private ordering and private control*" facente capo ad un manipolo di imprese private[374].

In merito alla conciliabilità di tali strumenti con la Direttiva E-commerce, la Commissione europea ha affermato che l'adozione di misure proattive volte a prevenire il caricamento di contenuti illeciti è conforme con la previsione di cui all'art. 15 Dir. 2000/31/CE e non comporta di per sé la decadenza del *safe harbour*[375]. Sebbene il ricorso a misure proattive non determini l'inquadramento dell'intermediario online come *hosting provider* attivo, la conoscenza della presenza di contenuti illeciti all'esito dell'impiego di tecnologie automatiche impone comunque alla piattaforma di agire tempestivamente ai fini della loro rimozione, là ove intenda beneficiare del meccanismo delle esenzioni dalla responsabilità.

Nonostante le rassicurazioni della Commissione Europea, la tendenza all'adozione di misure proattive suscita alcune perplessità[376]. Tanto si ricollega al fatto che Internet costituisce il principale meccanismo di disintermediazione e di libero mercato, ispirato alla neutralità tecnologica[377]. Per contro, l'attuale imposizione generalizzata di meccanismi di filtraggio finirebbe per devolvere la gestione della rete in capo a pochi grandi operatori a causa dell'elevato costo di sviluppo e di utilizzo di tali sistemi di selezione dei contenuti[378]. Come argomentato da Balkin, "Currently the Internet is

373 M. Gambini, *Intelligenza artificiale e diritto – algoritmi e sicurezza*, cit., 1660 e ss.

374 M. Sag, Internet Safe Harbors and the Transformation of Copyright Law, cit., 500 e ss.

375 Comunicazione (UE) 2017/555 della Commissione del 28 settembre 2017 al Parlamento Europeo, al Consiglio, al Comitato Economico e sociale Europeo e al Comitato delle Regioni Lotta ai contenuti illeciti online. Verso una maggiore responsabilizzazione delle piattaforme online, punto 11.

376 G. De Gregorio, *Expression on Platforms: freedom of Expression and ISP liability in The European digital Single Market*, cit., 204 e ss. Per l'Autore, "This system allows online platforms to exercise their discretion in removing flagged or signaled contents whose illicit nature is not always so evident, especially in the case in which fake news is involved. This framework is clearly dangerous for the protection of fundamental rights considering that the enforcement of such rights is left to the discretion of private actors without any public safeguard. Moreover, the development of new technologies, especially those embed algorithms and artificial intelligence systems, has made even more complex understandings the role of such actors in organizing and selecting contents in the digital environments, raising evident concerns related to users' right of free speech, privacy and human dignity".

377 Y. Benkler, *The Wealth of Networks: how social production transforms markets and freedom*, 2007, Yale University Press, 71 e ss.

378 U. Dolata, *Apple, Amazon, Google, Facebook, Microsoft: Market concentration competition - innovation strategies*, in Stuttgarter Beiträge zur Organisations - und Innovations forschung SOI Discussion Paper from Institut für Sozialwissenschaften, Universität Stuttgart, 2017, 1, 5 e ss.

mostly governed by the values of the least censorious regime – that of the United States. If nation states can enforce global filtering, blocking, and delinking, the Internet will eventually be governed by the most censorious regime. This will undermine the global public good of a free Internet"[379]. Invero, la previsione di meccanismi di filtraggio dei commenti degli utenti sembra oramai assurgere a nuovo paradigma per i cd. "partecipatory online media"[380].

In sostanza, occorre prudenza nell'incentivare l'utilizzo di misure proattive poiché non si conoscono ancora gli effetti di questa soluzione tra tutti i vari *stakeholders*. Ciò è dovuto alla segretezza delle regole di funzionamento delle piattaforme online, rese inaccessibili dall'esterno, le quali suscitano evidenti preoccupazioni in punto di rispetto dei valori della democrazia[381]. Se la circolazione dei contenuti in rete è governata dagli algoritmi, l'individuazione di una soluzione rimediale alla proliferazione di attività illecite necessiterebbe di una previa comprensione di questi meccanismi. La conoscenza delle procedure di funzionamento degli algoritmi degli intermediari online è però spesso ostacolata dalle stesse piattaforme online che oppongono barriere contrattuali e segreti commerciali[382]. Questa situazione costituisce l'emblema della cd. *black box society*[383].

A livello legislativo, quindi, maggiore attenzione andrebbe rivolta al funzionamento degli algoritmi sottesi all'agire delle piattaforme online. Non avrebbe senso, infatti, porre sotto osservazione solo il risultato finale dell'attività di intermediazione online senza un opportuno approfondimento dei meccanismi proattivi di filtraggio e delle altre misure automatiche[384]. Per intervenire, bisogna prima conoscere. L'attuale tendenza, viceversa, pare essere quella di intervenire prima e senza conoscere.

Peraltro, il ricorso a meccanismi di filtraggio rischia di incidere negativamente tanto sulla libertà di manifestazione del pensiero di cui all'art. 11 CDFUE, poiché potrebbe condurre ad una rimozione mirata dei contenuti immessi in rete dagli utenti sulla base di logiche di settore determinate da attori privati, quanto sulla la libertà di

379 J. M. Balkin, *Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation*, in University of California Davis Law Review, 2018, 51, 1206 e ss.

380 P. Valcke -A. Kuczerawy – P. J. Ombelet, *Did the Romans get it right? What Delfi, google, Ebay, and UPC TeleKabel Wien have in common*, cit., 107 e ss.;

381 Si segnala la recente lettera inoltrata da un gruppo di professori universitari a Google al fine di ottenere maggiore trasparenza circa la trattazione delle richieste di deindicizzazione e di oblio inoltrate dagli utenti J. Kiss, *Dear Google: Open Letter from 80 Academics on "Right to be Forgotten"*, 14-05--2015, https://www.theguardian.com/technology/2015/may/14/dear-google-open-letter-from-80-academics-on-right-to-be-forgotten

382 M. Perel – N. Elkin Koren, *Black Box Tinkering: Beyond Disclosure in Algorithmic Enforcement*, in Florida Law Review, 2017, 69, 184 e ss.

383 F. Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information*, Cambridge, 2015

384 D. K. Citron, *Extremist Speech, Compelled Conformity, and Censorship Creep*, in Notre Dame Law Review, 2018, 93, 3, 1035 e ss. In particolare, l'Autore ha evidenziato alcuni profili meritevoli di attenzione derivanti dall'attribuzione di oneri di vigilanza e di filtraggio in capo ai provider come l'ambiguità definitoria del concetto di hate speech, la rimozione di default dei contenuti segnalati per evitare ogni controversia e la corrispondente opacità delle procedure di cancellazione adottate dai provider; M. Thompson, *Beyond Gatekeeping: The Normative Responsibility of Internet Intermediaries*, cit., 795 e ss. "The limitation [of discussions on intermediary liability] is that such discussions have tended so far to focus predominantly on the outcomes of intermediaries' decisions, rather than on the reasons used by intermediaries in reaching them. In other words, those are discussions founded on the adoption of factual, outcomes-based perspectives, and on the consequential motives for pursuing these, rather than on a more in-depth inquiry concerning their normative underpinnings.

impresa di cui all'art. 16 CDFUE, perché le piccole imprese potrebbero uscire dal mercato a causa degli elevati costi dei meccanismi di filtraggio e dei rischi legali connessi all'omessa rimozione *ex ante* di materiale illegale[385].

Non trascurabile è poi il fatto che la qualificazione di certi contenuti immessi in rete come legali o illegali andrebbe riservata esclusivamente alle Corti giudiziarie e ad altri attori istituzionali anzichè alle decisioni private degli intermediari online[386]. Diversamente opinando, si corre il pericolo di rendere le piattaforme digitali custodi della democrazia e censori della legalità della rete attraverso l'esercizio di poteri insindacabili e imprevedibili senza i controlli tipici degli ordinamenti democratici.

L'odierna tendenza trasversale a favore dell'adozione di misure proattive di filtraggio da parte dei prestatori procede di pari passo con l'idea di abolire il regime di *safe harbour* degli ISP. Come suesposto, l'esistenza di quest'ultimo è centrale per l'operatività delle piattaforme online e per l'ampiezza dei servizi di intermediazione online. Ne deriva che occorre cautela e prudenza nella revisione del regime di responsabilità degli ISP in ragione delle molteplici implicazioni pratico applicative non solo economiche e giuridiche ma anche sociali ed etiche[387]. Da un punto di vista pratico, poi, qualsiasi intervento normativo a livello di Unione Europa in materia di responsabilità degli intermediari è destinato a riflettersi non solo oltreoceano ma anche sull'intero ecosistema digitale, stante il carattere aterritoriale dei servizi di intermediazione online. Ciò nondimeno, l'attuale dibattito sull'abolizione del *safe harbour* sembra denso di retorica e povero di fatti[388].

In sostanza, l'abolizione del regime di *safe harbour* provocherebbe un drammatico danno alla competizione, all'innovazione e alla libertà di manifestazione del pensiero e complessivamente allo sviluppo di Internet. Tanto deriva dalla considerazione per cui l'eliminazione del *safe harbour* potrebbe tradursi non in un depotenziamento bensì in un rafforzamento del potere di mercato delle piattaforme online con un costo significativo per quei diritti e valori che invece si intendono proteggere.

Ed ancora, l'attuale direttrice politica e normativa eurounitaria pare condurre verso una categoria "amorfa" di responsabilità degli ISP, svincolata da parametri legali

385 G. COLANGELO, "Digital Single Market strategy", diritto d'autore e responsabilità delle piattaforme online, cit.; 623 e ss.; J. URBAN – J. KARAGANIS – B. SCHOFIELD, Notice and Takedown: Online Service Provider and Rightsholder Accounts of Everyday Practice, in Journal Copyright Society of USA, 2017, 64, 400. Secondo gli Autori, "In some striking cases, it appears that the vulnerability of smaller OSPs to the costs of implementing large-scale notice and takedown systems and adopting expensive DMCA Plus practices can police market entry, success, and competition"

386) C. OMER, *Intermediary Liability for Harmful Speech: Lessons from Abroad*, in Harvard Law Journal, 2014, 28, 1, 315 e ss.

387 M. THOMPSON, *Beyond Gatekeeping: The Normative Responsibility of Internet Intermediaries*, in Vanderbilt Journal Entertainment & Technology Law, 2016, 18, 4, 797 e ss. Per l'Autore, "there is great consequence in the actions undertaken by intermediaries. Intermediaries are the designers of the heart valves through which the lifeblood of our information environment flows. Actions they take or refrain from taking can fundamentally alter medium and message, structure and content of information we impart and receive. In other words, intermediaries can transform the very constitution of the environments we inhabit and the lives we live therein". N. ELKIN KOREN – Y. NAHMIAS - M. PEREL, *Is It Time to Abolish Safe Harbor? When Rhetoric Clouds Policy Goals*, online su https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3344213 , 50 e ss. "Abolishing the safe harbor and making platforms liable for users' content could end up strengthening their economic power instead of defusing it, at a dangerous cost to the values we seek to protect".

388 G. COLANGELO, *"Digital Single Market strategy", diritto d'autore e responsabilità delle piattaforme online*, cit., 632 e ss.

e da esenzioni, che incentiva gli intermediari ad autointervenire al di fuori di meccanismi istituzionali per scongiurare presunte attività illecite online a monte e successivi eventuali addebiti a valle. Così operando, tuttavia, si corre il rischio di eludere attraverso l'*enforcement* tecnologico i principi del giusto processo e di ledere le libertà fondamentali[389].

Nonostante le forti pressioni di gruppi di settore circa l'eliminazione del *safe harbour*, evidenze empiriche hanno mostrato invece il buon funzionamento delle procedure di *notice and takedown*[390]. Ne deriva che l'efficientamento della lotta alle attività illegali in rete dovrebbe passare attraverso l'affinamento della configurazione delle procedure di segnalazione e di rimozione dei contenuti illeciti piuttosto che tramite la cancellazione *tout court* del meccanismo delle esenzioni dalla responsabilità. Con riguardo alle procedure di *notice and take down*, tuttavia, sorgono alcuni non trascurabili nodi relativi all'impenetrabilità dall'esterno delle modalità di funzionamento degli algoritmi[391]. In proposito, occorrerebbe una trasparente apertura e condivisione dei metodi di trattamento delle informazioni da parte delle piattaforme online.

In questo contesto, le politiche legislative europee sembrano peccare da una parte per difetto e dall'altra per eccesso. Sotto il primo profilo, infatti, non prendono minimamente in considerazione i comportamenti degli utenti, responsabili primari della diffusione di contenuti illegali in rete. Sotto il secondo profilo, invece, finiscono per gravare con pesanti oneri di diligenza gli ISP in relazione a condotte illecite perpetrate dai fruitori dei servizi internet.

4.7 Verso una forma di responsabilità partecipata e condivisa

Da quanto suesposto, si ricava tutta la complessità della questione relativa alla regolamentazione delle piattaforme online con particolare riferimento all'individuazione della linea di demarcazione tra la responsabilità degli Internet provider e quella degli utenti fruitori dei servizi della società dell'informazione. L'analisi di tale problematica risulta, poi, aggravata dalla necessità di salvaguardare la funzione sociale

389 G. De Gregorio, *Expression on Platforms: freedom of Expression and ISP liability in The European digital Single Market*, cit., 214 e ss. Secondo l'Autore, "Private actors are obliged to respect fundamental rights when they are expressed in legal acts issued by public bodies. This would mean that...the introduction of "due process" obligations would allow users to rely on new rights via-à-vis online platforms"; G. Frosio, *Why keep a dog and bark yourself? From intermediary liability to responsibility*, cit., 3 e ss. Per l'Autore, "due process and fundamental guarantees get mauled by technological enforcement, silencing speech according to the mainstream ethical discourse and trampling over the emerging idea of internet as fundamental right".

390 K. Erickson – M. Kretschmer, *Empirical, Approaches to Intermediary Liability*, cit., 18 e ss. Per gli Autori, "The concept of providing safe harbour to innovators while enabling a mechanism for rightsholders to protect their copyrights, appears to be achieving its purpose. Links to infringing materials are being pushed out of the top search results, infringing videos are being removed from sharing websites, and institutions are removing infringing materials hosted on their networks".

391 M. Perel – N. Elkin Koren, *Black Box Tinkering: Beyond Disclosure in Algorithmic Enforcement*, cit., 184 e ss. Come evidenziato dalle Autrici, "proper accountability mechanisms are vital for policymakers, legislators, courts and the general public to check algorithmic enforcement. Yet algorithmic enforcement largely remains a black box. It is unknown what decisions are made, how they are made, and what specific data and principles shape them".

esercitata dalle piattaforme online che consentono l'esercizio di diritti e libertà fondamentali in rete.

Nell'ecosistema digitale, gli ultimi interventi normativi eurounitari sembrano propendere verso un modello di responsabilità accentrata esclusivamente in capo ai prestatori della società dell'informazione. Tale direttrice di politica legislativa riposa su ragioni pratiche per cui risulta più agevole, efficiente e veloce ritenere imputabile un unico attore anziché distribuire il peso di attività illecite tra più soggetti.

Tuttavia, gli intermediari online sono solo parzialmente in grado di controllare la condotta degli utenti sulla rete. Pertanto, non risulta mutuabile per i prestatori della società dell'informazione un regime di responsabilità simile a quello dell'editore di un giornale o del datore di lavoro rispetto alle condotte perpetrate dai propri dipendenti. Nel caso di illeciti online, infatti, viene in rilievo l'attività di una molteplicità di attori cui corrisponde tendenzialmente l'impossibilità di identificare un singolo colpevole[392].

Ne deriva che l'allocazione della responsabilità per gli illeciti online non può non tener conto dell'intervento di una pluralità di protagonisti che incidono in vario modo sul problema ovvero sulla risoluzione del problema. A tal proposito, alcuni autori hanno etichettato questa situazione come un problema di "molte mani" e di "molte regole"[393]. Ciò posto, la soluzione non può non passare attraverso un coinvolgimento di tutti gli attori in causa per il tramite dell'elaborazione di un regime di responsabilità condivisa[394]. In questo contesto, sembra necessaria l'individuazione di un punto di equilibrio tra i vantaggi e gli svantaggi dell'adozione di misure proattive da parte degli intermediari online. Invero, l'elaborazione di un certo regime di responsabilità connesso allo svolgimento di una determinata attività si traduce in una voce di costo che può quindi dissuadere i piccoli operatori online ad entrare nel mercato[395].

Per l'effetto, alcuni autori sono giunti ad affermare che non esiste "one size fits all liability rule for all types of intermediaries and all types of harm"[396]. Invero, l'imposizione uguale e indiscriminata di elevati livelli di diligenza a carico di tutti i prestatori di servizi della società dell'informazione potrebbe rappresentare una barriera

392 Una situazione simile è rinvenibile nel caso del cambiamento climatico e del riscaldamento globale così come di danni ambientali.

393 A. De Streel - M. Buiten – M. Peitz, *Liability of online hosting platforms should exceptionalism end?*, cit., 6 e ss. Per "molte mani", si allude al fatto che vengono in rilievo nel caso di illeciti online una pluralità di attori pubblici e privati. Per "molte regole", si ha riguardo al fatto che la revisione della Direttiva sul commercio elettronico costituisce solo un tassello di un più ampio mosaico per rendere effettivamente sicuro l'ecosistema digitale.

394 N. Helberger - J. Pierson -T. Poell, *Governing online platforms: from contested to cooperative responsibility*, in The Information Society, 2018, 34, 3 e ss.

395 A riguardo, occorre confrontare congiuntamente: i) il costo dell'adozione di misure precauzionali con quelli degli strumenti a disposizione delle parti offese e degli utenti in modo tale da determinare quale categoria soggettiva sia in grado di sopportare meglio il peso economico delle misure di contrasto agli illeciti online; ii) la tipologia e l'estensione dell'illecito nonché la natura della parte danneggiata, poichè quanto maggiore è la gravità e la dispersione del danno nonché la vulnerabilità della parte offesa tanto più valide sono le ragioni sottese alla predisposizione di misure di prevenzione. Inoltre, si evidenzia che la responsabilità degli ISP non può essere dilatata ad un livello tale per cui i benefici derivanti dalla cancellazione ex ante di contenuti legali siano prevalenti rispetto ai costi dell'omessa eliminazione ex post di materiale illegale. Diversamente opinando, sorgerebbe un pericolo di cd. over removal che incentiverebbe la cancellazione anche di materiali di dubbia liceità al fine di evitare la successiva insorgenza della responsabilità con corrispondente nocumento alla libertà di espressione in rete. È il cd. "dilemma del provider"

396 A. De Streel - M. Buiten – M. Peitz, *Liability of online hosting platforms should exceptionalism end?*, cit., 8 e ss.

all'ingresso di nuovi intermediari online con un detrimento per l'innovazione e la competizione. Ne deriva che le Istituzioni sovranazionali e nazionali sono chiamate a stabilire un quadro normativo che tenga in giusta considerazione la funzione e il peso di ciascun attore nell'elaborazione di una forma di responsabilità distribuita in capo ai vari soggetti.

Ai fini di un ambiente digitale più sicuro, occorrerebbe che l'intera collettività di utenti della rete si comporti autonomamente in modo più responsabile, prestando attenzione ai contenuti immessi online ovvero a quelli condivisi con altri utenti. Per tal motivo, bisogna incentivare le piattaforme online a collaborare con gli utenti attraverso campagne di informazione, educazione e formazione con il fine di indirizzare il loro comportamento in rete verso pratiche virtuose. Nell'attività di sensibilizzazione del comportamento degli utenti in rete, poi, le piattaforme online dovrebbero enfatizzare maggiormente i cd. termini di utilizzo, volti a consentire una percezione chiara dei diritti e dei doveri derivanti dalla fruizione dei servizi di intermediazione. In proposito, si segnalano alcune recenti iniziative poste in essere dagli intermediari online[397].

Nell'attività di contrasto agli illeciti online, bisognerebbe poi porre maggiore attenzione all'architettura e al funzionamento delle piattaforme[398]. Si tratta, sostanzialmente, della cd. "prospective design responsibility"[399] sulla falsariga di quanto avvenuto in materia di trattamento dei dati mediante i principi di "privacy by design" e "privacy by default"[400] attraverso "l'estensione totalizzante dell'autoresponsabilità in ogni fase della vita dell'impresa"[401]. Con riferimento al presente campo di indagine, pertanto, gli intermediari online dovrebbero essere tenuti a modellare i meccanismi di filtraggio dei contenuti alla stregua dei principi di prevenzione, precauzione, adeguatezza, proporzionalità e minimizzazione dei rischi come avviene nell'ambito del trattamento dei dati, provvedendo a riesaminare e aggiornare nonché testare costantemente l'efficacia delle misure proattive[402]. Così operando, si intende stabilire un collegamento tra gestione del rischio e il funzionamento degli Internet provider nell'ottica di una

397 A titolo esemplificativo, si cita la diffusa creazione di un servizio clienti all'interno delle piattaforme e-commerce volto ad agevolare la comprensione da parte degli utenti dei termini di servizio dell'operatore con l'obiettivo di migliorare il rapporto con la clientela e prevenire pregiudizi ai fruitori della piattaforma.

398 M. THOMPSON, *Beyond Gatekeeping: The Normative Responsibility of Internet Intermediaries*, cit., 817 e ss. Per l'Autore, "Internet intermediaries are designers of technological platforms; they program their websites and services in different ways and make choices that are as much a matter of business and law as they are a matter of technology. When intermediaries enable their technological platforms to host certain types of content, or to take others down, they define what uses of their technological platforms are possible or proper—physically and normatively—and embed such definitions in the language of (and conceptions about) their software. Those definitions may happen more generally and spontaneously, at different moments of the life of their platform, or they may be provoked by specific complaints from an Internet user or by a court order. But, in each circumstance, a transformation is intentionally and physically operated in the world of bits, which, in turn, goes on to influence further uses of the technological platform and future actions by its users—and their reasons for choosing these"

399 M. THOMPSON, *Responsibility for failures of government: The problem of many hands*, in The American Review of Public Administration, 44, 3, 261 e ss.

400 F. BRAVO, *L'«architettura» del trattamento e la sicurezza dei dati e dei sistemi*, in V. CUFFARO – R. D'ORAZIO – V. RICCIUTO (a cura di), *I dati personali nel diritto europeo* (a cura di), Torino, 2019, 793 e ss.

401 L. D'AGOSTINO, *La tutela penale dei dati personali nel riformato quadro normativo: un primo commento al d.lgs. 10 agosto 2018, n. 101*, in Arch. Pen., 2019, 1, 52

402 M. GAMBINI, *Intelligenza artificiale e diritto – algoritmi e sicurezza*, cit., 1667 e ss.

maggiore *accountability* dei prestatori nella lotta agli illeciti online. La crescente attenzione verso una responsabilità organizzativa è maturata di recente anche a livello eurounitario ove è stata da poco approvata la Direttiva 2018/1808[403] che ha modificato la Direttiva 2010/13/UE[404] sui servizi audio media visivi ed ha delineato una forma di responsabilità cd. organizzativa delle piattaforme online[405].

Ed ancora, occorre sollecitare gli intermediari online a tenere in considerazione valori pubblici nell'elaborazione della forma organizzativa della piattaforma tramite la valorizzazione di regole procedurali incentrate sul giusto processo nonchè di meccanismi di controllo e di revisione umana. Ciò si giustifica in ragione del fatto che l'architettura di una piattaforma e le sue modalità di funzionamento, comprese le procedure di *notice and take down*, sono in grado di influenzare il comportamento degli utenti e dei titolari dei diritti.

L'adozione dei presidi di cui sopra dovrebbe essere trasversale e comune a tutte le piattaforme. Diversamente opinando, la disabilitazione di certi contenuti illeciti in una piattaforma non ne impedirebbe la riproposizione da un'altra parte. L'idea di una responsabilità "collaborativa" e "partecipata" delle piattaforme online ha trovato un terreno fertile anche all'interno del Comitato Economico e Sociale dell'Unione Europea, secondo cui gli ISP non possono essere ritenuti i responsabili esclusivi della proliferazione di attività illecite online ma è ragionevole attendersi che gli Internet provider investano risorse volte a guidare il comportamento degli utenti in rete [406]. A riguardo, l'OSCE però ammonisce che "making private intermediaries more transparent and accountable is a legitimate aim to be pursued by participating States through appropriate means. However, this must not lead to excessive control by public authorities over online content"[407].

In sostanza, il contrasto alle attività illecite online pare esigere un cambio di paradigma attraverso una maggiore valorizzazione del sistema di funzionamento organizzativo e strutturale delle piattaforme[408]. Ciò deriva dal fatto che la realizzazione di

403 Direttiva 2018/1808/UE del Parlamento europeo e del Consiglio del 14 novembre 2018 recante modifica della direttiva 2010/13/UE, relativa al coordinamento di determinate disposizioni legislative, regolamentari e amministrative degli Stati membri concernenti la fornitura di servizi di media audiovisivi (direttiva sui servizi di media audiovisivi), in considerazione dell'evoluzione delle realtà del mercato

404 Direttiva 2010/13/UE del Parlamento europeo e del Consiglio del 10 marzo 2010 relativa al coordinamento di determinate disposizioni legislative, regolamentari e amministrative degli Stati membri concernenti la fornitura di servizi di media audiovisivi (direttiva sui servizi di media audiovisivi)

405 In particolare, l'intento è stato quello di collegare la responsabilità degli intermediari online non all'ospitalità dei contenuti caricati dagli utenti bensì al "design" della piattaforma stessa con la finalità di ostacolare quanto più possibile la circolazione dei materiali illeciti attraverso il paradigma prevenzione mediante gestione. In tale direzione, si pone anche la bozza di Regolamento del Digital Service Act.

406 Parere del Comitato economico e sociale europeo sul tema «Il consumo collaborativo o partecipativo: un modello di sviluppo sostenibile per il XXI secolo» https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52013IE2788&from=SV

407 OSCE, Open Journalism: The Road Travelled and the Road Ahead, 68 e ss. disponibile al seguente link https://www.osce.org/representative-on-freedom-of-media/384432?download=true. Ed ancora, per l'OSCE "*Excessive and disproportionate provisions regarding content takedown and intermediaries' liability create a clear risk of transferring regulation and adjudication of Internet freedom rights to private actors and should be avoided. States should also discourage intermediaries from automatizing decisions with clear human rights implications*"

408 N. HELBERGER - J. PIERSON -T. POELL, *Governing online platforms: from contested to cooperative responsibility,* cit., 10 e ss. Gli Autori hanno identificato quattro punti per ridistribuire la responsabilità per gli illeciti online. "*The first step is*

un ambiente digitale sicuro richiede una partecipazione attiva degli utenti ed un'effettiva responsabilità dei fruitori dei servizi della società dell'informazione. Per l'effetto, occorre un quadro normativo che promuova una leale collaborazione tra piattaforme ed utenti, come parte della soluzione del problema del contrasto agli illeciti online. I costi dell'*enforcement*, quindi, andrebbero equamente ripartiti tra piattaforme, portatori di interessi e utenti.

4.8 Riflessioni finali

Nell'ambito dell'ecosistema digitale, la definizione del trattamento giuridico della responsabilità civile degli Internet service provider rappresenta una delle questioni più problematiche al momento.

Invero, la mancanza di regole cagiona irrimediabili vuoti di responsabilità che inficiano la fiducia dei fruitori dei servizi di intermediazione online e la stabilità dei traffici giuridici[409]. Quanto detto ha avuto un recente riflesso nel recente caso Gamestop[410] che ha finito per attirare l'attenzione anche dell'ESMA. Sebbene la vicenda sia avvenuta oltreoceano, l'Autorità ha ammonito circa il pericolo di verificazione di episodi simili anche in Europa a causa del fatto che gli investitori *retail* tendono sempre più ad assumere decisioni sulla base di informazioni circolanti nei social media al di fuori di meccanismi che ne garantiscano la qualità e affidabilità[411].

to collectively define the essential public values at play in particular economic activities and modes of public exchange. The next step is for each stakeholder (platforms, governments, users, advertisers, and others) to accept that they have a role to play in the realization of these values. The definition of the public value(s) and the specific contribution of each stakeholder are dependent on the context – the sector, type of service, regulatory situation, and socio-cultural sensitivities. The third step is to develop a (multi-stakeholder) process of public deliberation and exchange, in which agreement can be reached between platforms, users, and public institutions on how important public values can be advanced. For this kind of cooperative responsibility to be feasible, we argue that governments need to give some space to online platforms to experiment and operationalize workable solutions, without putting the realization of public policy objectives entirely at the mercy of self-regulatory initiatives. The fourth and final step is to translate the outcome of public deliberation and agreements into regulations, codes of conduct, terms of use and, last but not least, technologies (e.g. 'by design')".

409 L'incertezza normativa causa instabilità dei mercati e sfiducia degli utenti, cui fanno da contraltare strategie di autoregolamentazione e di "private ordering" da parte delle piattaforme telematiche. Il rischio è quello di trasformare gli intermediari online da guardiani dell'informazione a "cyber regulator" o "cyber-police". Il trasferimento della governance di Internet a soggetti privati rischia di pregiudicare le libertà fondamentali e le garanzie del giusto processo, ove non accompagnato dalla trasparenza.

410 Con il caso Gamestop, si fa riferimento alla vicenda americana in cui centinaia di investitori *retail* accordatisi sulla piattaforma social Reddit hanno cominciato ad acquistare in massa azioni del colosso dei videogiochi a seguito della collocazione sul mercato da parte dei grandi hedge fund di Wall Street di un elevato flottante di titoli. Così operando, il valore delle azioni di Gamestop è salito da pochi dollari fino a diverse centinaia nel giro di pochi giorni. Bisogna però sottolineare che in questo periodo la situazione finanziaria di Gamestop è rimasta invariata e che la volatilità delle sue azioni non è legata alla maggiore produttività aziendale. A riguardo, sono stati individuati tre fattori alla base del caso Gamestop: i) il crollo del costo della compravendita di titoli finanziari per gli investitori retail; ii) la rapida diffusione delle notizie nei social network; iii) la rabbia contro il "sistema" e le "regole". https://rep.repubblica.it/pwa/affari-e-finanza/2021/02/08/news/ecco_perche_la_rivolta_di_gamestop_non_e_la_lotta_di_classe_della_finanza-286142775/ ; https://www.italiaoggi.it/news/gamestop-e-un-vero-caso-giuffre-2508724 ;

411 https://www.esma.europa.eu/sites/default/files/library/esma70-155-11809_episodes_of_very_high_volatility_in_trading_of_certain_stocks_0.pdf

Certamente, la discussione e l'assunzione di scelte di investimento nelle piattaforme telematiche non integra gli estremi di un illecito. Non va però esclusa la commissione di fattispecie di manipolazione del mercato, laddove vi sia stata la diffusione di informazioni false o fuorvianti all'interno di piattaforme online con il fine di promuovere strategie coordinate di negoziazione a certe condizioni per spostare il prezzo dei titoli finanziari.

In questo contesto, forte è la preoccupazione per la *cybersecurity* a causa del crescente livello di digitalizzazione e di dipendenza tecnologica dei servizi finanziari. Come già osservato [412], "la recente proposta di Regolamento DORA rappresenta la giusta risposta con un quadro unitario UE per la vigilanza dei maggiori provider nonché la fissazione di obiettivi di risultato – piuttosto che di sola regolamentazione – sia per gli intermediari finanziari che per le autorità". La novella normativa citata [413] è finalizzata a stabilire un quadro normativo armonizzato in tema di resilienza operativa digitale e sicurezza dei servizi, permettendo a tutti gli operatori di settore di trarre vantaggio dal FinTech. In altri termini, il Regolamento DORA ha come obiettivo quello di creare un impianto che consenta alle imprese interessate di difendersi da tutti i tipi di minacce legate alle tecnologie dell'informazione e della comunicazione (ICT) tramite l'armonizzazione e lo snellimento delle norme esistenti nonchè l'introduzione di nuove regole su misura per test digitali, condivisione delle informazioni e gestione del rischio ICT. In materia di *cybersecurity*, aperto resta però il problema del coordinamento tra attività di vigilanza dell'Unione Europea e sicurezza nazionale di competenza degli Stati Membri.

Nella costruzione del mercato digitale unico europeo, altrettanto meritorie sono le recenti due proposte di Regolamento presentate dalla Commissione a metà dicembre 2020, Digital Market Act[414] e Digital Service Act[415]. La prima costituisce una forma di regolamentazione ex ante che si rivolge alle grandi piattaforme online cd. "*gatekeeper*", chiamate a rispettare una serie di obblighi e divieti per rendere competitivi, equi e trasparenti i mercati digitali. La seconda rappresenta un aggiornamento della Direttiva sul commercio elettronico nella parte relativa alla responsabilità civile degli Internet Service provider attraverso l'introduzione di varie novità come l'elaborazione di nuovi meccanismi di segnalazione e rimozione di contenuti illeciti immessi in rete dagli utenti, oltre alla previsione cogente di maggiori obblighi di trasparenza rispetto al passato.

412 P. Ciocca, Dati e finanza: nuove opportunità e nuove vulnerabilità. La necessità di cambiare paradigma, disponibile al seguente link: https://www.consob.it/documents/46180/46181/intervento_ciocca_20201118.pdf/d1d29034-5180-420a-adb2-a2f2248f4a8f

413 Proposta di Regolamento del Parlamento europeo e del Consiglio relativo relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014 e (UE) n. 909/2014 disponibile al seguente link: https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52020PC0595

414 Proposta di Regolamento del Parlamento europeo e del Consiglio relativo a mercati equi e contendibili nel settore digitale (legge sui mercati digitali) disponibile al seguente link: https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A52020PC0842&qid=1615143051224

415 Proposta di Regolamento del Parlamento europeo e del Consiglio relativo a un mercato unico dei servizi digitali (legge sui servizi digitali) e che modifica la direttiva 2000/31/CE disponibile al seguente link: https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=COM%3A2020%3A825%3AFIN

A livello sovranazionale si è, quindi, compreso – e tali e tante iniziative lo dimostrano – che occorre creare un ecosistema di fiducia e di eccellenza in cui tutti gli operatori possano confidare nel pieno rispetto del quadro normativo eurounitario in materia di protezione dei dati personali, affinchè l'Unione Europea possa divenire un modello di riferimento per cittadini e per imprese. Condivisibile è, infatti, il monito della Commissione Europea per cui "Se vuole conquistarsi un ruolo guida nell'economia dei dati, l'UE deve agire subito e affrontare in maniera concertata questioni che vanno dalla connettività all'elaborazione e alla conservazione dei dati, dalla potenza di calcolo alla cibersicurezza"[416]. La nascita di un mercato unico digitale dipenderà dalla capacità dell'Unione Europea di investire in tecnologie e infrastrutture d'avanguardia, così come nelle competenze digitali (cd. *data literacy*).

Forte di tali iniziative e della ritrovata spinta verso un ripensamento dell'architettura normativa della materia a livello eurounitario, la regolamentazione dell'attività delle piattaforme online esige ora più che mai un intervento a tutto campo, che passi auspicabilmente attraverso un approccio interdisciplinare e multilaterale, con un coinvolgimento attivo di tutti gli *stakeholders*. In particolare, occorre, dinanzi alla presente rivoluzione digitale, una cornice normativa che sappia bilanciare concorrenza e innovazione con la più elevata tutela dei diritti fondamentali.

In questo senso, si evidenzia che qualsiasi intervento di riforma dovrebbe essere supportato da sufficienti studi accademici ed effettive prove empiriche per scongiurare esternalità negative derivanti da affrettate novelle normative.

Rispetto ad un modello *entity-based* incentrato su una rigida classificazione soggettiva delle piattaforme online, pare preferibile un approccio *activity-based* che ponga l'attenzione sui prodotti e servizi offerti dall'intermediario online poiché ogni attività vanta proprie specificità[417]. In altri termini, la normativa dovrebbe polarizzarsi sulla natura e sul tipo di servizio di intermediazione online offerto dalle piattaforme telematiche piuttosto che su una rigida mappatura soggettiva a causa del carattere a geometria variabile delle odierne piattaforme telematiche che offrono contestualmente una pluralità di servizi.

Alla luce del carattere trasversale della rete, se appare ormai chiaro che la disciplina delle piattaforme online debba avvenire a livello europeo con strumenti di *hard law* al fine della creazione di un "*level playing field*" comune a tutti i Paesi membri, tramite un approccio regolatorio omogeneo ed orizzontale, dibattuta resta invece la strada[418].

416 Comunicazione della Commissione al Parlamento Europeo, al consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, Una strategia europea per i dati, 20-2-2020 disponibile al seguente link: https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52020DC0066&from=IT

417 V. Falce – G. Finocchiaro, *La Digital revolution nel settore finanziario*, in V. Falce – G. Finocchiaro (a cura di), *Fintech: diritti, concorrenza e regole*, cit, XXXIII e ss.

418 Sul punto, si ritiene che la revisione della responsabilità degli ISP debba ancorarsi non all'omesso espletamento di misure volontarie, bensì esclusivamente all'inadempimento di obbligazioni legali definite in modo chiaro dal legislatore sulla base di presupposti certi e oggettivi. Ciò giova alla prevedibilità e all'accessibilità delle regole che costituiscono presupposti impreteribili ai fini dello sviluppo della società dell'informazione. Secondo un'analisi economica del diritto, infatti, il regime giuridico della responsabilità è un "elemento di struttura del mercato" in grado di condizionare gli investimenti degli operatori. Fallace è quell'atteggiamento che richiede agli intermediari online l'azzeramento di tutte

Innegabile rimane il fatto che per evitare fenomeni di obsolescenza, la definizione delle regole di responsabilità degli ISP dovrà essere modellata sulla base di principi elastici cd. *future proof* in forza della rapidità dell'evoluzione tecnologica e della varietà dei modelli di business[419].

5 Evoluzione digitale e nuove misure a tutela dei "consumatori" ... di servizi finanziari

5.1 Le nuove misure dell'Unione Europea a tutela dei consumatori

Gli strumenti digitali hanno ormai permeato diversi settori produttivi, tra cui quello finanziario, e inciso sulle modalità di fornitura ed erogazione di prodotti e servizi, che avviene sempre più tramite canali digitali e remoti[420]. Ma a una più facile e immediata fruizione di prodotti e servizi digitali corrisponde un aumento del rischio che questi vengano acquistati senza un'adeguata valutazione delle loro caratteristiche e dei diritti che conseguono all'acquisto, soprattutto quando le informazioni necessarie a siffatte valutazioni non siano messe a disposizione dell'acquirente in una modalità tale da consentire una fruizione che possa essere rapida almeno quanto quella del prodotto o del servizio stesso. E lo squilibrio informativo già insito nell'acquisto digitale si aggrava ancora di più, sotto un profilo soggettivo, quando al professionista che fornisce il bene si contrapponga una parte che non li acquista nell'ambito della attività professionale o imprenditoriale eventualmente svolta, ovvero il consumatore; sotto un profilo oggettivo, quando il bene acquistato presenti caratteristiche complesse, come nel caso dei servizi finanziari.

le attività illecite in rete. Per converso, pare opportuno valorizzare nella disciplina degli Intenet Service Providers clausole generali come la "buona fede" e la "diligenza del professionista", affinché le piattaforme digitali realizzino secondo i mezzi e le risorse a disposizione tutti quei ragionevoli sforzi loro esigibili nella repressione delle attività illecite in rete. A favore dell'armonizzzazione delle regole di responsabilità: B. NORDEMANN, *Liability of Online Service Providers for Copyrighted Content – Regulatory Action Needed?,* cit., 21 e ss. Per l'Autore "The current system, which provides only a liability privilege (shield) for internet providers, seems incomplete, as long as there are no pan-EU liability rules to establish liability. The digital single market will not be realised, in cases where national liability rules dominate the establishment of liability"; A favore dell'armonizzazione solo delle esenzioni dale comuni regole di responsabilità: G. SARTOR, *Providers liability: from the ecommerce Directive to the future,* cit., 28 e ss. Per l'Autore, "However, it seems to me that, the need to ensure some consistency at the level strongly the need for EU regulation on the secondary liability of intermediaries. Relying on liability would not only fail to provide sufficient certainty at the EU level, but will also fail to provide sufficient harmonization at the level, given the confused dialectics of conflicting theories, views, and standard for decisions".

419 A. DE STREEL - M. BUITEN – M. PEITZ, *Liability of online hosting platforms should exceptionalism end?,* cit., 58 e ss. Per gli Autori, "liability rules of providers of hosting services should be principles-based to be easily adaptable to technology and business models, which evolve quickly and often in unpredictable ways. These principles-based rules could be clarified by the European Commission in delegated or implementing acts or interpretative guidance, which can easily be adapted to technology and market evolutions. In particular, guidance prevents that the liability rules remain vague, and ensures that online intermediaries have the necessary knowledge and legal certainty to fulfil their obligations and responsibilities".

420 Cfr. V. FALCE, G. FINOCCHIARO, *La* digital revolution *nel settore finanziario. Una nota di metodo*, in *Analisi Giuridica dell'Economia*, 2019, 1, 313 ss.; T. BROGGIATO, *La tutela del consumatore nel rinnovato contesto*, in G. Finocchiaro, V. Falce (a cura di), *Fintech: diritti, concorrenza, regole*, Bologna, 2019, 291.

All'evoluzione digitale del mercato, le istituzioni europee stanno rispondendo con nuove misure di *public* e *private enforcement* a tutela dei consumatori. Tra le misure di *public enforcement*, un primo e significativo intervento del legislatore europeo si è avuto con l'emanazione del Regolamento (UE) 2017/2394 sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa che tutela i consumatori[421], che ha abrogato il Regolamento (CE) 2006/2004[422]. Già in una comunicazione del 2015 sulle strategie per l'implementazione di un mercato unico digitale in Europa[423], la Commissione aveva rilevato che la disponibilità di un insieme comune di norme non è di per sé sufficiente ad assicurare una piena efficacia della normativa in materia di acquisti online e digitali da parte dei consumatori, essendo altresì necessario «garantirne il rispetto con maggiore rapidità, agilità e omogeneità». Alla comunicazione del 2015 ha poi fatto seguito un'altra comunicazione del 2016, che conteneva un pacchetto di proposte finalizzato a stimolare il commercio elettronico transfrontaliero tra cittadini e imprese in Europa[424]. Tra le proposte vi era anche quella di riforma del suddetto Regolamento sulla cooperazione tra le autorità nazionali competenti in materia di diritto dei consumatori, che si è poi tradotta nel Regolamento (UE) 2017/2394.

Un secondo intervento del legislatore europeo (sia di *public* sia di *private enforcement*) si è avuto con il *New Deal for Consumers*, un pacchetto di misure pubblicate dalla Commissione l'11 aprile 2018 e consistenti in una Comunicazione[425] e due proposte di Direttive, la prima relativa alle azioni rappresentative a tutela degli interessi collettivi dei consumatori in sostituzione della Direttiva 2009/22/CE[426]; la seconda finalizzata alla modifica di quattro direttive in materia di diritti dei consumatori[427].

Come si legge nella Comunicazione della Commissione "*Un "*New Deal*" per i consumatori*", che introduce le proposte di Direttive, l'obiettivo delle riforme è quello di consentire una migliore applicazione delle norme in materia di tutela dei consuma-

421 Regolamento (UE) 2017/2394 del Parlamento europeo e del Consiglio del 12 dicembre 2017 sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa che tutela i consumatori e che abroga il regolamento (CE) n. 2006/2004.

422 Regolamento (CE) 2006/2004 del Parlamento europeo e del Consiglio del 27 ottobre 2004 sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa che tutela i consumatori («Regolamento sulla cooperazione per la tutela dei consumatori»).

423 Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, *Strategia per il mercato unico digitale in Europa*, SWD(2015) 100 *final*, Bruxelles, 6 maggio 2015, COM(2015) 192 *final*.

424 Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, *Un approccio globale per stimolare il commercio elettronico transfrontaliero per i cittadini e le imprese in Europa*, SWD(2016) 163 *final*, Bruxelles, 25 maggio 2016, COM(2016), 320 *final*.

425 Comunicazione della Commissione al Parlamento europeo, al Consiglio e al Comitato economico e sociale europeo, *Un* "New Deal" *per i consumatori*, Bruxelles, 11 aprile 2018, COM(2018) 183 *final*.

426 Proposta di direttiva del Parlamento europeo e del Consiglio relativa alle azioni rappresentative a tutela degli interessi collettivi dei consumatori e che abroga la Direttiva 2009/22/CE, SWD(2018) 96 *final* – SWD(2018) 98 *final*, Bruxelles, 11 aprile 2018, COM(2018) 184 *final*.

427 Proposta di direttiva del Parlamento europeo e del Consiglio che modifica la direttiva 93/13/CEE del Consiglio del 5 aprile 1993, la direttiva 98/6/CE del Parlamento europeo e del Consiglio, la direttiva 2005/29/CE del Parlamento europeo e del Consiglio e la direttiva 2011/83/UE del Parlamento europeo e del Consiglio per una migliore applicazione e una modernizzazione delle norme dell'UE relative alla protezione dei consumatori, SWD(2018) 96 – SWD(2018) 98, Bruxelles, 11 aprile 2018, COM(2018) 185 *final*.

tori, fornire strumenti efficaci di ricorso e accrescere la conoscenza dei diritti dei consumatori, la fiducia e la sicurezza di questi ultimi[428]. Da un controllo dell'adeguatezza e dell'efficacia della normativa europea in materia di consumatori, effettuato dalla Commissione su sette Direttive in materia e pubblicato il 23 maggio 2017[429], era emerso come, da un lato, la normativa a tutela dei consumatori fosse stata comunque in grado di affrontare le violazioni commesse nel mercato online, nonostante questa fosse stata elaborata prima della diffusione del commercio elettronico; dall'altro lato, che il livello di protezione dei consumatori non era però aumentato significativamente negli ultimi anni. Ciò ha portato la Commissione a ritenere che la soluzione per migliorare la protezione dei consumatori fosse non lo stravolgimento della normativa (che comunque aveva retto l'evoluzione digitale), ma un intervento di modifica per una migliore applicazione delle norme esistenti[430].

La proposta della Commissione di modifica di quattro Direttive in materia di diritti dei consumatori si è tradotta nella Direttiva n. 2161 approvata il 27 novembre 2019[431], che dovrà essere recepita dagli Stati membri entro il 28 novembre 2021, con applicazione delle disposizioni nazionali a decorrere dal 28 maggio 2022 (art. 7 della Direttiva). La proposta della Commissione relativa alle azioni rappresentative a tutela

428 COM(2018) 183 *final*, pp. 3 e 4, ove si rileva come la fiducia e la sicurezza dei consumatori sia stata pregiudicata da eventi su vasta scala, come il *Dieselgate* o l'utilizzo diffuso, da parte delle banche, di clausole contrattuali abusive nei contratti ipotecari.

429.Si tratta del Commission staff working document, *Report of the Fitness Check on Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive'); Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts; Directive 98/6/EC of the European Parliament and of the Council of 16 February 1998 on consumer protection in the indication of the prices of products offered to consumers; Directive 1999/44/EC of the European Parliament and of the Council of 25 May 1999 on certain aspects of the sale of consumer goods and associated guarantees; Directive 2009/22/EC of the European Parliament and of the Council of 23 April 2009 on injunctions for the protection of consumers' interests; Directive 2006/114/EC of the European Parliament and of the Council of 12 December 2006 concerning misleading and comparative advertising*, SWD(2017) 208 *final*, Bruxelles, 23 maggio 2017, SWD(2017) 209 *final*, e della Relazione della Commissione al Parlamento europeo e al Consiglio sull'applicazione della direttiva 2011/83/UE del Parlamento europeo e del Consiglio, del 25 ottobre 2011, sui diritti dei consumatori, recante modifica della direttiva 93/13/CEE del Consiglio e della direttiva 1999/44/CE del Parlamento europeo e del Consiglio e che abroga la direttiva 85/577/CEE del Consiglio e la direttiva 97/7/CE del Parlamento europeo e del Consiglio, SWD(2017) 169 *final* – SWD(2017) 170 *final*, Bruxelles, 23 maggio 2017, COM(2017) 259 *final.*

430 Nel documento che accompagna le proposte di direttive (Documento di lavoro dei servizi della Commissione, Sintesi della valutazione d'impatto che accompagna il documento "Proposte di direttive del Parlamento europeo e del Consiglio 1) che modifica la direttiva 91/13/CEE del Consiglio, la direttiva 98/6/CE del Parlamento europeo e del Consiglio, la direttiva 2005/29/CE del Parlamento europeo e del Consiglio e la direttiva 2011/83/UE del Parlamento europeo e del Consiglio per una migliore applicazione e una modernizzazione delle norme dell'UE relative alla protezione dei consumatori e 2) relativa alle azioni rappresentative a tutela degli interessi collettivi dei consumatori e che abroga la direttiva 2009/22/CE", COM(2018) 184 *final*, SWD(2018) 96 *final*, Bruxelles, 11 aprile 2018, SWD(2018) 98 *final*, 5) la Commissione ha rilevato come la normativa in tema di diritti dei consumatori sia in linea di massima adeguata, ma che la sua efficacia sia ostacolata, da un lato, dalla mancanza di consapevolezza da parte dei consumatori; dall'altro lato, da una non sufficiente attuazione e opportunità di ricorso del consumatore. La Commissione ha dunque evidenziato la necessità di una modernizzazione del diritto dell'UE in materia di consumatori in vista degli sviluppi digitali, nonché una rimozione di oneri sproporzionati e non necessari peri i professionisti, sanzioni più efficaci e migliori possibilità di ricorso per i consumatori; SWD(2018) 98 *final*, 2; COM(2018) 183 *final*, pp. 4 e 9; cfr. T. Broggiato, *La tutela del consumatore nel rinnovato contesto*, cit., 304, e I. Speziale, *La Dir. 2019/2161 UE tra protezione dei consumatori e protezione della competitività sul mercato unico*, in *Corr. giur.*, 2020, 4, *passim* e p. 442.

431 Direttiva 2019/2161/UE del Parlamento europeo e del Consiglio del 27 novembre 2019, che modifica la dir. 93/13/CEE del Consiglio e le Dir. 98/6/CE e 2011/83/UE del Parlamento europeo e del Consiglio per una migliore applicazione e una modernizzazione delle norme dell'Unione relative alla protezione dei consumatori.

degli interessi collettivi dei consumatori si è tradotta nella Direttiva n. 1828 approvata il 25 novembre 2020[432], che dovrà essere recepita dagli Stati membri entro il 25 dicembre 2022, con applicazione delle disposizioni nazionali a decorrere dal 25 giugno 2023 (art. 24 della Direttiva).

A tali misure dell'Unione in favore dei consumatori di prodotti e servizi digitali potrebbero presto seguirne altre in materia di commercio elettronico: la Commissione europea ha infatti recentemente formulato una proposta di Regolamento per un Mercato Unico dei Servizi Digitali («*Digital Services Act*») contenente misure finalizzate a incrementare la tutela dei consumatori nel mercato digitale[433].

5.2 Le norme applicabili al "consumatore" di servizi finanziari

Tra le nuove misure dell'Unione Europea a tutela dei consumatori occorre però individuare quali siano applicabili al "consumatore" di servizi finanziari. La disciplina dei servizi finanziari è principalmente contenuta nel Testo Unico della Finanza (d.lgs. 24 febbraio 1998, n. 58), in cui, tra l'altro, sono già previste delle disposizioni a tutela dell'investitore, quale parte meno informata e dunque più debole nel rapporto contrattuale[434]. Gli investitori vengono anche distinti in: clienti professionali privati, che, ai sensi dell'art. 6, co. 2-*quinquies*, T.U.F., sono quelli individuati dalla Consob, sentita la Banca d'Italia; clienti professionali pubblici, che, ai sensi dell'art. 6, co. 2-*sexies*, T.U.F., sono individuati dal Ministero dell'Economia e delle Finanze, sentita la Consob e la Banca d'Italia; controparti qualificate, ai sensi dell'art. 6, co. 2-*quater*. Per i clienti non professionali, ovvero gli investitori diversi da quelli di cui all'art. 6, commi 2-*quinquies* e 2-*sexies*, T.U.F., sono previste anche delle disposizioni di maggior tutela. Ad esempio, l'art. 32-*ter*, co. 1, T.U.F. prevede l'obbligo per gli intermediari di aderire a sistemi di risoluzione stragiudiziale delle controversie con gli investitori non professionali. Per le controversie tra gli investitori non professionali diversi anche dalle controparti qualificate[435] e gli intermediari è inoltre previsto un meccanismo di risoluzione stragiudiziale delle controversie dinanzi all'Arbitro per le Controversie Finanziarie[436].

432 Direttiva 2020/1828/UE del Parlamento europeo e del Consiglio del 25 novembre 2020 relativa alle azioni rappresentative a tutela degli interessi collettivi dei consumatori e che abroga la direttiva 2009/22/CE.

433 *Proposal for a Regulation of the Euopean Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC*, SEC(2020) 423 *final*, SWD(2020) 348 *final*, SWD(2020) 349 *final*, Bruxelles, 15 dicembre 2020, COM(2020) 825 *final*.

434 Ad esempio, l'art. 21 T.U.F. prevede degli obblighi di comportamento e di informazione in capo agli intermediari; cfr. P. Bartolomucci, *Ancora sugli obblighi informativi nel settore del mercato finanziario tra doveri dell'intermediario e principio dell'autodeterminazione dell'investitore*, in *Nuova giur. civ. comm.*, 2009, p. 445, nt. 19, che rileva come gli obblighi di informazione possono essere distinti in attivi e passivi: tra i primi dovrebbe annoverarsi la *suitability rule*, che obbliga l'intermediario a non porre in essere operazioni non adeguate al profilo del cliente e di informarlo del rischio effettivo connesso a ciascuna operazione; tra quelli di informazione passiva si annovera la *know your costumer rule*, che obbliga l'intermediario ad acquisire tutte le informazioni relative alla propensione al rischio del cliente.

435 Ovvero i «clienti al dettaglio» ai sensi dell'art. 35, co. 1, lett. e), del Regolamento intermediari della CONSOB.

436 Istituito dalla Consob con Delibera n. 19602 del 4 maggio 2016, avente appunto a oggetto la "*Istituzione dell'Arbitro per le Controversie Finanziarie (ACF) e adozione del Regolamento di attuazione dell'art. 2, commi 5*-bis *e 5*-ter*, del Decreto Legislativo 8 ottobre 2007, n. 179*".

L'investitore non professionale o c.d. risparmiatore, ovvero il soggetto che acquista servizi finanziari al di fuori dell'attività professionale o imprenditoriale eventualmente svolta, si avvicina alla figura del consumatore, ma comunque non gli coincide, in quanto il risparmiatore può anche essere una persona giuridica[437]. Peraltro, la maggiore ampiezza della figura del risparmiatore e l'assenza, nella disciplina finanziaria, di un'esclusione generale delle norme a tutela del consumatore, potrebbero astrattamente consentire alla persona fisica che acquista servizi finanziari a titolo non professionale di beneficiare anche della normativa consumeristica, quando questa sia suscettibile di applicazione anche nel settore finanziario.

La compatibilità tra la tutela del risparmiatore e quella del consumatore è in effetti confermata da alcune disposizioni di legge, prima tra tutte la disciplina della commercializzazione a distanza di servizi finanziari (recepita nell'ordinamento italiano agli artt. Da 67-*bis* a 67-*vicies bis* del Codice del consumo), che riconosce espressamente la figura del "consumatore" di servizi finanziari[438]. Anche nel T.U.F. si trova una conferma della compatibilità delle due discipline, in quanto l'art. 32-*bis* attribuisce alle associazioni dei consumatori inserite nell'elenco di cui all'art. 137 cod. cons. la legittimazione ad esperire le azioni inibitorie di cui agli artt. 139 e 140 cod. cons. anche a tutela degli interessi collettivi degli investitori[439]. I servizi finanziari sono poi richiamati in tema di clausole vessatorie e pratiche commerciali scorrette, che per essi prevedono delle disposizioni specifiche[440]. Del resto, anche nei casi di esclusione dei servizi finanziari dall'ambito di applicazione di taluni diritti dei consumatori (come accade, ai sensi dell'art. 47, co. 1, lett. d), cod. cons., per la disciplina delle informazioni precontrattuali e di altri diritti dei consumatori, contenuta agli articoli da 48 a 67 dello stesso codice), si ha una conferma della tendenziale generalità e trasversalità della disciplina consumeristica, ove non dedicata già a specifici settori del mercato[441].

437 Vedi G. Meo, *Consumatori, mercato finanziario e impresa: pratiche scorrette e ordine giuridico del mercato*, in *Giur. comm.*, 2010, 5, 720 e 721.

438 Sebbene, da un lato, il concetto di consumo mal si attaglia ai servizi finanziari, che vengono acquistati per soddisfare un bisogno non tramite la loro consumazione, ma piuttosto tramite la possibilità di generare nuove ricchezze; dall'altro, la definizione di servizio finanziario, prevista all'art. 67-*ter*, co. 1, lett. b), cod. cons., ricomprende non solo i servizi di investimento, ma anche qualsiasi servizio bancario, creditizio, di pagamento, di assicurazione o di previdenza individuale.

439 Non è invece prevista espressamente anche la legittimazione ad esperire l'azione di classe di cui all'art. 140-*bis* cod. cons., in quanto in tal caso la legittimazione non è limitata alle associazioni dei consumatori. V. però *infra*, par. 5, sulla nuova collocazione e sulla riforma dell'azione inibitoria e dell'azione di classe a tutela dei consumatori. Cfr. anche G. Meo, *Consumatori, mercato finanziario e impresa: pratiche scorrette e ordine giuridico del mercato*, cit., 733 ss., secondo il quale l'art. 32-*bis* T.U.F. non può essere letto come introduzione di un'equazione investitore-consumatore, così che «tutela, principi e regole del diritto dei consumatori diventino per ciò stesso principi e regole della tutela degli investitori». Infatti, l'art. 139 cod. cons. circoscriveva le azioni alle violazioni di interessi collettivi dei consumatori, sicché la disposizione del T.U.F. non è idoneo a estenderla a tutela di interessi che possono riguardare investitori diversi dalle persone fisiche che operano al di fuori dell'attività professionale o imprenditoriale eventualmente svolta.

440 Nell'ambito della disciplina sulle clausole vessatorie, vedi l'art. 33, co. 4, 5, e 6, cod. cons.; nell'ambito della disciplina sulle pratiche commerciali scorrette, invece, l'art. 21, co. 3-*bis*, cod. cons., considera «scorretta la pratica commerciale di una banca, di un istituto di credito o di un intermediario finanziario che, ai fini della stipula di un contratto di mutuo, obbliga il cliente alla sottoscrizione di una polizza assicurativa erogata dalla medesima banca, istituto o intermediario ovvero all'apertura di un conto corrente presso la medesima banca, istituto o intermediario».

441 Vedi A. Genovese, *Regolazione finanziaria e consumeristica in tema di offerta di servizi finanziari e di investimento*, in AA.VV., *Studi per Luigi Carlo Ubertazzi. Proprietà intellettuale e concorrenza*, 2019, 359-360; L. Rossi-Carleo, *Consumatore, consumatore medio, investitore e cliente: frazionamento e sintesi nella disciplina delle pratiche commerciali*

Pertanto, qualora il risparmiatore sia anche una persona fisica, la normativa consumeristica, salvo che non sia esclusa espressamente dalle stesse disposizioni o implicitamente dalla tipologia di rapporto disciplinato, potrà concorrere con quella finanziaria nella sua tutela. In tali ipotesi, peraltro, potrebbe sorgere un conflitto tra norme appartenenti alle due discipline, con conseguente necessità di stabilire se queste siano suscettibili di applicazione congiunta ovvero di individuare la norma prevalente. In alcuni casi, l'ordine di prevalenza è già stabilito dal legislatore, come accade per la disciplina sulle pratiche commerciali scorrette, sulla commercializzazione a distanza di servizi finanziari ai consumatori e sul commercio elettronico. Quanto alla prima, l'art. 19, co. 3, cod. cons., che ha recepito l'art. 3, par. 4, della Direttiva 2005/29/CE, prevede che, nel «caso di contrasto tra le disposizioni della presente direttiva e altre norme comunitarie che disciplinino aspetti specifici delle pratiche commerciali sleali, prevalgono queste ultime e si applicano a tali aspetti specifici». Specularmente, il considerando n. 10 prevede che la Direttiva «si applica soltanto qualora non esistano norme di diritto comunitario specifiche che disciplinino aspetti specifici delle pratiche commerciali sleali, come gli obblighi di informazione e le regole sulle modalità di presentazione delle informazioni al consumatore». Quanto alle discipline sulla commercializzazione a distanza di servizi finanziari ai consumatori e sul commercio elettronico, queste, rispettivamente agli artt. 67-*bis*, co. 3, cod. cons., e 2, co. 3, d.lgs. 9 aprile 2003, n. 70[442], fanno «salve, ove non espressamente derogate, le disposizioni in materia bancaria, finanziaria, assicurativa», nonché le competenze «delle autorità indipendenti di settore».

Laddove sia già individuata la norma prevalente, occorrerà fare ricorso ai principi generali dell'ordinamento sull'interpretazione e l'applicazione della legge al fine di individuare i casi in cui le norme non siano suscettibili di applicazione congiunta. Al di fuori di un ordine prestabilito, si potrà fare ricorso unicamente ai principi dell'ordinamento.

scorrette, in *Europa e dir. priv.*, 2010, 3, 685 ss., *passim*, rileva che, soprattutto a seguito dell'introduzione della disciplina delle pratiche commerciali scorrette e del loro carattere orizzontale, la «nozione di consumatore e, quindi, la disciplina integrativa che il legislatore ha dettato, potrebbe estendersi al cliente, all'investitore, all'assicurato, al di là del suo essere persona fisica [...] a seguito della disciplina sulle pratiche commerciali scorrette, si registra un passaggio determinante: l'attenzione, incentrata in precedenza essenzialmente sull'atto, viene a focalizzarsi sull'attività determinando, in tal modo, un significativo ampliamento della nozione di «consumatore». La figura del consumatore viene quindi segmentata in sub-settori, a seconda del mercato in cui questo agisce; anche R. Di Raimo, *Ufficio di diritto privato e carattere delle parti professionali quali criteri ordinanti delle negoziazioni bancaria e finanziaria (e assicurativa)*, in *Giust. civ.*, 2020, 2, 320 ss., rileva che le figure del risparmiatore/investitore e del consumatore, tradizionalmente distinte sulla base della differenza tra atti di risparmio e di investimento e atti di consumo, sono state ricondotte a unità, ma non in conseguenza di una despecializzazione per "consumerizzazione" delle figure del risparmiatore e dell'investitore, quanto di un'espansione della figura del consumatore oltre l'atto di consumo.

442 Che attua la Direttiva 2000/31/CE, del Parlamento europeo e del Consiglio dell'8 giugno 2000 relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno («Direttiva sul commercio elettronico»), la quale al considerando n. 27 specifica che: «La presente direttiva, unitamente alla futura direttiva del Parlamento europeo e del Consiglio concernente la vendita a distanza di servizi finanziari ai consumatori, contribuisce alla creazione di un quadro giuridico per la fornitura di servizi finanziari in linea. La presente direttiva non pregiudica future iniziative nel settore dei servizi finanziari, in particolare per quanto riguarda l'armonizzazione delle regole di condotta in tale settore».

5.3 Il concorso tra normative consumeristica e finanziaria e il riparto di competenze tra autorità indipendenti

L'applicabilità della disciplina consumeristica al risparmiatore è stata però in parte messa in discussione anche al di fuori dei casi di esclusioni espresse, a causa del riparto di competenze sull'esecuzione delle norme a tutela dei consumatori tra le autorità indipendenti avvenuto a seguito dell'entrata in vigore dal Regolamento (CE) 2006/2004[443]. Infatti, l'attribuzione della competenza all'AGCM in alcune specifiche discipline, tra cui quelle sulle pratiche commerciali scorrette e sulle clausole abusive, suscettibili di applicazione trasversale nei settori regolati da altre autorità, e la competenza residuale di tali autorità nei relativi settori[444], ha anzitutto posto un problema di coordinamento tra queste e l'AGCM al fine di definire l'applicazione congiunta o la prevalenza tra le norme di rispettiva competenza, così da evitare sovrapposizioni di procedimenti e decisioni contrastanti.

Inoltre, nell'ambito della disciplina sulle pratiche commerciali scorrette, la prevalenza attribuita alle norme di settore disciplinanti «aspetti specifici» di tali pratiche, «come gli obblighi di informazione»[445], e la presenza, proprio nel settore finanziario, di specifici obblighi di informazione, trasparenza e correttezza in capo agli intermediari, come tali potenzialmente concorrenti con la disciplina generale[446], aveva sollevato una questione ben più ampia. A seguito del recepimento della Direttiva 2005/29/CE nel codice del consumo, l'AGCM aveva infatti chiesto al Consiglio di Stato di chiarire non solo in quali casi dovesse ritenersi prevalente la disciplina finanziaria e, pertanto, competente la relativa autorità di settore, ma, più in generale, se la disciplina sulle pratiche commerciali scorrette fosse applicabile al settore finanziario o se, piuttosto, quest'ultimo dovesse ritenersi sempre prevalente, con esclusione di ogni competenza dell'AGCM.

Con parere del 3 dicembre 2008[447], il Consiglio di Stato, al fine di evitare una duplicazione di soggetti preposti alla vigilanza dello stesso settore, con conseguente

443 V. *supra*, par. 1 e *infra*, par. 4.

444 V. esemplificativamente l'art. 144-*bis*, co. 1, cod. cons., che, nell'attribuire al Ministero dello Sviluppo Economico le funzioni di autorità competente, ai sensi dell'art. 3, par. 1, lett. c), del Regolamento (CE) 2006/2004, in certe norme a tutela dei consumatori (ovvero quelle sulla garanzia nella vendita dei beni di consumo, sul credito al consumo, sul commercio elettronico e sulla multiproprietà), fa «salve le disposizioni in materia bancaria, finanziaria, assicurativa e dei sistemi di pagamento e le competenze delle autorità indipendenti di settore, che continuano a svolgere le funzioni di autorità competenti ai sensi dell'art. 3, lett. c), del regolamento CE n. 2006/2004». Cfr. anche l'art. 141-*octies*, cod. cons.

445 Così l'art. 3, par. 4 (recepito dall'art. 19, co. 4, cod. cons.), e il considerando n. 10 della Direttiva 2005/29/CE.

446 A. Genovese, *Regolazione finanziaria e consumeristica in tema di offerta di servizi finanziari e di investimento*, cit, 357-358, rileva che, a seguito del recepimento della Direttiva c.d. Mifid II con il d.lgs. 3 agosto 2017, n. 129, sono state anche incrementate le tutele a favore dei risparmiatori tramite l'inserimento di disposizioni che impongono all'intermediario obblighi specifici di professionalità, trasparenza e correttezza, a cui è affiancato l'esplicito «divieto (norma di chiusura) di offrire al risparmiatore/investitore soluzioni di investimento inadeguate e da numerose altre disposizioni volte a proteggere il risparmiatore dall'opportunismo dell'intermediario».

447 Cons. St., sez. I consultiva, parere del 3 dicembre 2008, n. 3999; cfr. A. Genovese, *Il contrasto delle pratiche commerciali scorrette nel settore bancario*, in *Giur. comm.*, 2011, 2, pp. 200 ss.; V. Meli, *L'applicazione della disciplina delle pratiche commerciali scorrette nel «macrosettore creditizio e assicurazioni»*, in *Banca bors tit. cred.*, 2011, 3, pp. 334 ss.; M. Clarich, *Le competenze delle autorità indipendenti in materia di pratiche commerciali scorrette*, in *Giur. comm.*, 2010, 5, pp. 688 ss.

rischio di *bis in idem*, riteneva che la disciplina dei servizi finanziari, in quanto dotata di specifici obblighi di informazione posti a tutela del risparmiatore/consumatore, fosse sempre prevalente rispetto a quella generale sulle pratiche commerciali scorrette; pertanto, doveva escludersi la competenza dell'AGCM ad accertare tali pratiche nel settore finanziario, spettando tale competenza sempre ed esclusivamente alla CONSOB[448].

Il Consiglio di Stato, quindi, applicava un principio di specialità per settori, che derogava l'intera disciplina generale in favore di quella settoriale, ove quest'ultima fosse dotata di specifici obblighi a tutela del consumatore e a carico degli operatori, senza che fosse necessario dirimere un contrasto tra singole norme concorrenti. Il principio veniva poi confermato dalle sentenze dell'Adunanza Plenaria dell'11 maggio 2012, nn. 11, 12, 13, 15 e 16, che intendevano la nozione di «contrasto» dell'art. 19, co. 4, cod. cons. (che ha recepito l'art. 3, par. 4, della Direttiva 2005/29/CE) non come «antinomia normativa tra disciplina generale e speciale», ma come semplice «diversità di discipline» volta a evitarne la sovrapposizione tramite la prevalenza della disciplina che offra una tutela aggiuntiva e specifica rispetto a quella minima offerta dalla disciplina generale.

Peraltro, a seguito del recepimento del principio di specialità per settori anche da parte del legislatore, che con l'art. 23, co. 12-*quinquiesdecies*, del d.l. 95/2012, sanciva la competenza dell'AGCM ad accertare le pratiche commerciali scorrette, esclusi i casi in cui le stesse fossero state compiute in settori regolati da altre autorità, la Commissione europea avviava una procedura di infrazione nei confronti dello Stato italiano[449]. Secondo la Commissione, la deroga per settori e non per norme implicava il rischio che altre disposizioni generali a tutela del consumatore, seppur concretamente applicabili in quanto non contrastanti con disposizioni speciali, venissero invece escluse, con conseguente minore tutela del consumatore nell'ambito dei settori regolati[450].

448 V. però G. Meo, *Consumatori, mercato finanziario e impresa: pratiche scorrette e ordine giuridico del mercato*, cit., *passim*, il quale che rileva come la finalità del diritto del mercato finanziario, come si evince dall'art. 5 del TUF, non sia solamente la tutela degli investitori, ma anche la salvaguardia della fiducia nel sistema finanziario e dunque la stabilità, il buon funzionamento e la competitività del sistema stesso. Posta la maggiore ampiezza del diritto del mercato finanziario rispetto a quello dei consumatori, secondo l'A., il Consiglio di Stato aveva errato nell'attribuire al primo carattere di specialità e di prevalenza sostitutiva rispetto al secondo. Tuttavia, il riconoscimento espresso, nell'ambito della disciplina della commercializzazione a distanza di servizi finanziari ai consumatori di cui agli artt. 67-*bis* e ss. del Codice del consumo, della figura del "consumatore" di servizi finanziari, dovrebbe piuttosto portare a valutare, secondo l'A., l'ipotesi di una concorrenza dell'ordinamento consumeristico con quello finanziario, più che l'assorbimento del primo nel secondo. Anche A. Blandini, *Servizi finanziari per via telematica e le prospettive del diritto societario online*, in *Banca borsa e tit. cred.*, 2016, 1, pp. 46 ss., rileva in ogni caso come l'investimento in strumenti finanziari sia comunque un'operazione a rischio, sicché al consumatore investitore non professionale spettano certamente le tutele "informative" ed "educative", ma non la copertura del rischio.

449 Procedura di infrazione 2013/2169/Just del 18 ottobre 2013, ai sensi dell'art. 260 del Trattato TFUE (caso EU Pilot 4261/12/Just).

450 La Commissione aveva infatti rilevato che la «deroga alla disciplina generale, in quanto eccezionale, può trovare applicazione limitatamente agli «aspetti specifici» di una pratica commerciale presi in considerazione da singole disposizioni settoriali che posseggano lo status di legislazione comunitaria e contengano precetti incompatibili con le disposizioni generali contenute nella Direttiva 2005/29/CE». Cfr. A. Genovese, *Regolazione finanziaria e consumeristica in tema di offerta di servizi finanziari e di investimento*, cit., 362 e 367; M. Cappai, *La repressione delle pratiche commerciali scorrette nei mercati regolati: cosa aspettarsi dalla Corte di Giustizia?*, in *Riv. it. dir. pubb. com.*, 2017, 879 ss.

Al fine di rimediare alla procedura di infrazione avviata dalla Commissione, il legislatore italiano, in sede di recepimento della direttiva 2011/83/UE con il d.lgs. 21/2014[451], inseriva il comma 1-*bis* all'art. 27 cod. cons., il quale attribuisce espressamente all'AGCM la competenza in materia di pratiche commerciali scorrette anche nei settori regolati, fermi il rispetto delle norme di settore e la competenza delle relative autorità per le ipotesi di violazione che non integrassero gli estremi di una pratica commerciale scorretta[452]. Ma se, da un lato, la norma chiariva la competenza dell'AGCM ad applicare la disciplina generale delle pratiche commerciali scorrette anche nei settori regolati, dall'altro, la necessità per l'AGCM di rispettare «la regolazione vigente» e la riserva di competenza delle autorità di settore per le ipotesi «che non integrino gli estremi di una pratica commerciale scorretta», sollevavano l'ulteriore questione su quale fosse l'autorità competente ad applicare le norme di settore disciplinanti «aspetti specifici delle pratiche commerciali scorrette»; a una lettura più restrittiva, per cui la clausola di salvaguardia è semplicemente volta a evitare che l'AGCM possa sanzionare una condotta invece consentita dalla normativa di settore, se ne può in effetti contrapporre una più ampia, che abilita l'AGCM ad applicare i principi e le regole del settore coinvolto, quando questi disciplinino aspetti specifici delle pratiche commerciali scorrette[453].

Così, dopo che due sentenze del Consiglio di Stato avevano rimesso in discussione anche il concetto di contrasto di cui all'art. 3, par. 4, Direttiva 2005/29[454], l'Adunanza Plenaria, con ordinanze del 17 gennaio 2017, n. 167 e 168, rivolgeva alla Corte di Giustizia dell'Unione Europea alcune questioni pregiudiziali interpretative. In particolare, il Consiglio di Stato chiedeva alla Corte di chiarire, tra le altre cose: se fosse compatibile con il diritto dell'Unione una normativa nazionale che riconduca la valutazione del rispetto di obblighi specifici previsti dalla normativa settoriale nell'ambito della direttiva generale n. 2005/29/CE ed escluda la competenza dell'autorità di settore ad accertare una violazione della normativa regolata, ogni qualvolta tale violazione sia suscettibile di integrare anche gli estremi di una pratica commerciale scorretta; se il principio dell'art. 3, par. 4, regolasse rapporti tra ordinamenti, rapporti tra norme o rapporti tra autorità preposte alla regolazione e vigilanza dei rispettivi settori; se la nozione di contrasto dell'art. 3, par. 4, dovesse essere intesa come radicale antinomia

451 Nella Relazione illustrativa allo schema di decreto legislativo è infatti esplicitata tale finalità. Cfr. A. Genovese, *op. ult. cit.*, 368.

452 Cfr. T. Broggiato, *La tutela del consumatore nel rinnovato contesto*, cit., 299 ss.; Id., *La competenza in materia di tutela del consumatore di servizi bancari e finanziari: gli orientamenti dei giudici e le indicazioni del legislatore*, in *Conc. e merc.*, 2013, 1, 227 ss., e M. Bertani, *Pratiche commerciali scorrette e violazione della regolazione settoriale tra concorso apparente di norme e concorso formale di illeciti*, in *Nuove leggi civ. comm.*, 2018, 4, 926 ss.

453 Da un lato, infatti, le norme attribuiscono all'AGCM la competenza ad accertare le pratiche commerciali scorrette anche nei settori regolati, fermo il rispetto delle relative norme, e la prevalenza di queste ultime ove disciplinanti «aspetti specifici delle pratiche commerciali scorrette» contrastanti con quelli generali; dall'altro, esse fanno salva la competenza delle autorità di settore a intervenire nelle ipotesi che non integrino gli estremi di una pratica commerciale scorretta. Dalla lettura combinata degli artt. 19, co. 4, e 21, co. 1-*bis*, cod. cons. potrebbe quindi dedursi che l'AGCM possa applicare, nei settori regolati, le norme settoriali disciplinanti aspetti specifici delle pratiche commerciali scorrette. Cfr. S. Perugini, *I nuovi strumenti di intervento dell'AGCM*, in *Corr. giur.*, 2014, 7, 52; S. La Pergola, *Sub. art. 1, co. 6 e 7, d.lgs. n. 21/2014*, in A.M. Gambino-G. Nava (a cura di), *I nuovi diritti dei consumatori*, Torino, 2014, 386 ss.

454 Secondo il Cons. St., Ad. Plen., 3 febbraio 2016, nn. 3 e 4, il concetto di contrasto di cui all'art. 3, par. 4, della Direttiva 2005/29/CE doveva essere inteso, più che come «conflitto astratto di norme in senso stretto», quale «progressione illecita, descrivibile come ipotesi di assorbimento-consunzione» della disciplina generale nella normativa di settore.

tra norme sulle pratiche commerciali scorrette e norme di settore o se fosse sufficiente che queste ultime dettassero una disciplina sulle pratiche commerciali scorrette difforme da quella generale, in ragione della specificità del settore.

La Corte di Giustizia, quanto agli ultimi due quesiti, ha confermato che il contrasto è tra norme e che sussiste unicamente quando le disposizioni settoriali impongono ai professionisti obblighi incompatibili con quelli stabiliti dalla Direttiva 2005/29/CE; non, quindi, una mera difformità o semplice differenza «superabile mediante una formula inclusiva che permetta la coesistenza di entrambe le realtà, senza che sia necessario snaturarle»[455]. Quanto al primo quesito, invece, rilevata l'assenza di tale incompatibilità nel caso di specie, la Corte ha ritenuto che il diritto dell'Unione non osti a una normativa nazionale che escluda la competenza dell'autorità di regolazione (e la riconosca, dunque, all'AGCM) ad applicare la disciplina generale sulle pratiche commerciali scorrette nel settore regolato, senza affermare o negare la legittimità di tale esclusione anche per l'accertamento di una violazione della normativa regolata, ogni qualvolta tale violazione sia suscettibile di integrare gli estremi di una pratica commerciale scorretta.

Forse da tale affermazione, più circoscritta rispetto al quesito posto, il Consiglio di Stato, una volta reinvestito delle questioni, ha tratto l'ulteriore conclusione che, in mancanza di una norma di settore incompatibile e pertanto prevalente, sia illegittima non tanto l'esclusione della competenza dell'autorità di regolazione ad applicare la normativa regolata che integri anche una pratica commerciale scorretta, quanto l'applicazione in sé di tale normativa, contestualmente o successivamente a quella generale. Secondo il Consiglio di Stato, l'utilizzo del criterio di incompatibilità, invece dei criteri penalistici di specialità, escluderebbe qualsiasi rischio di *bis in idem*, in quanto implicherebbe che in assenza di tale incompatibilità, e dunque di "compatibilità" della violazione anche con i divieti della normativa regolata, questa non potrà comunque essere applicata dall'autorità di regolazione, potendo essere applicata solamente la disciplina generale da parte dell'AGCM[456].

Ma la Corte di Giustizia non ha affermato che all'assenza di incompatibilità consegue l'applicazione esclusiva della disciplina generale; al contrario, essa ha ricavato il principio di incompatibilità dall'impossibilità di utilizzare «una formula inclusiva che permetta la coesistenza di entrambe le realtà [normative], senza che sia necessario snaturarle». In effetti, a ben vedere, la Corte di Giustizia ha concluso per la legittimità dell'applicazione della sola disciplina delle pratiche commerciali scorrette non perché nel caso sussistesse una norma di settore, che però fosse compatibile e dunque soccombente nei confronti della disciplina generale, ma in quanto ha ritenuto che mancasse una norma di settore disciplinante «aspetti specifici» della pratica commerciale

455 Corte Giust. UE, 13 settembre 2018, cause riunite C-54-2017 e C-55/2017. A. GENOVESE-M. RANIELI, *Contratti bancari e disciplina delle pratiche commerciali scorrette*, in E. Capobianco (a cura di), *I contratti bancari*, Milano, 2021, 57, rilevano come tale interpretazione rafforzi la competenza dell'AGCM in materia di pratiche commerciali scorrette anche nei settori regolati, in quanto al di fuori di una stretta incompatibilità tra norma generale e norma di settore, la competenza ad accertare la pratica commerciale scorretta sarà sempre dell'AGCM.

456 Cons. St., sez. VI, 25 ottobre 2019, n. 7269, e 11 novembre 2019, n. 7699.

scorretta consistente nella fornitura non richiesta[457]. Tant'è che, in occasione di una precedente applicazione del principio espresso dalla Corte, il Consiglio di Stato aveva avuto modo di affermare la complementarità della disciplina generale dei consumatori con quella settoriale, con conseguente possibilità per l'AGCM di «valutare la scorrettezza di una pratica commerciale, anche alla luce dei principi generali e delle specifiche prescrizioni» della disciplina di settore[458].

Qualora venisse infine seguito il principio per cui, in assenza di incompatibilità, non potrà comunque farsi luogo a un'applicazione congiunta della disciplina generale con quella settoriale[459], non sarebbe da escludere un ulteriore intervento europeo, questa volta finalizzato a evitare il possibile vuoto di tutela derivante dalla mancata applicazione della disciplina settoriale, ove questa integri anche gli estremi di una pratica commerciale scorretta. In effetti, la "nuova" soluzione del Consiglio di Stato risolve la questione della sovrapposizione di competenze tra autorità, ancora una volta, con l'alternatività sostanziale tra disciplina generale e norme settoriali. Ma la specialità tra settori, come è stato rilevato, non è l'unica soluzione alla duplicazione di procedimenti[460]; tant'è che, nonostante le incertezze interpretative, le autorità hanno comunque fornito esempi di applicazione congiunta delle normative consumeristica e settoriale nell'ambito dell'accertamento di pratiche commerciali scorrette[461].

457 E anzi rilevando, per di più, come la disciplina di settore del caso (ovvero la Direttiva 2002/22/CE del Parlamento europeo e del Consiglio del 7 marzo 2002 relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica (direttiva servizio universale)) facesse addirittura salve le norme dell'Unione in materia di tutela dei consumatori e le norme nazionali conformi al diritto dell'Unione.

458 Cons. St., sez. VI, 29 novembre 2018, n. 6795. Cfr. anche Cons. St., sez. VI, 26 giugno 2019, n. 4357.

459 Al momento, in un'altra recente pronuncia, il Cons. St., sez. VI, 22 gennaio 2021, n. 665, ha applicato solamente quella parte del principio espresso dalle due sentenze gemelle del 2019 secondo cui «Alla luce di quanto affermato dalla Corte di Giustizia, la regola generale è che, in presenza di una pratica commerciale scorretta, la competenza è dell'Autorità garante della concorrenza e del mercato. La competenza delle altre Autorità di settore è residuale e ricorre soltanto quando la disciplina di settore regoli "*aspetti specifici*" delle pratiche che rendono le due discipline incompatibili». Così limitato, il principio non dovrebbe escludere la possibilità di un'applicazione congiunta delle due normative.

460 Così A. Genovese-M. Ranieli, *Contratti bancari e disciplina delle pratiche commerciali scorrette*, cit. p. 58, le quali rilevano come, al contrario, l'apertura all'applicazione congiunta tra corpi normativi, con conseguente doppio binario procedimentale, consentirebbe più efficacemente di perseguire gli illeciti plurioffensivi, a condizione che l'intervento congiunto tra autorità sia efficacemente regolato e coordinato.

461 A. Genovese, *Regolazione finanziaria e consumeristica in tema di offerta di servizi finanziari e di investimento*, cit., p. 364, rileva come non siano mancati casi di applicazione congiunta delle normative consumeristica e settoriali, sia in senso suppletivo sia in senso integrativo. Quanto ai casi di applicazione combinata a carattere suppletivo, l'A. riporta l'esempio della vendita di diamanti da investimento effettuata tramite il canale bancario, con tecniche di presentazione del prezzo in termini di "quotazione" e con possibilità di retrocessione del bene alla stregua della liquidazione dell'investimento; in tale ipotesi, il bene, non essendo un prodotto finanziario, non è assoggettato alla regolazione di settore, ma non di meno è presentato come tale e potrebbe essere soggetto alla relativa normativa, oltre che a quella consumeristica in materia di pratiche commerciali scorrette. Nel caso, infatti, la pratica è stata stigmatizzata dalla CONSOB con la Comunicazione n. 13038246 del 6 maggio 2013 e con il Richiamo di attenzione del 31 gennaio 2017 rivolto al pubblico e agli intermediari. Per i casi di applicazione combinata a carattere integrativo, l'A. riporta l'esempio delle pratiche commerciali scorrette poste in essere da Veneto Banca e dalla Banca Popolare di Vicenza e consistenti nella realizzazione di operazioni a "finanziamento baciato", ovvero nell'erogazione di mutui in cambio dell'apertura di conti correnti o dell'acquisto di azioni, che sono state sanzionate sia dall'AGCM quali pratiche commerciali scorrette (AGCM, PS10602 – Veneto Banca/Mutui in cambio di azioni e apertura di conti correnti, Provvedimento n. 26613 del 24 maggio 2017; PS10363 – Banca Popolare di Vicenza/Vendita abbinata finanziamenti-azioni, Provvedimento n. 26168 del 6 settembre 2016) sia dalla CONSOB nei confronti degli esponenti aziendali degli istituti bancari (CONSOB, Veneto Banca S.p.A., delibere n. 20022 del 1/6/2017; n. 20031 del 7/6/2017; n. 20033 del 14/6/2017; n. 20034 e 20035 del 21/6/17. CONSOB, Banca Popolare di Vicenza, delibere n. 19935 del 30/3/2017; n. 19934 del 5/4/2017; n. 20067, 20068, 20072 del 12/7/2017).

Bisogna però mettere in conto che un siffatto coordinamento sia stato possibile anche grazie a una più specifica – sebbene ancora non definitivamente chiara – disciplina della ripartizione delle competenze in tema di pratiche commerciali scorrette, che in alcuni casi ha anche portato alla stipulazione dei protocolli di cui all'art. 27, co. 1-*bis*, cod. cons. [462]; viste, però, le incertezze sul coordinamento nell'ambito delle pratiche commerciali scorrette, nonché la mancanza, in altri settori come quello delle clausole vessatorie, di norme volte a regolare dettagliatamente tale coordinamento[463], sarebbe forse opportuno un nuovo e più ampio intervento del legislatore, che oltre a dirimere le incertezze interpretative sul concorso tra disciplina generale e norme di settore, regoli esaustivamente il coordinamento tra le autorità competenti all'esecuzione delle norme a tutela dei consumatori, così da evitare che il riparto di competenze e il timore di una duplicazione di procedimenti e sanzioni impediscano ancora una volta l'applicazione congiunta della normativa generale con quella settoriale[464].

5.4 Il nuovo regolamento sulla cooperazione tra autorità nazionali per la tutela dei consumatori

Si è però visto come proprio il tema delle competenze delle autorità in materia di consumatori sia stato, nel frattempo, oggetto di intervento legislativo europeo. Nel pacchetto di misure per il settore del commercio elettronico finalizzate a eliminare gli ostacoli che si frappongono all'attività online transfrontaliera in Europa, pubblicato dalla Commissione nel maggio 2016, viene evidenziato che sebbene il Regolamento sulla cooperazione per la tutela dei consumatori del 2004 avesse rafforzato l'applicazione delle norme a tutela di questi ultimi, esso presentava delle lacune con riferimento ai meccanismi di assistenza e di risposta alle violazioni su vasta scala, che erano lenti e difficoltosi, soprattutto quando tali violazioni si verificavano nell'ambiente digitale e soprattutto quando si trattava di violazioni transfrontaliere[465].

462 Vedi A. Genovese-M. Ranieli, *Contratti bancari e disciplina delle pratiche commerciali scorrette*, cit., p. 54, nt. 120, e p. 49, nt. 110, in cui si segnala che, in attuazione dell'art. 27, co. 1-*bis*, cod. cons., il 14 ottobre 2014 è stato stipulato un protocollo tra la Banca d'Italia e l'AGCM (che ha sostituito un precedente protocollo del 22 febbraio 2011, che pur avviando una collaborazione più strutturata tra le due Autorità non entrava nel merito di questioni relative agli apparati normativi), il quale prevede, all'art. 3, co. 3, che «In base a quanto previsto nell'articolo 27, comma 1-*bis*, del decreto legislativo 6 settembre 2005, n. 206, il rispetto della regolazione vigente da parte del professionista esclude, limitatamente a tale profilo, la configurabilità di una condotta contraria alla diligenza professionale». Quanto ai rapporti tra CONSOB e AGCM, le due autorità hanno istituito un tavolo di lavoro nell'autunno del 2015 per valutare l'attivazione del protocollo ai sensi del comma 1-*bis*, ma che sulla mancata attuazione dello stesso potrebbe avere influito l'incertezza del quadro giurisprudenziale. Peraltro, tra la CONSOB e l'AGCM, la possibilità di stipulare un protocollo sulla collaborazione era già prevista dall'art. 20 della l. 262/2005.

463 Nell'ambito della disciplina sulle clausole vessatorie, l'art. 37-bis, co. 5, cod. cons. prevede solamente che l'AGCM, a cui è sempre attribuita la competenza esclusiva all'applicazione della normativa, «può sentire le autorità di regolazione o vigilanza dei settori in cui i professionisti interessati operano».

464 Secondo T. Broggiato, *La tutela del consumatore nel rinnovato contesto*, cit., p. 303, i tempi sono maturi per avviare una riflessione generale sui protocolli di collaborazione con l'AGCM in ambito bancario e finanziario. Secondo l'A., inoltre, potrebbe anche essere prevista la pubblicazione del parere reso dall'autorità di regolazione, al fine di consentire una valutazione più approfondita della decisione presa dall'AGCM.

465 COM(2016) 320 *final*, cit., pp. 10 ss.

La Commissione ha quindi proposto un nuovo Regolamento sulla cooperazione per la tutela dei consumatori, che avrebbe rafforzato la cooperazione tra le autorità nazionali e reso più efficiente l'applicazione delle norme a loro tutela, dotando altresì le autorità di poteri supplementari, che gli consentissero di agire congiuntamente e più rapidamente per far cessare le violazioni. La proposta di riforma si è tradotta nel Regolamento (UE) 2017/2394, entrato in vigore il 17 gennaio 2020, che ha appunto a oggetto la collaborazione e il coordinamento, fra loro e con la Commissione, delle autorità nazionali competenti in materia di diritti dei consumatori, nell'ambito delle norme elencate nell'allegato al Regolamento (art. 3, par. 1, n. 1).

Con il precipuo obiettivo di perseguire le «violazioni transfrontaliere, comprese le infrazioni nell'ambiente digitale, [che consentono] agli operatori di sottrarsi all'esecuzione, spostando le loro attività altrove all'interno dell'Unione»[466], il Regolamento, all'art. 2, par. 1, individua espressamente il suo àmbito di applicazione nelle «infrazioni intra-UE», nelle «infrazioni diffuse» e nelle «infrazioni diffuse aventi una dimensione unionale»[467], specificando che l'infrazione potrà essere perseguita anche ove sia cessata prima dell'inizio o del completamento dell'esecuzione da parte delle autorità competenti[468].

Agli artt. 11 ss. del Regolamento sono poi disciplinate le modalità di collaborazione e coordinamento tra le autorità di diversi Stati membri e tra le autorità e la Commissione europea. In particolare, il Capo III (artt. 11-14) disciplina i meccanismi di assistenza reciproca tra le autorità stabilendo la possibilità di scambio di informazioni tra le stesse e assistenza nelle attività di indagine (ad esempio, nella raccolta di prove in uno Stato membro differente da quello dell'autorità che fa richiesta di assistenza) ed esecutive, tramite la richiesta di un'autorità all'altra di applicazione di misure di esecuzione; inoltre, viene previsto in quali circostanze un'autorità possa rifiutarsi di dare seguito a una richiesta di assistenza reciproca.

Il Capo IV (artt. 15 ss.) disciplina specificamente la cooperazione tra le autorità nei casi di infrazioni diffuse e infrazioni diffuse aventi dimensione unionale, stabilendo le modalità dell'azione coordinata nella fase d'indagine e nell'applicazione delle

466 Considerando n. 3 del Regolamento (UE) 2017/2394.

467 Oltre alla nozione di «infrazione intra-UE», già conosciuta dall'art. 3, par. 1, lett. b), Regolamento (CE) 2006/2004, come «infrazione intracomunitaria», vengono introdotte due nuove definizioni, proprio per far fronte alle violazioni *online*. Le infrazioni sono definite all'art. 3, par. 1, nn. 2), 3) e 4), del Regolamento: l'infrazione intra-UE consiste nell'azione od omissione contraria alle norme dell'Unione a tutela dei consumatori, che abbia arrecato, arrechi o possa arrecare un danno agli interessi collettivi dei consumatori che risiedono in uno Stato membro diverso da quello in cui ha avuto origine o si è verificata l'azione o l'omissione lesiva, è stabilito l'operatore responsabile o si rinvengono elementi di prova o beni dell'operatore riconducibili all'atto o all'omissione; l'infrazione diffusa si distingue da quella intra-UE per la circostanza che i consumatori, i cui interessi collettivi sono violati, risiedono in almeno due Stati membri e non in uno soltanto; l'infrazione diffusa assume «dimensione unionale» nel momento in cui i consumatori lesi risiedano «in almeno due terzi degli Stati membri, che insieme rappresentano almeno i due terzi della popolazione dell'Unione».

468 T. Broggiato, *La tutela del consumatore nel rinnovato contesto*, cit., 295, spec. nt. 11, evidenzia che se le autorità non avessero potuto agire anche nei confronti di infrazioni già cessate, gli operatori avrebbero potuto sfuggire facilmente all'accertamento interrompendo l'infrazione a seguito della comunicazione dell'apertura dell'istruttoria da parte dell'autorità. Si risolve così una problematica del Regolamento del 2004, che imponeva invece alle autorità di corredare la propria richiesta di applicazione di misure esecutive (ai sensi dell'art. 8 del Regolamento) con la difficile prova dell'attualità dell'azione od omissione determinante l'infrazione, così da concedere all'operatore di porre fine alla condotta illegittima ove abbia sentore della pendenza di un accertamento.

eventuali misure di esecuzione. Ad esempio, viene prevista la designazione di un coordinatore dell'azione, che potrà essere un'autorità o anche la Commissione, qualora le autorità non siano in grado di raggiungere un accordo sulla designazione del coordinatore o nell'ipotesi di cui all'art. 17, par. 3, del Regolamento. Le autorità competenti interessate possono inoltre invitare l'operatore responsabile dell'infrazione, anche a seguito di iniziativa dell'operatore stesso, a proporre entro un certo termine degli impegni per porre fine all'infrazione (art. 20 del Regolamento)[469]. Qualora l'operatore non presenti gli impegni entro il termine stabilito, ovvero li presenti ma questi non siano sufficienti o non vengano attuati dall'operatore, o comunque quando è improbabile che l'infrazione cessi a seguito degli impegni proposti o sia in ogni caso necessario un intervento di esecuzione immediato, le autorità competenti interessate dell'azione coordinata potranno adottare tutte le misure di esecuzione necessarie, compresa l'irrogazione di sanzioni.

Inoltre, al fine di rendere più efficiente la risposta delle autorità nazionali alle violazioni, il Regolamento stabilisce, all'art. 9, i poteri minimi di cui queste devono essere dotate sia nella fase delle indagini sia in quella esecutiva[470]; viene invece lasciata agli Stati membri la scelta se attribuire ciascuno dei poteri minimi a ogni autorità competente in materia di tutela dei consumatori o se distribuirli tra tali autorità, purché ciascun potere possa essere effettivamente esercitato per ogni infrazione, a prescindere da quale sia l'autorità a cui lo specifico potere è stato attribuito. Ciò implica che, prima del coordinamento tra le autorità di diversi Stati membri, vi debba essere un coordinamento interno tra le autorità del singolo Paese con competenze in materia di diritti dei consumatori, sia nel caso in cui i poteri vengano distribuiti tra le autorità sia e soprattutto ove ciascuna autorità venga dotata di tutti i poteri. Tale necessità è esplicitata dall'art. 5, par. 5, del Regolamento, che richiede agli Stati membri, ove ab-

469 Il considerando n. 17 specifica che l'oggetto di tali impegni potrebbe consistere nell'offerta ai consumatori, da parte dell'operatore che ha commesso l'infrazione, della riparazione dei danni causati dall'infrazione stessa, ovvero la concessione di rimedi come «la riparazione, la sostituzione, riduzioni del prezzo, la risoluzione del contratto o il rimborso dei prezzi corrisposti per beni o servizi, nella misura adeguata, per attenuare le conseguenze negative dell'infrazione», senza tuttavia «pregiudicare il diritto del consumatore di chiedere un risarcimento del danno mediante gli strumenti adeguati». Ai sensi dell'art. 20, par. 2, del Regolamento, le autorità coinvolte e la Commissione possono anche chiedere il parere di organizzazioni dei consumatori, associazioni degli operatori e altre parti interessate, in merito all'adeguatezza degli impegni proposti.

470 Per la prima fase, l'art. 9, par. 3, del Regolamento prevede che le autorità devono essere dotate almeno dei poteri di accesso a documenti, dati e informazioni anche presso altre autorità pubbliche, organismi o agenzie dello Stato, ovvero persone fisiche o giuridiche, nonché del potere di effettuare ispezioni in loco e di acquistare beni o servizi campione, anche in forma anonima, al fine di individuare infrazioni e raccogliere prove. Per la fase esecutiva vengono invece previsti i poteri di: adottare misure cautelari per evitare il rischio di danni agli interessi collettivi dei consumatori; di ottenere e accettare impegni da parte degli operatori responsabili di infrazioni; di informare i consumatori lesi su come richiedere una compensazione; di obbligare per iscritto l'operatore a cessare le infrazioni ed eventualmente il potere di far cessare o vietare tali infrazioni e, nell'eventualità in cui non siano disponibili altri mezzi efficaci per far cessare o vietare l'infrazione: il potere di rimuovere i contenuti lesivi, limitare l'accesso all'interfaccia *online* (anche tramite imposizioni ai prestatori di servizi di *hosting* o ai registri e alle autorità di registrazione del dominio) o imporre la visualizzazione di un'avvertenza per i consumatori quando accedono all'interfaccia *online*. A questi si aggiunge, sempre nella fase esecutiva, il potere di irrogare sanzioni, quali ammende o penalità di mora, che siano effettive, proporzionate e dissuasive.

biano nel loro territorio più autorità competenti, di definirne chiaramente le competenze e garantire che operino in stretta collaborazione[471]. Il regolamento può dunque essere l'occasione per disciplinare in maniera più specifica il coordinamento tra le autorità competenti all'esecuzione delle norme poste a tutela dei consumatori.

5.5 La direttiva 2019/2161/UE

Sempre al fine di consentire una più efficace collaborazione tra le autorità nazionali competenti in materia di diritti dei consumatori, in linea con quanto previsto nel Regolamento (UE) 2017/2394, il legislatore europeo è poi intervenuto con la Direttiva 2019/2161/UE, che ha introdotto regole comuni per la Direttive 93/13/CEE sulle clausole abusive nei contratti stipulati con i consumatori, la Direttiva 98/6/CE riguardanti l'indicazione dei prezzi dei prodotti offerti ai consumatori, la Direttiva 2005/29/CE sulle pratiche commerciali sleali tra imprese e consumatori e la Direttiva 2011/83/UE sui diritti dei consumatori nel mercato interno. Si è però visto che, ai sensi dell'art. 3, par. 3, lett. d), della Direttiva 2011/83/UE (recepito dall'art. 47, co. 1, lett. d), cod. cons.), quest'ultima non riguarda i contratti aventi a oggetto servizi finanziari. Riguardano invece espressamente anche i servizi finanziari (in quanto richiamati in alcune delle loro disposizioni) le direttive sulle pratiche commerciali sleali e quelle sulle clausole abusive[472]. La Direttiva sull'indicazione dei prezzi dei prodotti offerti ai consumatori, invece, non richiama né esclude espressamente i servizi finanziari, che tuttavia sembrerebbero implicitamente esclusi dalla tipologia dei prodotti cui fa riferimento la Direttiva stessa.

Le quattro Direttive vengono aggiornate e implementate dalla Direttiva 2019/2161/UE sia sotto il profilo del *private enforcement* sia sotto quello del *public enforcement*. Quanto a quest'ultimo, viene reso omogeneo il regime sanzionatorio per le quattro direttive attraverso la fissazione di criteri comuni per la valutazione della gravità delle infrazioni. Infatti, le Direttive (98/6/CE), (2005/29/CE) e (2011/83/UE) contenevano solamente una clausola generale che demandava agli Stati membri la determinazione del regime delle sanzioni e l'adozione dei provvedimenti che ne consentissero l'applicazione, mentre la Direttiva (93/13/CEE) non prevedeva neppure una clausola generale e si limitava a chiedere agli Stati membri «mezzi adeguati ed efficaci per far cessare l'inserzione di clausole abusive nei contratti stipulati tra un professionista e dei consumatori» (art. 7). Ciò aveva comportato una disomogeneità tra le normative nazionali di recepimento delle Direttive e di individuazione dei regimi sanzionatori.

Pertanto, la Direttiva 2019/2161/UE ha inserito delle norme quasi identiche per le quattro direttive modificate[473], che, da un lato, stabiliscono che gli Stati membri

471 A differenza del Reg. (UE) 2017/2394, il previgente Reg. (CE) 2006/2004 stabiliva che ove lo Stato membro designasse più autorità pubbliche competenti, ciascuna di esse dovesse essere dotata dei necessari poteri investigativi ed esecutivi per l'applicazione del Regolamento.

472 V. *supra*, par. 2.

473 L'art. 8-*ter* per la Direttiva 93/13/CEE; l'art. 8 per la Direttiva 98/6/CE; l'art. 13 per la direttiva 2005/29/CE e l'art. 24 per la Direttiva 2011/83/UE.

debbano prevedere le disposizioni in materia di sanzioni conformemente alla Direttiva e fare in modo che tali sanzioni siano effettive, proporzionate e dissuasive, adottando quindi tutte le misure necessarie per garantirne l'attuazione; dall'altro, fissano dei criteri comuni, non esaustivi e indicativi, che devono essere tenuti in conto dagli Stati membri ai fini della determinazione delle sanzioni, come la natura, la gravità, l'entità e la durata dell'infrazione, eventuali precedenti dell'operatore o azioni intraprese dallo stesso per porre rimedio alle conseguenze dell'infrazione.

Inoltre, a eccezione delle sanzioni per infrazioni relative all'indicazione dei prezzi dei prodotti offerti ai consumatori (Direttiva 98/6/CE), in cui non è stata inserita analoga disposizione, qualora la sanzione debba essere inflitta nell'ambito di un'azione coordinata per un'infrazione diffusa o diffusa avente una dimensione unionale, ai sensi dell'art. 21 del Regolamento (UE) 2017/2394, gli Stati membri dovranno provvedere affinché tale sanzione possa essere di tipo pecuniario e «per un importo massimo almeno pari al 4% del fatturato annuo del venditore o fornitore nello Stato membro o negli Stati membri interessati»[474]. Qualora le informazioni sul fatturato non siano disponibili, l'importo massimo della sanzione dovrà essere di almeno 2 milioni di euro[475].

Le disposizioni sulle sanzioni adottate dagli Stati membri in recepimento della Direttiva 2019/2161/UE dovranno essere notificate alla Commissione entro il 28 novembre 2021.

Quanto alle misure di *private enforcement* contenute nella Direttiva 2019/2161/UE, queste riguardano principalmente la Direttiva 2005/29/CE sulle pratiche commerciali scorrette e la Direttiva 2011/83/UE su diritti del mercato interno, che però non si applica ai contratti aventi a oggetto servizi finanziari. Infatti, la modifica della Direttiva 93/13/CEE sulle clausole abusive è stata limitata all'introduzione delle sanzioni, mentre per la Direttiva 98/6/CE è stata introdotta un'unica disposizione (l'art. 6-*bis*), che stabilisce l'obbligo di indicare, negli annunci di riduzione del prezzo di un prodotto, il prezzo precedentemente applicato dal professionista per un determinato periodo di tempo prima della riduzione.

Con riferimento alla Direttiva sulle pratiche commerciali sleali tra imprese e consumatori (2005/29/CE), di interesse per il consumatore di servizi finanziari è l'in-

474 I. GARACI, *Il* Dieselgate. *Riflessioni sul* private e public enforcement *nella disciplina delle pratiche commerciali scorrette*, in *Riv. dir. ind.*, 2018, 2, 67, evidenzia come la sanzione inflitta dall'AGCM per la pratica commerciale scorretta posta in essere da Volkswagen, sebbene pari al massimo della pena prevista, fosse certamente inadeguata in relazione alle dimensioni economiche dell'impresa, come rilevato dall'autorità stessa.

475 I. SPEZIALE, *La Dir. 2019/2161 UE tra protezione dei consumatori e protezione della competitività sul mercato unico*, cit., 443, rileva come, in questo modo, la Direttiva armonizzi il livello minimo di sanzioni previste per le violazioni transfrontaliere, coerentemente con il considerando n. 16 del Reg. 2017/2394; T. BROGGIATO, *La tutela del consumatore nel rinnovato contesto*, cit., 307 e 314, non condivide invece la scelta del legislatore europeo di optare per un'armonizzazione minima stabilendo solamente l'importo minimo della sanzione massima; ciò potrebbe infatti implicare che, a fronte di identica violazione in diversi Stati membri, vi possa non essere uniformità di trattamento sotto il profilo sanzionatorio, posto che saranno poi i legislatori nazionali a stabilire il tetto massimo delle sanzioni. Si rischia così di penalizzare i professionisti senza peraltro assicurare un identico trattamento sanzionatorio tra i vari Stati membri. Ciò nondimeno, secondo l'A., questa potrebbe essere l'occasione per adottare un analogo sistema sanzionatorio per le violazioni domestiche, che non ricadono nel Regolamento sulla cooperazione, in quanto ciò rafforzerebbe il potere di *enforcement* dell'AGCM nei confronti di violazioni relative alla disciplina del Codice del consumo.

troduzione dell'art. 11-*bis*, in cui si stabilisce che ai consumatori lesi da pratiche commerciali scorrette devono essere concessi rimedi proporzionati ed effettivi, compreso il risarcimento del danno e, se pertinenti, la riduzione del prezzo o la risoluzione del contratto[476]. In precedenza, la Direttiva si limitava a stabilire, all'art. 3, par. 3, che le sue disposizioni non pregiudicavano l'applicazione del dritto contrattuale, con particolare riferimento alle norme su formazione, validità ed efficacia del contratto[477]. Non essendovi un obbligo di prevedere specifici rimedi nei confronti di pratiche commerciali sleali, gli Stati membri hanno adottato le soluzioni più varie, ad esempio non intervenendo con disposizioni specifiche, affermando che la pratica commerciale sleale non rende invalido il contratto stipulato tra il professionista e il consumatore, richiamando i rimedi civilistici tradizionali o introducendone appositamente di nuovi[478].

Rispetto alla proposta originaria, la Direttiva consente agli Stati membri di stabilire le condizioni cui sono subordinati l'applicazione e gli effetti dei rimedi[479], tenendo eventualmente conto della gravità e della natura della pratica commerciale sleale, del danno subito dai consumatori e di altre circostanze pertinenti. Peraltro, tali rimedi non dovranno pregiudicare l'applicazione di altri rimedi riconosciuti ai consumatori dalle norme dell'Unione o del diritto nazionale[480]. Sul punto si segnala la differenza tra le conseguenze dell'accertamento amministrativo dell'illecito consumeristico,

476 F. Denozza, *Incongruenze, paradossi e molti vizi della tesi del "solo risarcimento" per le vittime di intese e abusi*, in *Nuova giur. civ.*, 2020, 2, 412, rileva come tale norma consenta ora ai consumatori di liberarsi dal vincolo contrattuale nell'ipotesi di clausole imposte con mezzi scorretti.

477 C. Granelli, *Pratiche commerciali scorrette: tutele individuali*, in *Nuova giur. civ.*, 2019, 5, 1079, evidenzia che tale previsione aveva finito per addossare all'interprete il coordinamento del divieto di pratiche commerciali scorrette con i rimedi interni; si distinse così tra i rimedi risarcitori, con riferimento sia a un contratto concluso sia a un contratto non concluso, e rimedi caducatori, con eventuali conseguenti effetti restitutori.

478 Così I. Speziale, *La Dir. 2019/2161 UE tra protezione dei consumatori e protezione della competitività sul mercato unico*, cit., 444, che richiama De Cristofaro, *Le conseguenze privatistiche della violazione del divieto di pratiche commerciali sleali: analisi comparata delle soluzioni accolte nei diritti nazionali dei Paesi UE*, in *Rass. dir. civ.*, 2010, 2, 880 ss., rilevando altresì che, nello stesso senso dell'art. 3, il considerando n. 9 della dir. 2005, il quale prevede che non sono pregiudicati i ricorsi individuali proposti da soggetti che siano stati lesi da una pratica commerciale sleale, consentiva ancora ai legislatori nazionali di non accordare ai consumatori ricorsi individuali *ad hoc* diversi da quelli già esistenti, né li obbligava a riconoscere ai soggetti lesi la legittimazione a richiedere in giudizio il risarcimento dei danni. Secondo l'A., il nuovo art. 11-*bis* rappresenta un progresso rispetto a quanto stabilito dall'art. 3 e dal considerando 9, ma non risolve definitivamente le divergenze tra le normative nazionali, posto che l'individuazione dei soli rimedi minimi lascia ancora agli Stati membri un ampio margine di discrezionalità nell'individuazione concreta e nella disciplina dei rimedi.

479 Così T. Broggiato, *La tutela del consumatore nel rinnovato contesto*, cit., 309-310 e 314, secondo la quale, al contrario del rimedio risarcitorio, che non richiederà modifiche alla normativa nazionale, per i rimedi contrattuali servirà una modifica legislativa di rilievo, «il cui impatto nelle relazioni commerciali tra imprese e consumatori sarà verosimilmente tanto più significativo quanto maggiore sarà l'automatismo stabilito dal legislatore tra dichiarazione di scorrettezza della pratica e possibilità di richiedere la risoluzione del contratto inciso dalla pratica medesima». Sarà quindi opportuno che il legislatore utilizzi la facoltà, riconosciutagli dalla Direttiva, di individuare le condizioni cui è subordinata l'applicazione dei rimedi; una previsione generica dei rimedi rischierebbe di spingere i consumatori di servizi bancari e finanziari a un uso distorto dello strumento, con conseguente aumento dei contenziosi non solo a scapito delle imprese, ma anche dei consumatori che non abbiano valutato appieno le conseguenze dell'interruzione anticipata del rapporto contrattuale.

480 Come evidenziato da C. Granelli, *Pratiche commerciali scorrette: tutele individuali*, cit., 1080, anche la materia delle pratiche commerciali scorrette è oggetto del disegno di legge-delega per la revisione del codice civile, che all'art. 1, co. 1, lett. g), prevede proprio la disciplina dei casi in cui le pratiche negoziali ingannevoli, aggressive o comunque scorrette determinano l'invalidità del contratto. L'A., alla luce della più ampia proposta europea di riforma della direttiva 2005/29, che all'epoca in cui scriveva non si era ancora tradotta nella direttiva 2019/2161, si interrogava giustamente sull'opportunità di intervenire, a livello nazionale, sulla sola disciplina dell'invalidità del contratto stipulato in presenza di una pratica commerciale scorretta.

quale è la pratica commerciale scorretta, dall'illecito finanziario, ad esempio per violazione degli obblighi di informazione incombenti sull'intermediario: mentre nel primo caso, il consumatore potrà accedere a rimedi invalidativi e ripristinatori dello *status quo ante*, nel secondo potrà ottenere solamente la risoluzione del contratto e il risarcimento del danno da inadempimento degli obblighi incombenti sull'intermediario[481].

5.6 *(segue)* Le azioni rappresentative a tutela di interessi collettivi dei consumatori e la l. 31/2019

Sempre in tema di *private enforcement* e al fine di fornire ai consumatori strumenti efficaci di ricorso contro le violazioni dei loro diritti, nel *New Deal* è stata inserita anche una proposta di Direttiva finalizzata a disciplinare le azioni rappresentative a tutela degli interessi collettivi dei consumatori[482], che si è tradotta nella Direttiva 2020/1828/UE.

La nuova Direttiva abroga la precedente 2009/22/CE relativa ai provvedimenti inibitori a tutela degli interessi dei consumatori[483]; quest'ultima, come si legge nelle considerazioni della nuova[484], aveva consentito agli enti legittimati di agire per far cessare o vietare condotte lesive degli interessi collettivi dei consumatori, ma non aveva affrontato adeguatamente le problematiche relative all'applicazione della normativa a tutela dei consumatori. Pertanto, rispetto alla Direttiva 2009/22/CE viene anzitutto ampliato l'àmbito di applicazione dell'azione rappresentativa alle violazioni, nazionali e transfrontaliere, delle disposizioni relative ai 66 atti legislativi dell'Unione indicati nell'allegato I alla Direttiva stessa (art. 2), tra cui quelli riguardanti «la protezione dei dati, i servizi finanziari, i viaggi e il turismo, l'energia e le telecomunicazioni»[485].

Analogamente alla precedente Direttiva 2009/22/CE, la possibilità di intentare le azioni rappresentative è sempre riconosciuta agli «enti legittimati»; peraltro, la qualità di ente legittimato non viene più attribuita a qualsiasi organismo od organizzazione costituito secondo la legge di uno Stato membro, per il solo fatto che abbia un

481 Così A. GENOVESE, Regolazione finanziaria e consumeristica in tema di offerta di servizi finanziari e di investimento, cit., 365.

482 COM(2018) 184 *final*, cit.

483 La Direttiva 2009/22/CE del Parlamento europeo e del Consiglio del 23 aprile 2009 relativa a provvedimenti inibitori a tutela degli interessi dei consumatori è già stata modificata dal Regolamento (UE) 2018/302 del Parlamento europeo e del Consiglio del 28 febbraio 2018 recante misure volte a impedire i blocchi geografici ingiustificati e altre forme di discriminazione basate sulla nazionalità, sul luogo di residenza o sul luogo di stabilimento dei clienti nell'ambito del mercato interno e che modifica i regolamenti (CE) n. 2006/2004 e (UE) 2017/2394 e la direttiva 2009/22/CE; sul Regolamento (UE) 2018/302 vedi V. FALCE, *Appunti sul Regolamento europeo sul* geo-blocking *e la neutralità geografica. In cammino verso il mercato unico digitale*, in *Contratto e impr.*, 2019, 4, 1287 ss.

484 Considerando n. 5.

485 Direttiva 2020/1828, considerando n. 13, in cui si rileva che «Poiché i consumatori si muovono oggi in un mercato più vasto e sempre più digitalizzato, per offrire loro un livello elevato di protezione è necessario che, oltre al diritto generale dei consumatori, la presente direttiva copra settori quali la protezione dei dati, i servizi finanziari, i viaggi e il turismo, l'energia e le telecomunicazioni». L'elenco è comunque potenzialmente aperto; il successivo considerando n. 17 prevede, infatti, che ogni qualvolta venga adottato un nuovo atto dell'Unione in materia di tutela degli interessi collettivi dei consumatori, il legislatore dovrebbe valutare se modificare l'allegato I e farvi rientrare il nuovo atto dell'Unione nell'àmbito di applicazione della Direttiva.

legittimo interesse a far rispettare i diritti dei consumatori; questa volta viene previsto che sia lo Stato membro, a seguito di richiesta dell'ente, a valutare se esso soddisfi determinati criteri[486] e a designarlo quale ente legittimato in generale o per l'esercizio di una specifica azione rappresentativa. Il soddisfacimento dei criteri da parte degli enti legittimati designati va poi verificato ogni cinque anni dallo Stato membro, come previsto dall'art. 5, par. 3, della Direttiva 2020/1828/UE. Sempre ai sensi dell'art. 5, gli Stati membri devono predisporre un elenco degli enti legittimati, che deve essere reso accessibile al pubblico e comunicato anticipatamente alla Commissione, che a sua volta redige e rende pubblico un elenco degli enti legittimati di tutti gli Stati membri.

Al fine di tutelare i consumatori anche nei casi di violazioni transazionali, in particolare quando questi vivono in uno o più Stati membri diversi da quello del professionista responsabile della violazione[487], l'art. 6 della Direttiva prevede che l'ente legittimato di uno Stato membro, inserito nel relativo elenco pubblico, possa rivolgersi all'organo giurisdizionale o amministrativo di altro Stato, ferma restando la possibilità per l'organo di verificare se la finalità dell'ente lo legittimi a esperire la specifica azione; si tratta dell'azione rappresentativa transfrontaliera. Inoltre, l'art. 6, par. 2, prevede anche la possibilità di esperire una sorta di azione super-rappresentativa transfrontaliera, ovvero un'azione intentata da enti legittimati di diversi Stati membri, quando la violazione leda o possa ledere consumatori di diversi Stati[488]; rispetto alla proposta di direttiva, è stata eliminata la previsione circa la possibilità per gli enti legittimati di agire eleggendo tra di loro un unico rappresentante.

La Direttiva prevede che gli Stati membri debbano garantire agli enti legittimati di intentare azioni rappresentative dinanzi ai loro organi giurisdizionali o alle autorità amministrative e di poter chiedere l'emissione di provvedimenti almeno di tipo

486 Ai sensi dell'art. 4, par. 3, lett. a)-f), della Direttiva, l'ente deve essere: una persona giuridica costituita in conformità al diritto dello Stato membro che lo designa e dimostrare dodici mesi di attività pubblica effettiva nella tutela degli interessi dei consumatori prima della richiesta di designazione; il suo oggetto sociale deve dimostrare il perseguimento della finalità di tutela degli interessi dei consumatori tra quelli rientranti nell'àmbito di applicazione della Direttiva; non deve perseguire uno scopo di lucro; non dove essere soggetto a procedura di insolvenza o comunque dichiarato insolvente; deve essere indipendente e non influenzato da persone diverse dai consumatori e deve disporre di procedure atte a prevenire tale influenza; deve rendere pubblico, in un linguaggio semplice e comprensibile e con qualsiasi mezzo appropriato, in particolare sul suo sito web, informazioni che dimostrino il soddisfacimento dei primi due requisiti, nonché informazioni sulle fonti di finanziamento, sulla struttura organizzativa, gestionale e partecipativa, sull'oggetto sociale e sulle attività.

487 Così il considerando n. 20 della Direttiva; A. CILENTO, New deal *per i consumatori: risultati all'altezza delle ambizioni?*, cit., 1198, rileva come la nuova disciplina delle azioni rappresentative miri a fornire ai consumatori uno strumento omogeneo e facilmente applicabile negli Stati membri, che possa evitare una frammentazione dei mezzi di tutela e una conseguente disparità di trattamento tra consumatori e operatori commerciali di diversi Stati.

488 In tema di foro competente a conoscere dell'azione rappresentativa transfrontaliera, L. SERAFINELLI, *Ancora sulla tutela del consumatore, anche in forma collettiva*, in *Nuova giur. civ. comm.*, 2019, 3, 618 ss., rileva (con riferimento alla proposta di Direttiva, ma con ragionamento estendibile alla Direttiva 2020/1828/UE, posto che le disposizioni non sono state modificate) come dal combinato disposto dell'art. 16, par. 2 (ora art. 6, par. 2, della Direttiva) con l'art. 2, par. 3 (che fa salve le norme dell'Unione di diritto privato internazionale, in particolare quelle in materia di giurisdizione e diritto applicabile) deriva l'impossibilità di ritenere competente il foro del consumatore per le azioni rappresentative risarcitorie transfrontaliere, a meno che non siano gli Stati membri a prevedere la competenza del foro del consumatore, in deroga alla disciplina europea. Infatti, il considerando n. 31 della Direttiva prevede proprio che gli «enti legittimati di diversi Stati membri dovrebbero poter unire le forze in un'unica azione rappresentativa in un singolo foro, fatte salve le pertinenti norme sulla competenza giurisdizionale». Secondo l'A., sarebbe stato opportuno prevedere la competenza del foro del consumatore anche per la nuova azione rappresentativa europea, in quanto la necessità di proporre l'azione presso l'organo dello Stato membro in cui è stabilito il professionista potrebbe avere un effetto deterrente, proprio per il timore che tale organo possa essere più favorevole al professionista.

inibitorio e risarcitorio, eventualmente anche attraverso l'esercizio di un'unica azione e con un'unica decisione (art. 7). In ogni caso, l'azione rappresentativa deve poter essere esperita o continuata anche nei confronti di violazioni cessate prima che questa sia stata avviata o si sia conclusa (art. 2, par. 1)[489].

Quanto ai provvedimenti inibitori tesi a far cessare o vietare una pratica, questi devono poter essere sia provvisori sia definitivi, in quest'ultimo caso con la possibilità di contenere, oltre all'accertamento che la pratica costituisce una violazione di cui all'art. 2, par. 1, della Direttiva, anche un obbligo di pubblicare la decisione relativa al provvedimento o una dichiarazione di rettifica (art. 8, parr. 1 e 2). Quanto ai provvedimenti risarcitori, questi devono poter imporre al professionista di offrire ai consumatori interessati rimedi quali l'indennizzo, la riparazione o la sostituzione del bene, la riduzione o il rimborso del prezzo e la risoluzione del contratto. La loro emissione non è subordinata al precedente accertamento della violazione da parte di un organo giurisdizionale o di un'autorità amministrativa, potendo l'accertamento essere effettuato direttamente nell'ambito dell'azione risarcitoria (art. 9, par. 8); qualora la violazione sia stata già accertata con decisione definitiva di un organo giurisdizionale o di un'autorità amministrativa di qualsiasi Stato membro, invece, tale decisione potrà essere utilizzata da tutte le parti come prova nell'ambito dell'azione rappresentativa risarcitoria nei confronti dello stesso professionista e per la stessa pratica, conformemente al diritto nazionale in materia di valutazione delle prove (art. 15)[490].

Con riferimento ai meccanismi di partecipazione dei singoli consumatori alle azioni rappresentative, la Direttiva prevede che, in caso di azione volta a ottenere un provvedimento inibitorio, l'ente legittimato non debba essere tenuto a ottenere mandato dai consumatori né a provare la perdita o i danni effettivi subiti dagli stessi in conseguenza della violazione. Specularmente, i consumatori non devono essere tenuti a manifestare la volontà di farsi rappresentare dall'ente nell'azione inibitoria (art. 8, par. 3); ciò in quanto essi beneficerebbero comunque della cessazione o della proibizione della pratica commerciale costituente violazione, senza la necessità di conferire

489 Nel considerando n. 20 della Direttiva si rileva, infatti, che l'azione rappresentativa dovrebbe potere essere altresì esperita nei confronti di violazioni già cessate, in quanto potrebbe essere necessario prevenire il ripetersi della pratica.

490 La Direttiva 2020/1828/UE non riproduce il sistema che era stato delineato nella relativa proposta: quest'ultima, ai fini dell'esperimento di azioni rappresentative volte all'eliminazione degli effetti perduranti della violazione (ovvero le azioni risarcitorie), richiedeva che tale violazione fosse stata già accertata da una decisione definitiva, salvo la possibilità di chiedere i provvedimenti tesi a eliminare gli effetti della violazione unitamente all'accertamento della violazione stessa (COM(2018) 184 *final*, cit., art. 5, par.par. 3 e 4). Inoltre, «Al fine di aumentare la certezza giuridica, evitare incoerenze nell'applicazione del diritto dell'Unione e incrementare l'efficacia e l'efficienza procedurale delle azioni rappresentative» (così il considerando n. 33 della proposta di Direttiva) l'art. 10 della proposta di Direttiva richiedeva agli Stati membri di garantire che la decisione definitiva, anche ricognitiva della responsabilità di un professionista, emessa dall'organo giurisdizionale o amministrativo, che accertasse una violazione a danno degli interessi collettivi dei consumatori, non potesse essere rimessa in discussione e fosse vincolante ai fini di eventuali e successive azioni di natura risarcitoria dinanzi ai loro organi giurisdizionali. Diversamente, le decisioni definitive emesse da organi di altri Stati membri, a eccezione di quelle ricognitive della responsabilità del professionista, potevano essere considerate quali presunzioni relative dell'avvenuta violazione. Già T. Broggiato, *La tutela del consumatore nel rinnovato contesto*, cit., 312 ss., segnalava come l'eventuale recepimento di una simile disposizione a livello nazionale sarebbe stato problematico (posto che l'unica deroga al giudicato, rappresentata dalla disciplina antitrust, è stata per lungo tempo oggetto di discussione, vista la sua estraneità al sistema processuale italiano) e auspicava l'accoglimento della proposta alternativa emersa in sede di discussione al Parlamento europeo, che prevedeva proprio l'attenuazione dell'efficacia delle decisioni definitive nel giudizio civile da presunzioni inconfutabili della violazione a presunzioni semplici, come tali suscettibili di prova contraria e non vincolanti per il giudice.

mandato all'ente o che questo provi il loro specifico danno[491]. Inoltre, l'ente legittimato non è tenuto a dimostrare la condotta intenzionale o negligente del professionista (sempre art. 8, par. 3), in quanto la cessazione e la proibizione di una violazione potenzialmente lesiva per i consumatori non deve dipendere dal fatto che questa sia stata posta in essere dal professionista con dolo o colpa[492].

Per le azioni rappresentative risarcitorie, invece, la Direttiva lascia agli Stati membri la possibilità di scegliere se i singoli consumatori debbano manifestare espressamente o tacitamente la loro volontà di aderire all'azione e di esserne vincolati dall'esito[493] (sebbene entro un limite di tempo appropriato dopo la sua proposizione), con l'unica eccezione dei consumatori che non risiedono abitualmente nello Stato membro dell'organo giurisdizionale o dell'autorità amministrativa adita, che invece devono manifestare espressamente la volontà di essere rappresentati nell'azione al fine di esserne vincolati dall'esito[494]. Peraltro, la Direttiva stabilisce che, a prescindere dall'adesione all'azione, gli Stati membri debbano consentire ai consumatori di beneficiare dei rimedi previsti dal provvedimento risarcitorio anche successivamente alla sua emissione, senza che sia necessario intentare un'azione distinta e purché sia sempre stabilito un limite di tempo per beneficiare del provvedimento (art. 9, par.par. 6 e 7). Al fine di consentire l'adesione successiva, la Direttiva prevede che, qualora il provvedimento risarcitorio non individui i singoli consumatori che hanno diritto di beneficiare dei rimedi dallo stesso previsti, tale provvedimento dovrà almeno contenere una descrizione del gruppo dei consumatori che hanno diritto di beneficiarne (art. 9, par. 5)[495].

Per le azioni risarcitorie, inoltre, gli enti legittimati devono comunicare all'organo giurisdizionale o all'autorità amministrativa un resoconto finanziario che elenca

491 Cfr. il considerando n. 37.

492 Così il considerando n. 33.

493 In realtà, più che della scelta tra l'adesione esplicita all'azione e quella tacita, si tratterebbe della scelta tra i contrapposti meccanismi dell'*opt-in* e dell'*opt-out*, in base ai quali i consumatori devono, rispettivamente, manifestare espressamente la propria volontà di aderire all'azione per esserne vincolati dagli effetti, ovvero, sempre espressamente, quella di esserne esclusi al fine di evitare l'inclusione automatica quale conseguenza dell'appartenenza a una determinata classe di consumatori. A. CILENTO, New deal *per i consumatori: risultati all'altezza delle ambizioni?*, cit., 1205-1206, spec. nt. 41, rileva evidenzia come la scelta non sia priva di conseguenze pratiche, in quanto il meccanismo può pregiudicare i diritti individuali dei singoli a beneficio di una tutela effettiva (nel caso dell'*opt-out*) o viceversa (nel caso dell'*opt-in*); secondo I. GARACI, *Il* Dieselgate. *Riflessioni sul* private *e* public enforcement *nella disciplina delle pratiche commerciali scorrette*, cit., 69, il meccanismo dell'*opt-in* può invece rivelarsi un punto debole, in quanto il grado di deterrenza dello strumento dipenderà dal numero di aderenti alla *class action*.

494 Come indicato nel considerando n. 43, la *ratio* della disposizione è quella di rispettare le tradizioni giuridiche degli Stati membri. Quanto alla *ratio* dell'eccezione, invece, nel considerando n. 45 si rileva che la necessità dell'adesione espressa da parte dei consumatori non abitualmente residenti è finalizzata a garantire la buona amministrazione della giustizia e a evitare decisioni incompatibili. In effetti, se, ai sensi dell'art. 9, par. 4, della Direttiva 2020/1828/UE, l'adesione all'azione rappresentativa deve precludere al consumatore la possibilità di essere rappresentato in un'altra azione rappresentativa o di agire individualmente nei confronti dello stesso professionista e per la medesima *causa petendi*, l'eventualità di una nuova ed eventualmente incompatibile decisione vincolante per il medesimo consumatore non sarebbe facilmente scongiurabile ove questo fosse stato rappresentato automaticamente in un'azione rappresentativa intentata in uno Stato membro in cui il consumatore non risiede abitualmente; ciò sia in termini di conoscibilità dell'inclusione per il consumatore sia in termini di conoscibilità del precedente per il nuovo giudicante.

495 A differenza di quanto era stato inizialmente proposto (COM(2018) 184 *final*, cit., art. 6, par. 2 e 3), non viene invece prevista la possibilità per gli Stati membri di autorizzare l'organo giurisdizionale o amministrativo a emettere una decisione semplicemente ricognitiva della responsabilità del professionista in caso di difficoltà nella quantificazione dei risarcimenti individuali (cfr. A. CILENTO, New deal *per i consumatori: risultati all'altezza delle ambizioni?*, cit., 1201-1202).

la fonte dei fondi utilizzati per finanziare la specifica azione rappresentativa (art. 10, par. 3). Per i casi di azioni finanziate da terzi, gli Stati membri devono adottare disposizioni idonee a evitare conflitti di interessi e a impedire che il finanziamento da parte di un terzo che abbia un interesse economico nella proposizione o nell'esito dell'azione rappresentativa possa allontanare questa dalla tutela degli interessi collettivi dei consumatori (art. 10, par. 1); in particolare, gli Stati devono evitare che tali finanziatori possano influenzare le decisioni dell'ente legittimato nel contesto dell'azione rappresentativa e dell'eventuale transazione, ovvero che possa essere finanziata un'azione contro un concorrente del terzo finanziatore o contro un soggetto dal quale il finanziatore dipende (art. 10, par. 2). Qualora l'organo giurisdizionale o amministrativo accerti tali circostanze, dovrà potere imporre all'ente di rifiutare o apportare modifiche riguardo al finanziamento, e, se necessario, opporsi alla legittimazione dell'ente ad agire nel caso specifico, senza che tale opposizione pregiudichi i diritti dei consumatori interessati dall'azione rappresentativa[496].

Al fine di garantire l'efficacia, anche deterrente, delle azioni rappresentative e l'effettività della tutela dei consumatori, la Direttiva prevede dei meccanismi di *enforcement* quali l'informazione dei consumatori danneggiati circa i provvedimenti emessi e le transazioni approvate[497], nonché sanzioni per l'inottemperanza del professionista a determinati obblighi. Quanto all'informazione dei consumatori danneggiati, l'art. 13, par. 3, della Direttiva prevede che l'organo giurisdizionale o l'autorità amministrativa che dispone i provvedimenti di cui all'articolo 7, ovvero approva una transazione nell'ambito di un'azione risarcitoria ai sensi dell'art. 11, deve fare obbligo al professionista di informarne a sue spese i consumatori interessati dall'azione attraverso mezzi appropriati alle circostanze del caso ed entro limiti di tempo prestabiliti[498]. Nel caso di rigetto di un'azione rappresentativa volta a ottenere provvedimenti risarcitori, l'obbligo di informazione incomberà invece sull'ente legittimato (art. 13, par. 4).

Quanto alle sanzioni, l'art. 19 della Direttiva prevede che gli Stati membri debbano prevedere delle sanzioni effettive, proporzionate e dissuasive, anche sotto forma di ammenda, per l'inadempimento del professionista al provvedimento inibitorio o all'obbligo di pubblicare la decisione o una dichiarazione di rettifica ai sensi dell'art. 8, par. 2, lett. b), al predetto obbligo di informazione di cui all'art. 13, par. 3, ovvero all'obbligo di esibizione delle prove imposto dall'organo giudicante, come previsto dall'art. 18 della Direttiva.

496 Probabilmente anche per evitare tali ipotesi, oltre che per attribuire ai consumatori mezzi di tutela effettivi e accessibili, l'art. 20 della Direttiva 2020/1828/UE prevede che gli Stati membri adottino le misure necessarie per garantire che le spese procedurali delle azioni rappresentative non costituiscano un impedimento per gli enti legittimati, ad esempio eliminando o riducendo i diritti amministrativi e giudiziari, concedendo agli enti il patrocinio a spese dello Stato o fornendogli finanziamenti pubblici.

497 Il considerando n. 60 della Direttiva rileva come i rischi reputazionali associati alla diffusione delle informazioni relative a una violazione siano importanti per l'effetto deterrente che esercitano sui professionisti.

498 Nel considerando n. 61 della Direttiva viene specificato che i mezzi da utilizzare per l'informazione potrebbero essere lo stesso sito web del professionista, i *social media*, i mercati online o quotidiani diffusi, nonché, ove possibile, anche la posta orinaria o elettronica.

Infine, la Direttiva prevede una serie di disposizioni finalizzate a riconoscere e preservare la disciplina procedurale e i meccanismi di ricorso già presenti negli ordinamenti nazionali: da un lato, l'art. 1, par. 2, stabilisce che la Direttiva non dovrebbe impedire agli Stati membri di adottare o mantenere altri mezzi procedurali di tutela degli interessi collettivi dei consumatori; dall'altro, viene previsto che la disciplina procedurale specifica della stessa azione rappresentativa debba essere lasciata alla discrezionalità degli Stati membri, affinché questi possano regolarla secondo la propria tradizione giuridica, riconducendola a un meccanismo di ricorso già esistente o prevedendone uno *ad hoc*, purché almeno un meccanismo procedurale nazionale sia conforme alla Direttiva[499].

Nell'ordinamento italiano, la Direttiva 2020/1828/UE potrebbe essere recepita conformando o integrando, ove necessario, la nuova disciplina dell'azione di classe, riformata e trasferita dal codice del consumo al codice di procedura civile dalla l. 12 aprile 2019, n. 31. Gli abrogati artt. 139 e 140 cod. cons. prevedevano la possibilità, per le associazioni dei consumatori e degli utenti rappresentative a livello nazionale e iscritte nell'elenco tenuto presso il Ministero dello sviluppo economico, di agire a tutela degli interessi collettivi dei consumatori e degli utenti al fine di ottenere provvedimenti inibitori dei comportamenti lesivi, l'adozione di misure idonee a eliminare gli effetti dannosi delle violazioni e l'eventuale pubblicazione del provvedimento[500]. L'art. 140-*bis*, invece, prevedeva la possibilità di tutelare interessi collettivi o diritti individuali omogenei dei consumatori attraverso un'azione di classe finalizzata a ottenere l'accertamento della responsabilità e la condanna al risarcimento del danno e alle restituzioni. In tal caso, la legittimazione ad agire era però riconosciuta a ciascun componente della classe, che poteva intentarla anche mediante un'associazione o comitato; all'azione intrapresa da un componente potevano poi aderirne altri, ma così rinunciando a ogni azione restitutoria o risarcitoria individuale fondata sul medesimo titolo[501].

L'azione inibitoria è stata trasferita all'art. 840-*sexiesdecies* c.p.c. e, come previsto anche dall'art. 7, par. 5, della Direttiva 2020/1828/UE, può ora essere proposta congiuntamente all'azione di classe, ora disciplinata agli artt. 840-*bis* e ss. c.p.c. Il trasferimento delle azioni dal codice del consumo a quello di rito ha comportato un notevole ampliamento sia dal punto di vista dei soggetti legittimati ad agire sia da quello dei diritti azionabili, in quanto le azioni non sono più limitate ai consumatori e ai relativi diritti. L'azione inibitoria collettiva è stata estesa a "chiunque" abbia interesse a

499 Così il considerando n. 11 della Direttiva 2020/1828; secondo A. Cilento, New deal *per i consumatori: risultati all'altezza delle ambizioni?*, cit., 1207-1208, la scelta dello strumento della Direttiva non consentirà di raggiungere l'obiettivo di armonizzazione della tutela, posta la discrezionalità lasciata agli Stati membri nella fase di recepimento e le peculiarità degli ordinamenti processuali nazionali.

500 Si è poi visto che l'art. 32-bis T.U.F. attribuisce alle associazioni dei consumatori inserite nell'elenco di cui all'art. 137 cod. cons. la legittimazione ad agire ai sensi degli abrogati artt. 139 e 140 cod. cons. anche per la tutela degli interessi degli investitori. L'art. 137 cod. cons. non è stato modificato dalla l. 31/2019, sicché le associazioni dei consumatori possono sempre agire a tutela degli interessi degli investitori.

501 A. Cilento, New deal *per i consumatori: risultati all'altezza delle ambizioni?*, cit., 1204-1205, evidenzia come alla luce del fatto che l'azione di classe non poteva essere instaurata da un'associazione consumeristica intesa come parte processuale, ma doveva essere instaurata necessariamente da un singolo attore in rappresentanza della classe, la giurisprudenza (Trib. Milano, 9 dicembre 2013, ma v. anche Trib. Milano, ord. 3 luglio 2017) aveva escluso che questa potesse essere cumulata con l'azione inibitoria prevista dagli artt. 139-140 cod. cons.

ottenere l'inibizione di atti e comportamenti pregiudizievoli per una pluralità di individui o enti, mentre l'azione di classe è ora esperibile dal componente di una qualsiasi classe e a tutela di qualsiasi diritto omogeneo[502]. Inoltre, entrambe le azioni, e non solo quella inibitoria, possono ora essere esperite da organizzazioni e associazioni senza scopo di lucro, i cui obiettivi statutari comprendono la tutela degli specifici diritti che si assumono lesi e che siano iscritte in un elenco pubblico istituito presso il Ministero della giustizia[503]. Con riferimento specifico all'azione di classe, va infine segnalato l'inserimento della possibilità di aderire all'azione, oltre che al momento della sua introduzione (art. 840-*quinquies* c.p.c.), anche successivamente all'emissione del provvedimento di accoglimento (art. 840-*sexies*, co. 1, lett. e), c.p.c.), in linea con quanto è ora richiesto dall'art. 9, par. 7, della Direttiva 2020/1828/UE.

La disciplina delle azioni collettive del codice di procedura civile presenta quindi evidenti similitudini con l'azione rappresentativa europea, ma le differenze sono altrettanto evidenti e significative. Ad esempio, le azioni collettive hanno una portata più ampia dell'azione rappresentativa sia sotto il profilo soggettivo (in quanto non azionabili dai soli enti legittimati) sia sotto quello oggettivo (in quanto non limitate a determinati atti normativi). D'altra parte, l'azione rappresentativa consente di tutelare i consumatori anche nei confronti di violazioni transfrontaliere. Il legislatore italiano è quindi chiamato a un accurato lavoro di coordinamento tra le due normative, al fine di evitare che incertezze applicative possano pregiudicare l'effettività della tutela[504].

5.7 Il commercio elettronico e il Digital Services Act

L'Unione europea è in procinto di emanare anche delle norme volte ad adeguare le regole del mercato digitale all'evoluzione sociale, economica e tecnologica. Nella comunicazione "*Shaping Europe's Digital Future*"[505], la Commissione europea si è infatti impegnata ad aggiornare le norme che disciplinano i servizi digitali. Da tale impegno sono conseguite due proposte di Regolamento, uno finalizzato a disciplinare obbligazioni e responsabilità dei fornitori di servizi digitali – con particolare riferimento ai fornitori di piattaforme online – nei confronti dei consumatori ("*Digital Services*

502 T. Broggiato, *La tutela del consumatore nel rinnovato contesto*, cit., 312 ss., rileva come la platea dei possibili attori sia ora allargata anche a imprese e pubbliche amministrazioni, mentre l'àmbito di tutela delle situazioni giuridiche sia stato esteso a qualunque condotta lesiva e non solo alla violazione di diritti spettanti al consumatore o all'utente, così come era previsto dall'art. 140-*bis* cod. cons.

503 Secondo C. Granelli, *Pratiche commerciali scorrette: tutele individuali*, cit., 1078 ss., la situazione non cambia molto neppure con il nuovo art. 840-*sexiesdecies* c.p.c., posto che i provvedimenti richiedibili con la nuova azione inibitoria sono analoghi a quelli che potevano essere richiesti con l'abrogato art. 140 cod. cons., sicché non vi è motivo di ritenere che l'indirizzo giurisprudenziale, teso a escludere la possibilità di richiedere il risarcimento dei danni nell'ambito dell'azione inibitoria, possa mutare a seguito della riforma. Sul punto va però segnalato che proprio la possibilità di cumulare l'azione inibitoria *ex* art. 840-*sexiesdecies* con quella riparatoria *ex* art. 840-*bis*, nonché la possibilità che anche quest'ultima azione, al pari di quella inibitoria, possa essere introdotta da organizzazioni e associazioni, dovrebbe fare venire meno le ragioni che avevano portato la giurisprudenza a escludere che, nell'ambito di un'azione inibitoria introdotta da tali enti, potesse essere richiesto il risarcimento del danno, che era invece riservato all'azione individuale o collettiva dei consumatori.

504 T. Broggiato, La tutela del consumatore nel rinnovato contesto, cit., 315; A. Cilento, New deal per i consumatori: risultati all'altezza delle ambizioni?, cit., 1207.

505 Comunicazione della Commissione europea "*Shaping Europe's Digital Future*" del 19 febbraio 2020.

Act"[506]), l'altro finalizzato a regolare la concorrenza nel mercato digitale ("*Digital Markets Act*"[507]), in particolare nelle piattaforme digitali, quali motori di ricerca, *social network* o piattaforme di condivisione di video, in cui è presente un soggetto che gestisce la piattaforma o che ha comunque una posizione in grado di incidere significativamente nel mercato interno (i cc.dd. «*gatekeepers*»)[508].

Quanto al *Digital Services Act*, esso si pone quale riforma dell'attuale disciplina europea sull'*e-commerce*, e in particolare della Direttiva sul commercio elettronico (2000/31/CE)[509], che verrebbe appunto modificata dal Regolamento mantenendone i principi chiave in tema, ad esempio, di responsabilità per i fornitori di servizi digitali e per gli intermediari, ma al tempo stesso adattandone le disposizioni all'evoluzione digitale, in particolare prevedendo degli standard più alti in tema di trasparenza e *accountability* per i fornitori di piattaforme digitali. A tal fine, viene ritenuto opportuno utilizzare lo strumento del Regolamento invece della Direttiva, proprio per assicurare un'effettiva armonizzazione ed evitare una frammentazione legale, come era accaduto per la Direttiva sul commercio elettronico.

Anche in questo caso, la proposta legislativa prevede misure di *private enforcement* e di *public enforcement*. Tra le prime si annoverano le già menzionate disposizioni in tema di obbligazioni e responsabilità dei *providers* di servizi di informazione.

Da un lato, come detto, la proposta di Regolamento mantiene i principi chiave della Direttiva 2000/31/CE in tema di esonero da responsabilità dei *providers*. Le ipotesi di esonero da responsabilità dei *providers* per «*mere conduit*», «*caching*» e «*hosting*» (artt. 12, 13 e 14 della Direttiva)[510] vengono sostanzialmente trasposte negli artt. 3, 4 e 5 della proposta di Regolamento, con un'unica aggiunta per il caso di memorizzazione di informazioni (*hosting*) volta a escludere l'esonero da responsabilità dei *providers* di piattaforme per *l'e-commerce* nei confronti dei consumatori, quando la piattaforma mostri specifiche informazioni o comunque consenta le transazioni in maniera tale da poter far credere a un consumatore avveduto che il prodotto o servizio oggetto della transazione sia fornito dalla stessa piattaforma online o comunque da un soggetto che agisce sotto l'autorità o il controllo della piattaforma. Peraltro, benché i casi di esonero da responsabilità vengano riproposti senza recepire nuove definizioni oramai acquisite nel linguaggio della giurisprudenza e della dottrina, come quelle di *hosting provider* passivo e *hosting provider* attivo[511], la proposta di Regolamento tiene comunque conto

506 COM(2020) 825 *final*, cit.

507 *Proposal for a Regulation of the Euopean Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act)*, SEC(2020) 437 *final*, SWD(2020) 363 *final*, SWD(2020) 364 *final*, Bruxelles, 15 dicembre 2020, COM(2020) 842 *final*.

508 Cfr. artt. 1, 3 e 3 della proposta di Regolamento.

509 Direttiva 2000/31/CE del Parlamento europeo e del Consiglio dell'8 giugno 2000 relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno («Direttiva sul commercio elettronico»), recepita in Italia dal D.Lgs. 9 aprile 2003, n. 70; Direttiva che si applica anche ai servizi finanziari (v. *supra*, par. 2).

510 Artt. 14, 15 e 16 del D.Lgs. 9 aprile 2003, n. 70.

511 Cfr. R. Bocchini, *Responsabilità civile dell'*hosting provider. *La responsabilità civile plurisoggettiva, successiva ed eventuale dell'ISP*, nota a Cass., civ., sez. I, 19 marzo 2019, n. 7708, in *Giur. it.*, 2019, 12, pp. 2604 ss.; E. Bassoli, *Il caso RTI vs. Vimeo e la responsabilità civile dell'*hosting provider *attivo: sentenza n. 693/2019 del Tribunale di Roma*, in *Nuovo dir. civ.*, 2019, 2, pp. 123 ss.

dell'evoluzione giurisprudenziale, e in particolare delle interpretazioni della Corte di Giustizia dell'Unione Europea, che hanno appunto portato a distinguere i casi in cui il *provider* svolga una mera funzione "passiva" di memorizzazione o trasmissione delle informazioni dai casi in cui, invece, il *provider* abbia un ruolo attivo, tale da consentirgli di conoscere o controllare le informazioni; in quest'ultima ipotesi, non dovrebbero applicarsi le esenzioni da responsabilità previste dalla proposta di Regolamento per le attività di *mere conduit*, *caching* e *hosting*[512].

Dall'altro lato, la proposta di Regolamento stabilisce degli specifici obblighi per i *providers* in tema di trasparenza e *accountability*, volti a incrementare la sicurezza dei mercati online. Agli obblighi per i *providers* in generale (artt. 10-15), si affiancano obblighi specifici per i fornitori di piattaforme online più piccole, fatta eccezione per le piattaforme online qualificabili come microimprese e piccole imprese ai sensi dell'Allegato I alla Raccomandazione 2003/361/EC[513] (artt. 16-24) e per le «*very large online platforms*» (artt. 25-33), ovvero le piattaforme il cui numero medio mensile di utenti nell'Unione è pari o superiore ai 45 milioni.

In tema di *public enforcement*, invece, la proposta di Regolamento, oltre a demandare agli Stati membri l'individuazione di regole specifiche che stabiliscano delle penali per le violazioni delle obbligazioni previste dal Regolamento da parte dei *providers* (art. 42), prevede anche che gli Stati debbano designare una o più autorità competenti quali responsabili dell'applicazione e del rispetto delle disposizioni del Regolamento (art. 38), attribuendo a una di queste la funzione di coordinamento a livello nazionale («*Digital Services Coordinator*»), che assieme alle autorità di coordinamento degli altri Stati membri comporrà l'*European Board for Digital Services*.

Peraltro, la materia del commercio elettronico rientra nell'àmbito di applicazione del Regolamento (UE) 2017/2394 sulla cooperazione e il coordinamento delle autorità nazionali per la tutela dei consumatori[514], il quale consente agli Stati membri di scegliere se attribuire i poteri minimi stabiliti dal Regolamento a ciascuna autorità nazionale competente in materia di diritti dei consumatori, ovvero se distribuirli tra queste[515]. Pertanto, a seguito dell'approvazione e dell'entrata in vigore del Regolamento sul *Digital Services Act*, gli Stati membri, in sede di adeguamento dei propri ordinamenti alla nuova normativa europea e di conferimento dei poteri alle autorità nazionali competenti in materia di consumatori, saranno chiamati anche a un coordinamento tra i due Regolamenti.

512 V. i considerando 18-22 della proposta di Regolamento. Con riferimento alla giurisprudenza cui fanno riferimento i considerando, v. Corte Giust. UE, sez. III, 7 agosto 2018, n. 521, *Coöperative Vereniging SNB-REACT U.A.* c. *De. Me.*, C-521/17; Corte Giust. UE, sez. VII, 11 settembre 2014, n. 291, *Sotiris Papasavvas* c. *O Fileleftheros Dimosia Etaireia Ltd* e altri, C-291/13; Cort. Giust. UE, Grande Sez., 12 luglio 2011, n. 324, *L'Oréal S.A.* e altri c. *eBay International AG* e altri, C-324/09; Corte Giust. UE, Grande Sez., 23 marzo 2010, n. 236, *Google France S.A.R.L.* e *Google Inc.* c. *Luis Vuitton Malletier S.A.* e altri, da C-236/08 a C-238/08. Nella giurisprudenza italiana v. Trib. Roma, sez. XVII, 10 gennaio 2019, n. 693; Corte App. Milano, sez. impr., 7 gennaio 2015, n. 29; Trib. Milano, sez. propr. ind. e int., 7 giugno 2011, n. 7680.

513 Raccomandazione della Commissione del 6 maggio 2003 relativa alla definizione delle microimprese, piccole e medie imprese, 2003/361/CE.

514 La Direttiva 2000/31/CE è infatti indicata nell'allegato al Regolamento (UE) 2017/2394, che elenca le norme che rientrano nel suo àmbito di applicazione.

515 V. *supra*, par. 2.

Infine, con specifico riferimento alle *very large online platforms*, la proposta di Regolamento prevede delle disposizioni relative alla supervisione, alle indagini e all'*enforcement*, attribuendo i corrispondenti poteri alla Commissione, la quale, in caso di violazioni, potrà adottare decisioni, irrogare sanzioni e penali con obbligo di pagamento periodico (art. 58-60).

Quaderni FinTech

8 – aprile 2021 **La portabilità dei dati in ambito finanziario**
A cura di A. Genovese e V. Falce

7 – settembre 2020 **Do investors rely on robots?**
Evidence from an experimental study
B. Alemanni, A. Angelovski, D. Di Cagno, A. Galliera, N. Linciano, F. Marazzi, P. Soccorso

6 – dicembre 2019 **Valore della consulenza finanziaria e *robo advice* nella percezione degli investitori**
Evidenze da un'analisi qualitative
M. Caratelli, C. Giannotti, N. Linciano, P. Soccorso

5 – luglio 2019 **Marketplace lending**
Verso nuove forme di intermediazione finanziaria?
A. *Sciarrone Alibrandi, G. Borello, R. Ferretti, F. Lenoci, E. Macchiavello, F. Mattassoglio, F. Panisi*

4 – marzo 2019 **Financial Data Aggregation e Account Information Services**
Questioni regolamentari e profili di business
A. Burchi, S. Mezzacapo, P. Musile Tanzi, V. Troiano

3 – gennaio 2019 **La digitalizzazione della consulenza in materia di investimenti finanziari**
Gruppo di lavoro CONSOB, Scuola Superiore Sant'Anna di Pisa, Università Bocconi, Università di Pavia, Università di Roma 'Tor Vergata', Università di Verona

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

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