DALL'*OPEN BANKING* ALL'*OPEN FINANCE*

Profili di diritto dell'economia

a cura di

VALERIA FALCE e UMBERTO MORERA

con contributi di

Filippo Annunziata
Magda Bianco
Marco Cassese
Giuseppe Colangelo
Valeria Falce
Stefano Firpo
Tommaso Edoardo Frosini
Sara Landini
Marino Ottavio Perassi
Liliana Fratini Passi
Maddalena Rabitti
Biancamaria Raganelli
Pasquale Stanzione
Andrea Stazi
Maria Iride Vangelisti

G. GIAPPICHELLI EDITORE – TORINO

UNIVERSITÀ EUROPEA DI ROMA

Collana del
Dipartimento di Scienze Umane

Fondata da Alberto M. Gambino

Diretta da

Emanuele Bilotti - Valeria Falce - Alberto M. Gambino
Loredana Giani - Marco Maugeri - Filippo Vari

Sezione Giuridica – Materiali

10

DALL'*OPEN BANKING* ALL'*OPEN FINANCE*

Profili di diritto dell'economia

a cura di

VALERIA FALCE e UMBERTO MORERA

con contributi di

Filippo Annunziata
Magda Bianco
Marco Cassese
Giuseppe Colangelo
Valeria Falce
Stefano Firpo
Tommaso Edoardo Frosini
Sara Landini
Marino Ottavio Perassi
Liliana Fratini Passi
Maddalena Rabitti
Biancamaria Raganelli
Pasquale Stanzione
Andrea Stazi
Maria Iride Vangelisti

G. GIAPPICHELLI EDITORE – TORINO

VIA PO, 21 - TEL. 011-81.53.111
http://www.giappichelli.it

ISBN/EAN 979-12-211-0693-0
ISBN/EAN 979-12-211-5695-9 (ebook - pdf)

La pubblicazione di volumi nella Collana del Dipartimento di Scienze Umane dell'Università Europea di Roma è disciplinata da apposito regolamento, disponibile sul sito internet dell'Editore (*www.giappichelli.it*) e dell'Università Europea di Roma (*www.universitaeuropeadiroma.it*).

Si ringraziano la Banca d'Italia, il Deep-in Research network e il Dipartimento di Scienze Umane dell'Università Europea di Roma per il contributo e il sostegno alle attività di ricerca e alla pubblicazione del Volume.

Composizione: Voxel Informatica s.a.s. - Chieri (TO)

Stampa: Stampatre s.r.l. - Torino

Indice

pag.

pag.

Marino Ottavio Perassi

Prefazione

Nel guardare allo sviluppo dell'integrazione europea si incontra frequentemente l'affermazione secondo cui l'evoluzione istituzionale del nostro continente avviene per effetto di improvvise accelerazioni, seguite da lunghi periodi di bonaccia. E le accelerazioni sarebbero per lo più generate dalla necessità, di far fronte a crisi sistemiche, talvolta estremamente gravi.

Se pensiamo al quadro di riferimento normativo ed alle istituzioni che compongono oggi l'Unione Bancaria, il legame con il momento di grande difficoltà del sistema finanziario, vissuto a partire dal 2008, e la relativa reazione risulta evidente.

Una linea evolutiva differente riguarda l'introduzione della moneta unica. L'Euro è arrivato al termine di una serie di rilevanti eventi, fra i quali, indubbiamente, anche momenti di tensione sul fronte valutario nei rapporti fra paese europei, ma il suo meccanismo di gestione, imperniato sulla Banca Centrale Europea e sull'Eurosistema, è stato codificato in norme di rango primario (Trattato TFUE e Statuto SEBC/BCE) dopo un adeguato periodo di convergenza economica e legale, di armonizzazione delle regole.

Prima come moneta virtuale, poi anche in forma concreta, con la diffusione di banconote e monete, l'Euro si è affermato come mezzo di pagamento avente corso legale in un numero crescente di Stati Membri nel corso degli anni, superando gelosia nazionali legate alla regola, che sembrava inscalfibile, della sovranità monetaria statale, realizzando una storica cessione di sovranità ad una istituzione europea.

L'effetto dell'Euro è andato ben al di là della possibilità di pagare beni e servizi in gran parte d'Europa con le stesse banconote, la moneta unica ha svolto un effetto ben più ampio.

È cresciuta, per effetto della crisi di debitori sovrani e di interi sistemi bancari, la consapevolezza della necessità di difendere il metro monetario come bene comune, con le inevitabili ricadute, in senso evolutivo, sul ruolo della BCE e dell'Eurosistema.

E si è verificato un effetto trainante nell'evoluzione dei servizi concernenti il trasferimento della moneta bancaria, superando la limitazione dovuta alle frontiere ed alle diverse giurisdizioni, con una fortissima spinta alla uniformazione di regole e prassi.

Non si può certo dire che una sola moneta significhi anche un solo sistema bancario, in quanto rilevanti differenze rimangono fra le varie economie ed i sistemi finanziari europei, ma certo la *driving force* dell'Euro si fa sentire con tutta la sua influenza anche al di là del mondo delle istituzioni creditizie, fino a giungere a sostenere, insieme ad altri fattori, il progetto di *Capital Market Union*.

L'Europa ed il suo sistema bancario e finanziario non crescono perciò solo per effetto delle reazioni, talvolta frettolose, alle crisi, ma anche grazie a progetti di lungo periodo ed alla costruzione di soluzioni istituzionali innovative.

Superate, quindi, le barriere valutarie con i connessi rischi di cambio, il passo successivo è stato rappresentato dalla uniformazione delle regole in materia di fornitura di servizi, nel movimento e nella circolazione della moneta scritturale ed in questo contesto si colloca la normativa sull'*Open Banking* adottata a livello europeo.

Veniamo ora ai contenuti del volume.

A quasi dieci anni dalla direttiva che ha introdotto lo strumento dell'*Open Banking* e che ha innescato un processo di sviluppo, è arrivato il momento di parlare di *Open Finance* nel quadro di un complesso progetto di regole che si inquadrano nell'ambito della strategia europea per la finanza digitale, come ci ricorda Valeria Falce.

La numerosità e la complessità degli atti previsti in questo progetto ci portano necessariamente ad affrontare il tema della qualità della regolazione e sulla difficoltà, messa in luce da Giuseppe Colangelo, di calibrare accuratamente l'impostazione dell'intervento di regolazione, in un contesto con mercati di riferimento assai differenti.

Ancora una volta si affronta il dilemma fra intervenire preventivamente in via legislativa, in un sistema complesso e multilivello come quello europeo, in materie suscettibili di evoluzioni rapide ed imprevedibili, ovvero attendere la sedimentazione di rapporti giuridici inter-privati, prima di disciplinare il settore.

La prima opzione sconta il rischio inevitabile della rapidissima obsolescenza del tessuto normativo, si pensi al caso del regolamento MICAR, appena adottato e ancora da attuare in concreto, ma già considerato superato da alcuni studiosi; la seconda lascia spazio ad iniziative innovative e creati-

ve, ma talvolta dannose per utenti e sistema, con le relative critiche ai regolatori per la mancanza di tempestivi interventi.

L'attivismo delle istituzioni europee, nella grande prateria generata dalla unificazione monetaria, si muove nella prima direzione e non solo nel settore bancario e finanziario, se si pensa che il cd. *AI act* sarà con tutta probabilità la prima disciplina a livello globale sull'intelligenza artificiale.

Vedremo se anche su questo terreno si realizzerà il cd. *Brussels effect*.

Un punto di equilibrio fra le diverse possibili soluzioni, che eviti il rischio di ipertrofia normativa, si può forse trovare nella legislazione per principi, lasciando poi al mercato lo spazio per generare prassi condivise e costantemente osservate, da elevare eventualmente a normativa secondaria in un secondo momento, come suggeriscono Stefano Firpo e Maddalena Rabitti.

Il ruolo dell'intervento pubblico non si limita ovviamente alla miglior regolamentazione, ma coinvolge il ruolo delle autorità di volta in volta chiamate ad intervenire laddove occorre una tutela del patrimonio informativo della clientela, finalità da bilanciare con gli effetti positivi dell'apertura a forme di concorrenza nella loro gestione, lo ricorda Andrea Stazi.

Del resto la protezione dei dati personali, il cui valore non si misura solo nel campo della tutela della riservatezza, ma anche in termini economici, diviene un elemento molto importante nel momento in cui il sistema si apre alla loro circolazione, lo sottolinea Pasquale Stanzione.

E Marco Cassese osserva come l'attività di profilazione dei dati rappresenti un punto di contatto fra la normativa di *Open Banking* e le regole, ancora una volta molto complesse, del Regolamento europeo cd. GDPR.

E le autorità sono chiamate anche ad agire laddove gli effetti della rivoluzione dell'*Open Banking* può trovare ancora spazi ulteriori per portare effetti positivi per l'utenza, in particolare per la clientela meno evoluta e ancora priva di adeguata educazione finanziaria, secondo l'analisi di Magda Bianco e Maria Iride Vangelisti.

Gli effetti della rivoluzione digitale e la possibilità di gestire grandi masse di dati con sistemi sempre più sofisticati raggiungono ormai settori diversi da quello tradizionale creditizio. Si pensi al comparto assicurativo, lo ricorda Sara Landini, e, più in generale, al già citato fenomeno di *Open Finance*, con il coinvolgimento di vari settori e le molteplici problematiche messe in luce da Liliana Passi Fratini e Biancamaria Raganelli.

Ed è infine lecito spingersi oltre i confini della finanza tradizionale nel settore ancora in gran parte inesplorato del cripto-attività, dove si attende

l'effetto regolatorio del già citato Regolamento MICAR, secondo la ricostruzione di Filippo Annunziata, che ritrova negli strumenti che consentono ad una data applicazione di accedere a funzionalità e a dati di altre applicazioni, o più in generale, di altri servizi digitali il punto di contatto fra *Open Finance* e cripto-attività.

18 marzo 2024

Valeria Falce e Umberto Morera

Introduzione

Un volume incentrato su *Open Banking* e *Open Finance* appare scontare in prima battuta un difetto di definizione; risultando ancora troppo vaghe concettualmente tali locuzioni, anche nel ristretto àmbito degli operatori del settore bancario e finanziario.

D'altra parte, ad un'analisi più attenta del fenomeno sussiste l'impressione che l'*Open Banking* e l'*Open Finance* – che indiscutibilmente rappresentano un modo nuovo di concepire la gestione dell'impresa bancaria e finanziaria – se vengono spesso ricondotti alla più generale cultura e filosofia dei c.d. *open data*, in realtà esprimono e rappresentano una sorta di declinazione della c.d. *open innovation*, così ben teorizzata all'inizio degli anni 2000.

Inserendosi in questo solco, l'ambizione del volume, che si inserisce in un più ampio progetto dedicato alla finanza aperta, è dunque quella di mettere a fuoco i molti profili che restano ancora eccessivamente opachi, sia nel campo dell'*Open Banking*, che in quello dell'*Open Finance*.

Il guanto di sfida è raccolto dalle Istituzioni, dai cultori della materia e dagli operatori del settore che, ciascuno per parte sua, ha dapprima contribuito a sgombrare il campo da dubbi ricostruttivi, per poi offrire proposte di analisi e soluzioni operative.

L'auspicio consegnato dal volume a regolatori e interpreti è innanzitutto di ordine, nel groviglio normativo che ormai caratterizza la c.d. economia digitale. Ove invero sembra difficile negare che coesistano *ratio legis* tra loro a dir poco contraddittorie; con "intrecci" di (*i*) incentivi e libertà sui dati (si pensi alle regole delle PSD2 e PSD3) e (*ii*) divieti e protezioni (si pensi al Regolamento 679/2016 sulla protezione dei dati personali).

Ma c'è anche da confidare in un approccio multidisciplinare rispetto ai molti altri profili critici che caratterizzano la materia. Ad esempio, le conseguenze dell'*Open Banking* in termini di concorrenza; o anche le relazioni, e le possibili "sovrapposizioni", tra *Open Banking* e *Open Finance*.

Senza comunque sottovalutare l'analisi di quello che appare uno degli obiettivi fondamentali (seppur ancora piuttosto trascurato) dell'*Open Banking*: l'inclusione finanziaria dei soggetti meno evoluti e vulnerabili; obiettivo affatto secondario rispetto a quelli, più studiati, della competizione e dell'innovazione.

Infine, rimangono da indagare i tanti fattori *behavioral* che sembrano remare contro l'*Open Banking*. E si pensi soltanto a quei diffusi comportamenti umani per cui, perlomeno in principio, si tende a preferire l'anonimato; o si è spesso restii a condividere con altri i propri dati personali; ovvero si possiede una tendenziale sfiducia nei confronti degli operatori non bancari.

Adelante, dunque, Pedro, ma con juicio. Si puedes …

Roma, 23 aprile 2024

V.F. – U.M.

Valeria Falce

Verso l'*Open Finance*

SOMMARIO: 1. Introduzione. – 2. Il quadro regolamentare del pacchetto "Financial Data Access and Payments Package". – 2.1. Cenni alla direttiva sui servizi di pagamento e sui servizi di moneta elettronica nel mercato interno (PSD3). – 2.2. ... al regolamento relativo ai servizi di pagamento nel mercato interno (PSR). – 2.3. ... e al regolamento relativo a un quadro per l'accesso ai dati finanziari (FiDA). – 3. Conclusioni preliminari.

1. Introduzione

Concepito come evoluzione dell'*Open Banking*[1], l'*Open Finance*[2] prosegue il percorso segnato dal "decennio digitale" e dalla Strategia europea[3]

[1] Per una approfondita analisi del fenomeno si veda, tra i vari: R. PELLITTIERI, R. PARRINI, C. CAFAROTTI, B.A. DE VENDICTIS, *Mercati, infrastrutture, sistemi di pagamento. L'Open Banking nel sistema dei pagamenti: evoluzione infrastrutturale, innovazione e sicurezza, prassi di vigilanza e sorveglianza*, in *Quaderno Banca d'Italia,* n. 31, marzo 2023; A. BOT, P. HOFFMANN, L. LAEVEN, L. RATNOVSKI, *Discussion Paper Series Financial intermediation and technology: what's old, what's new? No. 11*, in *European Central Bank Discussion Paper Series*, 2023.

[2] Sul punto e per un inquadramento di ampio respiro dello stato dell'arte si veda: OECD, *Shifting from Open Banking to Open Finance: Results from the 2022 OECD survey on data sharing frameworks*, in *OECD Business and Finance Policy Papers*, 2023; OECD, *Data Portability in Open Banking. Privacy and The Other Cross-Cutting Issues*, in *OECD Digital Economy Papers*, 348, February 2023, in *oecd-ilibrary.org*.

[3] Nell'ambito del programma strategico per il decennio digitale si sono già percorse diverse tappe. Tra le più rilevanti aventi carattere trasversale si annoverano l'adozione della Carta dei diritti e principi digitali (*European Declaration on Digital Rights and Principles for the Digital Decade* 2023/C 23/01, PUB/2023/89, OJ C 23, 23.1.2023, p. 1-7), la presentazione di una proposta di regolamento sull'intelligenza artificiale (Brussels, COM/2021/206 final), la previsione di regimi normativi in materia di condivisione e gestione dei dati, da affiancarsi al regolamento 2016/679/UE, quali il *Data Act* e il *Data Governance Act* (rispettivamente, regolamento 2023/2854/UE e regolamento 2022/868/UE).

per la finanza digitale [4], con l'obiettivo di dare impulso al mercato europeo dei dati.

Punto di partenza è l'urgenza di una soluzione di sistema in risposta ad una doppia forza centrifuga (che attraversa anche il settore finanziario).

La prima, di natura verticale, si registra a livello di comunicazione, determinando per un verso il graduale ridimensionamento del ruolo tradizionalmente rivestito dalle banche di "primo punto di contatto", e per altro verso (o meglio come naturale conseguenza) l'espansione delle piattaforme digitali [5], che si arrogano il ruolo di "re-intermediari" del mercato e si inseriscono nell'offerta di servizi specializzati, spesso integrati con altri servizi finanziari e non finanziari. La seconda, di rilievo orizzontale [6], si coglie a livello di informazione, determinando per un

[4] La strategia è stata adottata dalla Commissione con la comunicazione COM(2020) 591 final, del 24 settembre 2020. Il percorso viene, però, da più lontano ed è stato modulato da un gruppo di comunicazioni, l'una susseguente all'altra. Dapprima, la Commissione ha adottato il "*FinTech Action Plan For a more competitive and innovative European financial sector*", COM(2018)109; nel 2020, la Commissione ha anche adottato la comunicazione relativa a "*una strategia in materia di pagamenti al dettaglio per l'UE*", COM(2020) 592 final, del 24 settembre 2020 in cui ha definito le priorità della Commissione per il settore dei pagamenti al dettaglio per la durata del mandato dell'attuale collegio dei commissari (2019-2024); poi, nel 2021, la Commissione ha adottato la comunicazione "*Il sistema economico e finanziario europeo: promuovere l'apertura, la forza e la resilienza*", COM(2021) 32 final, del 19 gennaio 2021.

[5] Il punto è efficacemente illustrato da A. BOT, P. HOFFMANN, L. LAEVEN, L. RATNOVSKI, *Discussion Paper Series Financial intermediation and technology: what's old, what's new? No. 11, ibidem*, in cui si rileva come tramite la piattaformizzazione dei servizi finanziari si sia incentivata l'inclusione finanziaria e si siano praticamente azzerati i costi di ricerca, potendo i consumatori agevolmente comparare prezzi e fornitori, ricevere prodotti e servizi modulati e personalizzati a prezzi più contenuti. Del pari, si rileva come ciò incrementi inevitabilmente rischi di *lock-in* e massimizzi il ruolo rivestito dai dati nel settore finanziario, ponendo i Big Player in una situazione di vantaggio competitivo rispetto agli altri operatori. Ciò, però, si precisa, solo nelle relazioni B2C, dal momento che il mercato B2B è ancora fortemente legato e dipendente dagli istituti bancari tradizionali.

Quanto sopra, è anche confortato da vari studi economici. Si veda, tra i vari: Stein, 2002; L. LAEVEN, L. RATNOVSKI, H. TONG, *Bank size, capital, and systemic risk: Some international evidence*, in *Journal of Banking & Finance*, Volume 69, Supplement 1, 2016; A. FUSTER, P.S. GOLDSMITH-PINKHAM, T. RAMADORAI, A. WALTHER, *Predictably Unequal? The Effects of Machine Learning on Credit Markets* (June 21, 2021), in *Journal of Finance, Forthcoming*, Available at SSRN: https://ssrn.com/abstract=3072038 or http://dx.doi.org/10.2139/ssrn.3072038.

[6] Anche qui, il punto è efficacemente illustrato da A. BOT, P. HOFFMANN, L. LAEVEN, L. RATNOVSKI, *Discussion Paper Series Financial intermediation and technology: what's old, what's new? No. 11*, *ibidem*, in cui si rileva come il settore sia sempre più ricco di informazioni, finanziarie e non finanziarie, facilmente condivisibili, che sono sempre più utilizzate per abilitare intelligenza artificiale e machine learning. Il paper evidenzia come la disgregazione orizzontale non sia stata facilitata solo dalle innovazioni tecnologiche, ma anche dalla regolamentazione che

verso il crescente ricorso all'*hard information*, anche di natura non finanziaria (che non solo si propone come più completa, precisa, strutturata e facilmente condivisibile, ma che abilita tecnologie come l'intelligenza artificiale e il *machine learning*) e per altro verso accelerando l'emersione di nuovi servizi [7].

La risposta, che trova nel sistema dei pagamenti digitali un fondamentale antecedente logico ancor prima che giuridico [8-9], è rappresentata dal *Financial Data Access and Payments Package* e passa per il regolamento relativo ai servizi di pagamento nel mercato interno [10] (PSR o regolamento), la direttiva sui servizi di pagamento e sui servizi di moneta elettronica nel mercato interno [11] (PSD3 o direttiva) e il regolamento relativo a un quadro per l'accesso ai dati finanziari [12] (o FiDA).

Si tratta di un pacchetto che, esprimendo al contempo una ulteriore tappa per l'*Open Banking* e una leva fondamentale per l'*Open Finance*,

---

spesso non richiede, ad esempio, licenze specifiche per l'offerta di determinati servizi finanziari (es. servizi di pagamento elettronico).

[7] Da questo tipo di disgregazione, i benefici che se ne traggono sono molteplici: bassi costi di ricerca, facilità di incontro tra domanda e offerta, potenziale riduzione delle inefficienze di mercato, facilitazione nella erogazione dei prestiti. Parimenti sono molteplici i rischi cui può andarsi incontro: frodi, sfruttamento di gruppi statistici errati, discriminazione dei consumatori e inefficienze di mercato.

[8] Per un approfondimento sulle iniziative regolamentari nel settore FinTech, aggiornato al 2021, si veda Banca d'Italia, Intervento di ALESSANDRA PERRAZZELLI, *Le iniziative regolamentari per il Fintech: a che punto siamo?*, Università degli Studi dell'Insurbia, Laboratorio di Finanza Digitale, 2021, p. 2. Mi si permetta di rinviare a: 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; C. SCHENA, A. TANDA, C. ARLOTTA, G. POTENZA, *Lo Sviluppo del Fintech – Opportunità e Rischi per l'Industria Finanziaria nell'Era Digitale*, CONSOB, Milano, 2018; BANCA D'ITALIA, *Fintech in Italia – Indagine Conoscitiva sull'Adozione delle Innovazioni Tecnologiche Applicate ai Servizi Finanziari*, Banca d'Italia, Roma, 2017; R. LENER, *Fintech: Diritto, Tecnologia e Finanza*, Minerva bancaria, Roma, 2018; A. JANCZUK-GORYWODA, *Evolution of EU Retail Payments Law*, in (2015) 40 *European Law Review* 858; R. FERRARI, *L'era del Fintech. La Rivoluzione Digitale nei Servizi Finanziari*, Franco Angeli, Milano, 2016; M. ZACHARIADIS-P. OZCAN, *The API economy and digital transformation in financial services: the case of Open Banking*, in (2016) *SWIFT Institute Working Paper* n. 2016-001; D. ZAOTTINI, L. LO PRATO, *La centralità dell'Unione Europea nei Settori Bancario, Finanziario ed Assicurativo*, Servizio Studi del Senato, 2018; D. MILANESI, *A new banking paradigm: the state of Open Banking in Europe, the United Kingdom and the United States*, in (2017) *TTLF Working Papers* n. 29; ISO/TC 307 – Blockchain and Distributed Ledger Technologies.

[9] EXPERT GROUP ON EUROPEAN FINANCIAL DATA SPACE, *Report on Open Finance*, (2022) 35, https://finance.ec.europa.eu/publications/report-open-finance_en.

[10] Bruxelles, 28 giugno 2023 COM(2023) 367 final.

[11] Bruxelles, 28 giugno 2023 COM(2023) 366 final.

[12] Bruxelles, 28 giugno 2023 COM(2023) 360 final.

raccorda la Strategia europea sui pagamenti [13] e la più ampia Strategia europea sulla finanza digitale [14].

Il pacchetto opera su due distinti ed intrecciati piani. L'uno, finalizzato alla revisione della PSD2, e l'altro, funzionale alla instaurazione di un regime di condivisione dei dati finanziari all'interno dell'Unione europea.

I due piani muovono da un comun denominatore: la PSD2, che, come noto, impone, attraverso la regola del c.d. *access to account rule*, obblighi di condivisione dei dati dei conti di pagamento [15], che non risultano aver sbloccato il mercato. Nonostante le nuove regole di accesso [16], infatti, i prestatori di servizi bancari aperti stentano a penetrare i mercati, mentre i prestatori di servizi di pagamento scontano la perdurante condizione di incertezza normativa e di arbitraggio nella fase di enforcement.

L'antidoto del legislatore è a tutto tondo e passa per un ventaglio di proposte.

Dalla predisposizione e previsione, in favore dei consumatori, di diritti e strumenti pratici per gestire i propri dati personali tra cui, su tutti, i pannelli di gestione; alla collocazione, nell'ambito di una normativa di massima armonizzazione – e dunque in un regolamento – di gran parte della disciplina; alla previsione di modelli comuni e interoperabili di dati e inter-

---

[13] Bruxelles, 24 settembre 2020 COM(2020) 592 final, dalla quale emergono quattro pilastri chiave, che sono strettamente interconnessi: 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.

[14] Bruxelles, 24 settembre 2020 COM(2020) 591 final. Il *Digital Finance Package*, annunciato originariamente il 24 settembre 2020, è un insieme di strategie e regolamenti che mirano a fornire un quadro normativo che promuove l'innovazione e affronta i rischi potenziali, suddiviso in due documenti di strategia: *Digital Finance Strategy* e *Retail Payments Strategy*. Su quest'ultima strategia si veda B. COEURÉ, *Towards the retail payments of tomorrow: a European strategy*, speech at the Joint Conference of the ECB and the National Bank of Belgium on Crossing the chasm to the retail payments of tomorrow, 26 November 2019.

[15] La "*rule*", contenuta nell'art. 36 della PSD2, prevede che "*Gli Stati membri provvedono affinché gli istituti di pagamento abbiano accesso ai servizi relativi ai conti di pagamento degli enti creditizi in maniera obiettiva, proporzionata e non discriminatoria. L'accesso è sufficientemente ampio da consentire all'istituto di pagamento di fornire servizi di pagamento in modo agevole ed efficiente*" ed è considerata la norma cardine dell'impianto *Open Banking* unitamente al regime di licenze accordato ai prestatori di servizi di informazione su conti o di ordine di disposizione di pagamento.

[16] Nella valutazione d'impatto della PSD2 si evidenzia che, nonostante i diversi risultati conseguiti, vi è la persistenza di un generale clima di sfiducia, da parte dei consumatori, nei pagamenti, di un funzionamento imperfetto dell'*Open Banking*, di una disparità di condizioni tra banca e prestatori di servizi di pagamento non bancari e di una generale incoerenza dei poteri e degli obblighi delle autorità di vigilanza dei diversi Stati membri.

facce, nonché di schemi di condivisione dei dati; alla fissazione di compensi, almeno limitatamente al FiDA, per coloro che mettono a disposizione strumenti che garantiscano effettività della tutela dei consumatore e un certo grado di qualità dei pannelli di gestione; all'integrazione della norma XS2A predisponendo un obbligo di fornire l'accesso ai dati finanziari diversi da quelli relativi ai conti di pagamento; alla predisposizione di regole di *liability* anche in presenza di esternalizzazioni; all'allineamento normativo tra i diversi prestatori di servizi così da promuovere la concorrenza.

2. Il quadro regolamentare del pacchetto "Financial Data Access and Payments Package"

2.1. Cenni alla direttiva sui servizi di pagamento e sui servizi di moneta elettronica nel mercato interno (PSD3)

Il PSR e la PSD3 incidono la PSD2 su lati distinti. Mentre la proposta di direttiva [17] contiene in particolare norme in materia di autorizzazione e vigilanza degli istituti di pagamento [18], la proposta di regolamento che la accompagna contiene una disciplina completa dei prestatori di servizi di pagamento.

La PSD3, in primo luogo, allinea il quadro regolatorio in materia di autorizzazione [19] e di vigilanza tra i prestatori di servizi di pagamento e di

[17] La scelta di continuare a ricorrere allo strumento della direttiva in materia di vigilanza e autorizzazione è connessa al fatto che queste restano di competenza nazionale degli Stati membri.

[18] La direttiva, in particolare, disciplina le norme relative all'autorizzazione a svolgere l'attività di prestazione di servizi di pagamento e di servizi di moneta elettronica da parte degli istituti di pagamento, e non da parte di enti creditizi, e alla vigilanza degli stessi. Si veda: art. 1 della direttiva. In particolare, il comma 2 riconosce agli Stati membri "*esentare gli enti di cui all'articolo 2, paragrafo 5, punti da 4) a 23), della direttiva 2013/36/UE dall'applicazione della totalità o di una parte delle disposizioni della presente direttiva*". In aggiunta, nei commi successivi si chiarisce che, salvo diversa disposizione, con l'espressione "servizi di pagamento" suole farsi riferimento sia ai servizi di pagamento che a quelli di moneta elettronica; con "prestatori di servizi di pagamento" si intendono sia prestatori di servizi di pagamento che i prestatori di servizi di moneta elettronica.

[19] L'EDPS sottolinea come entrambe le proposte dovrebbero specificare che la concessione di "autorizzazioni" per accedere ai dati finanziari non equivale a dare il consenso o consenso esplicito ai sensi del GDPR. Di conseguenza, tutti i trattamenti di dati personali a seguito di una richiesta di accesso ai dati finanziari di un individuo devono avere una base giuridica adeguata

servizi di moneta elettronica. In secondo luogo, chiarisce e adatta alcune definizioni già presenti nella PSD2, al fine di garantire che la normativa dell'UE continui ad essere conforme al principio della neutralità tecnologica [20]. Il riferimento è, in particolare, alla definizione di conto di pagamento, di fondi e di strumento di pagamento [21].

Il titolo II della direttiva detta poi i requisiti, le condizioni, le procedure di controllo [22] e il procedimento richiesti ai fini del rilascio dell'autorizzazione [23], che sono rimasti quasi del tutto invariati rispetto alla PSD2.

Scorrendo il testo normativo, si riscontrano innanzitutto novità [24] relative al passaggio ad un'unica autorizzazione per i PSP e per gli IMEL che non raccolgono depositi e per l'obbligo di presentare, insieme alla domanda, un piano di liquidazione in caso di dissesto, proporzionato al modello commerciale dell'istituto di pagamento richiedente [25]. Al fine di garantire condizioni di parità tra gli istituti di pagamento e di moneta elettronica e un certo grado di armonizzazione e coerenza per il rilascio dell'autorizzazione, è previsto un termine di tre mesi, dal ricevimento della domanda, per la conclusione del processo di autorizzazione [26], affidando all'EBA il compito di elaborare progetti di norme tecniche di regolamentazione in materia di autorizzazione che specificano le informazioni da fornire alle autorità competenti nella relativa domanda degli istituti di pagamento, una metodologia di valutazione comune per il rilascio dell'autorizzazione o per la registrazione, cosa intendere per garanzia analoga a un'assicurazione per responsabilità civile professionale e i criteri da utilizzare per stabilire

ai sensi del GDPR. Si veda: EDPS, Opinion n. 39/2023 on the *Proposal for a Regulation on payments services*.

[20] Considerando n. 8 della direttiva.

[21] Si veda, in particolare, l'art. 2, nn. 13, 15 e 23 della direttiva.

[22] Art. 4 della direttiva.

[23] L'autorizzazione è in particolare necessaria solo per quei servizi di pagamento che l'istituto intende effettivamente fornire. Art. 3, comma 2, della direttiva.

[24] Art. 3, comma 3, della direttiva, che contiene l'elenco di tutte le informazioni necessarie da fornire insieme alla domanda di autorizzazione.

[25] Art. 3, comma 1, lett. s), della direttiva; Considerando n. 17 della direttiva, ai sensi del quale "*tale piano di liquidazione dovrebbe essere idoneo ad agevolare una liquidazione ordinata delle attività in conformità del diritto nazionale applicabile, nonché la continuità o la ripresa di eventuali attività critiche svolte da prestatori, agenti o distributori di servizi esternalizzati*".

[26] Art. 14 della direttiva, inoltre, in caso di diniego dell'autorizzazione le autorità competenti devono fornire le relative motivazioni. Sul punto, l'art. 13 comma 5, fornisce un elenco dei casi in cui le autorità negano l'autorizzazione.

l'importo minimo monetario dell'assicurazione per la responsabilità civile professionale o di altra garanzia [27].

In tale contesto sarà compito delle autorità competenti valutare attentamente il piano di *governance* presentato insieme alla domanda di autorizzazione, verificando, in particolar modo, l'adeguatezza dei dispositivi interni di governo societario [28]. L'EBA, in applicazione del principio di proporzionalità, avrà il compito di adottare orientamenti sui questi dispositivi interni, tenendo conto delle differenze tra gli istituti di pagamento in termini di dimensioni e di modelli commerciali. Inoltre, sempre ai fini di rilascio dell'autorizzazione e con l'obiettivo di evitare l'ipotesi in cui un istituto di pagamento si stabilisca fittiziamente in uno Stato membro, e dunque senza avere l'intenzione di esercitarvi alcuna attività, si richiede, innanzitutto, al suddetto istituto, di svolgere almeno parte della sua attività in materia di servizi di pagamento in tale Stato membro [29]. Poi, se l'istituto vi esercita attività diverse dalla prestazione di servizi di pagamento o di servizi di moneta elettronica, le autorità nazionali competenti possono imporre, come condizione per il rilascio dell'autorizzazione, la creazione di un'entità separata per la prestazione di servizi di pagamento o di servizi di moneta elettronica [30].

In materia di requisiti per il rilascio dell'autorizzazione occorre inoltre mettere in evidenza la previsione secondo cui ai prestatori di servizi di disposizione di ordine di pagamento e ai prestatori di servizi di informazione sui conti è riconosciuta la possibilità di detenere un capitale iniziale [31], al-

---

[27] Art. 3, comma 5, della direttiva.

[28] Art. 13, comma 1, della direttiva, che prevede che i dispositivi di governance e i meccanismi di controllo devono essere "*completi e proporzionati alla natura, all'ampiezza e alla complessità dei servizi di pagamento o dei servizi di moneta elettronica che gli istituti di pagamento richiedenti intendono prestare*".

[29] Art. 13, comma 3, della direttiva.

[30] Art. 13, comma 4, della direttiva in combinato disposto con il Considerando n. 39 della medesima direttiva, ove tale obbligo è imposto al fine di garantire una vigilanza adeguata dell'istituto di pagamento. La decisione di imporre la creazione della suddetta entità separata "*dovrebbe tenere conto del potenziale impatto negativo che un evento che interessa le altre attività commerciali potrebbe avere sulla solidità finanziaria dell'istituto di pagamento o del potenziale impatto negativo derivante da una situazione in cui l'istituto di pagamento non sia in grado di fornire rendicontazioni separate sui fondi propri rispetto alle sue attività di pagamento e di moneta elettronica e alle altre sue attività*".

[31] Art. 5 della direttiva. Tale possibilità deve tuttavia lasciare impregiudicato l'obbligo gravante su tali operatori di stipulare un'assicurazione per responsabilità civile professionale una volta ottenuta l'autorizzazione suddetta.

l'atto dell'autorizzazione, anziché di possedere un'assicurazione per responsabilità civile professionale. Al fine di affrontare i rischi connessi con le rispettive attività è in particolare richiesto che gli istituti di pagamento siano dotati di un capitale iniziale combinato con fondi propri[32], i cui requisiti patrimoniali iniziali sono stati aggiornati per tenere conto dell'inflazione registrata dall'adozione della PSD2[33]. Rimangono invariati, invece, i metodi di calcolo dei fondi propri[34], nonché le regole dettate in materia di custodia degli stessi[35], fatta eccezione per l'introduzione della possibilità di provvedere alla custodia in un conto presso una banca centrale, senza pregiudicare la discrezionalità della banca a non offrire tale opzione, e dell'obbligo per gli istituti di pagamento di adoperarsi per evitare il rischio di concentrazione nei fondi custoditi[36].

La disciplina proposta include ulteriori obblighi in capo agli istituti di pagamento una volta ottenuta l'autorizzazione. Invero, si richiede che questi conservino tutte le registrazioni adeguate e ivi previste per un periodo di almeno cinque anni e, nel caso in cui tali registrazioni includano dati personali, che gli stessi non dovrebbero essere conservati più a lungo di quanto sia necessario a tale scopo e, in caso di revoca[37] dell'autorizzazione, che i dati stessi non dovrebbero in ogni caso essere conservati per più di

---

[32] Art. 6, comma 1, ai sensi del quale "*Gli Stati membri esigono che i fondi propri degli istituti di pagamento non siano inferiori all'importo più elevato tra il capitale iniziale di cui all'articolo 5 e l'ammontare dei fondi propri calcolati ai sensi dell'articolo 7 per gli istituti di pagamento che non offrono servizi di moneta elettronica o ai sensi dell'articolo 8 per gli istituti di pagamento che offrono servizi di moneta elettronica*". Difatti, come si evince dal Considerando n. 23 della direttiva "*I prestatori di servizi di disposizione di ordine di pagamento e i prestatori di servizi di informazione sui conti, nel prestare tali servizi, non detengono fondi dei clienti. Conseguentemente sarebbe sproporzionato imporre a tali operatori del mercato requisiti di fondi propri. È tuttavia importante garantire che i prestatori di servizi di disposizione di ordine di pagamento e i prestatori di servizi di informazione sui conti siano in grado di far fronte alle proprie responsabilità in relazione alle attività svolte*".

[33] Considerando n. 26 della direttiva.

[34] Il riferimento è agli artt. 7 ss. della direttiva.

[35] Per quanto riguarda gli istituti di pagamento che prestano servizi di moneta elettronica, al fine di garantire condizioni di parità e di allineare i regimi applicabili ai fondi degli utenti, le prescrizioni relative alla custodia sono pienamente conformi a quelle che si applicano agli istituti di pagamento che forniscono esclusivamente servizi di pagamento. Considerando n. 31 della direttiva.

[36] Art. 9, comma 2, della direttiva. A tal riguardo, l'EBA deve adottare norme tecniche di regolamentazione sulla gestione dei rischi di tali fondi. Art. 9, comma 7, della direttiva.

[37] La revoca è disciplinata dall'art. 16 della direttiva, che indica i casi in cui le autorità motivatamente revocano l'autorizzazione concessa.

cinque anni dalla revoca[38]. Inoltre, è previsto l'obbligo per gli istituti di pagamento di comunicare alle autorità nazionali competenti[39] ogni eventuale modifica delle proprie attività tale da incidere sull'accuratezza delle informazioni fornite in relazione all'autorizzazione, anche in relazione a nuovi agenti o entità cui vengono esternalizzate determinate attività[40]. Parallelamente alle autorità nazionali, anche l'EBA continuerà a gestire un registro elettronico centrale, accessibile tramite il proprio sito *web*, contenente l'elenco dei nomi delle imprese registrate o autorizzate a prestare servizi di pagamento o di moneta elettronica, atto a garantire che le relative informazioni siano disponibili in tutta l'Unione[41].

L'art. 10 della direttiva consente, poi, agli istituti di pagamento di esercitare altre attività, al di là di quelle previste nella medesima, tra cui la prestazione di servizi operativi e di servizi accessori strettamente connessi alla gestione dei sistemi di pagamento o ad altre attività commerciali disciplinate dalle disposizioni dell'Unione e nazionali applicabili. Considerati i rischi specifici connessi all'attività di raccolta di depositi, è posto però il divieto di esercitare tale attività con la precisazione che gli istituti di pagamento possono usare esclusivamente i fondi consegnati dagli utenti per fornire servizi di pagamento[42].

Nella sezione II della direttiva sono previste invece le norme relative al "ricorso ad agenti, distributori, succursali e all'esternalizzazione" da parte degli istituti di pagamento per lo svolgimento dei propri servizi. La disciplina non diverge dalle disposizioni della PSD2 e continua a seguire il principio per cui gli istituti di pagamento rimangono pienamente responsabili di tutti gli atti compiuti da qualsiasi agente, distributore o entità a cui le attività sono state esternalizzate[43]. Novità specifiche concernono solamente l'aggiunta di una nuova definizione di distributore di moneta elettronica[44].

---

[38] Art. 12 della direttiva.

[39] In un'ottica di rafforzamento della protezione dei consumatori e della trasparenza delle operazioni degli istituti di pagamento che sono autorizzati dalle autorità nazionali competenti dello Stato membro di origine, compresi i rispettivi agenti, distributori e succursali, si deve continuare a garantire un facile accesso al registro pubblico degli stessi che deve, altresì, essere aggiornato tempestivamente.

[40] Art. 15 della direttiva.

[41] Art. 18 della direttiva in combinato disposto con il Considerando n. 43 della direttiva medesima.

[42] Art. 10, comma 6, della direttiva.

[43] Art. 23 della direttiva.

[44] Definito ai sensi dell'art. 2, n. 36 della direttiva come "*una persona fisica o giuridica che distribuisce o rimborsa moneta elettronica per conto di un istituto di pagamento*".

In linea di continuità con la PSD2 e con la direttiva sulla moneta elettronica, nella sezione III è poi previsto che gli Stati membri debbano designare autorità competenti, dotate di poteri adeguati, ai fini del rilascio delle autorizzazioni e di vigilanza [45]. Sono ivi stabilite disposizioni riguardanti la cooperazione tra autorità nazionali competenti ed è introdotta la possibilità per le autorità competenti nazionali di richiedere l'assistenza dell'EBA per la risoluzione di possibili controversie con altre autorità [46].

Con riferimento all'esercizio del diritto di stabilimento e della libera prestazione di servizi da parte di un istituto di pagamento, è previsto in capo a quest'ultimo l'obbligo di fornire all'autorità competente dello Stato membro di origine qualsiasi informazione pertinente riguardante la sua attività e di comunicare, altresì, allo Stato membro o agli Stati membri in cui intende operare, se ha intenzione di avvalersi di succursali, agenti o distributori e se intende fare ricorso all'esternalizzazione [47]. In tali ultimi casi sono previste specifiche disposizioni qualora siano coinvolti tre Stati membri, ovverosia lo Stato membro di stabilimento dell'istituto di pagamento, quello dell'agente e un terzo Stato membro nel quale l'agente presta servizi su base transfrontaliera [48]. Sul punto, in considerazione delle difficoltà presenti nella cooperazione transfrontaliera tra autorità competenti, è richiesto all'EBA di elaborare progetti di norme tecniche di regolamentazione sulla cooperazione e lo scambio di informazioni tra le autorità competenti dello Stato membro di origine e quelle dello Stato membro ospitante [49].

---

[45] Art. 24 della direttiva. In particolare gli Stati membri provvedono affinché le autorità competenti siano dotate di tutte le risorse e poteri necessari, anche in termini di personale, per svolgere in modo adeguato le proprie funzioni. Inoltre, ai sensi dell'art. 25 della medesima direttiva, a tali autorità sono conferiti poteri investigativi e, altresì, dotate della possibilità di irrogare sanzioni amministrative e di imporre le misure necessarie per lo svolgimento dei loro compiti.

[46] Art. 29 della direttiva, prevedendo inoltre la possibilità per l'EBA di prestare, di propria iniziativa, assistenza alle autorità competenti per trovare un accordo.

[47] Si richiede inoltre una collaborazione tra le autorità competenti dello Stato membro di origine e quelle dello stato membro ospitante, al fine di scambiarsi reciprocamente tutte le informazioni necessarie, comprese, altresì, quelle relative ad eventuali violazioni da parte di un agente, di un distributore o di una succursale, nonché qualora tali violazioni si siano verificate nell'esercizio della libera prestazione dei servizi. Si veda: art. 31, comma 3, della direttiva.

[48] Art. 30, comma 2, della direttiva, ove si specifica che in tal caso, al fine di promuovere una cooperazione tra le autorità competenti ed una efficace vigilanza sull'operato degli istituti di pagamento, le autorità dello Stato membro di origine devono comunicare le informazioni allo Stato membro ospitante.

[49] Art. 30, comma 5, della direttiva, prosegue disponendo che "*Tali progetti di norme tecniche di regolamentazione precisano il metodo, i mezzi e le modalità dettagliate della cooperazione in materia di notifica degli istituti di pagamento che esercitano la loro attività su base transfronta-*

Venendo ora al Capo II della proposta di direttiva, dedicato alle "esenzioni e notifiche", appare invariata la possibilità per gli Stati membri di esentare le entità che forniscono servizi di pagamento – tra cui i prestatori di servizi di informazione sui conti ai sensi dell'art. 36 della direttiva – dalle condizioni richieste per l'autorizzazione [50]. Tuttavia, anche in caso di esenzione, le medesime dovranno comunque procedere ad iscriversi nel registro nazionale degli istituti di pagamento [51].

Le disposizioni successive che compongono la proposta sono invece relative ai prelievi di contante e attuative della volontà della Commissione di aumentare ulteriormente la sua accessibilità. In particolare, è prevista la sopraindicata esenzione dall'obbligo di autorizzazione a operare come istituti di pagamento tanto per gli esercenti dei negozi al dettaglio che offrono servizi di fornitura di contante, anche in assenza di acquisto da parte del cliente [52], quanto per i gestori di ATM indipendenti, ovverosia coloro che non prestano servizi di pagamento di radicamento del conto.

Degna di rilievo è infine la norma di chiusura prevista nel titolo III della direttiva, relativa all'obbligo di notifica incombente sui prestatori di servizi di pagamento. In particolare, qualora questi intendano beneficiare di un'esclusione dall'ambito di applicazione della direttiva, hanno l'obbligo di notificare alle autorità competenti una lista delle attività dagli stessi offerte sulla base di quanto disposto dal PSR [53], se il valore delle operazioni di pagamento è superiore a una determinata soglia [54]. Ricevuta la notifica, le autorità competenti verificano se le suddette at-

---

liera, in particolare la portata e il trattamento delle informazioni da presentare, compresi una terminologia comune e modelli di notifica standardizzati al fine di garantire una procedura di notifica uniforme ed efficiente.".

[50] Al fine di garantire maggiore trasparenza in materia di esenzioni si impone agli Stati di comunicare alla Commissione ogni decisione di esenzione. Vedi: art. 35 della direttiva.

[51] Per un maggiore approfondimento si veda l'art. 34 in combinato disposto con il Considerando n. 59 della direttiva.

[52] L'art. 37 della direttiva specifica le condizioni richieste per l'esenzione, ovvero che "*a) il servizio è offerto da una persona fisica o giuridica che, a titolo di occupazione principale, vende beni o servizi nei suoi locali; b) l'importo del contante fornito non supera 50 EUR per prelievo*", al fine di evitare la concorrenza sleale con i gestori di ATM. Sul punto, si veda anche Considerando n. 62.

[53] L'art. 39 della direttiva è relativo a tale obbligo di notifica e richiama i criteri indicati dall'art. 2 par. 1, lett. j), punti i) e ii). Sul punto, si veda anche Considerando n. 64 della direttiva.

[54] Art. 39, comma 1, della direttiva, fa riferimento a quelle attività "*per le quali il valore complessivo delle operazioni di pagamento eseguite nei precedenti 12 mesi sia superiore all'importo di 1 milione di EUR*".

tività siano prestate entro il quadro normativo previsto e ne danno riscontro al prestatore di servizi, che dovrà adeguarsi in base alle risultanze della verifica.

2.2. ... al regolamento relativo ai servizi di pagamento nel mercato interno (PSR)

Venendo ora alla connessa proposta di regolamento PSR, si nota immediatamente come la stessa non apporti alcuna modifica all'elenco dei servizi di pagamento previsto dalla PSD2 e al correlativo elenco delle esclusioni[55]. Diversamente, è ampliato l'elenco delle definizioni contenuto nella PSD2, includendo più termini e fornendo diversi chiarimenti[56] e semplificazioni, con particolare riguardo alle definizioni di "disposizione di un'operazione di pagamento"[57] e di "disposizione a distanza di un'operazione di pagamento"[58].

Il titolo II, rubricato "trasparenza delle condizioni e requisiti informativi per i servizi di pagamento" contiene tutte le norme relative alle informazioni generali e specifiche, preliminari e successive all'operazione di pagamento, elaborate al fine di mantenere elevato il grado di protezione degli utenti consentendogli, tra l'altro, di compiere scelte consapevoli[59]. Tra le novità proposte si riscontrano l'applicazione del regime informativo tanto alle singole operazioni di pagamento, quanto ai contratti quadro e alle operazioni di pagamento contemplate da tali contratti[60], la eliminazione della possibilità per gli Stati membri di adeguare i limiti di spesa[61] che consen-

[55] Si veda art. 2 del PSR per l'elenco completo sia delle categorie di prestatori cui si applica il presente regolamento, sia quelle che ne sono esentate.

[56] Le molteplici definizioni rilevanti per la presente direttiva sono analiticamente indicate nell'art. 3.

[57] Art. 3, n. 6 del PSR*: "disposizione di un'operazione di pagamento": le fasi necessarie per preparare l'esecuzione di un'operazione di pagamento, compresi la trasmissione di un ordine di pagamento e il completamento del processo di autenticazione.*

[58] Art. 3, n. 7, del PSR: "*disposizione a distanza di un'operazione di pagamento": un'operazione di pagamento per la quale è impartito un ordine di pagamento via internet".*

[59] Sul punto, il considerando n. 38 specifica che i prestatori di servizi di pagamento "*dovrebbero comunicare attivamente le informazioni al momento opportuno, senza alcuna sollecitazione da parte dell'utente di servizi di pagamento, oppure dovrebbero renderle disponibili dietro richiesta degli utenti di servizi di pagamento*".

[60] Art. 4 del PSR.

[61] Art. 10 e Considerando n. 42 del PSR.

tono di derogare agli obblighi informativi, e l'estensione dell'obbligo di informare l'utente di servizi di pagamento sulle procedure di risoluzione alternative delle controversie, attualmente previsto per i contratti quadro, alle singole operazioni di pagamento [62]. Con riguardo alle transazioni internazionali, e sempre in tema di trasparenza, si propone inoltre l'introduzione dell'obbligo per i prestatori di servizi di pagamento di specificare all'utente del servizio, per un verso una stima del tempo entro cui i fondi devono essere ricevuti dal prestatore di servizi di pagamento del beneficiario situato al di fuori dell'UE [63], e per altro verso le spese stimate per la conversione di valuta di tali transazioni internazionali [64]. Un ulteriore chiarimento in tema di trasparenza è infine offerto in relazione al caso in cui, nell'ambito di un contratto quadro, i servizi di pagamento siano offerti congiuntamente ai servizi tecnici a sostegno della prestazione di servizi di pagamento e siano prestati dal prestatore di servizi di pagamento o da un terzo con cui questi si è consorziato. In tale ipotesi, e al dichiarato fine di evitare che gli utenti di servizi di pagamento siano vincolati al loro prestatore di servizi attraverso condizioni più onerose previste nelle clausole contrattuali dei servizi tecnici, la proposta dispone che tali servizi tecnici devono essere soggetti agli stessi obblighi del contratto quadro in materia di oneri di risoluzione.

Passando ora, al titolo III relativo ai "diritti e obblighi in relazione alla prestazione e all'uso di servizi di pagamento", la prima novità riscontrata consiste nell'estensione del divieto di imporre un prezzo maggiorato per i servizi di pagamento soggetti al regolamento relativo alle commissioni ban-

---

[62] Art. 13, comma 1, lett. g), previsto nel Capo 2 del PSR relativo alle operazioni di pagamento singole e art. 13, comma 1, lett. g), contenuto nel Capo 3 relativo alle operazioni rientranti in un contratto quadro. Inoltre, si richiama anche il comma 3 dell'art. 13 il quale dispone espressamente che "*Se del caso, tutte le altre informazioni e condizioni pertinenti di cui all'articolo 20 sono rese disponibili all'utente di servizi di pagamento in una forma facilmente accessibile*". In aggiunta, sempre in un'ottica di maggiore coerenza e uniformità interna, è stato chiarito che i prestatori di servizi di pagamento devono inserire, negli estratti del conto di pagamento, "*le informazioni necessarie al pagatore per identificare con chiarezza il beneficiario, compresa la denominazione commerciale del beneficiario*", ai senti dell'art. 16, comma 1, lett. a) – relativo alle operazioni di pagamento singole – e il corrispondente art. 25, comma 1, lett. a), applicabile alle singole operazioni di pagamento rientranti nel contratto quadro.

[63] Art. 13, comma 1, lett. c) e corrispondente art. 20, comma 1, lett. b), punto vi), del PSR.

[64] Tali spese devono, dunque, essere espresse come "*maggiorazione percentuale rispetto all'ultimo tasso di cambio di riferimento applicabile disponibile emesso dalla banca centrale interessata*". Ciò è disposto dagli art. 13, comma 1, lett. f), art. 20, comma 1, lett. c), punto v) e Considerando n. 50 del PSR.

carie [65], ai bonifici e agli addebiti diretti in tutte le valute dell'UE [66]. Il capo II del suddetto titolo, col fine di assicurare parità di trattamento tra le diverse categorie di prestatori di servizi di pagamento, detta norme specifiche prescrivendo, sia in capo ai gestori dei sistemi di pagamento che ai sistemi di pagamento designati da uno Stato membro ai sensi della direttiva 98/26/CE [67], l'obbligo generale di adottare regole e procedure proporzionate [68], obiettive e non discriminatorie in merito all'accesso ad un sistema di pagamento da parte dei prestatori di servizi di pagamento [69]. Dunque, gestori di sistemi di pagamento e sistemi di pagamento, nel momento in cui ricevono una domanda di partecipazione da parte di un prestatore di servizi di pagamento, sono tenuti a effettuare una valutazione dei rischi pertinenti, quali il rischio operativo, il rischio di credito, il rischio di liquidità e il rischio d'impresa [70]. Il gestore, inoltre, deve comunicare per iscritto al richiedente se la domanda di partecipazione è accolta o meno, potendo, quest'ultimo, esperire ricorso [71].

Per quanto riguarda l'*Open Banking*, nel capo III del PSR si registrano alcune modifiche rispetto al testo della PSD2 tra cui, su tutte, la previsione degli obblighi, tranne in circostanze eccezionali, in capo ai prestatori di servizi di pagamento di radicamento del conto di avere un'interfaccia dedicata per l'accesso ai dati dei conti di pagamento [72] e di mantenere permanentemente un'interfaccia c.d. di riserva ai fini dello scambio dei dati con i TPPs [73]. Le norme novellate introduco ulteriori requisiti sulle inter-

[65] Regolamento (UE) 2015/751 del Parlamento europeo e del Consiglio, del 29 aprile 2015, relativo alle commissioni interbancarie sulle operazioni di pagamento basate su carta.

[66] La PSD2 prevedeva tale divieto soltanto per i bonifici e agli addebiti diretti denominati in euro e non in altre valute dell'UE. Sul tema, si veda art. 28 e i Considerando nn. 52 e 53 del PSR.

[67] Direttiva sul carattere definitivo del regolamento.

[68] Qualora i sistemi di pagamento non siano soggetti alla sorveglianza da parte del Sistema europeo di banche centrali, gli Stati membri devono designare le autorità competenti al fine di garantire che i gestori delle infrastrutture dei sistemi di pagamento rispettino obblighi relativi le rispettive attività. Art. 31, comma 7, del PSR.

[69] Art. 31, comma 1, del PSR. Sul punto, invero si ricorda che i prestatori di servizi di pagamento devono avere accesso ai sistemi di pagamento al fine di fornire i relativi servizi agli utenti. Tale accesso può essere diretto o indiretto.

[70] Art. 31, comma 1, del PSR.

[71] Art. 31, comma 3, e art. 32, comma 3, del PSR.

[72] Art. 35, comma 1, in combinato disposto con il Considerando n. 57 del PSR.

[73] Art. 35, comma 2, del PSR.

facce dedicate per quanto riguarda le prestazioni e le funzionalità [74], incorporando alcune delle disposizioni contenute nelle norme tecniche di regolamentazione [75].

Unitamente a quanto sopra, il PSR richiede, altresì, che i prestatori di servizi di pagamento di radicamento del conto mettano a disposizione degli utenti di servizi di pagamento un "pannello di gestione", integrato nella sua interfaccia utente, per monitorare e gestire le autorizzazioni rilasciate dall'utente di servizi di pagamento ai fini dei servizi di informazione sui conti o dei servizi di disposizione di ordine di pagamento per pagamenti multipli o ricorrenti [76]. L'interfaccia, in particolare, non deve creare ostacoli alla prestazione dei servizi di disposizione di ordine di pagamento e di informazione sui conti [77]: questi, difatti, accedono ai dati sui conti di pagamento esclusivamente attraverso l'interfaccia dedicata [78] secondo quanto previsto, rispettivamente, agli artt. 46 e 47 del PSR.

Quanto all'operazione di pagamento (o a una serie di operazioni) la normativa prevede che questa è suscettibile di autorizzazione, prima o, se concordato dal pagatore e dal prestatore di servizi di pagamento di radicamento del conto, dopo l'esecuzione del pagamento, solo se il pagatore ha dato il proprio consenso all'esecuzione medesima [79]. I prestatori di servizi di pagamento di radicamento del conto non verificano l'autorizzazione concessa dall'utente di servizi di pagamento al prestatore di servizi di in-

---

[74] Per un approfondimento in merito ai requisiti delle interfacce dedicate di accesso ai dati, le misure da adottare in caso di guasto o indisponibilità delle stesse e in riferimento alle deroghe dell'obbligo di disporre tali interfacce si vedano gli artt. 36 ss. In tale ultimo caso, l'art. 39 riconosce in capo all'ABE il compito di elaborare le norme tecniche di regolamentazione che specificano i criteri dettagliati in base ai quali un prestatore di servizi di pagamento di radicamento del conto può essere esentato dall'obbligo di disporre di un'interfaccia dedicata.

[75] Regolamento delegato (UE) 2018/389 della Commissione per quanto riguarda le norme tecniche di regolamentazione per l'autenticazione forte del cliente e gli standard aperti di comunicazione comuni e sicuri.

[76] Art. 43, comma 1, del PSR; il relativo comma 2 elenca le caratteristiche di tali pannelli di gestione.

[77] Art. 43 del PSR. Nel comma due della medesima norma è previsto un elenco di quelli che sono considerati ostacoli vietati.

[78] Art. 45 del PSR.

[79] Art. 49 del PSR, dal quale al par. 3 si evince che "*L'accesso a un conto di pagamento ai fini dei servizi di informazione sui conti o dei servizi di ordine di pagamento da parte dei prestatori di servizi di pagamento è autorizzato solo se l'utente di servizi di pagamento ha dato al prestatore di servizi di informazione sui conti o, rispettivamente, al prestatore di servizi di disposizione di ordine di pagamento l'autorizzazione ad accedere al conto di pagamento e ai dati pertinenti in tale conto*".

formazione sui conti o al prestatore di servizi di disposizione di ordine di pagamento [80].

Passando al capo IV, dedicato all'"autorizzazione di operazioni di pagamento" si può notare come sia imposto al prestatore di servizi di pagamento del beneficiario di fornire gratuitamente all'utente, su richiesta, un servizio [81] che verifichi la corrispondenza dell'identificativo unico del beneficiario con il nome del beneficiario fornito dal pagatore, e di notificare [82] l'esito al pagatore, in caso di discrepanze. Si chiarisce, poi, come i prestatori di pagamento non debbano innalzare unilateralmente i limiti di spesa concordati con i loro utenti di servizi di pagamento [83].

Con riferimento alle responsabilità per operazioni di pagamento non autorizzate si notano alcune modifiche normative e/o chiarimenti. In primo luogo, la proposta chiarisce che, ove il prestatore di servizi di pagamento del pagatore abbia ragionevoli motivi per sospettare una frode commessa dal pagatore, può svolgere delle indagini prima di rimborsarlo. Il rifiuto del rimborso dovrà essere necessariamente corroborato da adeguata motivazione e indicare al pagatore gli organismi ai quali deferire la questione [84]. In secondo luogo, e ove non sia stato correttamente eseguito il servizio di verifica della corrispondenza tra l'identificativo unico e il nome del beneficiario, la medesima proposta prevede che il prestatore di servizi di pagamento del pagatore sia responsabile dell'intero importo del bonifico [85]. Diversamente,

---

[80] L'EDPS raccomanda di riconsiderare il divieto, posto a carico dei PSP di radicamento di conto di verificare l'autorizzazione concessa dall'utente di servizi di pagamento al PiSP o AiSP. EDPS, Opinion n. 39/2023, *Opinion on a Proposal for a Regulation on payment services in the interal market and the Proposal for a Directive on payment services and electronic money services in the internal Market*, Raccomandazione n. 3.

[81] Sul punto, la proposta della Commissione che modifica il regolamento SEPA relativo ai pagamenti istantanei prevede, anch'essa, un servizio di verifica della corrispondenza tra l'identificativo unico e il nome del beneficiario da offrire agli utenti dei bonifici istantanei in euro. Pertanto, con l'obiettivo di assicurare un quadro coerente per tutti i bonifici, evitando nel contempo qualsiasi sovrapposizione, il servizio di verifica di cui al presente regolamento dovrebbe applicarsi solo ai bonifici che non sono contemplati dalla suddetta proposta che modifica il regolamento (UE) n. 260/2012. Si veda: Proposta COM(2022) 546 finale del 26 ottobre 2022, che modifica il regolamento (UE) n. 260/2012.

[82] Art. 50 del PSR. Inoltre, ai sensi del comma 3, tale notifica deve essere effettuata prima che il pagatore autorizzi l'operazione per consentire a quest'ultimo di decidere liberamente se procedere o meno. Sul punto, si veda anche il Considerando n. 69 sottolinea che tale tipologia di servizio ha un rilevante impatto positivo "*sul livello di frode e di errore*".

[83] Art. 51 del PSR.

[84] Art. 56 e considerando n. 77, del PSR.

[85] Art. 57, comma 1, del PSR.

se l'errore del prestatore di servizi di pagamento del pagatore è imputabile al prestatore di servizi di pagamento del beneficiario, spetta a quest'ultimo rimborsare il danno finanziario subito [86].

Il prestatore di servizi di pagamento è, altresì, considerato responsabile quando un consumatore è stato indotto ad autorizzare un'operazione di pagamento da un terzo che ha finto di essere un dipendente del prestatore di servizi di pagamento ricorrendo alla manipolazione e all'inganno [87]. Sul punto, proprio al fine di prevenire episodi di frode, è previsto l'obbligo per i prestatori di servizi di comunicazione elettronica di cooperare con i prestatori di servizi di pagamento [88]. È stata, inoltre, introdotta una nuova disposizione in materia di responsabilità per i prestatori di servizi tecnici e i gestori di schemi di pagamento per la mancata assistenza nell'autenticazione forte del cliente [89], chiarendo, inoltre, che il pagatore non sopporta alcuna perdita finanziaria nel caso in cui il prestatore di servizi di pagamento del pagatore o del beneficiario applichi un'esenzione dall'applicazione dell'autenticazione forte del cliente [90].

Sul tema, da ultimo, in considerazione della particolare vulnerabilità dei consumatori in caso di operazioni di pagamento basate su carta in cui l'esatto importo dell'operazione non è noto al momento del pagamento, è stato introdotto sia l'obbligo per il beneficiario di informare il prestatore di servizi di pagamento dell'importo esatto dell'operazione di pagamento subito dopo la consegna del servizio o dei beni al pagatore, si l'obbligo, per il prestatore di servizi di pagamento del pagatore, di bloccare l'importo di fondi, sul conto di pagamento del pagatore, in proporzione a quello dell'operazione di pagamento che ci si può ragionevolmente aspettare da quest'ultimo [91].

Ponendo, adesso, l'attenzione agli ultimi capi della proposta si nota subito come questa confermi il fatto che qualsiasi trattamento dei dati deve essere conforme al GDPR [92]. Quanto ai rischi operativi e di sicurezza e autenticazione, viene introdotto l'obbligo per i prestatori di servizi di pagamento

---

[86] Art. 57, comma 3, del PSR.

[87] Art. 59 del PSR.

[88] Art. 59, comma 5, e il Considerando n. 81 del PSR.

[89] Art. 58 del PSR.

[90] Art. 60, commi 2 e 3, del PSR.

[91] Art. 61 in combinato disposto con il Considerando n. 84 del PSR.

[92] Regolamento (UE) 2016/679.

di mettere a disposizione sistemi e meccanismi per il monitoraggio delle transazioni, al fine di applicare correttamente l'autenticazione forte del cliente [93] e migliorare la prevenzione e il rilevamento delle transazioni fraudolente [94]. Sempre a tali fini, le norme che consentono ai prestatori di servizi di pagamento di scambiare dati personali, come gli identificativi unici di un beneficiario, nell'ambito di accordi di condivisione delle informazioni [95], richiedono previamente l'effettuazione di una valutazione d'impatto sulla protezione dei dati conformemente al regolamento (UE) 2016/679 [96].

Per quanto riguarda l'applicazione dell'autenticazione forte del cliente, al fine di evitarne l'elusione, sono stati introdotti chiarimenti in ordine alle operazioni disposte da esercenti e degli ordini per corrispondenza o ordini telefonici [97]: nel caso di operazioni di pagamento disposte da esercenti, è necessario che l'autenticazione forte del cliente sia applicata al momento dell'istituzione del mandato, senza doverla ri-applicare per le successive operazioni [98]; nel caso di ordini per corrispondenza e ordini telefonici, si chiarisce invece che solo la disposizione delle operazioni di pagamento che avviene in forma non digitale è esclusa dagli obblighi di autenticazione forte del cliente. Tuttavia, le operazioni di pagamento basate su ordini di pagamento su supporto cartaceo, ordini per corrispondenza o ordini telefonici impartiti dal pagatore devono, comunque, essere soggette ai requisiti e controlli di sicurezza da parte del prestatore di servizi di pagamento del pagatore che consentano, ugualmente, l'autenticazione dell'operazione di pagamento [99].

---

[93] Sul punto, il Considerando n. 107 del PSR ne ribadisce la sua importanza poiché "*la sicurezza dei pagamenti elettronici è fondamentale per garantire la protezione degli utenti e lo sviluppo di un contesto affidabile per il commercio elettronico*".

[94] Art. 83, comma 2, del PSR.

[95] Art. 83, comma 3, del PSR. Sul tema, infatti, il Considerando n. 103 del PSR sottolinea, anzitutto, l'importanza di un sistema di monitoraggio delle operazioni costantemente aggiornato e migliorato per l'individuazione dei casi di frode. Al fine di effettuarne una individuazione tempestiva, si ritiene necessario avere una "*una maggiore quantità di informazioni sulle attività potenzialmente fraudolente provenienti da altri prestatori di servizi di pagamento. Pertanto dovrebbe essere possibile condividere tutte le informazioni pertinenti tra i prestatori di servizi di pagamento*". In aggiunta, ai sensi del comma 4 del suddetto articolo, tali accordi devono definire i dettagli della partecipazione e specificare i dettagli degli elementi operativi, compreso l'uso di piattaforme informatiche dedicate.

[96] Art. 83, comma 4, insieme al Considerando n. 103 del PSR.

[97] Considerando n. 108 del PSR.

[98] Art. 85, comma 3, del PSR.

[99] Art. 85, comma 7, del PSR. In aggiunta, ai sensi dei i commi 4 e 5, si evince come l'ambito di applicazione della SCA sia circoscritto nei casi di operazioni di pagamento per le quali il beneficiario impartisce ordini di pagamento sulla base di un mandato conferito dal pagatore; tut-

Allo scopo di favorire l'inclusione finanziaria e di mitigare i rischi di frode, e nel rispetto della direttiva UE 2019/882 [100], sono altresì migliorate le condizioni di accessibilità all'autenticazione forte del cliente prevedendo, in capo agli utenti, comprese le persone con disabilità, con scarse competenze o mezzi digitali e le persone anziane, il diritto di disporre di almeno un metodo di esecuzione dell'autenticazione forte del cliente adeguato alla loro situazione specifica [101]. In aggiunta, e infine, sono previsti obblighi di applicare l'autenticazione forte del cliente per le operazioni di pagamento a distanza [102] e di concludere accordi di esternalizzazione tra i prestatori di servizi di pagamento e i prestatori di servizi tecnici, qualora questi ultimi forniscano e verifichino gli elementi dell'autenticazione forte del cliente [103].

2.3. ... e al regolamento relativo a un quadro per l'accesso ai dati finanziari (FiDA)

Il regolamento FiDA [104] chiarisce immediatamente, nei primi due commi dell'art. 1, obiettivi e oggetto promossi quali, da un lato, la regolazione dell'accesso e dell'utilizzo di talune categorie di dati dei consumatori nell'ambito finanziario al di fuori del settore dei conti di pagamento [105], e

tavia per tali addebiti diretti, è prevista l'applicazione dell'autenticazione forte del cliente nei casi in cui un mandato è conferito tramite un canale a distanza con il coinvolgimento diretto di un prestatore di servizi di pagamento.

[100] Direttiva (UE) 2019/882 del Parlamento europeo e del Consiglio, del 17 aprile 2019, sui requisiti di accessibilità dei prodotti e dei servizi.

[101] Art. 88 del PSR.

[102] Art. 85, comma 8, del PSR. Inoltre, si veda il Considerando n. 114, che specifica come tale collegamento dinamico risponde all'esigenza di contrastare, da un lato, i rischi di manipolazione del nome del beneficiario e dell'importo dell'operazione "*tra il momento in cui è impartito un ordine di pagamento e l'autenticazione dei pagamenti, dall'altro i rischi di frode in generale*". Pertanto, ai sensi del seguente comma 9, tale obbligo di applicazione della SCA, opera anche con riferimento alle operazioni di pagamento elettronico per le quali un ordine di pagamento è impartito tramite un dispositivo del pagatore che utilizza la tecnologia di prossimità per lo scambio di informazioni con l'infrastruttura del beneficiario e per le quali l'esecuzione di un'autenticazione forte del cliente richiede l'uso di internet sul dispositivo del pagatore.

[103] Art. 87 del PSR.

[104] Proposta di regolamento del Parlamento europeo e del Consiglio relativo a un quadro per l'accesso ai dati finanziari e che modifica i regolamenti (UE) n. 1093/2010, (UE) n. 1094/2010, (UE) n. 1095/2010 e (UE) 2022/2554 – COM/2023/360 final.

[105] Nel regolamento si evince espressamente come esso sia preordinato ad evitare sovrapposizioni con le disposizioni relative ai conti di pagamento dettate dalla direttiva (UE) 2015/2366,

dall'altro la creazione di un nuovo soggetto giuridico denominato "Prestatore di Servizi di Informazione Finanziaria" (o Financial Information Service Provider o FISP [106]), senza con ciò interferire con l'applicazione del diritto dell'Unione in materia di accesso ai dati del cliente, e di condivisione degli stessi, salvo quanto espressamente previsto nel medesimo regolamento [107].

Le categorie di dati oggetto del regolamento sono descritte puntualmente dall'art. 2, par. 1, che ne delinea quindi l'ambito di applicazione oggettivo [108], preordinato alla inclusione dei dati che apportano "*un elevato valore aggiunto per l'innovazione finanziaria nonché un basso rischio di esclusione finanziaria per i consumatori*" [109]. In particolare, anche se non prive di eccezioni, sei sono le categorie di dati [110] che rientrano nella disciplina proposta [111]. La lett. a) dell'art. 2 del regolamento FiDA comprende, in primo luogo, gli elementi indefettibili dei rapporti finan-

evitando così disallineamenti e incertezze normative. Si veda, tra l'altro: Considerando n. 12 del regolamento.

[106] I FISP sono disciplinati, in particolare, dal Titolo V del regolamento FiDA.

[107] Art. 2, par. 4, del regolamento, che nient'altro fa che esplicitare l'applicazione del *principio lex specialis derogat generali* nei limiti della incompatibilità tra normative orizzontali e verticali.

[108] L'EDPB rileva che sul punto acquisteranno valore dirimente gli orientamenti, nonostante il loro carattere non vincolante, per definire il "perimetro" dei dati considerati necessari per fornire specifici prodotti e servizi finanziari. Si veda: EDPS, Opinion n. 38/2023 on the *Proposal for a Regulation on a framework for Financial Data Access*.

[109] Si veda: Considerando n. 9 del regolamento.

[110] L'EDPS, sul punto, raccomanda anche l'esclusione esplicita dei dati creati come risultato della profilazione dalla definizione di "dati dei clienti", come modo per ridurre al minimo i rischi per i diritti e le libertà delle persone. Si veda: EDPS, Opinion n. 38/2023 *on the Proposal for a Regulation on a framework for Financial Data Access*. A questo proposito, il EDPS sottolinea che tali combinazioni di dati personali sono già soggette ai requisiti del GDPR, in particolare per quanto riguarda i principi di legittimità, correttezza, limitazione delle finalità, minimizzazione dei dati e adeguatezza. Si veda: Opinion n. 38, par. 33. La medesima Opinion rileva inoltre che alcune combinazioni di dati possono già essere esplicitamente vietate dal diritto nazionale o dell'UE applicabile, come nel caso del trattamento di categorie particolari di dati e di dati personali ottenuti da reti di social media nel contesto della valutazione del merito di credito dei consumatori. (ad esempio, i dati ottenuti da fonti terze, come le reti di social media: tale pratica è già esplicitamente vietata nella legislazione settoriale in riferimento a determinati servizi finanziari: Si veda il testo finale concordato della direttiva sui crediti al consumo, art. 19, par. 3-*bis*, che prevede che "*I creditori e gli intermediari del credito non trattano le categorie particolari di dati di cui all'articolo 9, paragrafo 1, del regolamento (UE) 2016/679 e i dati personali trattati dai social network che possono essere contenuti nelle banche dati di cui al paragrafo 1*".

[111] Art. 2, par. 1 del regolamento.

ziari quali i contratti di credito ipotecario, i prestiti e i conti, da questi esclusi, come già indicato, i conti di pagamento, il tutto con l'obiettivo di individuare quei dati che "*possono consentire ai clienti di avere una migliore visione d'insieme dei loro depositi e di soddisfare meglio le loro esigenze di risparmio sulla base dei dati sul credito*" [112]. La lettera b) contenuta nella medesima disposizione estende l'applicazione ad ulteriori dati relativi a servizi talvolta accessori, quali risparmi, investimenti in strumenti finanziari, prodotti di investimento assicurativi, cripto-attività, beni immobili e altre attività finanziarie correlate [113]. Le lettere c) e d) includono invece i dati dei clienti sui diritti pensionistici, relativi ai vari prodotti pensionistici sia aziendali, professionali [114] o individuali [115], la cui accessibilità e condivisione si ritiene fondamentale in quanto dovrebbe contribuire allo sviluppo di strumenti di tracciamento delle pensioni che forniscano ai risparmiatori una panoramica completa dei loro diritti [116], per un verso, e consentirebbe agli operatori di poter offrire prodotti e servizi assicurativi rilevanti per le esigenze del cliente, come la protezione di abitazioni, veicoli e altri beni [117], per altro verso. La lett. e) si sofferma poi sui prodotti di assicurazione (non vita), escludendo esplicitamente i prodotti di assicurazione malattia e le valutazio-

---

[112] Si veda: Considerando n. 12 del regolamento.

[113] Nonché i benefici economici derivanti da tali attività, compresi i dati raccolti ai fini della valutazione dell'appropriatezza e dell'adeguatezza a norma dell'art. 25, direttiva 2014/65/UE relativa ai mercati degli strumenti finanziari. La finalità di includere tali dati nella presente disciplina ben si coglie nel Considerando n. 11, nel quale è riportato che "*Consentire ai clienti di condividere i loro dati sui loro investimenti correnti può incoraggiare l'innovazione nell'offerta di servizi di investimento al dettaglio*".

[114] Si veda: Considerando n. 15 del regolamento. La norma sul punto fa richiamo ai prodotti paneuropei a norma del regolamento (UE) 2019/1238 e alla direttiva 2009/138/CE e alla direttiva (UE) 2016/2341 del Parlamento europeo e del Consiglio.

[115] La norma, sul punto, fa rinvio ai prodotti pensionistici individuali paneuropei, a norma del regolamento (UE) 2019/1238.

[116] Si veda: Considerando n. 15 del regolamento, ove è altresì precisato che i dati sui diritti pensionistici riguardano in particolare "*i diritti pensionistici maturati, i livelli previsti delle prestazioni pensionistiche, i rischi e le garanzie per gli aderenti e i beneficiari*", giudicati dal legislatore un mercato particolarmente promettente che incontra attualmente numerose difficoltà proprio in considerazione della difficoltà nella circolazione dei dati.

[117] Si veda: Considerando n. 14 del regolamento, in cui si precisa che i dati del cliente sui prodotti assicurativi che rientrano nell'ambito di applicazione del presente regolamento dovrebbero includere sia informazioni sui prodotti assicurativi, quali dettagli sulla copertura assicurativa, sia dati specifici relativi alle attività assicurate dei consumatori che sono raccolti al fine di verificare le richieste e le esigenze.

ni ad esse connesse [118], dato il loro carattere strettamente personale che, altrimenti, comprometterebbe la *privacy* dei consumatori in maniera non proporzionata [119]. In ultimo, la lett. f) consente di ricomprendere nella normativa in analisi anche i dati utilizzati per la valutazione del merito creditizio di imprese raccolti nell'ambito di procedure di richiesta di prestito o di *rating* del credito. La scelta di non estendere questa categoria di dati a quella relativa alla valutazione del merito dei consumatori è voluta e valutata a valle di certe considerazioni in merito ai rischi per i diritti fondamentali della persona, tra i quali quelli garantiti dagli artt. 7 e 8 della Carta dei diritti fondamentali dell'Unione, laddove risulta più opportuno sfruttare tali dati unicamente nell'ambito delle micro e delle grandi imprese [120].

L'art. 2 del regolamento FiDA disciplina anche l'ambito di applicazione soggettivo della normativa in esame disponendo che, ad eccezione delle entità di cui all'art. 2, par. 3, lett. da a) a e), regolamento UE 2022/2554, sono assoggettati alla normativa gli enti creditizi, gli istituti di pagamento, compresi i prestatori di servizi di informazione sui conti e gli istituti di pagamento a cui è stata concessa un'esenzione a norma della direttiva UE 2015/2366, gli istituti di moneta elettronica, le imprese di investimento, i prestatori di servizi per le cripto-attività, gli emittenti di token collegati ad attività, i gestori di fondi di investimento alternativi, le società di gestione di organismi d'investimento collettivo in valori mobiliari, le imprese di assicurazione e di riassicurazione, gli intermediari assicurativi e intermediari assicurativi a titolo accessorio, gli enti pensionistici aziendali o professionali, le agenzie di *rating* del credito e i fornitori di servizi di crowdfunding, purché agiscano in qualità di titolari [121] o utenti [122] dei dati sopra illustrati.

Chiarito oggetto e ambito di applicazione, il FiDA, nel successivo titolo II, "raddoppia la scommessa" dischiudendo sul piano normativo l'*Open Finance*, come precedentemente fatto in materia di *Open Banking*. Esso prevede la predisposizione di obblighi specifici in capo ai diversi attori

[118] Ovvero i dati raccolti a norma degli artt. 20 e 30 della direttiva (UE) 2016/97 sulla distribuzione assicurativa.

[119] Si veda: Considerando n. 9 del regolamento.

[120] Si veda: Considerando n. 16 del regolamento.

[121] Tale è, ai sensi dell'art. 3, n. 5), del regolamento "*un ente finanziario diverso da un prestatore di servizi di informazione sui conti che raccoglie, conserva e altrimenti tratta i dati di cui all'articolo 2, paragrafo 1*".

[122] Tale è, ai sensi dell'art. 3, n. 6), del regolamento "*una delle entità di cui all'articolo 2, paragrafo 2, che, previa autorizzazione di un cliente, ha accesso legittimo ai dati del cliente di cui all'articolo 2, paragrafo 1*".

coinvolti in materia che innescano un vero e proprio regime di condivisione e circolazione dei dati finanziari [123], attualmente ostacolato dalla disomogeneità della materia [124].

I primi due articoli (artt. 4 e 5 del regolamento) disciplinano gli obblighi in capo ai titolari dei dati [125] declinando e rafforzando nello specifico ambito finanziario i diritti di accesso, di portabilità e di condivisione dei dati come già predisposti, rispettivamente, dal GDPR e dalla PSD2. In particolare, l'art. 4 obbliga i titolari a mettere a disposizione del cliente i dati appartenenti a una delle categorie già sopra indicate, senza indebito ritardo, gratuitamente [126], in maniera continuativa e in tempo reale ogni qualvolta siano richiesti per via elettronica. L'art. 5, invece, predispone l'obbligo dei titolari di mettere a disposizione, dietro richiesta del cliente, gli stessi dati ad ogni utente dei dati [127] debitamente autorizzato [128].

La condivisione dei dati dei clienti, da parte dei titolari, nei confronti degli utenti soggiace ai medesimi canoni espressi precedentemente, ad eccezione della gratuità: è infatti prevista, al comma 2 dell'art. 5, la possibilità per il titolare di richiedere un compenso [129] all'utente qualora siano forniti dati nelle modalità prescritte dal regolamento medesimo [130]. Sono poi specificate al terzo comma ulteriori regole atte a disciplinare lo scambio di queste informazioni, a garanzia dell'integrità delle stesse e della tutela del cliente; in particolare, si richiede che i dati siano condivisi in un formato basato su norme generalmente riconosciute, che abbiano almeno la stessa

---

[123] Si veda: Considerando n. 11 del regolamento.

[124] Si vedano: Considerando nn. 6 e 8 del regolamento.

[125] Ovvero a norma dell'art. 3, n. 5 del regolamento "*un ente finanziario diverso da un prestatore di servizi di informazione sui conti che raccoglie, conserva e altrimenti tratta i dati di cui all'articolo 2, paragrafo 1*".

[126] In deroga all'esplicito diritto di rimborso del titolare alle spese amministrative di cui allo stesso art. 15, par. 3 del GDPR.

[127] Ovvero a norma dell'art. 3, n. 6 del regolamento "*una delle entità di cui all'articolo 2, paragrafo 2, che, previa autorizzazione di un cliente, ha accesso legittimo ai dati del cliente di cui all'articolo 2, paragrafo 1*".

[128] Qualora i dati siano classificabili come personali l'utente dovrà disporre di una lecita e valida base per il trattamento a norma del regolamento (UE) 2016/679. Si veda, tra l'altro: Considerando n. 10 del regolamento.

[129] Il compenso è giustificato anche – e soprattutto – al fine di garantire che i titolari abbiano un interesse nel fornire interfacce di elevata qualità. Si veda: Considerando n. 29 del regolamento.

[130] Artt. 9 e 10 del regolamento.

qualità di quelli posseduti dal titolare [131] e che siano comunicati solo tramite canali sicuri e solo a seguito di apposita autorizzazione rilasciata dal cliente.

Anche l'utente dei dati è sottoposto a obblighi non dissimili, che sono delineati dall'art. 6 [132]. Primariamente, è disposto un obbligo di autorizzazione preventiva da parte dell'autorità competente ovvero, qualora l'ente rientri nella nuova categoria dei FiSPs, l'ottenimento di una concessione specifica a norma dell'art. 14. Si rafforza, poi, il principio di limitazione [133], imponendo all'utente l'uso esclusivo dei dati per le finalità e alle condizioni per le quali il cliente ha concesso l'autorizzazione [134], la quale potrà essere revocata *ad nutum,* qualora il rapporto si basi sul consenso, o conformemente agli eventuali obblighi contrattuali alla base del trattamento. In ossequio al noto criterio della *privacy by design* [135], nell'ottica dell'*accountability*, sono richieste all'utente dei dati anche la predisposizione di "*adeguate misure tecniche, giuridiche e organizzative*", nonché "*un livello adeguato di sicurezza per la conservazione*", al fine di minimizzare i danni dovuti al fisiologico accentramento informatico di dati rilevanti [136].

Il titolo III del FiDA predispone una disciplina volta ad un uso responsabile dei dati da parte delle imprese, regolando innanzitutto il loro perimetro di utilizzo e, poi, la sicurezza. Si ribadisce il generale principio di minimizzazione e limitazione del trattamento [137] per i dati personali del cliente, mentre la concreta individuazione dei livelli e strumenti di tutela è rimandata ai futuri orientamenti elaborati dall'EBA, per i prodotti e i servizi connessi al punteggio di affidabilità creditizia del consumatore, e all'Autorità europea delle assicurazioni e delle pensioni aziendali e professionali per i prodotti e i servizi connessi alla valutazione del rischio e

[131] Si veda: Considerando n. 24 del regolamento.

[132] L'EDPS, sul punto, raccomanda l'inserimento di uno specifico obbligo per gli utenti dei dati consistente nell'informare chiaramente l'interessato, nell'ambito della propria richiesta di accesso, le singole categorie dei dati per cui esso è richiesto. Si veda: EDPS, Opinion n. 38/2023 *on the Proposal for a Regulation on a framework for Financial Data Access*, raccomandazione n. (7).

[133] Di cui all'art. 5, lett. b) del GDPR.

[134] È esplicitamente vietato l'utilizzo dei dati del cliente per finalità pubblicitarie, ad eccezione del marketing diretto conformemente al diritto dell'Unione e nazionale.

[135] Di cui all'art. 25 GDPR.

[136] Il Considerando n. 32 ricorda a tal proposito le prescrizioni in materia di *cyberesilienza* dettate dal regolamento (UE) 2022/2554, con l'esplicita volontà di includervi i prestatori di servizi di informazione finanziaria.

[137] Di cui all'art. 5, comma 1, lett. b) e c) del GDPR.

alla determinazione dei prezzi per un consumatore nel caso di prodotti di assicurazione vita e malattia. La cooperazione tra le dette Autorità è incentivata dalla normativa, che promuove anche la collaborazione di queste con il comitato europeo per la protezione dei dati al fine di fornire un quadro proporzionato sulle modalità di utilizzo dei dati personali dei consumatori.

Sul punto, dal momento che gran parte del successo della proposta passa per l'utilizzo virtuoso di tecniche di intelligenza artificiale (es. *machine learning*), è da alcuni [138] stato evidenziato come sia necessario dare applicazione ai suindicati principi, elaborati nell'ambito del GDPR, di modo da non escludere l'uso dei dati personali per le finalità di *machine-learning*. In particolare, sfruttando le potenzialità di tali tecnologie, questi non dovrebbero precludere la creazione di training sets e la costruzione di modelli algoritmici ogni volta in cui il sistema di IA risulti avere un impatto sociale positivo e conforme ai diritti sulla protezione dei dati. Il continuo aggiornamento di tali sistemi potrebbe, invero, condurre a mitigare i diversi rischi di discriminazione e di *biases* attualmente correnti.

L'uso responsabile dei dati passa anche – e soprattutto – per un vero e proprio quadro giuridico autorizzatorio che trova nel pannello di gestione [139] il suo elemento centrale. Questo è espressamente disciplinato dall'art. 8 del regolamento e può definirsi come uno strumento sviluppato dal titolare dei dati [140] con lo scopo di fornire al cliente un'interfaccia front-end atta a monitorare e gestire le autorizzazioni da lui fornite agli utenti dei dati [141]. L'intero impianto di condivisione dei dati è dunque basato, princi-

---

[138] A.C. PENEDO, P.T. KRAMCSAK, *Can the European Financial Data Space remove bias in financial AI development? Opportunities and regulatory challenges*, in *International Journal of Law and Information Technology*, 2023, 31, p. 253-275, https://doi.org/10.1093/ijlit/eaad020.

[139] Talvolta già presente nella prassi per vari altri tipi di autorizzazioni, ma mai positivizzato e comunque diffuso in modo non uniforme dati i suoi costi di attuazione. Si veda: Considerando n. 7 del regolamento.

[140] Il Considerando n. 22 del regolamento fa salva la possibilità che piccole e medie imprese che agiscono in qualità di titolari dei dati siano autorizzate a istituire congiuntamente un'interfaccia per programmi applicativi, in modo da ridurre i costi a carico di ciascuna, ovvero avvalersi di fornitori esterni di tecnologia che gestiscono interfacce di programmazione in modalità "pay-per-call".

[141] Anche quando i dati personali sono condivisi sulla base del consenso o sono necessari per l'esecuzione di un contratto". Si veda: Considerando n. 22 del regolamento. Le funzionalità essenziali che deve avere il pannello in esame sono previste dall'art. 8, par. 2, del regolamento, che dispone che le funzionalità essenziali di questa interfaccia, la quale: "*a) offre al cliente una panoramica di ogni autorizzazione in corso concessa agli utenti dei dati, tra cui: i) il nome dell'utente dei dati cui è stato concesso l'accesso; ii) il conto, prodotto finanziario o servizio finan-*

palmente, al pari di quello relativo all'*Open Banking*, sul consenso prestato dal cliente quale base giuridica di trattamento sul presupposto di incontrare consumatori avveduti, responsabili e consapevoli [142]. Come è stato da alcuni sostenuto, nel Considerando 10 della medesima normativa potrebbe però scorgersi anche un'altra prospettiva nella parte in cui si lascia aperta la porta ad altre basi giuridiche di trattamento, che potrebbero ora consistere nel legittimo interesse [143], ora nell'obbligo di esecuzione di un contratto o di un obbligo di legge [144].

Venendo ora al funzionamento pratico del pannello di gestione, la normativa prevede che questo debba essere facilmente reperibile e che le informazioni ivi contenute debbano essere chiare, accurate e facilmente comprensibili per il cliente, nonché aggiornate in tempo reale. A tali fini, e per garantire la miglior tutela ai diritti degli utenti, è richiesto quale presupposto essenziale un elevato grado di collaborazione [145] tra

ziario del cliente cui è stato concesso l'accesso; iii) la finalità dell'autorizzazione; iv) le categorie di dati condivisi; v) il periodo di validità dell'autorizzazione; b) consente al cliente di revocare l'autorizzazione concessa a un utente dei dati; c) consente al cliente di ripristinare un'autorizzazione revocata; d) comprende un registro delle autorizzazioni revocate o scadute per un periodo di due anni".

[142] Occorre considerare che impostare l'intero sistema, almeno in via principale, sul consenso espresso dagli interessati quale base giuridica di trattamento potrebbe produrre distorsioni, o comunque disincentivi, in materia di intelligenza artificiale. Essa, invero, si nutre di dati e ha bisogno di essi per alimentarsi, aggiornarsi, essere più efficiente ed equa. Si veda: A.C. PENEDO, P.T. KRAMCSAK, *Can the European Financial Data Space remove bias in financial AI development? Opportunities and regulatory challenges*, in *International Journal of Law and Information Technology*, 2023, 31, p. 253-275, https://doi.org/10.1093/ijlit/eaad020, sul punto gli autori evidenziano come il consenso prestato dagli utenti possa costituire un freno allo sviluppo dell'IA, necessario ai fini dello sviluppo di uno spazio europeo dei dati finanziari. Gli autori, in particolare, sostengono che dal momento che esso deve essere prestato, tra l'altro, in modo chiaro, preciso, trasparente, informato e consapevole risulta oltremodo arduo elaborare per ciascuna fase di implementazione, sviluppo o aggiornamento dell'intelligenza artificiale un consenso dotato di questi requisiti; invero, queste tecnologie sono intrinsecamente dotate di un certo grado di incertezza e di imprevedibilità che rendono di fatto impossibile illustrare agli interessati gli scopi di volta in volta perseguiti dal relativo trattamento.

[143] Anche tale base giuridica di trattamento annida alcune difficoltà operative in quanto basata costantemente su un'operazione di bilanciamento di interessi.

[144] Nell'ambito del credito scoring, ad esempio, occorre tenere conto che sussistono degli obblighi di legge gravanti sui mutuanti consistenti nel verificare la solvibilità dei mutuatari e la loro capienza. Si veda, sul punto M. ROVATSOS, B. MITTELSTADT, A. KOENE, *'Landscape Summary: Bias In Algorithmic Decision-Making: What Is Bias in Algorithmic Decision-Making, How Can We Identify It, and How Can We Mitigate It?*'.

[145] La collaborazione tra titolari e utenti dei dati è dunque elemento essenziale per la corretta tutela dei diritti dei clienti, la sua organizzazione pertanto non è liberamente demandata alle dinamiche del mercato ma disciplinata tramite l'individuazione puntuale di "sistemi di condivi-

titolari e utenti dei dati, che devono aggiornarsi reciprocamente di qualsiasi modifica intervenuta sull'autorizzazione originariamente rilasciata dal cliente, dell'ottenimento di eventuali nuove autorizzazioni, ivi incluse le relative finalità, il periodo di validità e le categorie di dati interessate [146].

La condivisione dei dati è, dunque, ispirata al principio di collaborazione, ed è soggetta ad ulteriori norme meritevoli di analisi. In particolare, il legislatore europeo, anche sulla scorta degli insegnamenti appresi durante l'applicazione della PSD2, opta per norme che richiedono una standardizzazione comune e dispone, nello specifico, che i titolari e gli utenti dei dati debbano aderire a uno (o più [147]) sistemi di condivisione dei dati finanziari [148], che regolino l'accesso a specifiche serie di dati e norme di *governance* interne, il tutto al fine di consentire l'interazione contrattuale e tecnica necessaria per attuare l'accesso ai dati tra più enti finanziari. Il contenuto di tali sistemi di condivisione è disciplinato dall'art. 10 che, sotto il profilo della *governance*, include non sono solo utenti e titolari "*che rappresentano una quota significativa del mercato del prodotto o del servizio in questione*", ma anche organizzazioni dei clienti e associazioni dei consumatori, e prevede un sistema di governo interno tale da garantire che le adesioni dei nuovi membri sia sempre possibile alle stesse condizioni applicate in qualsiasi momento ai membri esistenti. Il sistema di governo richiesto è inoltre rigorosamente paritario, sia con riguardo alla rappresentanza nei processi decisionali interni [149], in quanto deve adottarsi un sistema maggioritario per teste e talvolta per categorie [150], che in merito all'accesso, non dovendo

---

sione dei dati finanziari" al Titolo IV. Si veda, tra l'altro, il Considerando n. 25. L'EDPS raccomanda l'inserimento di un obbligo per gli utenti dei dati consistente nel dimostrare ai titolari dei dati l'ottenimento dell'autorizzazione ad accedere ai dati. Si veda: EDPS, Opinion n. 38/2023 *on the Proposal for a Regulation on a framework for Financial Data Access*, raccomandazione n. (17).

[146] Art. 8, parr. 3 e 4, del regolamento. Con riferimento all'art. 8, par. 4, l'EDPS raccomanda l'inserimento di un obbligo per gli utenti dei dati consistente nell'informare i titolari dei dati anche ai prodotti e servizi finanziari del consumatore, ricompresi nell'autorizzazione di accesso. Si veda: EDPS, Opinion n. 38/2023 *on the Proposal for a Regulation on a framework for Financial Data Access*, raccomandazione n. (14).

[147] Art. 9, par. 2, del regolamento.

[148] Entro 18 mesi dall'entrata in vigore del regolamento sarà fatto obbligo per titolari e utenti di aderire ad uno o più di questi sistemi di condivisione dei dati finanziari.

[149] L'art. 10, lett. a), *sub*-lett. i), del regolamento chiarisce che la quota di mercato non influenza i diritti del soggetto e "*ciascuna parte gode di una pari ed equa rappresentanza nei processi decisionali interni del sistema e di pari peso nelle procedure di voto*".

[150] L'art. 10, lett. e), del regolamento impone al sistema di prevedere un meccanismo "*at-*

comportare oneri ulteriori rispetto a quanto previsto dallo stesso regolamento e da altre norme dell'Unione applicabili.

La condivisione dei dati deve inoltre sottostare a diversi obblighi di comunicazione nonché a "*norme comuni per i dati e le interfacce tecniche per consentire ai clienti di richiedere la condivisione dei dati*" [151]. Sotto il profilo squisitamente economico, poi, è stabilito un modello per determinare il compenso massimo che il titolare dei dati ha il diritto di addebitare per la messa a disposizione dei dati attraverso il pannello di gestione. All'uopo, sono in particolare elencate sei caratteristiche di questo modello di determinazione del compenso atte a garantire parità di trattamento, efficienza e uno scambio ordinato dei dati: in breve, si richiede una correlazione diretta tra la messa a disposizione dei dati e l'imputazione del compenso dovuto, basandosi su una "*metodologia obiettiva, trasparente e non discriminatoria*" che in ogni caso sia orientata "*verso i livelli più bassi prevalenti sul mercato*", da adattare periodicamente tenendo in considerazione i progressi tecnologici [152].

Il titolo V è invece dedicato all'istituzione dei FiSP, futuri attori nel panorama prospettato di condivisione dei dati finanziari, ai quali viene riconosciuto per l'appunto un regime speciale di accesso ai dati finanziari diversi da quelli relativi ai conti di pagamento [153]. Si mutua, in breve, quanto creato con la PSD2 con i PISP e gli AISP limitatamente ai dati dei conti di pagamento, e si ritiene sufficiente l'ottenimento di una autorizzazione dell'autorità competente a svolgere il servizio. La domanda di autorizzazione, ai sensi dell'art. 12, par. 2, deve illustrare dettagliatamente gli assetti tecnici [154] e or-

---

traverso il quale è possibile modificarne le norme, a seguito di un'analisi d'impatto e del consenso della maggioranza, rispettivamente, di ciascuna comunità di titolari dei dati e di utenti dei dati".

[151] Queste ultime "*elaborate dagli aderenti al sistema o da altre parti od organismi*" (art. 10, lett. g), coerentemente ad una linea che incoraggia la standardizzazione degli aspetti tecnici per motivi sia economici che di sicurezza. Si veda, tra molti: Considerando nn. 5, 23, 24 e 28 del regolamento.

[152] Qualora l'utente sia un soggetto particolarmente debole come PMI o microimpresa, il compenso non può superare "*i costi direttamente connessi alla messa a disposizione dei dati al destinatario dei dati e imputabili alla richiesta*". Il legislatore ritiene infatti che "*la proporzionalità per i partecipanti al mercato più piccoli dovrebbe essere garantita limitando rigorosamente il compenso ai costi sostenuti per agevolare l'accesso ai dati*". Si veda: Considerando n. 29 del regolamento.

[153] In deroga, dunque, alle modalità descritte dall'art. 5, par. 1, del regolamento.

[154] Sono ricordati in via generale gli obblighi del regolamento (UE) 2022/2554, Capo II, in materia di resilienza operativa digitale (art. 12, par. 2, comma 3) e altre disposizioni specifiche

ganizzativi [155] dell'ente e delle sue attività, deve essere indicato il tipo di accesso ai dati previsto, la natura giuridica e lo statuto del richiedente, con puntuale indicazione degli amministratori e delle persone responsabili della gestione, che dovranno attestare la loro onorabilità e il possesso di conoscenze e di esperienza adeguate. Ogni FiSP deve inoltre dotarsi di un capitale minimo pari ad Euro cinquantamila ovvero sottoscrivere un'assicurazione per responsabilità civile professionale per la copertura della responsabilità derivante dall'accesso o l'uso non autorizzato o fraudolento dei dati [156], o prestare una garanzia analoga. Accertati i presupposti per l'ottenimento dell'autorizzazione, l'EBA provvede all'iscrizione del FiSP nell'apposito registro; se il FiSP non è stabilito all'interno dell'Unione sarà necessaria, inoltre, l'individuazione di un rappresentate all'interno del territorio europeo che si assuma la responsabilità per la ricezione, il rispetto e l'applicazione del regolamento [157]. L'autorizzazione può essere revocata qualora non ce ne si avvalga per un periodo superiore a 12 mesi, ovvero quando le dichiarazioni fornite dovessero risultare false, incomplete o non più sussistenti e in ogni caso qualora la gestione costituisse "*un rischio per la protezione dei consumatori e la sicurezza dei dati*".

Passando in rassegna, ad ultimo, la disciplina proposta dedicata alla supervisione e alla vigilanza, v'è in primo luogo da rilevare che l'art. 17 del regolamento affida ad ogni Stato membro il compito di designare un'autorità competente. I poteri di indagine di questa sono riconosciuti dall'art. 18 del regolamento e sono di diversa tipologia e natura. Tra i vari, si annoverano poteri di accesso finalizzati al controllo di tutte le informazioni ne-

---

dello stesso in materia di operazioni critiche e servizi TIC, in particolare al Capo III relativo alla gestione degli incidenti e ai reclami (art. 12, par. 2, lett. c, d, e).

[155] I dispositivi di governance, gli assetti di controllo, l'organizzazione strutturale compresi eventuali accordi di esternalizzazione nonché un piano aziendale contenente la stima provvisoria del bilancio per i primi 3 esercizi (art. 12, par. 2, lett. b, c, g).

[156] In alternativa è possibile iniziare ugualmente l'attività con un capitale iniziale minimo di 50.000€, che potrà essere sostituito successivamente dall'assicurazione. L'Autorità Bancaria Europea presenterà entro 9 mesi dall'entrata in vigore del regolamento alla Commissione dei progetti di norme tecniche atte a delineare una metodologia di valutazione comune per la concessione dell'autorizzazione e integrare i requisiti della domanda.

[157] A patto che il paese terzo non sia inserito nell'elenco delle giurisdizioni non cooperative a fini fiscali ai sensi della pertinente politica dell'Unione. L'accesso transfrontaliero intraeuropeo è invece disciplinato dall'art. 28, che richiede al primo accesso una notifica all'autorità competente dello Stato membro di origine con riferimento al tipo di dati a cui si desidera accedere, lo Stato membro o gli Stati membri in cui intende accedere e il sistema di condivisione finanziaria a cui aderisce, in modo da permettere una corretta comunicazione tra le diverse autorità.

cessarie, nonché veri e propri poteri istruttori di ispezione e la facoltà di richiede misure cautelari, quali il congelamento o il sequestro di beni. Ai sensi della normativa, le autorità possono inoltre imporre ai prestatori di servizi di *hosting* di sopprimere, disabilitare o limitare l'accesso a un'interfaccia online ovvero ordinare alle autorità di registrazione del dominio di cancellare un nome di dominio completo, tenendo in debita considerazione il danno complessivo effettivo o potenziale della violazione, ed irrogare le sanzioni amministrative previste agli artt. 20 e 21 del regolamento direttamente ovvero in collaborazione con altre autorità ovvero delegando i poteri ad altre autorità od organismi.

3. Conclusioni preliminari

Le discontinuità che si registrano sul fronte dell'informazione e della comunicazione confermano la profonda trasformazione dell'industria finanziaria che partecipa, insieme ad ogni altro settore e industria, all'emersione di un nuovo ordine giuridico del mercato, in termini di soggetti (*tech*), processi e servizi (*unbundled*), mercati (disintermediati), modelli (*market place model*) e rapporti (non più fiduciari) [158].

Come per gli altri settori, si tratta ora di incanalare le opportunità offerte da fenomeni e tecnologie nuovi entro contorni regolatori che favoriscano la certezza nei rapporti insieme alla trasparenza e alla fiducia negli assetti di mercato che ne scaturiscano.

Certo, per proseguire il percorso inaugurato dall'*Open Banking* e poi dell'*Open Finance*, all'apertura della comunicazione e delle informazioni deve accompagnarsi la standardizzazione dei dati e l'interoperabilità tra le infrastrutture così da consentire l'effettiva portabilità dei dati e dei servizi sul mercato contemperando, al contempo, aspetti economici, di sicurezza e di privacy. A tale scopo appaiono evidentemente preordinate diverse disposizioni normative contenute nella nuova proposta, tra le quali risalta, nel FiDA, la previsione dell'obbligo di adesione ad uno o più schemi di condivisione dei dati di futura elaborazione.

Rimangono ferme le linee di indirizzo e i principi generali che ispirano la Strategia digitale soprattutto in relazione ai profili soggettivi e agli ambiti di esternalizzazione.

---

[158] V. FALCE, *Strategia dei dati e intelligenza artificiale. Verso un nuovo ordine giuridico del mercato*, Giappichelli, Torino, 2023.

Indipendentemente, quindi, dai soggetti, sono attività e rischi ad attrarre responsabilità e regole. Da applicare e interpretare nel rispetto del principio di proporzionalità e con la chiara finalità di non interferire eccessivamente ed ingiustificatamente sulle potenzialità delle medesime tecnologie, dalle quali si può – e si deve, alla luce delle Strategie digitali – ricavare un supporto regolatorio e di *compliance*.

Magda Bianco e Maria Iride Vangelisti [*]

Open Banking e inclusione finanziaria

SOMMARIO: 1. Introduzione. – 2. Inclusione finanziaria digitale: opportunità e rischi. – 3. I possibili benefici dell'*Open Banking* per i clienti più vulnerabili. – 4. *Open Banking* in Europa: ha favorito l'inclusione? – 5. Quali scelte nelle nuove proposte legislative?. – 6. Conclusioni.

1. Introduzione [1]

Non esiste una definizione univoca di *Open Banking* che sia valida per tutti diversi paesi del mondo [2]. In Europa, si è in presenza di un servizio di *Open Banking* quando il titolare di un conto autorizza un terzo – diverso dall'intermediario presso cui è aperto il conto – ad accedere ai suoi dati affinché possa offrigli: a) servizi aggiuntivi rispetto a quelli disciplinati nel contratto sottoscritto con l'intermediario che detiene il conto; oppure b) servizi simili, ma a condizioni diverse.

Appare chiaro già dalla stessa definizione che l'*Open Banking* offre al titolare di un conto una possibilità in più rispetto al passato: avvalersi dei

[*] Le opinioni espresse nell'articolo sono personali degli autori e non riflettono necessariamente la posizione dell'istituzione di appartenenza.

[1] Il lavoro riprende molte delle considerazioni svolte nel lavoro "*Open Banking and Financial Inclusion*" di Magda Bianco e Maria Iride Vangelisti, *European Economy Banks, Regulation and the Real Sector* (2022) https://european-economy.eu/2022/open-banking-and-financial-inclusion/. Si ringrazia Riccardo Luongo per le interessanti discussioni e gli utili commenti.

[2] La Banca dei regolamenti internazionali offre nel *Report on Open Banking and application programming interfaces* di novembre 2019 una definizione molto generica che non riesce a cogliere tutti gli aspetti rilevanti per le diverse giurisdizioni: "condivisione e sfruttamento dei dati autorizzata dai clienti da parte delle banche con sviluppatori e aziende di terze parti per costruire nuovi servizi e applicazioni, come quelli che offrono pagamenti in tempo reale, maggiori possibilità di trasparenza finanziaria per i titolari di conti e opportunità di marketing e cross-selling".

servizi di un terzo in alternativa a quelli offerti dalla sua banca, utilizzando i dati registrati sul suo conto. Come tutte le innovazioni, anche l'*Open Banking* porta con sé opportunità – prima fra tutte una maggiore concorrenza – che possono essere colte a condizione che siano adeguatamente presidiati i rischi [3].

Mentre in alcuni paesi i servizi di *Open Banking* sono stati sviluppati spontaneamente dal mercato, in assenza di una disciplina specifica, in altri paesi è stata la normativa ad introdurli disciplinandoli in modo specifico [4]. I motivi principali di questa scelta sembrano due.

In primo luogo, dare ai titolari di un conto la possibilità di sfruttare appieno le potenzialità insite nell'utilizzo dei propri dati, ad esempio per ricevere un finanziamento alle condizioni più vantaggiose o per conoscere quali strumenti di investimento possano essere più adatti. In linea di principio, anche in assenza di un regime legale di *Open Banking*, i titolari potrebbero comunicare a un terzo le informazioni registrate sui conti per ricevere consigli o servizi finanziari; la regolamentazione, però, rende tutto più facile perché crea le condizioni per uno scambio di dati efficiente e sicuro, tutelando il cliente rispetto a comportamenti scorretti.

In secondo luogo, e su un piano più generale, l'*Open Banking*, nel momento in cui favorisce lo scambio dei dati, aumenta la concorrenza e, anche per tale via, promuove l'innovazione. L'idea di fondo è di favorire l'ingresso nel mercato di nuovi operatori – spesso anche più avanzati dal punto di vista tecnologico – per proporre servizi innovativi che gli intermediari tradizionali potrebbero essere riluttanti ad offrire.

La regolamentazione sull'*Open Banking* può riguardare diversi aspetti: quale tipo di autorizzazione deve avere il terzo per accedere ai dati, quali

---

[3] BIS (*Bank for International Settlement*) *Basel Committee on Banking Supervision*, *Sound Practices Implications of Fintech developments for Banks and Bank Supervisors*, febbraio 2018, offra una panoramica sui nuovi servizi resi possibili dall'innovazione digitale che hanno avuto impatti sul settore bancario. Per una discussione più generale si veda: *Economia digitale*, Intervento di Luigi Federico Signorini, Firenze, 21 settembre 2023.

[4] Nel 2013 Singapore ha pubblicato il *Finance-as-a-service: API Playbook* (https://abs.org.sg/docs/library/abs-api-playbook.pdf), una guida per sviluppare interfaccia di programmazione (in inglese *application programming interface* (API) per facilitare la comunicazione e lo scambio di dati fra due soggetti. L'Europa, così come Hong Kong, ha emanato una prima disciplina dell'*Open Banking* nel 2018, l'Australia nel 2020. In Giappone nel 2020 è stato introdotto l'obbligo per le banche di rende pubbliche le policy in materia di API. NEGLI Stati Uniti i servizi di *Open Banking* sono offerti in assenza di una specifica normativa. Si veda anche: BIS (*Bank for International Settlement*), Basel *Committee on Banking Supervision, Report on open banking and application programming interfaces*, novembre 2019; www.deloitte.com/global/en/Industries/financial-services/perspectives/open-banking-around-the-world.html.

dati possono essere condivisi, che tipo di servizi può offrire il terzo al cliente, quale piattaforma può essere utilizzata per lo scambio dei dati, quali sono i requisiti di sicurezza applicabili, quale il regime di responsabilità fra le parti coinvolte, se l'intermediario che detiene il conto sia obbligato a concedere l'accesso del terzo o può rifiutarlo, se sia necessario un contratto fra intermediario e terzo per accedere ai dati.

Scopo del presente lavoro è indagare quali sono le condizioni che possono favorire lo sviluppo di servizi di *Open Banking* utili per le persone più vulnerabili e finanziariamente meno evolute, promuovendo una maggiore inclusione finanziaria. Fino ad oggi sembra che questo obiettivo sia stato in qualche modo trascurato, anche nei Paesi in cui lo sviluppo dell'*Open Banking* è stato guidato dalla regolamentazione.

Il primo paragrafo introduce il concetto di inclusione finanziaria e discute opportunità e rischi dell'inclusione finanziaria digitale. Il secondo si concentra su quali servizi collegati all'*Open Banking* possono essere utili per favorire l'inclusione delle persone più vulnerabili e finanziariamente meno evolute, e quali ostacoli si sovrappongono ad un effettivo utilizzo dei servizi di *Open Banking*. Il terzo paragrafo propone un'analisi della legislazione europea in materia di *Open Banking*, anche rispetto alle linee guida internazionali dettate per favorire l'inclusione finanziaria. Il quarto paragrafo discute le più recenti proposte del legislatore europeo in tema di *Open Banking* e *Open Finance*. Il quinto paragrafo conclude.

2. Inclusione finanziaria digitale: opportunità e rischi

L'inclusione finanziaria è definita come una condizione in cui le famiglie e le imprese hanno accesso a servizi finanziari offerti da intermediari formali (i.e. vigilati e controllati) e sono in grado di sceglierli e utilizzarli sulla base delle loro esigenze migliorando la propria situazione economica e finanziaria, attuale e prospettica [5].

[5] Non esiste una definizione univoca di inclusione finanziaria ma c'è condivisione sul fatto che accesso, utilizzo e qualità siano gli elementi fondati di un sistema finanziario inclusivo. Già nel 2016 Raghuram Rajan, allora Governatore della *Reserve Bank of India*, aveva affermato che l'inclusione finanziaria ha tre dimensioni, dove l'aspetto della qualità dell'inclusione, il più difficile da misurare, passa attraverso la protezione del cliente e l'educazione finanziaria: "*financial inclusion is about (a) the broadening of financial services to those people and enterprises who do not have access to financial services sector; (b) the deepening of financial services for those who have minimal financial services; and (c) greater financial literacy and consumer protection so that those who are offered financial products can make appropriate choices*" (*Hyderabad*, 18 luglio 2016).

In questo senso, l'inclusione finanziaria è stata riconosciuta come un mezzo per aumentare il benessere finanziario e l'*empowerment* economico delle famiglie e delle imprese[6]. L'inclusione finanziaria è stata documentata anche come un fattore di stabilità e solidità del settore finanziario[7].

Nel 2010 a Seoul i *Leaders* del G20 hanno riconosciuto l'inclusione finanziaria come uno dei pilastri dell'Agenda Globale per lo Sviluppo e hanno approvato un piano d'azione per l'inclusione finanziaria, il cd. *Financial Inclusion Action Plan* (FIAP). Hanno quindi istituito la *Global Partnership for Financial Inclusion* (GPFI)[8], con il mandato di promuovere l'inclusione finanziaria nel mondo e dare attuazione al piano d'azione del G20.

Nell'ambito dei lavori del GPFI, dal 2011, la Banca Mondiale conduce, con cadenza triennale, un'indagine (cd. *Global Findex*) che misura l'accesso e l'utilizzo dei servizi finanziari in quasi tutti i Paesi del mondo[9]. L'analisi condotta confrontando i dati raccolti nelle diverse *survey* dimostra che l'inclusione finanziaria ha registrato negli ultimi dieci anni notevoli progressi anche nei paesi meno sviluppati dove fino poco tempo fa molti individui non avevano la possibilità di aprire un conto, risparmiare o prendere a prestito dei soldi.

La percentuale di adulti titolari di un conto presso un intermediario finanziario è costantemente aumentata (dal 51% nel 2011 al 77% nel 2021). I progressi sono stati notevoli non solo nell'Africa subsahariana, dove oggi circa il 60% della popolazione detiene un conto telefonico (un aumento di 36 punti percentuali in un decennio), ma anche nei paesi emergenti come Brasile (84%, +30 punti percentuali) e India (78%, +43 punti percentuali). Varie sono le ragioni: da un lato, la digitalizzazione ha permesso un'offerta più diffusa a prezzi più bassi, con l'entrata di nuovi operatori anche provenienti dal settore telefonico (come Vodaphone in Kenia)[10], dall'altro, alcu-

---

[6] Sul punto si veda F. ALLEN, A. DEMIRGUC-KUNT, L. KLAPPER, M. MARTINEZ PERIA, *The foundations of financial inclusion: Understanding ownership and use of formal accounts*, in *Journal of Financial Intermediation*, 27, issue C, 2016, pp. 1-30.

[7] P. KHERA, S.Y NG, S. OGAWA, R. SAHAY, *Is Digital Financial Inclusion Unlocking Growth?*, in *IMF Working Paper* No. 2021/167, 2021.

[8] Per maggiori informazioni su obiettivi e attività del GPFI si consulti il sito: https://www.gpfi.org/.

[9] I dati del *Global Findex* vengono raccolti in un *database* pubblico che può essere utilizzato per analizzare come le persone risparmiano, prendono prestiti, effettuano pagamenti e gestiscono i rischi. https://microdata.worldbank.org/index.php/catalog/global-findex/?page=1&ps=15&repo=global-findex.

[10] Per un racconto sulla nascita di un sistema di pagamento in moneta telefonica in Kenya. M-pesa di Vodaphone, si veda: M-Pesa – a success story of digital financial inclusion by Njugu-na Ndung'u, https://www.bsg.ox.ac.uk/sites/default/files/2018-06/2017-07-M-Pesa-Practitioners-Insight.pdf, luglio 2017.

ni governi come l'India hanno avviato importanti investimenti pubblici diretti alla realizzazione di Infrastrutture Pubbliche Digitali (DPI) a supporto del sistema finanziario [11]. Negli ultimi anni è aumentato non solo l'accesso al conto, ma anche l'utilizzo dei servizi finanziari digitali, soprattutto dei pagamenti elettronici [12], favoriti anche dal periodo di pandemia [13].

Per accompagnare lo sviluppo del mercato dei servizi finanziari, nel 2016 il GPFI ha pubblicato gli *High Level Principles for Digital Financial Inclusion* (*HLPs*) [14] che costituiscono un punto di riferimento per i Governi nello sviluppo di politiche a supporto di una maggiore inclusione finanziaria. Il rapporto riconosce l'importanza dell'offerta di servizi finanziari digitali per l'inclusione finanziaria – grazie alla possibilità di ridurre i costi, aumentare la scalabilità e consentire più accesso – ma sottolinea come la tecnologia digitale aumenti i rischi, ad esempio quello legale e quello operativo. L'aumento di frodi e malfunzionamenti può portare, se non contrastato e gestito, a una perdita di fiducia e, in ultima analisi, a forme di esclusione finanziaria. La tecnologia digitale, inoltre, consente di generare, raccogliere e analizzare in modo automatico enormi quantità di dati riferiti ai clienti e alle loro abitudini. Anche questo aspetto presenta vantaggi e rischi che vanno attentamente presidiati. Inoltre, per poter beneficiare delle innovazioni, i clienti devono possedere un minimo di capacità digitali, in assenza delle quali potrebbero ritrovarsi esclusi.

Regolamentazione e controlli sono essenziali per assicurare concorrenza e parità di trattamento tra i diversi operatori, chiari perimetri di responsabilità e misure di gestione dei rischi. A ciò si aggiungono le regole per la protezione del consumatore – e del cliente più in generale – sia nell'uso dei

---

[11] Per una analisi dei benefici possibili in termini di inclusione finanziaria dello sviluppo di *Digital Public Infrastructures* si veda: G20, *POLICY RECOMMENDATIONS FOR ADVANCING FINANCIAL INCLUSION AND PRODUCTIVITY GAINS THROUGH DIGITAL PUBLIC INFRASTRUCTURE*, GPFI 2023 https://www.gpfi.org/sites/gpfi/files/G20%20Policy%20Recommendations%20for%20Advancing%20Financial%20Inclusion%20and%20Productivity%20Gains%20through%20Digital%20Public%20Infrastructure.pdf.

[12] Si veda A. DEMIRGÜÇ-Kunt, L. KLAPPER, D. SINGER, S. ANSAR, J. HESS, *The Global Findex Database 2017: Measuring Financial Inclusion and the Fintech Revolution*, World Bank, Washington, 2018; A. DEMIRGÜÇ-Kunt, L. KLAPPER *Measuring Financial Inclusion: The Global Findex Database*, World Bank, Washington, 2012; A. DEMIRGÜÇ-Kunt, L. KLAPPER, D. SINGER, S. ANSAR, *The Global Findex Database 2021: Financial Inclusion, Digital Payments, and Resilience in the Age of COVID-19*, World Bank, Washington, 2022.

[13] N.Y. BOAKYE-ADJEI, *COVID-19: Boon and bane for digital payments and financial inclusion*, *Bank for International Settlements*, in *FSI Brief* No. 9, 2020.

[14] GPFI, *G20 High-Level Principles for Digital Financial Inclusion*, 2016, https://www.gpfi.org/publications/g20-high-level-principles-digital-financial-inclusion.

servizi finanziari, sia in quello dei dati personali. Infine, è importante garantire che in un mondo sempre più complesso i clienti siano in grado di fare scelte consapevoli, conoscendo le caratteristiche principali dei prodotti che utilizzano, i loro vantaggi e svantaggi, i diritti che hanno e gli obblighi che si assumono; in questo senso anche l'educazione finanziaria e digitale può svolgere un ruolo importante [15]. In particolare, affinché l'innovazione finanziaria possa effettivamente favorire una maggiore inclusione delle persone e delle imprese, soprattutto quelle più vulnerabili, è necessario che sia accompagnata da politiche che aiutino i clienti a capire cosa è regolamentato e cosa non lo è, come evitare le frodi, quando un servizio risponde alle loro esigenze, come e a chi presentare un reclamo se qualcosa va storto [16]. Le *policy* si possono spingere fino a prevedere specifiche misure di supporto per le categorie più vulnerabili nell'utilizzo dei prodotti finanziari digitali.

Con lo scopo di fornire ai diversi paesi esempi concreti di buone prassi per favorire l'inclusione finanziaria digitale, il GPFI ha pubblicato sotto la Presidenza italiana del G20 il "*Menu of Policy Options for digital financial literacy and consumer protection*" [17], che delinea le seguenti linee di azione: a) favorire una "*protection by design*", incentivando i prestatori dei servizi a disegnare i prodotti finanziari in modo da soddisfare al meglio le esigenze dei clienti, evitando pratiche di mercato aggressive e garantendo il legittimo uso dei dati personali [18]; b) inserire l'inclusione finanziaria fra gli obiettivi delle politiche di innovazione, in modo che le autorità e il mercato siano spinti a prendere in considerazione anche le esigenze dei gruppi più vulnerabili [19]; c) individuare misure adeguate di protezione dai rischi di frode, truffa e uso non autorizzato dei dati personali, che colpiscono maggiormente le persone finanziariamente e digitalmente meno evolute; d)

[15] In questa direzione si è espresso anche il Direttore Generale della Banca d'Italia Luigi Federico Signorini al OECD-Banca d'Italia *Symposium on Financial Literacy and Empowerment: Data, Policies and Evaluation*, Banca d'Italia Roma, 17 novembre 2023, https://www.bancaditalia.it/pubblicazioni/interventi-direttorio/int-dir-2023/Signorini-OECD-17112023.pdf.

[16] J. FROST, L. GAMBACORTA, H.S. SHIN, *From financial Innovation to Inclusion*, in *IMF Finance and Development*, marzo 2021, https://www.imf.org/external/pubs/ft/fandd/2021/03/making-financial-innovation-more-inclusive-frost.htm.

[17] GPFI, G20 *Menu of Policy Options for Digital Financial Literacy and Financial Consumer and MSME Protection* https://www.gpfi.org/sites/gpfi/files/1_G20%20Menu%20of%20Policy%20Options.pdf.

[18] La *product governance* è un esempio concreto di "*protection by design*" (si veda p. 16 dell'Allegato tecnico del GPFI *Menu* 2021.

[19] Nell'Allegato tecnico del GPFI *Menu* (p. 16) si citano come esempi virtuosi lo sviluppo di *regulatory sandbox* e *innovation hubs* che favoriscano la progettazione, da parte del mercato, di prodotti finanziari adatti per le persone e le imprese meno servite.

prevedere sistemi di risoluzione delle controversie alternativi alla giustizia ordinaria, tempestivi e a basso costo, essenziali per assicurare la fiducia del pubblico nel sistema finanziario; e) progettare programmi di educazione finanziaria efficaci, anche sfruttando le opportunità offerte dalla digitalizzazione.

3. I possibili benefici dell'*Open Banking* per i clienti più vulnerabili

Il modello di *Open Banking* introdotto dalla seconda direttiva sui servizi di Pagamento (PSD2) in Europa nasce anche dall'esigenza di regolamentare due servizi che già venivano offerti sul mercato, in assenza di disciplina e con rischi per la clientela[20]. Il primo servizio è il *payment initiation service* (PIS) che consente a un intermediario terzo (il *payment initiation service provider* – PISP) di avviare un pagamento per conto di un cliente, utilizzando il denaro depositato sul conto bancario *on-line*. Il servizio era stato pensato principalmente per consentire il pagamento con bonifico nelle transazioni di commercio *on-line*, senza dover necessariamente utilizzare una carta di pagamento; il PISP può garantire al venditore che il pagamento della merce è avvenuto, e il commerciante può chiudere la transazione e avviare la spedizione[21]. Il secondo servizio è l'*account information service* (AIS) che consente a un AISP (*account information service provider*) di prendere visione delle transazioni registrate su un conto *on-line*, con l'autorizzazione del titolare, per fornirgli informazioni consolidate su uno o più conti da lui detenuti.

Entrambi i servizi si basano sulla possibilità che PISP e AISP avviino uno scambio di dati con l'intermediario che detiene il conto, utilizzando una piattaforma sicura su cui possono essere verificate anche informazioni aggiuntive, quali ad esempio il consenso dato dal titolare del conto e l'identità del soggetto richiedente. La previsione normativa ha, di fatto,

[20] Il considerando 27 della PSD2 spiega con chiarezza che "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".

[21] R. DE BONIS, M.I. VANGELISTI, *Moneta. Dai buoi di Omero ai Bitcoin*, il Mulino, Bologna, 2019.

posto le basi in Europa anche per lo sviluppo di servizi ulteriori rispetto a quelli prospettati dalla normativa sull'*Open Banking*: *budgeting*, *credit scoring* e servizi di consulenza [22]. Un'evoluzione in tal senso non era ovvia all'inizio: solo nel 2019 la *European Banking Authority* (EBA) ha chiarito che i dati acquisiti dall'AISP potevano essere utilizzati anche per offrire, al titolare del conto o a terzi, prestazioni diverse rispetto alle previsioni della PSD2 [23], sempre che il titolare dei dati fosse d'accordo e fornisse il suo consenso ai sensi della legge sulla *privacy* [24].

Quali di questi servizi di "*Open Banking*" possono essere utili per i gruppi finanziariamente meno inclusi e più vulnerabili? Vediamoli uno a uno.

Le persone più vulnerabili dal punto di vista finanziario tendono ad avere un reddito irregolare, hanno difficoltà ad accedere a un finanziamento e a ottenere una carta di credito; inoltre, il basso livello di alfabetizzazione digitale e finanziaria li rende meno attenti alla gestione dei propri soldi e più vulnerabili alle frodi quando utilizzano strumenti di pagamento digitali. A questa categoria di persone i servizi di *payment initiation* potrebbero offrire la possibilità di acquistare *on-line* pur non avendo una carta di credito, tramite un bonifico; in aggiunta, potrebbero essere loro proposti servizi che li aiutino nella gestione delle entrate, delle uscite e delle spese ricorrenti; ad esempio, il PISP potrebbe avviare il pagamento delle bollette alla scadenza e ricaricare quando necessario carte prepagate o canoni telefonici, evitando spese extra e penali per il ritardo [25].

---

[22] Per una disamina dei servizi offerti si veda Banca d'Italia, Psd2 e Open Banking, Nuovi modelli di business e rischi emergenti, novembre 2021, https://www.bancaditalia.it/compiti/vigilanza/analisi-sistema/approfondimenti-banche-int/2021-PSD2-Open-Banking.pdf.

[23] Il considerando 28 della direttiva PSD2 precisa, con riferimento al servizio di informazione sui conti che "tali servizi forniscono all'utente di servizi di pagamento informazioni online aggregate su uno o più conti di pagamento, detenuti presso un altro o altri prestatori di servizi di pagamento, a cui si ha accesso mediante interfacce online del prestatore di servizi di pagamento di radicamento del conto. L'utente di servizi di pagamento può così disporre immediatamente di un quadro generale della sua situazione finanziaria in un dato momento".

[24] Parere EBA n. 4631/2019 pubblicato il 13 settembre 2019 in risposta al quesito ID 2018-4098.

[25] Per ulteriori esempi si vedano: BANCA DEI REGOLAMENTI INTERNAZIONALI, BANCA MONDIALE, *Payments aspects of financial inclusion in the Fintech era*, 2020, https://www.bis.org/cpmi/publ/d191.pdf; A. PLAITAKIS e S. STASCHEN, *Open banking: How to design for financial inclusion*, 2020, https://www.cgap.org/sites/default/files/publications/2020_10_Working_Paper_Open_Banking.pdf; F. REYNOLDS, M. CHIDLEY, *Consumer priorities for Open Banking,* https://www.openbanking.org.uk/wp-content/uploads/Consumer-Priorities-for-Open-Banking-report-June-2019.pdf, 2019.

I servizi di *account information* forniscono ai clienti una visione completa dei movimenti e del saldo dei loro conti. Le persone più vulnerabili dal punto di vista finanziario potrebbero beneficiare di un monitoraggio sui propri conti finalizzato a pianificare le spese, evitando scoperti; potrebbe essere favorito anche l'accesso al credito attraverso servizi di *rating* basati sulla valutazione dei movimenti e della gestione del conto. Il monitoraggio del conto potrebbe anche essere abbinato a strumenti di *budgeting* per favorire la regolarità dei pagamenti ricorrenti e promuovere forme di risparmio mensili, anche piccole. In aggiunta, gli AISP potrebbero fornire attività di consulenza aiutando nella comparazione dei costi e nella scelta dei servizi finanziari più adatti, agevolando anche eventuali cambi di fornitore. Se i servizi di informazione sui conti comprendessero anche la visibilità *ex ante* sulle operazioni di pagamento elettronico disposte dal titolare, gli AISP potrebbero offrire una protezione rafforzata da truffe e frodi, ad esempio rilevando tempestivamente transazioni non coerenti con il modello di spesa del cliente e chiedendo, in questi casi, alla banca un controllo aggiuntivo prima dell'esecuzione. Questa tipologia di servizio potrebbe essere molto utile, fra i clienti più vulnerabili, in particolare agli anziani, più soggetti a frodi perché digitalmente meno esperti.

A fronte, però delle opportunità che l'introduzione dell'*Open Banking* può offrire ai soggetti più vulnerabili ci sono almeno quattro punti di attenzione.

In primo luogo, l'*Open Banking* richiede l'apertura di un conto, spesso *on-line* (ciò è vero in Europa ma anche in altri paesi del mondo), escludendo la possibilità che servizi simili possano essere offerti a soggetti non bancarizzati. Un passo avanti potrebbe venire dal passaggio dall'*Open Banking* all'*open data*, che prevede la condivisione di dati e informazioni non solo fra istituzioni finanziarie, ma fra queste e le società di forniture elettriche, di telecomunicazioni e, più in generale, offerenti altri servizi non finanziari. L'apertura allo scambio dei dati fra diversi settori potrebbe dare un effettivo impulso all'inclusione dei soggetti non bancarizzati, la cui reputazione come clienti, ad esempio, potrebbe essere valutata anche dal comportamento tenuto nei confronti di società non finanziarie. Pochi paesi si sono tuttavia mossi fino ad oggi in questa direzione – fra questi Regno Unito [26] e Au-

[26] La strategia *smart data* punta a estendere nel Regno Unito la condivisione dei dati dei clienti nei mercati regolamentati. Nel 2020 era stato costituito lo *smart data working group* con l'obiettivo di promuovere lo sviluppo di standard e infrastrutture per lo scambio dei dati, anche a vantaggio dei consumatori vulnerabili, e favorire l'interoperabilità delle soluzioni evitando duplicazioni (https://www.gov.uk/government/groups/smart-data-working-group). Nel 2023

stralia [27] – per le intrinseche difficoltà del modello, legate anche alla necessità di coordinamento fra operatori con caratteristiche diverse e fra più autorità competenti.

Un secondo punto riguarda il tema della consapevolezza e della fiducia. Da un lato, le persone finanziariamente più vulnerabili tendono ad essere meno istruite e, pertanto, non sempre in grado di comprendere appieno le caratteristiche dei prodotti che vengono offerti e di gestire in modo proficuo il rapporto con l'intermediario [28]. Dall'altro, le stesse persone tendono a diffidare del sistema finanziario [29]. La combinazione di questi due elementi potrebbe far ritenere che le persone finanziariamente meno evolute siano riluttanti ad usufruire dei servizi di *Open Banking*, già di per sé abbastanza complessi.

Il terzo punto riguarda la gestione dei dati personali. Il messaggio standard – veicolato sia dalle autorità sia dagli intermediari – è quello di non condividere i propri dati personali con soggetti terzi. L'obiettivo è quello di proteggere i clienti bancari dalle frodi; in una certa misura, la condivisione dei dati personali con terzi potrebbe anche essere interpretata come grave negligenza del cliente, con conseguenze negative sulla possibilità di ottenere un rimborso in caso di transazioni non autorizzate. L'*Open Banking* si basa sulla condivisione sicura dei dati con controparti autorizzate, ma per i clienti può essere difficile capire: di chi si possono fidare e di chi no; quali condizioni devono essere soddisfatte per operare in tranquillità; quali tipi di dati possono essere condivisi; quali sono diritti e doveri delle parti coinvolte. Soprattutto le persone più vulnerabili possono avere diffi-

è stata proposta la *Data Protection and Digital Information Bill* che, fra l'altro, consentirà lo scambio di *smart data* nei diversi settori dell'economia per aumentare la competizione e ridurre i costi.

[27] Il Governo australiano ha definito un quadro per la condivisione dei dati (*consumer data right* – CDR) che permette ai consumatori di scambiare in modo sicuro i propri dati con terze parti accreditate per poter accedere a servizi migliori a prezzi più competitivi. Il settore bancario è il primo individuato per l'applicazione del CDR, seguito da energia e telecomunicazioni. Si veda sul punto: P. BUCKLEY ROSS, N. JEVGLEVSKAJA, S. FARRELL, *Australia's Data-Sharing Regime: Six Lessons for Europe*, in *King's Law Journal*, 33:1, 61-91, 2022.

[28] In questo senso M. AMPUDIA, M. EHRMANN, *Financial inclusion: what's it worth?*, in *European Central Bank Working Paper*, No. 1990, 2017; J. COFFINET, C. JADEAU, *Household financial exclusion in the Eurozone: the contribution of the Household Finance and Consumption survey*, *Data needs and Statistics compilation for macroprudential analysis*, volume 46, in *Bank for International Settlements*, 2017.

[29] La mancanza di fiducia nelle istituzioni finanziarie è associata a una minore tendenza a detenere un conto bancario (M. AMPUDIA, S. PALLIGKINIS, *Trust and the Household–Bank Relationship*, in *European Central Bank Working Paper* No. 2184, 2018) o un conto di risparmio (E. BECKMANN, D.S. MARE, *Formal and Informal Household Savings: How Does Trust in Financial Institutions Influence the Choice of Saving Instruments?*, in *MPRA Paper* 81141, 2017. https://mpra.ub.uni-muenchen.de/81141/1/MPRA_paper_81141.pdf).

coltà a gestire correttamente i propri dati, con il rischio di cadere vittime di comportamenti inconsapevoli e subire abusi o frodi[30].

L'ultimo punto riguarda i costi. Le persone finanziariamente più vulnerabili sono solitamente più attente ai costi perché possono disporre di limitate risorse economiche. Potrebbero quindi essere meno incentivate all'acquisto di servizi di *Open Banking*, se costosi e di non immediata utilità.

4. *Open Banking* in Europa: ha favorito l'inclusione?

La PSD2 offre un quadro giuridico completo per l'offerta di servizi di *Open Banking* in Europa. In particolare, stabilisce quali tipi di intermediari possono offrire i servizi e, se i *provider* non sono banche, li obbliga a chiedere all'autorità competente un'autorizzazione *ex ante* per l'ingresso nel mercato. Sono poi previsti controlli *ex post* per garantire che vengano rispettati nell'offerta del servizio i requisiti previsti dalla normativa. Esistono anche norme specifiche che assicurano uno scambio sicuro dei dati, con un attento presidio dei rischi, anche quello operativo[31].

In Europa, però, fino ad oggi, i servizi di *Open Banking* non si sono diffusi molto, con differenze significative fra paesi. In Italia, ad esempio, nel primo semestre del 2022 i clienti dei servizi di *Open Banking* erano circa 407.000[32]; nel Regno Unito invece gli utenti regolari dei servizi di *Open Banking* sono oggi più di otto milioni (sei milioni a giugno 2022).

Un'indagine condotta su 5.500 intervistati di 22 paesi europei rilevato che i servizi di *Open Banking* sono stati utilizzati soprattutto da clienti che già avevano comprato prodotti finanziari digitali e, in generale, mostrato interesse per l'innovazione finanziaria. Lo studio trova che la preferenza per l'anonimato, la riluttanza a condividere i propri dati e la sfiducia nei confronti dei prestatori di servizi non bancari incidono negativamente sulla propensione all'utilizzo dell'*Open Banking*. In particolare, non ci sono evi-

---

[30] O. Borgogno, G. Colangelo, *Consumer inertia and competition-sensitive data governance: the case of Open Banking*, in *Journal of European Consumer and Market Law*, vol. 9, Issue 4, 2020, pp. 143-150.

[31] Regolamento delegato (UE) 2018/389 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, modificato nel 2022 proprio per tenere

[32] R. Pellitteri, R. Parrini, C. Cafarotti, B.A. De Vendictis, *L'*Open Banking *nel sistema dei pagamenti: evoluzione infrastrutturale, innovazione e sicurezza, prassi di vigilanza e sorveglianza*, in *Questioni istituzionali* n. 31, Banca d'Italia, marzo 2023.

denze sull'utilità dell'*Open Banking* per le persone finanziariamente meno evolute e a basso reddito [33]. Un altro studio condotto su consumatori olandesi nel 2019 ha rilevato che gli individui tendono a fidarsi di più della loro banca che di intermediari terzi, confermando quindi una certa riluttanza ad utilizzare servizi di *Open Banking* [34]. Una ricerca condotta, sempre in Olanda, intervistando un gruppo di intermediari che offrono servizi di pagamento, conferma lo scarso interesse della popolazione, soprattutto la più vulnerabile, per i servizi di *Open Banking* a causa, fra l'altro, della difficoltà intrinseca nel modello, delle preoccupazioni per l'utilizzo dei dati e della scarsa conoscenza sulle caratteristiche del servizio [35].

Per investigare le ragioni del finora limitato successo dell'*Open Banking* in Europa, la tabella 1 confronta il regime introdotto dalla normativa PSD2 con le *policy options* proposte dal GPFI per favorire l'introduzione nel mercato di innovazioni che abbiamo effetti positivi in termini di inclusione [36].

GPFI policy options 2021	**PSD2**
Favorire la «*protection by design*».	Non c'è menzione dell'opportunità di valutare il profilo del cliente prima di offrire i servizi di *Open Banking*, né di porre particolare attenzione alle esigenze dei clienti vulnerabili.
Includere l'inclusione finanziaria fra gli obiettivi delle politiche che favoriscono l'innovazione.	Tra gli obiettivi non viene fatto riferimento all'inclusione finanziaria.
Gestire i rischi di frode e di malversazione nell'utilizzo dei dati personali.	Si prevede l'applicazione del GDPR; in caso di transazioni non autorizzate l'intermediario che detiene il conto deve rifondere il cliente, salvo il caso di frode del cliente stesso.

segue

[33] M. POLASIK, R. KOTKOWSKI, *The Open Banking Adoption Among Consumers in Europe: The Role of Privacy, Trust, and Digital Financial Inclusion*, 2022, https://ssrn.com/abstract=4105648.

[34] M. BIJLSMAA, C. VAN DER CRUIJSENA, N. JONKERA, *Consumer propensity to adopt PSD2 services: trust for sale?*, in *Working Paper* No. 671, De Nederlandsche Bank (DNB), The Netherlands Tilburg University, January 2020.

[35] M. PERIUSO, F. KOEFER e M.Ehrenhard, *Open banking and inclusive finance in the European Union: perspectives from the Dutch stakeholder ecosystem*, Financial Innovation 2023, 9 (1), 11, https://doi.org/10.1186/s40854-023-00522-1.

[36] GPFI (2021), *G20 Menu of Policy Options for Digital Financial Literacy and Financial Consumer and MSME Protection*, https://www.gpfi.org/sites/gpfi/files/1_G20%20Menu%20of%20Policy%20Options.pdf.

GPFI policy options 2021	**PSD2**
Introdurre meccanismi di risoluzione delle controversie alternativi alla giustizia ordinaria (ADR).	Sono previsti ADR per la risoluzione di controversie originate dall'offerta di servizi di *Open Banking*.
Disegnare programmi di educazione finanziaria efficaci.	Non è previsto che l'offerta dei servizi di *Open Banking* venga accompagnata da iniziative di educazione finanziaria.

Il confronto mostra come la normativa europea offra un quadro chiaro per la protezione degli utenti, ma non prenda in considerazione in modo esplicito l'inclusione finanziaria. In particolare, l'inclusione finanziaria non è mai menzionata come obiettivo dell'*Open Banking*, accanto a innovazione e concorrenza. Questo può aver portato a due importanti conseguenze. Da un lato, gli intermediari non sono stati incentivati ad offrire servizi pensati anche per le categorie di clienti più vulnerabili; dall'altro, le autorità nazionali non hanno ritenuto di avviare forme di monitoraggio del mercato per verificare se l'offerta di servizi di *Open Banking* fosse effettivamente adatta a favorire l'inclusione. In questo contesto non è stata neppure favorita la messa a disposizione dei clienti – soprattutto quelli più vulnerabili – di strumenti che consentissero loro di gestire il proprio consenso all'utilizzo dei dati da parte degli intermediari terzi in modo tempestivo e trasparente, ad esempio attraverso cruscotti che aumentino il controllo da parte del titolare e favoriscano la fiducia.

Un altro punto che la normativa avrebbe potuto prendere in considerazione riguarda la necessità di fornire ai clienti informazioni aggiuntive su prodotti complessi, come quelli che sottendono l'offerta dei servizi di *Open Banking*, dove sono coinvolti molti intermediari diversi. L'art. 106[37]

[37] Art. 106 – *Obbligo di informare i consumatori in merito ai loro diritti.* 1. Entro il 13 gennaio 2018 la Commissione realizza un opuscolo elettronico di agevole consultazione che elenca in modo chiaro e facilmente comprensibile i diritti dei consumatori ai sensi della presente direttiva e del diritto dell'Unione. 2. La Commissione informa gli Stati membri, le associazioni europee dei prestatori di servizi di pagamento e le associazioni europee dei consumatori della pubblicazione dell'opuscolo di cui al paragrafo 1. Sia la Commissione, sia l'ABE, sia le autorità competenti assicurano che l'opuscolo sia reso disponibile in modo facilmente accessibile sui rispettivi siti web. 3. I prestatori di servizi di pagamento assicurano che l'opuscolo sia messo a disposizione in modo facilmente accessibile nei rispettivi siti web se esistenti e su supporto cartaceo presso le succursali, gli agenti e le entità a cui vengono esternalizzate le loro attività. 4. I prestatori di servizi di pagamento non addebitano spese ai clienti per la messa a disposizione delle informazioni di cui al presente articolo. 5. Per quanto concerne le persone con disabilità, le disposizioni del presente articolo si applicano facendo ricorso a mezzi alternativi adeguati, che consentano di rendere disponibili le informazioni in un formato accessibile.

della PSD2 prevede che gli Stati membri e gli intermediari mettano a disposizione dei consumatori un "opuscolo elettronico di agevole consultazione" che spieghi i loro diritti. La brochure "I tuoi diritti quando effettui un pagamento in Europa" sui nuovi servizi di *Open Banking* si limita ad affermare: "Grazie alle moderne tecnologie oggi puoi utilizzare servizi finanziari innovativi che possono essere offerti da banche e da altri prestatori di servizi di pagamento. Ciò significa, ad esempio, che puoi monitorare le tue finanze personali o effettuare acquisti online senza una carta di credito o di debito. Proprio come le banche, questi nuovi prestatori di servizi di pagamento devono essere autorizzati e sono soggetti a vigilanza, e devono gestire i tuoi dati in modo sicuro", senza offrire spiegazioni sui servizi offerti, senza descrivere i potenziali vantaggi, senza chiarire ruoli e responsabilità degli intermediari coinvolti.

La PSD2 non prevede neppure che vengano organizzate, dagli enti competenti nei diversi paesi, iniziative di educazione finanziaria dirette ad accompagnare l'offerta dei servizi e il loro utilizzo consapevole da parte dei clienti. Su questo punto, invece, la *Payment Accounts Directive* (PAD) avrebbe potuto costituire un esempio di buona prassi. Il considerando 48, infatti, richiama l'opportunità che gli Stati membri e gli enti creditizi forniscano ai consumatori informazioni chiare e comprensibili sul diritto ad aprire un conto di pagamento con caratteristiche di base. Gli Stati membri dovrebbero anche garantire che le azioni di comunicazione siano dirette, in particolare, ai consumatori vulnerabili, sprovvisti di un conto bancario. Inoltre, gli enti creditizi sono chiamati a dare un'assistenza specifica ai consumatori nell'apertura del conto di base. Il considerando 49 prosegue nella stessa direzione chiedendo agli Stati membri di promuovere misure a sostegno dell'educazione dei consumatori più vulnerabili, anche incoraggiando gli enti creditizi ad accompagnare l'apertura di un conto di pagamento con caratteristiche di base con iniziative di educazione finanziaria.

L'analisi porta a suggerire, in prospettiva, quattro interventi migliorativi della normativa sui servizi di *Open Banking*: 1) riconoscere l'inclusione finanziaria come obiettivo, accanto a innovazione e competizione; 2) prevedere meccanismi (es. *dashboards* o pannelli di gestione) che facilitino i clienti nel monitoraggio dell'uso dei dati e nella revoca del consenso; 3) supportare i più vulnerabili nell'accesso e nella comprensione dei servizi; 4) favorire iniziative di educazione finanziaria e digitale nonché campagne di sensibilizzazione sull'uso e la condivisione dei dati personali.

5. Quali scelte nelle nuove proposte legislative?

Il 28 giugno 2023 la Commissione europea ha presentato un nuovo pacchetto per disciplinare i servizi di pagamento e l'accesso ai dati dei clienti dei servizi finanziari. L'obiettivo è quello di spingere il mercato verso una maggiore digitalizzazione, rafforzando la tutela dei consumatori e la concorrenza.

Il pacchetto è composto da una direttiva (PSD3) e da un regolamento sui servizi di pagamento (PSR), che modificano le previsioni della PSD2. C'è inoltre una nuova proposta legislativa per definire un quadro di riferimento per l'accesso ai dati finanziari, che stabilirà diritti e obblighi per la condivisione dei dati dei clienti nel settore finanziario (FIDA), anche diversi da quelli registrati nei conti di pagamento, che rimarranno invece disciplinati dal PSR. Il pacchetto normativo dovrebbe garantire servizi finanziari più innovativi e più adatti alle esigenze degli utenti per gli utenti, stimolando la concorrenza nel settore finanziario.

Ci sono alcune novità positive nelle proposte sotto il profilo dell'inclusione finanziaria, anche se limitate. Vediamole una alla volta, partendo dalla regolamentazione più nuova, quella dell'accesso ai dati finanziari.

Il regolamento FIDA origina dall'idea che gli utenti potrebbero beneficiare da un maggiore e più efficiente scambio di dati per ottenere servizi finanziari adatti alle loro necessità. Regole incerte e infrastrutture non standardizzate minano invece la fiducia degli utenti e non consentono loro di condividere in sicurezza i propri dati. La proposta suggerisce quindi di ampliare le previsioni della PSD2 sull'*Open Banking*, che si limitavano ai dati registrati sui conti di pagamento, includendo anche i dati su prestiti, depositi, assicurazioni e forme di risparmio pensionistico.

Il legislatore amplia, così facendo, la platea dei potenziali interessati e, di conseguenza, la possibilità di sfruttamento dei dati, con effetti potenzialmente positivi in termini di inclusione. Non si spinge, tuttavia, fino alla condivisione di dati non finanziari che avrebbe probabilmente apportato benefici maggiori soprattutto ai clienti più vulnerabili ancora esclusi dal mondo finanziario.

Il regolamento FIDA apporta anche aggiustamenti su due punti che erano stati segnalati come possibili problemi per l'accesso all'*Open Banking*. In primo luogo, il regolamento prevede che gli intermediari mettano a disposizione dei clienti «pannelli di gestione» per gestire autorizzazioni e revoche, che non era richiesti nella PDS2 per l'*Open Banking* e, come ar-

gomentato nel paragrafo precedente, avrebbero potuto agevolare l'utilizzo soprattutto da parte delle persone più vulnerabili. Viene poi previsto che l'intermediario che accede ai dati debba in qualche modo compensare l'intermediario presso cui i dati sono registrati, laddove nella PSD2 tutte le spese per l'infrastruttura erano invece a carico dell'intermediario presso cui il conto era aperto. Anche questo aspetto, che sanciva uno squilibrio fra operatori, era stato individuato come un potenziale deterrente allo sviluppo dei servizi[38].

Passando all'analisi del PSR, che contiene le previsioni più rilevanti sui pagamenti in termini di inclusione, purtroppo si evidenzia che nella parte relativa all'*Open Banking* non sono state replicate previsioni analoghe a quelle appena ricordate per lo scambio dei dati finanziari. Continuano a non essere previsti pannelli di gestione del consenso per l'accesso ai dati sul conto così come non è variato il regime per la ripartizione dei costi fra intermediari.

Il regolamento, invece, richiama il tema dell'inclusione finanziaria in due punti, non legati però allo scambio dei dati. Il primo è quello relativo ai requisiti di sicurezza per l'effettuazione dei pagamenti elettronici. Ad oggi, la capacità di utilizzare correttamente uno *smartphone* è spesso alla base del processo di autenticazione; vi sono però gruppi vulnerabili (ad esempio persone con disabilità e anziani) che non hanno sufficienti competenze digitali e rischiano di essere esclusi. La PSR richiede quindi agli intermediari di individuare fattori alternativi di autenticazione che siano accessibili per tutti e non creino discriminazioni. Il secondo punto è il richiamo che il PSR fa agli intermediari sulla necessità di migliorare la comprensione e la consapevolezza degli utenti di servizi di pagamento, attraverso specifiche iniziative di educazione finanziaria e campagne di sensibilizzazione. Tuttavia, tale richiamo riguarda, nello specifico, solo i rischi di frode e non la generalità dei servizi disciplinati, compresi quelli di *Open Banking*.

[38] Si veda al riguardo, per un confronto internazionale, A. PLAITAKIS, S. STASCHEN, *Open banking: how to design for financial inclusion*, CGAP https://www.cgap.org/research/publication/open-banking-how-to-design-for-financialinclusion, ottobre 2020. Si veda anche la *European consultation on Open Finance* (https://finance.ec.europa.eu/regulation-andsupervision/consultations/finance-2022-open-finance_en) e la proposta inclusa nel *Commission Work Program* del 2023(https://commission.europa.eu/strategy-documents/commission-workprogramme/commission-work-programme-2023_en).

6. Conclusioni

Un maggiore accesso e utilizzo dei servizi finanziari digitali, da parte della popolazione, compresi i gruppi più vulnerabili, può portare a un miglioramento del loro benessere finanziario. L'innovazione può aiutare in questo sviluppo, ma deve essere accompagnata da politiche che guidino il mercato verso un'offerta di servizi più adatti alle esigenze dei clienti meno evoluti dal punto di vista finanziario e che tengano in adeguata considerazione i rischi di esclusione. In questa logica, devono essere anche previsti incentivi per aumentare la consapevolezza degli utilizzatori dei servizi e le loro capacità di scelta.

Le normative su *Open Banking* e *Open Finance* vanno nella giusta direzione, ma se l'inclusione finanziaria non viene presa in considerazione come uno degli obiettivi fin dall'inizio, e non si declinano norme che diano chiare indicazioni in tal senso, i benefici della condivisione dei dati finiscono per non essere disponibili per i clienti meno evoluti, che rischiano di continuare ad essere esclusi.

Giuseppe Colangelo

Open Banking e *Open Finance*: sfide, opportunità e rischi per la regolazione

SOMMARIO: 1. Introduzione. – 2. Regolazione e *Open Banking*: ragioni, opportunità, rischi. – 3. L'esperienza europea: successi e limiti della PSD2. – 3.1. L'avvento della *Open Finance*: la proposta FIDA. – 4. Conclusioni.

1. Introduzione

Alcune importanti iniziative legislative all'orizzonte rendono sempre più attuale una attenta riflessione sul fenomeno dell'*Open Banking* e, in particolare, sulla scelta di policy, largamente prevalente sullo scenario internazionale [1], di promuovere l'*Open Banking* attraverso un intervento obbligatorio, ossia imponendo la condivisione dei dati bancari e finanziari dei consumatori. Si fa riferimento, nello specifico, alla proposta in tema di "Personal Financial Data Rights" avanzata dalla *Consumer Financial Protection Bureau* (CFPB) [2], alla proposta europea di revisione della Direttiva sui servizi di pagamento (PSD2) [3] nonché di introduzione dell'*Open Finan-*

[1] OECD, *Shifting from Open Banking to Open Finance: Results from the 2022 OECD survey on data sharing frameworks*, (2023) https://doi.org/10.1787/9f881c0c-en.

[2] U.S. CONSUMER FINANCIAL PROTECTION BUREAU, *Required Rulemaking on Personal Financial Data Rights*, in *Docket* No. 2023-CFPB-0052, https://www.consumerfinance.gov/rules-policy/notice-opportunities-comment/open-notices/required-rulemaking-on-personal-financial-data-rights/.

[3] Direttiva (UE) 2015/2366 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, [2015] OJ L 337/35. La proposta di riforma si struttura in due interventi che mirano a separare la disciplina dei servizi di pagamento da quella sulle autorizzazioni e sulla supervisione degli istituti di pagamento: alla prima è dedicata la proposta di Regolamento relativo ai servizi di pagamento nel mercato interno e che modifica il regolamento (UE) n. 1093/2010, COM(2023)367 final; alla seconda è, invece, indirizzata la proposta di Direttiva rela-

ce (FIDA), ossia dell'estensione anche ai dati finanziari dell'attuale quadro regolamentare che disciplina l'accesso ai dati sui conti di pagamento [4].

In questo scenario, gli eventuali punti di contatti tra la proposta americana e gli sviluppi legislativi europei sono di particolare interesse per due ragioni. In primo luogo, gli Stati Uniti hanno sinora rappresentato il principale paese nel quale l'*Open Banking* si è sviluppato a seguito di un impulso proveniente dal mercato: con il "Personal Financial Data Rights" si verificherebbe, dunque, una transizione verso, invece, un modello regolatorio che l'Europa per prima ha promosso. In secondo luogo, nella proposta statunitense il termine *Open Banking* comprende anche il fenomeno dell'*Open Finance*, sicché il confronto con l'esperienza europea diventa ancor più opportuno in ragione sia della revisione della PSD2, ma altresì in vista della discussione sulla proposta FIDA.

Partendo da tali premesse e traendo spunto dal dibattito europeo sulla revisione della PSD2 e sulla sua estensione all'*Open Finance*, il presente contributo ambisce a fornire un quadro delle ragioni che hanno supportato l'azione regolatoria nel promuovere l'*Open Banking*, dei benefici e dei rischi derivanti dalla condivisione dei dati in ambito bancario e finanziario, nonché delle delicate scelte di policy che i legislatori sono chiamati a compiere.

2. Regolazione e *Open Banking*: ragioni, opportunità, rischi

Le iniziative legislative dirette a promuovere l'*Open Banking* rientrano nella recente ondata di interventi normativi volti a favorire il *data sharing* e conferire agli individui un maggiore controllo sui dati per favorire concorrenza innovazione nei mercati. La logica dell'*Open Banking* è, infatti, quella di garantire ai consumatori un controllo effettivo sui propri dati e l'opportunità di beneficiare di servizi innovativi e più competitivi che potrebbero essere forniti dall'applicazione dell'innovazione tecnologica al settore bancario e finanziario (FinTech). Grazie all'accesso e all'elaborazione di grandi volumi di dati, compresi quelli non finanziari (ad esempio, le impronte digitali), prodotti e servizi FinTech possono promuovere

tiva ai servizi di pagamento e ai servizi di moneta elettronica nel mercato interno, che modifica la direttiva 98/26/CE e abroga le direttive (UE) 2015/2366 e 2009/110/CE, COM(2023)366 final.

[4] COMMISSIONE EUROPEA, Proposta di Regolamento relativo a un quadro per l'accesso ai dati finanziari e che modifica i Regolamenti (UE) n. 1093/2010, (UE) n. 1094/2010, (UE) n. 1095/2010 e (UE) 2022/2554, COM/2023/360 final.

l'inclusione finanziaria, attenuare la riluttanza o l'incapacità dei consumatori di passare da un'impresa all'altra e aiutarli a fare scelte informate, nonché a trarre beneficio da offerte più convenienti [5].

Del resto, le dinamiche di mercato sono modellate dal comportamento dei consumatori, per cui il maggior coinvolgimento dei consumatori svolge un ruolo cruciale nella promozione di una concorrenza efficace. Per promuovere il ruolo attivo dei consumatori, l'obiettivo fondamentale delle iniziative di regolamentazione della condivisione dei dati è quello di consentire loro di optare agevolmente tra le diverse piattaforme disponibili, riducendo *switching costs* ed evitando il blocco dei dati personali. Nel caso dell'*Open Banking*, tale responsabilizzazione dei consumatori mira a rafforzare la loro posizione negoziale nei confronti delle banche.

Pertanto, l'obiettivo è aumentare la concorrenza, stimolare l'innovazione e rendere il mercato più contendibile attraverso la condivisione dei dati. In sintesi, la logica economica sottesa all'*Open Banking* è essenzialmente di tipo concorrenziale. Ciò è ben illustrato dall'esperienza del Regno Unito dove il rimedio normativo è stato concepito da un'autorità antitrust a seguito di un'indagine di mercato sul settore bancario che ha evidenziato una grave debolezza in termini di dinamiche competitive a causa dell'elevata concentrazione del mercato e della bassa propensione dei consumatori a modificare il proprio fornitore di servizi [6].

In questo scenario, l'intervento regolatorio è quindi sostenuto dalla tradizionale giustificazione del fallimento del mercato. Del resto, senza un obbligo legislativo di condivisione dei dati, le banche possono avere una valida giustificazione per rifiutare l'accesso a informazioni sensibili da parte di fornitori terzi a causa di problematiche legate alla proprietà intellettuale, alla sicurezza [7].

Ciò non toglie che, anche in assenza di un intervento regolamentare, l'*Open Banking* possa esistere. Tuttavia, in quest'ultimo caso, qualora le

---

[5] Si vedano, tra gli altri, T. Babina, S. Bahaj, G. Buchak, F. De Marco, A. Foulis, W. Gornall, F. Mazzola, T. Yu, *Customer Data Access and Fintech Entry: Early Evidence from Open Banking*, in *NBER Working Paper* 32089, 2024, http://www.nber.org/papers/w32089; T. Berg, V. Burg, A. Gombovic, M. Puri, *On the rise of fintechs: Credit scoring using digital footprints*, in in 33 *Review of Financial Studies*, 2020, 2845; T. Philippon, *On fintech and financial inclusion*, in *NBER Working Paper* No. 26330, 2019, https://www.nber.org/papers/w26330.

[6] UK Competition, Markets Authority, *The Retail Banking Market Investigation Order 2017*, 2017 https://www.gov.uk/government/publications/retail-banking-market-investigation-order-2017.

[7] Commissione europea, *Impact Assessment Accompanying the Proposal for a Directive on Payment Service in the Internal Market*, SWD(2013)288 final, 137.

banche fossero restie a collaborare commercialmente con altri *provider* e potenziali concorrenti (*third-party payment service providers* – TPP), in assenza di un intervento normativo, l'accesso ai conti correnti dei clienti può avvenire solo tramite *screen scraping*[8]. Quest'ultimo costituisce una soluzione tecnologica di raccolta dei dati rischiosa talmente inefficiente e pericolosa per i consumatori da rappresentare un'ulteriore giustificazione per la regolamentazione dell'*Open Banking*. Infatti, lo *screen scraping* implica che i consumatori condividano le loro credenziali con i TPP e che questi ultimi accedano alle informazioni impersonificando i consumatori stessi, lasciandoli senza protezione riguardo ai dati raccolti e al modo in cui gli stessi vengono utilizzati e divulgati, aumentando così i rischi di inesattezze, frodi e violazioni dei dati. Queste preoccupazioni sono ulteriormente accentuate dal fatto che lo *screen scraping* consente di accedere a tutti i dati dei consumatori, anziché solo a quelli necessari per fornire servizi finanziari e di pagamento. Pertanto, le proposte di *Open Banking* mirano anche a garantire la protezione dei consumatori, fornendo un quadro sicuro di condivisione dei dati tramite la transizione dallo *screen scraping* alle interfacce per sviluppatori (API), di solito prive di credenziali gestite dai fornitori di dati o dai loro fornitori di servizi. Ciò aumenterebbe a sua volta la fiducia dei consumatori nella condivisione dei dati.

Tuttavia, oltre alle opportunità, l'innovazione finanziaria porta con sé anche preoccupazioni per la tutela dei consumatori. In particolare, la digitalizzazione delle transazioni finanziarie aumenta il rischio di discriminazione, manipolazione e sfruttamento dei clienti vulnerabili[9]. Il basso livello di alfabetizzazione digitale e finanziaria, insieme all'opacità delle decisioni guidate da algoritmi, può esporre i consumatori più fragili a processi decisionali complessi e a danni alla privacy e alla sicurezza.

In aggiunta, sebbene esista un consenso generale sul fatto che le interfacce per gli sviluppatori dovrebbero soppiantare lo *screen scraping*, significative divergenze emergono riguardo alla standardizzazione delle API,

---

[8] COMMISSIONE EUROPEA, *Report on the review of Directive 2015/2366/EU of the European Parliament and of the Council on payment services in the internal market*, COM(2023)365 final, 4.

[9] Si vedano, tra gli altri, OECD, *Access to finance for inclusive and social entrepreneurship. What role can fintech and financial literacy play?*, 2022, https://www.oecd-ilibrary.org/industry-and-services/policy-brief-on-access-to-finance-for-inclusive-and-social-entrepreneurship_77a15208-en; I. EREL, J. LIEBERSOHN, *Can fintech reduce disparities in access to finance? Evidence from the paycheck protection program*, in 146 *Journal of Financial Economics* 90, 2022; Y.W. TOK, D. HENG, *Fintech: Financial Inclusion or Exclusion?*, in *IMF Working Paper* No. 80, 2022, https://www.imf.org/en/Publications/WP/Issues/2022/05/06/Fintech-Financial-Inclusion-or-Exclusion-517619.

ovvero se il *policy maker* debbano imporre l'adozione di uno standard API comune o optare, invece, per un approccio guidato dal mercato che lasci gli operatori liberi di creare le proprie interfacce o di partecipare a iniziative di standardizzazione [10]. Da un lato, infatti, si segnala come uno standard API comune potrebbe compromettere la concorrenza dinamica tra standard e minare gli incentivi all'innovazione e alla fornitura di interfacce di alta qualità. Dall'altro, la frammentazione degli standard API potrebbe esacerbare i costi dell'interoperabilità e tradursi in maggiori barriere per i nuovi operatori entranti sul mercato [11]. Le conseguenze indesiderate derivanti dall'assenza di standardizzazione sono aggravate dagli interessi contrastanti dei partecipanti al mercato, in particolare dalla mancanza di incentivi per le banche a concedere l'accesso ai TPP.

Dubbi sono stati, inoltre, espressi sull'efficacia della condivisione dei dati nel promuovere la concorrenza, in quanto l'ingresso di nuovi operatori nel settore bancario e dei servizi finanziari genera crescenti preoccupazioni anche in termini di stabilità finanziaria e politica monetaria [12]. Infatti, se, da un lato, la regolamentazione dell'*Open Banking* è stata concepita essenzialmente per creare opportunità per le start-up FinTech, i cui servizi possono essere commercialmente danneggiati dalla mancanza di accesso ai dati delle transazioni dei clienti, dall'altro gli obblighi di condivisione dei dati imposti alle banche hanno avvantaggiato anche gli operatori non regolamentati finanziariamente. In particolare, gli obblighi di condivisione dei dati hanno favorito l'ingresso delle BigTech, che inizialmente sono entrate nel settore finanziario attraverso i servizi di pagamento, ma hanno rapidamente diversificato la loro offerta per includere prodotti di credito, assicurativi, di risparmio e di investimento.

Mentre non è ancora chiaro se le FinTech siano effettivamente in grado di competere con le banche tradizionali, anziché collaborare con esse for-

---

[10] D. DINÇKOL, P. OZCAN, M. ZACHARIADIS, *Regulatory standards and consequences for industry architecture: The case of UK Open Banking*, in 52 *Research Policy* 104760, 2023.

[11] OECD, *Shifting from Open Banking to Open Finance*, cit., p. 32.

[12] Si vedano G. CORNELLI, F. DE FIORE, L. GAMBACORTA, C. MANEA, *Fintech vs bank credit: How do they react to monetary policy?*, in 234 *Economics Letters* 111475, 2024; K. CROXSON, J. FROST, L. GAMBACORTA, T. VALLETTI, *Platform-Based Business Models and Financial Inclusion: Policy Trade-Offs and Approaches*, in 19 *Journal of Competition Law & Economics* 75, 2023; C. BORIO, S. CLAESSENS, N. TARASHEV, *Entity-based vs activity-based regulation: a framework and applications to traditional financial firms and big techs*, in *FSI Occasional Paper* No. 19, 2022, https://www.bis.org/fsi/fsipapers19.htm; J. EHRENTRAUD, J.L. EVANS, A. MONTEIL, F. RESTOY, *Big tech regulation: in search of a new framework*, in *FSI Occasional Paper* No. 20, 2022, https://www.bis.org/fsi/fsipapers20.htm; R. ZAMIL, A. LAWSON, *Gatekeeping the gatekeepers: when big techs and fintechs own banks – benefits, risks and policy options,* in *FSI Insights* No. 39, 2022, https://www.bis.org/fsi/publ/insights39.htm.

nendo servizi complementari [13], le BigTech rappresentano una minaccia competitiva concreta per le banche, in quanto possono scalare rapidamente i mercati finanziari sfruttando i silos di dati proprietari derivanti dalla fornitura di servizi non finanziari, nonché le competenze analitiche e le tecnologie avanzate per fornire ai consumatori offerte personalizzate [14]. A tal proposito, dal punto di vista della concorrenza, è stata messa in discussione anche la natura asimmetrica delle disposizioni sulla condivisione dei dati che, in contrasto con l'obiettivo di garantire condizioni informative uniformi, impongono alle banche l'obbligo di concedere l'accesso ai TPP senza includere un obbligo reciproco per questi ultimi che consentirebbe alle banche di migliorare i servizi digitali [15].

Ulteriori preoccupazioni sono associate al ruolo svolto dagli aggregatori di dati (noti anche come aggregatori di API o hub di API), emersi in risposta alla molteplicità di API bancarie disponibili sul mercato e che agiscono come intermediari tra le banche e i TPP integrando diverse API per fornire un unico punto di implementazione per i TPP. Da un punto di vista tecnico, gli aggregatori di dati apportano miglioramenti all'ecosistema in quanto la fornitura di un'API standardizzata consente ai TPP di connettersi senza problemi a diverse API senza dover affrontare problemi di configurazione e formattazione dei dati e delle interfacce. Tuttavia, l'emergere dei *data aggregators* porta con sé anche rischi in termini di dinamiche competitive del mercato [16]. In particolare, economie di scale e ampio acces-

---

[13] Si vedano O. KOWALEWSKI, P. PISANY, *The rise of fintech: A cross-country perspective*, in 122 *Technovation* 102642, 2023; E. LI, M.Q. MAO, H.F. ZHANG, H. ZHENG, *Banks' investments in fintech ventures*, in 149 *Journal of Banking & Finance* 106754, 2023; V. MURINDE, E. RIZOPOULOS, e M. ZACHARIADIS, *The impact of FinTech revolution on the future of banking: Opportunities and risks*, in 81 *International review of Financial Analysis* 102103, 2022; A. BOOT, P. HOFFMANN, L. LAEVEN, L. RATNOVSKI, *Fintech: what's old, what's new?*, in 53 *Journal of Financial Stability* 100836, 2021; L. ENRIQUES, W.-G. RINGE, *Bank-Fintech Partnerships, Outsourcing Arrangements and the Case for a Mentorship Regime*, in 15 *Capital Markets Law Journal* 374, 2020; A.V. THAKOR, *Fintech and banking: What do we know?*, in 41 *Journal of Financial Intermediation* 100833, 2020; A. ZERNIK, *The (Unfulfilled) Fintech Potential*, in 1 *Notre Dame Journal on Emerging Technology* 352, 2020; R.M. STULZ, *FinTech, BigTech, and the Future of Banks*, in 31 *Journal of Applied Corporate Finance* 86, 2019; X. VIVES, *Digital disruption in banking*, in 11 *Annual Review of Financial Economics* 243, 2019.

[14] Oscar BORGOGNO e Giuseppe COLANGELO, *The data sharing paradox: BigTechs in Finance*, in 16 *European Competition Journal* 492, 2020.

[15] M. DE LA MANO, J. PADILLA, *Big Tech Banking*, in 14 *Journal of Competition Law and Economics* 494, 503, 2018.

[16] OECD, *Open finance policy considerations*, 2023, pp. 30-31, https://doi.org/10.1787/19ef3608-en.

so ai dati finanziari dei consumatori potrebbero favorire l'affermazione di pochi operatori e, quindi, una concentrazione di mercato.

Soprattutto in un mercato altamente frammentato come quello statunitense, gli aggregatori di dati possono attrarre una massa critica di sviluppatori di software API beneficiando delle stesse economie di accumulo dei dati che possono favorire la concentrazione del settore e il radicamento della posizione dominante di alcune BigTech [17]. Inoltre, il servizio di connessione alle API fornito dagli aggregatori può essere visto come un fattore che contribuisce all'inefficienza, in quanto allunga la catena di transazioni e introduce costi dovuti al fatto che viene fornito dietro compenso.

3. L'esperienza europea: successi e limiti della PSD2

Da un punto di vista regolamentare, con l'introduzione sin dal 2015 di un diritto di accesso ai dati dei conti di pagamento, l'Unione europea ha rappresentato il principale punto di riferimento dell'*Open Banking* nello scenario internazionale. Pur basandosi sullo stesso quadro normativo, il Regno Unito ha adottato un modello tecnologico diverso per quanto riguarda la standardizzazione delle API che gestiscono la condivisione dei dati tra banche e TPP, distinguendosi per essere uno dei casi più avanzati di interoperabilità.

La PSD2 ha introdotto una regola di accesso ai conti correnti (cd. XS2A) che obbliga i prestatori di servizi di pagamento di radicamento del conto (*account servicing payment service providers* – ASPSPs) a condividere in tempo reale, su richiesta dell'utente, i dati del conto corrente di quest'ultimo con TPP, siano essi prestatori di servizi di disposizione di ordine di pagamento (*payment initiation services providers* – PISPs) o prestatori di servizi di informazione sui conti (*account information service providers* – AISP), nonché ad eseguire ordini di pagamento [18].

La PSD2 si basa sul principio dell'accesso senza la necessità di un rapporto contrattuale tra ASPSP e TPP, quindi senza remunerazione.

---

[17] Si vedano D. AWREY, J. MACEY, *The Promise & Perils of Open Finance*, in 40 *Yale Journal of Regulation* 1, 2023; J. ALCAZAR, F. HAYASHI, *Data Aggregators: The Connective Tissue for Open Banking*, (2022) FEDERAL RESERVE BANK OF KANSAS CITY, https://www.kansascityfed.org/research/payments-system-research-briefings/data-aggregators-the-connective-tissue-for-open-banking/.

[18] Per un'analisi si vedano O. BORGOGNO, G. COLANGELO, *Data, Innovation and Competition in Finance: The Case of the Access to Account Rule*, in 31 *European Business Law Review* 573, 2020.

Sebbene l'*Open Banking* fosse presente in Europa anche prima della PSD2, l'obiettivo della direttiva era quello di fornire un quadro normativo sicuro rispetto alla situazione precedente nella quale i TPP operavano in un ambiente largamente non regolamentato e accedevano ai conti dei clienti principalmente attraverso lo *screen scraping* [19].

Ai sensi della PSD2, l'accesso ai dati è facilitato attraverso API o concedendo ai TPP l'accesso diretto ai dati di pagamento utilizzando l'interfaccia che le banche utilizzano per le interazioni con i clienti (*customer-facing interface*). Al fine di salvaguardare la continuità operativa dei TPP, la PSD2 richiede agli ASPSP che optano per un'interfaccia dedicata (PSD2 API) di fornire anche un'interfaccia alternativa ai TPP (*fallback interface*) in caso di malfunzionamento o di problemi con l'interfaccia dedicata. Per non ostacolare l'innovazione e la concorrenza tra gli standard, la PSD2 e le relative norme tecniche di regolamentazione (RTS) hanno scelto di non imporre uno standard API unico e, dopo quasi dieci anni, non esiste ancora un unico standard API paneuropeo per l'*Open Banking*.

Il recente rapporto di valutazione sull'applicazione e l'impatto della PSD2 ha, da un lato, concluso che la direttiva è riuscita a ridurre le frodi grazie all'introduzione di un efficace sistema di autenticazione del cliente, dall'altro lato, non ha mancato di rivelare limiti nel nell'adozione dell'*Open Banking* [20]. In particolare, sono stati evidenziati problemi ricorrenti per quanto riguarda l'accesso dei TPP ai dati in possesso degli ASPSP che non hanno permesso di superare lo squilibrio tra fornitori di servizi bancari e non bancari [21]. Nello specifico, né gli ASPSP né i TPP sono pienamente soddisfatti della situazione attuale [22]. Questi ultimi si lamentano delle prestazioni delle interfacce di accesso ai dati, riferendo di avere difficoltà a fornire servizi di base a causa di API PSD2 inadeguate e di bassa qualità [23]. I TPP notano, inoltre, che, poiché gli RTS lasciano che gli standard delle API siano stabiliti dall'industria, la frammentazione delle API li pone nella posizione svantaggiosa di dover sostenere i costi di sviluppo di soluzioni differenziate per accedere alle API di diverse banche [24]. Dall'altro lato, gli ASPSP manifestano insoddisfazione per i significativi costi di implementazione per lo sviluppo di API e si rammaricano del fatto che la PSD2 impedisca loro di ad-

[19] COMMISSIONE EUROPEA, *Report on the review of Directive 2015/2366/EU*, cit., p. 4.

[20] *Ibid.*, p. 3.

[21] *Ibid.*, p. 4.

[22] COMMISSIONE EUROPEA, *Impact Assessment*, cit., p. 16.

[23] *Ibid.*, pp. 13-14.

[24] *Ibid.*, p. 120.

debitare ai TPP l'accesso ai dati dei clienti[25]. In altre parole, le banche percepiscono le API come un costo regolatorio e sostengono che l'accesso gratuito non le incentiva a offrire le migliori API possibili[26]. Inoltre, le banche sono insoddisfatte dello scarso utilizzo delle loro API, lamentando che gli aggregatori trasferiscono i dati degli utenti a terzi non regolamentati[27].

Nonostante queste constatazioni sul funzionamento imperfetto dell'*Open Banking*, la Commissione ritiene preferibile non introdurre cambiamenti radicali. Pertanto, per quanto riguarda le richieste dei TPP, pur riconoscendo i vantaggi che una soluzione diversa apporterebbe in termini di accesso ai dati, le modifiche proposte alla PSD2 non prevedono l'imposizione di un'interfaccia di accesso ai dati completamente standardizzata n, in quanto i costi dell'introduzione di un nuovo standard API unico supererebbero i benefici. In effetti, la Commissione osserva che, nonostante l'esistenza di diversi standard API in Europa, gli standard in vigore sono sostanzialmente convergenti nel tempo verso due soluzioni principali (ossia, lo standard del Gruppo di Berlino e lo standard STET)[28]. Inoltre, anche se non previsto dalla PSD2, l'emergere degli aggregatori è considerato positivamente per via della loro capacità di ridurre gli attriti derivanti dalla frammentazione degli standard API[29]. Partendo dalla premessa che lo *screen scraping* non debba essere consentito, la proposta suggerisce di semplificare il regime eliminando i due requisiti di interfaccia (cioè, un'interfaccia principale e un'interfaccia di riserva) e imponendo, come regola generale, l'uso obbligatorio di API progettate e dedicate a scopi di *Open Banking* per fornire accesso ai dati ai TPP[30]. In aggiunta, per garantire la continuità operativa dei TPP e la possibilità di fornire servizi di alta qualità ai loro clienti, la proposta concede ai TPP il diritto di beneficiare della *data parity* con l'interfaccia cliente fornita dagli ASPSP ai loro utenti[31].

Allo stesso modo, in risposta alle richieste delle banche di modificare la PSD2 per consentire un compenso per l'accesso ai dati, le modifiche proposte salvaguarderebbero il regime attuale (ossia i TPP che beneficiano dei servizi di base della PSD2 senza accordi contrattuali o addebiti), ma consentirebbero di prevedere un rapporto contrattuale accompagnato da una

[25] *Ibid.*, p. 15.

[26] *Ibid.*

[27] *Ibid.*

[28] COMMISSIONE EUROPEA, *Report on the review of Directive 2015/2366/EU*, cit., pp. 4-5.

[29] *Ibid.*

[30] *Ibid.*, Considerando 57.

[31] *Ibid.*, Considerando 59.

remunerazione per i servizi che vanno oltre quelli regolamentati dalla PSD2[32]. In particolare, questo sarebbe il caso delle *premium* API, che forniscono informazioni sulle transazioni da altri tipi di conti (ad esempio, conti di risparmio) e consentono di programmare pagamenti ricorrenti[33].

Infine, per accrescere la fiducia nei servizi *Open Banking* e consentire ai consumatori di avere il pieno controllo dei propri dati, la proposta prevede che gli ASPSP rendano disponibile un *dashboard* per il monitoraggio e la revoca o il ripristino dell'accesso ai dati concesso ai fornitori di servizi[34].

Come anticipato, la valutazione dell'esperienza europea della PSD2 diventa particolarmente interessata se confrontata con le diverse scelte di policy adottate dal Regno Unito nell'implementazione della direttiva. Infatti, basandosi sullo stesso quadro regolamentare fornito dalla PSD2, il Regno Unito ha optato per un'implementazione più invasiva della regola XS2A.

Mentre la PSD2 è neutrale dal punto di vista tecnologico, il Regno Unito ha promosso un modello standardizzato di *Open Banking*. In particolare, l'autorità britannica per la concorrenza (CMA) ha richiesto alle nove banche più grandi (CMA9) di concordare standard API comuni e aperti, formati di dati e protocolli di sicurezza che consentano ai TPP di connettersi ai conti bancari dei clienti secondo un unico insieme di specifiche. Inoltre, è stata creata una *Open Banking Implementation Entity*, finanziata dal CMA9, per supervisionare la diffusione degli standard API e supportare le parti nell'uso di tali standard.

Dopo sette anni dalla sua introduzione, il Regno Unito celebra il successo del suo modello, dichiarando una significativa adozione e un'accelerazione della crescita dell'*Open Banking*, dato che oggi oltre 7 milioni di consumatori e imprese (di cui 750.000 piccole e medie imprese) utilizzano prodotti e servizi abilitati all'*Open Banking*[35]. I dati mostrano che un riscontro fortemente positivo da parte dei clienti: se i consumatori dichiara-

---

[32] *Ibid*., Considerando 56.

[33] Si veda anche UK JOINT REGULATORY OVERSIGHT COMMITTEE, *Principles for commercial frameworks for premium APIs*, 2023, https://www.fca.org.uk/publication/corporate/jroc-principles-commercial-frameworks-premium-apis.pdf.

[34] COMMISSIONE EUROPEA, *Proposta di Regolamento relativo ai servizi di pagamento*, cit., Considerando 65.

[35] UK JOINT REGULATORY OVERSIGHT COMMITTEE, *Recommendations for the next phase of open banking in the UK*, 2023, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1150988/JROC_report_recommendations_and_actions_paper_April_2023.pdf; UK GOVERNMENT, *Joint statement by HM Treasury, the CMA, the FCA and the PSR on the future of Open Banking*, 2022, https://www.gov.uk/government/publications/joint-statement-by-hm-treasury-the-cma-the-fca-and-the-psr-on-the-future-of-open-banking.

no di avere un migliore controllo delle proprie finanze personali, la maggior parte dei TPP ritiene che l'implementazione standardizzata dell'API sia stata particolarmente efficace [36]. Per queste ragioni, il governo britannico ha annunciato il lancio dell'*Open Finance*, ovvero l'intenzione di estendere il proprio modello di *Open Banking* oltre i conti di pagamento a una gamma più ampia di servizi e prodotti finanziari.

3.1. L'avvento della *Open Finance*: la proposta FIDA

Oltre alle proposte di revisione della PSD2, la Commissione europea ha presentato anche una proposta legislativa che integra la norma XS2A con l'obbligo di fornire l'accesso ai dati finanziari (FIDA) [37].

La proposta FIDA si basa sulla stessa logica della PSD2, ovvero promuovere la concorrenza e l'innovazione in un ecosistema guidato dai dati, affidando ai clienti delle istituzioni finanziarie (cioè sia ai consumatori che alle imprese) un controllo effettivo sui loro dati finanziari per beneficiare di prodotti e servizi finanziari personalizzati [38]. La formulazione degli obiettivi della proposta ricorda chiaramente la PSD2. Di conseguenza, viene sottolineato come la mancanza di prodotti finanziari personalizzati ostacoli il potenziale di innovazione, in quanto limita la capacità di fornire una gamma più ampia di scelte e servizi finanziari ai consumatori che potrebbero altrimenti trarre vantaggio da strumenti basati sui dati che li aiutino a prendere decisioni informate, a confrontare facilmente le offerte e a selezionare prodotti più favorevoli in linea con le loro preferenze [39]. Analogamente, un'attenzione particolare è rivolta ai piccoli operatori, che sono i più penalizzati dalle barriere esistenti alla condivisione dei dati [40].

Inoltre, la proposta FIDA adotta lo stesso approccio della PSD2 (confermato dalla sua proposta di revisione) nei confronti della mancanza di reciprocità negli obblighi di accesso ai dati, che, come già detto, ha suscitato critiche in quanto apparentemente in contrasto con l'obiettivo dichiarato di riequilibrare il *playing field* informativo. Contro il rischio di favorire le BigTech rispetto agli operatori finanziari storici e ai nuovi operatori, la

[36] COMMISSIONE EUROPEA, *Impact Assessment*, cit., pp. 195-196.

[37] COMMISSIONE EUROPEA, *Proposta di Regolamento relativo a un quadro per l'accesso ai dati finanziari*, cit.

[38] *Ibid*., Considerando 2.

[39] *Ibid*., Considerando 6.

[40] *Ibid*.

Commissione osserva che il Digital Markets Act (DMA) garantirebbe la reciprocità in termini di accesso ai dati tra le imprese del settore finanziario e le grandi aziende tecnologiche [41]. Ai sensi della DMA, le piattaforme *gatekeeper* sono tenute a garantire l'accesso in tempo reale ai dati forniti o generati sulla piattaforma da utenti commerciali e consumatori nel contesto dei servizi di base della piattaforma. In ogni caso, per salvaguardare la stabilità finanziaria, l'integrità del mercato e la protezione dei consumatori, la proposta fissa regole di ammissibilità per l'accesso ai dati dei clienti, stabilendo che questi ultimi possono essere consultati solo da istituzioni finanziarie regolamentate o da imprese soggette ad un'autorizzazione specifica come fornitori di servizi di informazione finanziaria [42]. La disposizione mette in pratica il principio "stessa attività, stessi rischi, stesse regole", secondo il quale tutti i partecipanti ai mercati finanziari che svolgono la stessa attività e generano gli stessi rischi sono soggetti agli stessi standard in relazione alla protezione dei consumatori e alla resilienza operativa [43].

In poche parole, l'iniziativa FIDA intende estendere il quadro regolamentare Open Banking della PSD2 all'*Open Finance* poggiandosi sul medesimo approccio *customer-centric* ma, al tempo stesso, traendo insegnamento da alcune lezioni apprese sulla PSD2 alla luce dei riscontri raccolti nelle analisi che hanno supportato il suo progetto di revisione [44]. Pertanto, sebbene la proposta FIDA includa le stesse modifiche relative all'introduzione di *dashboard* di autorizzazione all'accesso ai dati per i clienti [45], si differenzia in modo significativo dalla proposta di revisione della PSD2 per quanto riguarda le soluzioni previste contro il rischio di veder emergere un quadro di API frammentato e di bassa qualità.

In particolare, la proposta FIDA riconosce esplicitamente che la messa a disposizione dei dati tramite API di alta qualità è essenziale per facilitare l'accesso continuo ed efficace ai dati e che, a tal fine, per salvaguardare gli incentivi all'investimento da parte dei detentori di dati, è opportuno consentire loro di chiedere un compenso ragionevole ai fruitori dei dati [46]. Tale

---

[41] COMMISSIONE EUROPEA, *Impact Assessment Report accompanying the Proposal for a Regulation on a framework for Financial Data Access*, SWD(2023) 224 final, 113.

[42] COMMISSIONE EUROPEA, *Proposta di Regolamento relativo a un quadro per l'accesso ai dati finanziari*, cit., Considerando 31.

[43] EXPERT GROUP ON EUROPEAN FINANCIAL DATA SPACE, *Report on Open Finance*, 2022, p. 35, https://finance.ec.europa.eu/publications/report-open-finance_en.

[44] COMMISSIONE EUROPEA, *Proposta di Regolamento relativo a un quadro per l'accesso ai dati finanziari*, cit., Considerando 49.

[45] *Ibid*., Considerando 21.

[46] *Ibid*., Considerando 7 e 29.

soluzione sarebbe in linea con il principio recentemente introdotto nel *Data Act* e basato su un modello contrattuale di condivisione dei dati. Di conseguenza, secondo la proposta FIDA, il titolare dei dati può chiedere un risarcimento solo se i dati del cliente vengono messi a disposizione di un fruitore secondo le regole e le modalità di un sistema di condivisione dei dati finanziari [47].

In aggiunta, dal momento che la consultazione svolta ha indicato con forza la mancanza di standardizzazione come uno dei principali ostacoli alla condivisione dei dati nel settore finanziario [48], la proposta FIDA prevede l'obbligo per i partecipanti al mercato di sviluppare congiuntamente standard comuni per i dati e le interfacce dei clienti come parte dei suddetti schemi di condivisione dei dati finanziari [49]. L'opzione di conferire alle autorità di vigilanza europee il potere di sviluppare un unico standard europeo per l'intero settore finanziario è stata, invece, scartata a causa dei suoi svantaggi, della sua complessità e dei suoi costi complessivi. In particolare, si ritiene improbabile che un unico standard possa soddisfare le diverse esigenze degli utenti dei dati nei vari settori dell'industria finanziaria e potrebbe essere difficile per le autorità pubbliche tenere il passo degli sviluppi tecnologici aggiornando gli standard in modo tempestivo [50].

La spiegazione fornita per questa discrepanza tra la regolazione dell'*Open Banking* e quella dell'*Open Finance* in Europa riguarda essenzialmente una sorta di *path dependence*. Dal momento che l'*Open Finance* è un mercato emergente che verrebbe regolamentato per la prima volta, non avendo quindi un'eredità in termini scelte compiute relativamente al regime di remunerazione e di investimenti in API già effettuati, non vi è un rischio di *disruption* [51].

---

[47] *Ibid*., artt. 5, 9-11.

[48] COMMISSIONE EUROPEA, *Impact Assessment Report accompanying the Proposal for a Regulation on a framework for Financial Data Access*, cit., p. 19.

[49] COMMISSIONE EUROPEA, *Proposta di Regolamento relativo a un quadro per l'accesso ai dati finanziari*, cit., artt. 9 e 10, Considerando 25.

[50] COMMISSIONE EUROPEA, *Impact Assessment Report accompanying the Proposal for a Regulation on a framework for Financial Data Access*, cit., p. 55.

[51] COMMISSIONE EUROPEA, *Proposta di Regolamento relativo ai servizi di pagamento*, cit., Considerando 55.

4. Conclusioni

L'analisi svolta ha messo in luce opportunità e rischi dell'*Open Banking*, nonché ragioni e sfide di un intervento regolatorio finalizzato ad imporre dall'alto un regime di accesso ai dati.

In tal senso, successi e limiti dell'esperienza europea della PSD2 e il confronto con il diverso modello di implementazione della stessa adottato nel Regno Unito forniscono importanti spunti di riflessione, anche in vista dell'adozione di un regime regolatorio di accesso ai dati esteso a quelli finanziari. In particolare, l'analisi dell'esperienza europea dell'*Open Banking* conferma che progettare un quadro normativo adatto allo scopo implica delicate scelte di policy con riferimento agli standard comuni per i dati e le interfacce tecniche, alle soluzioni che consentono ai clienti di gestire le autorizzazioni per i dati, alle regole di ammissibilità e ai requisiti per i terzi che desiderano accedere ai dati, al ruolo degli aggregatori.

Le motivazioni, gli obiettivi e le sfide dell'*Open Banking* suggeriscono, dunque, che "*one size does not fit all*". Per queste ragioni, nel valutare interventi tesi a facilitare la condivisione dei dati nel settore bancario e finanziario, i *policy maker* dovrebbero adottare un approccio su misura, tenendo conto delle peculiarità del mercato geografico di riferimento e dei risultati maturati in altre esperienze, al fine di valutare attentamente vantaggi e svantaggi dei regimi *market-led* e di quelli *regulatory-led*.

Pasquale Stanzione

Open Banking, Open Finance e protezione dei dati personali

SOMMARIO: 1. Il contesto. – 2. Il paradigma dell'*Open Banking* e dell'*Open Finance*. – 3. Le sfide per la protezione dei dati.

1. Il contesto

Il settore bancario rappresenta, non da ora, un laboratorio assolutamente innovativo per la protezione dati. In tale contesto sono maturate, ad esempio, decisioni importanti sul bilanciamento tra controllo degli accessi e privacy, delineando limiti e condizioni per il ricorso alla biometria o alla videosorveglianza. Proprio in relazione al settore bancario sono stati affermati alcuni dei principi essenziali sulla responsabilità per omesso impedimento di frodi informatiche, così come criteri regolativi importanti rispetto ai trattamenti dei dati nei gruppi societari.

Dei principi affermati in tale contesto dovrà farsi tesoro anche oggi, a fronte di un'evoluzione tecnologica "disruptive" che incide su di un settore cruciale dal punto di vista economico, sociale, persino politico.

Da un lato, infatti, le nuove tecnologie hanno reso il ricorso alla profilazione del cliente sempre più ampio e invasivo, con implicazioni importanti sull'identità personale. Dall'altro lato, la convergenza tra fintech e disintermediazione bancaria e finanziaria ha reso assai più articolata e complessa la filiera lungo cui si snoda il trattamento dei dati personali dei clienti.

La normativa europea recente ha, infatti, promosso un processo di pluralizzazione soggettiva del settore, legittimando l'emersione di nuovi organismi finanziari e figure intermediatrici aliene al tradizionale ambito bancario e che, se non sostituiscono tout court gli istituti di credito, comunque si affiancano loro rendendo più articolata la fisionomia del comparto: si pensi alla concessione di credito da parte delle imprese di assicurazione, ad

alcune particolari tipologie di fondi di investimento come pure ai moduli alternativi di gestione collettiva del risparmio.

Le innovazioni maggiori si sono registrate nel settore dei servizi di pagamento, in cui l'esclusività del rapporto banca-cliente è stata scardinata non solo dall'emersione di soggetti quali gli istituti eroganti moneta elettronica e gli istituti di pagamento, ma soprattutto dalla "rivoluzione" della direttiva PSD2 (2015/2366/UE), in cui le innovazioni del Fintech sono state più profonde per l'assenza di riserve di attività.

Tale disciplina, dal chiaro intento di liberalizzazione e promozione della concorrenza, ha imposto condivisione dei dati bancari del cliente (consenziente) tra i diversi attori dell'ecosistema bancario erodendo, in favore di una nebulosa di "terze parti", il tradizionale monopolio della banca sulla posizione soggettiva individuale. I conti correnti vengono, dunque, per la prima volta aperti anche a soggetti non bancari, al di fuori del quadro di obblighi cui questi ultimi soggiacciono, con le relative garanzie per i clienti.

2. Il paradigma dell'*Open Banking* e dell'*Open Finance*

Questo processo di progressiva pluralizzazione soggettiva dei rapporti finanziari comporta, sotto il profilo della protezione dati, un grado di complessità nell'articolazione della filiera del trattamento che esige garanzie supplementari per impedire che l'*Open Banking* degeneri in una licenza di abuso o in un'occasione di agevolazione delle frodi informatiche. La protezione dati è, in questo senso, un fattore di promozione della sicurezza informatica e di garanzia della corretta gestione delle informazioni bancarie e dei servizi di pagamento, in un contesto in cui la legittima apertura dei rapporti di credito non deve degenerare in permeabilità dei flussi informativi, con tutti i rischi (di frodi, *cyber attacks*, manovre speculative) che inevitabilmente ne conseguono.

E in tale contesto di destrutturazione del panorama soggettivo tradizionale del settore, la variabile tecnologica – che modifica profondamente relazioni e dinamiche di mercato – impone ulteriori cautele per la complessiva sostenibilità del sistema. Il digitale sviluppa, infatti, servizi nuovi e in forme nuove, mettendo in discussione l'ambito delle riserve di attività oggi esistenti: si pensi alla gestione automatizzata dei conti o alle cripto-valute gestite su registri *blockchain*, oggi definiti addirittura normativamente.

La tradizionale catena del valore si disarticola, così, con l'emersione di operatori che gestiscono (solo) specifici segmenti della filiera disintermediandola: si pensi alle piattaforme di *peer to peer (P2P) lending* e di *crowd-*

funding quali canali di raccolta del capitale alternativi a quello bancario o anche ai nuovi servizi di pagamento digitali.

Ma gli effetti che ne derivano non si limitano alla (pur rilevantissima) sfera privata, investendo aspetti di sistema e ridelineando l'allocazione del potere, con il rischio dell'emersione di nuovi oligopoli, più potenti di quelli tradizionali e, assai più di questi, votati all'espansione in settori diversi, politicamente sensibili.

Il paradigma dell'*Open Banking* favorisce, infatti, l'emersione di nuovi modelli di mercati a due versanti, basati su piattaforme bancarie *on line* che agiscono come intermediari tra i titolari di conti e le imprese FinTech, generando potenziale valore per entrambe le parti pur al netto di una mutazione genetica dell'attività bancaria e di un effetto paradossale, forse preterintenzionale.

La direttiva PSD2, volta a promuovere la concorrenza nei servizi di pagamento, ha mutato profondamente le dinamiche competitive e la stessa articolazione del potere nel contesto dell'economia delle piattaforme.

Ma se le innovazioni della direttiva PSD2 sono state dirimenti, non meno significative sono quelle connesse all'annunciato pacchetto sulla finanza digitale. Esso, con le proposte di regolamento *Open Finance* o – *Financial Data Access Framework* – (FIDA), di regolamento relativo ai servizi di pagamento nel mercato interno (PSR) e di direttiva PSD3 che modifica la PSD2, intende fornire una regolamentazione organica delle implicazioni che la digitalizzazione ha sul settore finanziario, con un impatto trasformativo che investe ogni ambito.

Si tratta di proposte con le quali prende corpo la Strategia europea per la finanza digitale, nella direzione anzitutto dell'estensione del paradigma dell'*Open Banking* a tutto il settore finanziario. In questo senso, il pacchetto sulla finanza digitale sviluppa, rilancia e valorizza l'idea di fondo sottesa alla direttiva PSD2 (e già essa innovativa), di "apertura" del sistema (finanziario in senso lato) a soggetti nuovi e plurali, pur mantenendo la centralità del cliente e dei suoi dati. È, anzi, proprio il valore del dato il profilo maggiormente innovativo della Strategia europea per la finanza digitale che, in questo, sembra rappresentare una declinazione, nuova e ulteriore, della Strategia europea dei dati.

Tutte e tre le proposte normative, presentate dalla Commissione a giugno 2023 e dunque soggette all'esame parlamentare proprio a cavallo delle due legislature, mirano infatti a valorizzare i dati del cliente promuovendone la condivisione e il riutilizzo per la personalizzazione di prodotti e servizi finanziari per i consumatori e per le piccole e medie imprese, in un contesto che parrebbe delineare l'idea di un'economia ricolare dei dati.

3. Le sfide per la protezione dei dati

Molte delle soluzioni normative proposte ricordano (e traspongono, sul piano finanziario) istituti e paradigmi propri del *Data Governance Act* e del *Data Act* ma, soprattutto, ne condividono lo spirito di fondo: accrescere il valore del dato promuovendone l'accesso, il riutilizzo a fini anche di interesse generale, in questo caso riferito al buon funzionamento del mercato interno dei servizi di pagamento. Naturalmente, ancora una volta il confine tra valorizzazione del dato e sua mera *commodification* è sottile ma va rimarcato, come del resto ha fatto il Garante europeo per la protezione dati, con due pareri resi sulla proposta di regolamento sull'accesso ai dati finanziari e uno sulla proposta di regolamento e direttiva sui servizi di pagamento nel mercato interno dell'UE[1].

Pur apprezzando l'intento di normare gli effetti che le tecnologie emergenti spiegano sul settore finanziario, il Garante europeo ha infatti sottolineato l'esigenza di introdurre nelle proposte alcune garanzie ulteriori per gli interessati (*data subjects*, appunto).

In primo luogo, si è rappresentata l'esigenza di assicurare maggiore trasparenza in ordine alle richieste di accesso da parte dei terzi ai dati personali, chiarendo comunque che l'autorizzazione prestata dall'interessato esprime un atto dispositivo diverso dal consenso al trattamento dei dati e che dunque l'accesso esige un autonomo presupposto di liceità.

Dietro questa notazione apparentemente nominalistica vi è l'esigenza di impedire che le prassi circolatorie instaurate nell'economia delle piattaforme snaturino a tal punto il consenso al trattamento da eluderne (con effetti potenzialmente e pericolosamente estensivi ad altri ambiti) le caratteristiche essenziali. Tra le quali vi è, come noto, la revocabilità *ad nutum* e la reale opzionalità e non condizionalità, suscettibili di elusione ogniqualvolta l'atto dispositivo sia in qualche modo e sia pur indirettamente inserito in un sinallagma contrattuale.

Per promuovere un uso responsabile e non discriminatorio dei dati, il Garante europeo sottolinea inoltre l'esigenza di escludere la profilazione dalle pratiche suscettibili di svolgimento nel contesto dell'*Open Finance*. Si tratta di un punto importante, in quanto la combinazione tra opacità algoritmica e asimmetria informativa che spesso caratterizzano questi ambiti potrebbe avere effetti potenzialmente critici sulla libertà e l'identità del soggetto.

---

[1] Pareri nn. 38 e 39/2023.

L'esperienza della *product governance* è, in questo senso, significativa: il principio del miglior interesse del cliente (*suitability rule*) ha favorito infatti un'ampia profilazione del cliente finalizzata alla prestazione dei servizi di investimento. Tale disciplina promuove, infatti, la targettizzazione dei «prodotti» offerti alla clientela sulla base della specifica classe di propensione al rischio in cui l'algoritmo abbia collocato il soggetto. In questo caso la "clusterizzazione" della clientela è funzionale all'offerta, a ciascun cliente, di prodotti finanziari conformi alla sua condizione patrimoniale e alla propensione al rischio che gli sia attribuita. Una profilazione funzionale ad un tempo al singolo e alla stessa sostenibilità del sistema finanziario nel suo complesso, dunque, ma dall'indubbia rilevanza in ragione dell'invasività del monitoraggio cui il singolo e le sue scelte individuali sono sottoposti. Se, dunque, tanto nel settore bancario quanto in quello finanziario in senso lato, la tendenza alla profilazione, allo scoring del cliente è diffusa, bene ha fatto il Garante europeo a sottolinearne, sia pur indirettamente, il rischio che essa degeneri in una forma di controllo massivo e, finanche, predittivo, dalle potenzialità discriminatorie troppo spesso sottovalutate.

Condivisibile è anche l'invito ad approfondire, con apposite linee guida, i limiti di ammissibilità della combinazione delle informazioni finanziarie individuali con altri dati personali, come quelli ottenuti da fonti terze, quali i social media, già vietata per determinati servizi finanziari, così da impedire tanto un'eccessiva concentrazione di potere informativo, quanto un ulteriore e diverso rischio di profilazione per il soggetto.

Sotto questo profilo la disciplina di protezione dati – attraverso la rigorosa regolamentazione della filiera economica, i limiti all'utilizzo secondario dei dati, gli obblighi di trasparenza volti a colmare l'asimmetria informativa – offre sicuramente strumenti importanti per il governo di un settore sempre più disarticolato quale quello dell'*Open Finance*.

In questo senso, la protezione dati si dimostra anche valida alleata tanto della disciplina consumeristica quanto di quella concorrenziale in senso proprio, ostacolando le condizioni per la concentrazione del potere, anzitutto (ma, appunto, non solo) informativo.

Al fondo vi è, però, una grande questione democratica e politica (nel senso più alto del termine), che involge anzitutto la capacità degli Stati di regolamentare, necessariamente su base non più soltanto nazionale, le sempre più incisive innovazioni indotte dalle nuove tecnologie e le relative implicazioni sulla dinamica e l'articolazione del potere e sulle corrispettive garanzie democratiche. *Hic Rhodus, hic salta*.

Rita Camporeale [*]

Le asimmetrie della PSD2 e il nuovo *Payments Package*

SOMMARIO: 1. Introduzione. – 2. Il nuovo *Payments Package*. – 3. Asimmetrie e PSD3/PSR. – 3.1. Asimmetrie e altre normative. – 3.2. Asimmetrie e concorrenza. – 3.3. Asimmetrie e sicurezza. – 3.4. Asimmetria e inclusione. – 4. Conclusioni.

1. Introduzione

Nel gennaio 2018 entrò in vigore la Seconda Direttiva sui Servizi di Pagamento (direttiva UE 2015/2366, c.d. PSD2) fornendo un rinnovato quadro di riferimento normativo per i pagamenti in Europa, in valuta euro e non, sia domestici sia transfrontalieri.

La PSD2 sostituì integralmente la prima Direttiva sui Servizi di Pagamento del 2007 (direttiva 2007/64/EC, c.d. PSD1), primo quadro normativo per i pagamenti nel Mercato unico, ponendosi molteplici obiettivi tra i quali: favorire l'innovazione e la digitalizzazione dei pagamenti, aumentare la concorrenza tra operatori e tra prodotti/canali di pagamento, garantire un miglior livello di protezione e sicurezza dei consumatori, oltre che accrescere il grado di armonizzazione all'interno del Mercato unico.

La PSD2 fu concepita dal Legislatore europeo in risposta a nuovi fenomeni e nuovi attori apparsi nel mondo dei pagamenti e si è rivelata nel tempo anche motore di un ulteriore sviluppo di questo mondo, che negli ultimi anni, ad un ritmo più sostenuto che nei precedenti, è stato attraversato da profondi cambiamenti.

È quindi possibile annoverare la PSD2 tra quei fattori che sono stati sia

[*] Sinceri ringraziamenti vanno a Cinzia Sippelli, Cinzia Di Bartolo e Rebecca Vanelli per il contributo di idee e l'assistenza alla redazione. Le opinioni espresse non impegnano l'istituzione di appartenenza.

causa sia effetto dell'evoluzione del mercato dei pagamenti, così come, ad esempio, la crescente digitalizzazione, il cambiamento nelle abitudini del consumatore, la diversificazione dei metodi di pagamento e l'emergere di nuovi attori di mercato.

Proprio in considerazione della continua evoluzione del mercato e per stare al passo con i suoi cambiamenti, nell'ambito della Strategia per i pagamenti al dettaglio (cd. "*Retail Payments Strategy – RPS*") e della Strategia per la finanza digitale del 2020 [1], la Commissione europea aveva preannunciato una revisione della PSD2. Questo con l'impegno di garantire l'adeguatezza e l'aggiornamento delle norme applicabili al settore dei pagamenti, tenendo in dovuta considerazione le evoluzioni del mercato e promuovendo al tempo stesso lo sviluppo dei pagamenti istantanei in Europa.

La Commissione riconoscendo "*l'ampiezza e la complessità della transizione imposta dalla PSD2*" [2] ha effettuato un'ampia ricognizione degli effetti sul mercato della PSD2 [3] prima di procedere ad avanzare una proposta di revisione, pubblicata il 28 giugno 2023.

La proposta di revisione PSD2 si sostanzia in due atti legislativi distinti: un regolamento (*Payment Services Regulation* – PSR) contenente norme direttamente applicabili per i prestatori di servizi di pagamento (*Payment Service Providers* – PSPs) e una direttiva (PSD3) contenente le norme relative alle licenze e alla vigilanza degli istituti di pagamento (IP) e degli istituti di moneta elettronica (IMEL), integrando la disciplina prevista dalla Direttiva sulla moneta elettronica (*E-money Directive* – EMD) [4]. Tale pro-

---

[1] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni relativa a una strategia in materia di pagamenti al dettaglio per l'UE, COM/2020/592 final e Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni relativa a una strategia in materia di finanza digitale per l'UE, COM/2020/591 final, entrambe contenute nel *Digital Finance Package*, pubblicato dalla Commissione europea il 24 settembre 2020.

[2] *RPS*, p. 17.

[3] EUROPEAN COMMISSION, DIRECTORATE-GENERAL FOR FINANCIAL STABILITY, FINANCIAL SERVICES, CAPITAL MARKETS UNION, I. BOSCH CHEN, D. FINA, P. HAUSEMER *et al.*, *A study on the application and impact of Directive (EU) 2015/2366 on Payment Services (PSD2)*, Publications Office of the European Union, 2023.

[4] Proposal for a Regulation of the European Parliament and of the Council on payment services in the internal market and amending regulation (EU) no 1093/2010, COM(2023) 367 final; Proposal for a Directive of the European parliament and of the Council on payment services and electronic money services in the internal market amending directive 98/26/EC and repealing directives 2015/2366/EU and 2009/110/EC, COM(2023) 366 final.

posta di suddivisione delle norme in un regolamento e in una direttiva ha il merito di veicolare tutti i diritti e gli obblighi in capo agli operatori che prendono parte alla catena del pagamento tramite uno strumento ad armonizzazione massima quale è appunto il Regolamento.

La direttiva regola le modalità di autorizzazione e licenza degli istituti di pagamento e moneta elettronica, e contiene disposizioni riguardanti i servizi di prelievo di contante forniti da dettaglianti (senza un acquisto) o da gestori di ATM indipendenti; il regolamento, focalizza le previsioni sul perimetro dei servizi di pagamento, gli obblighi di trasparenza e utilizzo dei servizi, incluse le norme di accesso ai conti e di applicazione della Autenticazione Forte del Cliente (*Strong Customer Authentication* – SCA).

Nell'insieme, il "pacchetto" si focalizza sul contrasto alle frodi, sul miglioramento dei diritti dei consumatori e del funzionamento dell'*Open Banking*, ponendo attenzione alle condizioni di concorrenza per garantire un piano di gioco livellato tra banche e soggetti non bancari e rafforzare l'armonizzazione e l'applicazione delle norme.

Questo "pacchetto" pare voler affrontare alcune asimmetrie introdotte o non rimosse dalla PSD2 – elementi che a nostro giudizio, ne hanno limitato l'incisività ed efficacia nella regolazione del mercato – ma non tutte appaiono risolte compiutamente.

Tra queste asimmetrie annoveriamo, per il particolare rilievo, quelle relative al rapporto con altre normative, alla gratuità dell'accesso ai conti di pagamento, alla sicurezza delle transazioni soprattutto in relazione ai nuovi tipi di frodi.

2. Il nuovo *Payments Package*

Per poter valutare in che modo il nuovo *Payments Package* intende affrontare i profili irrisolti della PSD2, ciò che in questo contributo definiamo "asimmetrie", è innanzitutto necessaria una premessa circa quello che solitamente è il contesto di elaborazione di una norma europea.

In passato, come oggi, nel momento in cui nel mercato si sono affermati nuovi fenomeni o attori che hanno determinato un cambiamento sostanziale nel settore, è emersa nel Regolatore l'esigenza di normare questi cambiamenti, al fine di tutelare l'equilibrio di mercato e la sicurezza dei consumatori. A tal proposito, si può considerare come esempio proprio la PSD2, che ha avuto tra l'altro l'obiettivo di regolamentare i prestatori di servizi informativi e dispostivi (*Account Information Service Provider* –

AISP e *Payment Initiation Service Provider* – PISP) e aprire la strada all'*Open Banking*. Un secondo esempio è MiCAR[5] (*Markets in Crypto-Assets Regulation*), che norma l'emissione, la diffusione e l'uso di cripto-attività. Nella stessa logica si pongono i lavori di revisione della PSD2, mirati tra l'altro a contrastare nuovi fenomeni nell'ambito delle frodi, o coinvolgere attori della catena di pagamento precedentemente esclusi.

Si comprende che le norme sono elaborate come risposta a un bisogno già esistente, con lo scopo di tutelare i consumatori e regolare il corretto comportamento degli attori di mercato, sostenendo il buon funzionamento di quest'ultimo. Al tempo stesso, tuttavia, è importante sottolineare che esse, nel regolamentare un fenomeno esistente, influenzano l'evoluzione del mercato e i suoi partecipanti, a volte anche in modi "imprevedibili". In altre parole, sebbene il Regolatore abbia in mente degli obiettivi delle norme che va ad introdurre, nel momento in cui esse vengono implementate, possono emergere dei fattori esterni che non potevano essere previsti a priori e che possono avere impatti divergenti rispetto al progetto originario.

Insomma, una sorta di "principio di indeterminazione di Heisenberg"[6]: come la misura della posizione influisce sulla velocità dell'elettrone, così la norma ha un impatto sull'evoluzione del mercato e non siamo in grado di capire se, in sua assenza, l'assetto del mercato sarebbe stato migliore o meno.

Ci troviamo oggi di fronte a un assetto di regole e di mercato certamente diversi se confrontati al momento in cui è stata introdotta la PSD2, e su cui le norme hanno influito fortemente; tuttavia, siamo anche in una fase di transizione ancora incompleta rispetto al disegno originario del Legislatore europeo.

In questo contesto, la nuova proposta di PSD3/PSR risulta peculiare perché, da un lato, essa si pone in un'ottica continuativa e migliorativa rispetto alla PSD2, senza l'intenzione di rivoluzionare quanto è stato fatto in precedenza e, dall'altro, in un'ottica innovativa. In ottica continuativa, si può leggere la fusione della PSD2 con la Seconda Direttiva sulla moneta elettronica[7]

---

[5] Regolamento (UE) 2023/1114 del Parlamento europeo e del Consiglio, del 31 maggio 2023, relativo ai mercati delle cripto-attività e che modifica i regolamenti (UE) n. 1093/2010 e (UE) n. 1095/2010 e le direttive 2013/36/UE e (UE) 2019/1937.

[6] In parole semplici (che spero i fisici perdoneranno), secondo il principio di Heisenberg qualsiasi misura della posizione di un elettrone influisce sulla sua velocità ed è impossibile misurarle in uno stesso istante.

[7] 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.

(*E-money Directive* – EMD2), con l'obiettivo di semplificazione e miglioramento dell'impianto normativo esistente, a beneficio dei fornitori di servizi di pagamento. Questi, infatti, potranno così contare su un regime facilitato nell'applicazione degli obblighi di conformità, con evidenti vantaggi anche per l'utente, che potrà disporre di un'informazione più trasparente, semplice e comprensibile.

Dall'altro, in ottica innovativa all'interno della proposta di Regolamento si ha, ad esempio, il nuovo impianto del trattamento di nuove tipologie di frode che minano la sicurezza dei consumatori e dei PSP e la possibilità di scambio informativo a fini di prevenzione frodi.

C'è da chiedersi se il *mix* di continuità ed innovazione e la scelta (già collaudata in altri ambiti normativi a livello europeo) del duplice mezzo – direttiva e regolamento – siano atti a rimuovere le asimmetrie che ancora si ravvisano, punti di attenzione che dovrebbero essere chiariti, al fine di evitare incertezze normative e svantaggi competitivi, i quali potrebbero influire negativamente sul mercato.

3. Asimmetrie e PSD3/PSR

Si esaminano brevemente a seguire le **asimmetrie** cui si è fatto cenno in introduzione. Queste asimmetrie sono riscontrabili in più ambiti come, ad esempio, nell'allineamento con altre normative europee, nella sicurezza, nella competitività, e nell'inclusione digitale del consumatore.

3.1. Asimmetrie e altre normative

Una delle questioni irrisolte della PSD2 è senza dubbio la relazione tra questa e altre normative, con cui, nella fase di elaborazione essa non è stata armonizzata, in primo luogo ad esempio, vediamo la GDPR[8] per il concetto di "*consent*" e "*permission*", la MiCAR[9] per l'utilizzo dei *token* di mone-

[8] 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).

[9] Regolamento (UE) 2023/1114 del Parlamento europeo e del Consiglio, del 31 maggio 2023, relativo ai mercati delle cripto-attività e che modifica i regolamenti (UE) n. 1093/2010 e (UE) n. 1095/2010 e le direttive 2013/36/UE e (UE) 2019/1937.

ta elettronica come mezzi di pagamento, l'e-iID [10]/eIDAS [11], per l'accesso ai conti di pagamento e l'autenticazione, o con FiDA [12] e *Data Act* [13] in relazione al concetto di remunerazione per l'accesso ai dati. Il "pacchetto", da un lato, comporterà l'emanazione di normative di secondo livello (ad esempio, *Regulatory Technical Standards*, *Guidelines*) ed esso collegate, dall'altro, si andrà ad inserire in un panorama normativo articolato. Questi due elementi potrebbero perpetuare profonde asimmetrie derivanti da incertezze interpretative e sovrapposizioni.

Prima di tutto, è necessario prendere in attenta considerazione il ruolo e anche la numerosità delle normative di secondo livello collegate a PSD3/PSR. Guardando al passato, si osserva come la PSD2 sia stata "integrata" con numerose norme di secondo livello le quali, pur con lo scopo di precisare, dettagliare meglio e colmare alcune lacune, hanno creato invece incertezze normative e una complessa implementazione durata anni. Seppur riconosciuta l'utilità di tali strumenti, è necessario evitare la proliferazione di questo tipo di norme su più livelli emanate in momenti successivi che potrebbero minare i benefici prospettati dal nuovo "pacchetto" PSD3/PSR e condurre alla frammentarietà del mercato.

In secondo luogo, sussiste il rischio che emergano asimmetrie nel rapporto tra PSD3/PSR e le altre norme del contesto europeo, costituito dalle disposizioni esistenti o in via di emanazione, come, ad esempio, il regolamento relativo ai mercati delle cripto-attività MiCAR, il regolamento FiDA, il regolamento sull'Euro Digitale, la direttiva sull'identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno (*Directive on electronic identification and trust services for electronic transactions in the internal market* – e-IDAS/EUID), la direttiva sui Requisiti di Accessibilità dei prodotti e dei servizi (*European Accessibility Act* –

[10] Regolamento (UE) n. 910/2014 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.

[11] Proposta di regolamento del Parlamento europeo e del Consiglio che modifica il regolamento (UE) n. 910/2014 per quanto riguarda l'istituzione di un quadro per un'identità digitale europea, COM/2021/281 final.

[12] Proposta di regolamento del Parlamento europeo e del Consiglio relativo a un quadro per l'accesso ai dati finanziari e che modifica i regolamenti (UE) n. 1093/2010, (UE) n. 1094/2010, (UE) n. 1095/2010 e (UE) 2022/2554, COM(2023) 360 final.

[13] Regolamento (UE) 2023/2854 del Parlamento europeo e del Consiglio, del 13 dicembre 2023, riguardante norme armonizzate sull'accesso equo ai dati e che modifica il regolamento (UE) 2017/2394 e la direttiva (UE) 2020/1828 (regolamento sui dati).

EAA [14]), il regolamento per i bonifici istantanei in euro (*Instant Payment Regulation* – IPR [15]), il *Data Act*.

È necessario che venga garantita l'armonia e il coordinamento tra le varie norme, le quali, pur trattando temi diversi, sono tutte strettamente collegate e hanno il compito di disegnare un ecosistema interconnesso in modo logico e coerente, che non permetta l'emergere di possibili contraddizioni, incomprensioni o lacune. In particolare, un'attenzione di riguardo dovrebbe essere posta nel garantire un armonico allineamento tra PSD3/PSR e FiDA e *Data Act* per quanto riguarda la possibilità di remunerazione per i servizi offerti e l'accesso ai dati.

In relazione alla GDPR, la PSR presenta due principali asimmetrie. La prima riguarda la terminologia adottata in merito alla distinzione tra "*consent*", "*explicit consent*" e "*permission*". I primi due termini sono utilizzati ripetutamente nella GDPR e di "*consent*" viene data anche una chiara definizione. Anche in PSD2 è utilizzato il termine "*consent*". Nella PSR invece viene introdotto il nuovo termine "*permission*" senza tuttavia fornire una chiara definizione nell'art. 3. Questa mancanza potrebbe determinare poca chiarezza nell'interpretazione del testo legislativo e una sua erronea applicazione. Un tentativo per sopperire a questa lacuna sembra essere presente nel considerando (69), il quale riporta: "*When reference is made to 'permission' that reference should be without prejudice to obligations of payment service providers under Article 6 of Regulation (EU) 2016/679. Therefore, permission should not be construed* ***exclusively*** *as 'consent' or 'explicit consent' as defined in Regulation (EU) 2016/679*". Tuttavia, sebbene sia apprezzabile l'inserimento del passaggio, questo non è esaustivo e il termine "*exclusively*" lascia ancora adito a possibili fraintendimenti tra i tre termini.

Un secondo punto di interesse è il generale allineamento che deve essere garantito tra quanto previsto nella GDPR, in merito alla tutela dei dati e della *privacy* del cliente, con le disposizioni della PSR, anche in riferimento all'art. 80 circa la protezione dei dati. Specifico riguardo dovrebbe essere posto alla base giuridica che supporta l'erogazione dei servizi previsti dalla PSR. Nel dettaglio, sarebbe auspicabile definire il perimetro dei trattamenti per i quali è necessario unicamente fornire un'informativa e quelli per i

[14] Direttiva 2019/882 del Parlamento europeo e del Consiglio del 17 aprile 2019 sui requisiti di accessibilità dei prodotti e dei servizi.

[15] Proposta di regolamento del Parlamento europeo e del Consiglio che modifica i regolamenti (UE) n. 260/2012 e (UE) 2021/1230 per quanto riguarda i bonifici istantanei in euro COM/2022/546 final/2.

quali è necessario ottenere un consenso esplicito, in modo tale da garantire maggiore chiarezza e lasciare minor spazio nell'interpretazione.

3.2. Asimmetrie e concorrenza

La PSD2 rappresenta una rivoluzione nell'ambito del mondo dei pagamenti, che ha consentito lo sviluppo di nuovi servizi basati sull'accesso ai conti da parte dei prestatori di servizi informativi e dispositivi (i sopra citati AISP e PISP) e ha favorito l'insorgere di nuovi modelli di servizio che vengono ricompresi sotto l'ampio termine di *Open Banking*. Tuttavia, essa ha richiesto – soprattutto per le banche, chiamate ad implementare apposite interfacce di colloquio sicuro con AISP e PISP – costi di implementazione ingenti rispetto ai benefici attesi, ai quali si debbono aggiungere i costi di mantenimento e aggiornamento dell'infrastruttura, tutt'ora presenti e da affrontare anche in vista dei cambiamenti prospettati dal nuovo regolamento. L'accesso ai conti normato dalla PSD2 non è stato accompagnato da un principio di remunerazione che potesse garantire l'equa distribuzione del valore generato dai servizi stessi, generando così un'asimmetria concorrenziale tra operatori bancari e non bancari, laddove i primi sono stati obbligati ad aprire l'accesso ai dati dei conti di pagamento dei propri clienti e assicurare un'efficiente infrastruttura per consentire tale accesso, mentre i secondi hanno potuto costruire servizi innovativi per la clientela sulla base di tali dati senza sostenere i costi per l'accesso alla "materia prima" grazie alla quale questi servizi sono realizzati.

Come ampiamente riconosciuto in letteratura, e anche nel richiamato *Digital Finance Package*, l'accesso ai dati è volano di innovazione, di sviluppo del business e di competitività. L'auspicio era dunque che il nuovo *Payments Package* introducesse un cambiamento, permettendo, tra le altre cose, di raggiungere quella parità di condizioni attesa, rispetto ad altre normative in corso di definizione (es. FiDA), e che dovrebbe essere garantita in prospettiva di un'ulteriore spinta allo sviluppo dell'*Open Banking*. Invece, nella proposta di nuovo *Payments Package* è ancora assente la possibilità di remunerazione per l'offerta di questi servizi, seppure sia da ritenere apprezzabile l'idea di mantenere il servizio informativo sui conti (*Account Information Service* – AIS) nell'ambito del perimetro della PSR e quindi dei servizi di *Open Banking* almeno fintanto che non si chiariscano bene le prospettive aperte da FiDA – a garanzia degli investimenti effettuati in passato dal settore, che ha sviluppato il servizio secondo le logiche e il regime normativo previsti dalla PSD2.

Non includendo il principio di remunerazione, il "pacchetto" PSD3/PSR si discosta dal percorso intrapreso da altre normative, quali FiDA e *Data Act*, dove invece viene prospettato e argomentato proprio nell'ottica di una corretta remunerazione degli *asset* (cioè, in questo caso, dei dati) messi a disposizione dagli *asset holders*.

Nella proposta di regolamento è mantenuto l'impianto della PSD2, in cui la creazione e il mantenimento delle interfacce di *Open Banking* e la condivisione dei dati deve avvenire in modo gratuito. Tale principio rischia però di perpetuare uno squilibrio e di non tenere il passo con i tempi, minando possibili sviluppi ottimali e innovazioni. Inoltre, la PSR prevede anche che i prestatori di servizio di pagamento di radicamento del conto (*Account Servicing Payment Service Providers* – ASPSP) forniscano all'utente "*un pannello di gestione, integrato nella sua interfaccia utente, per monitorare e gestire le autorizzazioni rilasciate dall'utente di servizi di pagamento ai fini dei servizi di informazione sui conti o dei servizi di disposizione di ordine di pagamento per pagamenti multipli o ricorrenti*" [16] e anche per quest'ultimo non è prevista alcuna remunerazione.

Diversamente, il regolamento FiDA riconosce l'esigenza di una remunerazione per la condivisione dei dati all'interno di appositi Schemi di condivisione. Il regolamento FiDA, infatti, prospetta la possibilità per i clienti di gestire le proprie *dashboard*, l'allargamento dell'accesso ai dati finanziari dei clienti e la condivisione degli stessi nell'ambito di Schemi di mercato. All'interno di ogni Schema viene data la possibilità ai partecipanti di stabilire le condizioni per una ragionevole compensazione spettante ai titolari dei dati per la messa a disposizione degli stessi agli utenti dei dati. Tale compensazione dovrebbe riflettere almeno i costi sostenuti per mettere a disposizione un'interfaccia tecnica per la condivisione dei dati richiesti.

Il regolamento FiDA è in linea con il *Data Act* che, all'art. 9, stabilisce la generale possibilità di compensazione per la messa a disposizione dei dati. Questo non è riconosciuto in PSR, dove, sebbene sia prevista la condivisione dati, non sono tenuti in considerazione fattori di particolare rilevanza quali:

i) l'elevato livello di sicurezza/protezione e gli elevati standard seguiti per la gestione dei dati da parte dell'ASPSP;

ii) i costi per l'infrastruttura messa in atto per la condivisione dei dati;

iii) i costi associati alla raccolta, ai processi di trasformazione e alla gestione dei dati.

Considerando quanto sopra, è chiara l'asimmetria persistente tra la PSR e le altre normative europee citate che dovrebbe invece essere sanata/eli-

[16] COMMISSIONE EUROPEA, *Payment Services Regulation*, art. 43.

minata al fine di evitare disallineamenti nell'impianto normativo europeo che potrebbero creare effetti distorsivi sul mercato.

3.3. Asimmetrie e sicurezza

Benché siano stati apportati dei cambiamenti in PSD3/PSR rispetto a quanto previsto in PSD2, il regime di responsabilità tra gli attori coinvolti nella catena del pagamento attualmente individuato lascia ancora adito a possibili asimmetrie. Infatti, sebbene il regolamento introduca il fondamentale concetto di cooperazione tra i PSP e i prestatori di servizi di comunicazione elettronica (cd. Telco) nell'ottica di prevenzione e contrasto alle frodi, questa misura sembra essere ancora largamente insufficiente.

Negli ultimi anni è aumentata la diffusione di nuove tipologie di frode sempre più complesse (in particolare il cd. *social engineering*[17]) e in questo nuovo contesto è necessario sia avvalersi di strumenti idonei e comuni per accertare la frode e recuperare i fondi, sia includere nel perimetro del regolamento tutti i fornitori a supporto del servizio di pagamento e/o che interagiscono con gli utenti finali. In questo gruppo rientrano anche i sopra citati fornitori di servizi di comunicazione elettronica (cd. Telco) che forniscono i canali di comunicazione tra l'utente e il prestatore di servizi di pagamento. Dato che le nuove tipologie di frode sono perpetrate principalmente tramite i canali di comunicazione elettronica, i fornitori di servizi di comunicazione elettronica dovrebbero essere opportunamente assoggettati alle previsioni normative relative alle frodi, con specifico riguardo alle responsabilità e alla condivisione delle informazioni, proprio in considerazione del ruolo sempre maggiore che ricoprono nella catena dei pagamenti. La *stretta cooperazione* attualmente prevista nell'art. 59[18] del regolamento non è sufficiente a garantire un'adeguata protezione dell'utente, la generale sicurezza dei servizi di pagamento e la corretta allocazione delle effettive responsabilità. Infatti, solo l'effettiva partecipazione delle Telco e degli al-

[17] FSB, Cyber Lexicon: Updated in 2023 (fsb.org): "*A general term for trying to deceive people into revealing information or performing certain actions*".

[18] COMMISSIONE EUROPEA, *Payment Services Regulation*, art. 59, comma 5: "*Se informati da un prestatore di servizi di pagamento del verificarsi del tipo di frode di cui al paragrafo 1, i prestatori di servizi di comunicazione elettronica cooperano strettamente con i prestatori di servizi di pagamento e agiscono rapidamente per garantire l'adozione di misure organizzative e tecniche adeguate per salvaguardare la sicurezza e la riservatezza delle comunicazioni conformemente alla direttiva 2002/58/CE, anche per quanto riguarda l'identificazione della linea chiamante e l'indirizzo di posta elettronica.*".

tri fornitori di servizi nel ristoro dei fondi del cliente laddove la responsabilità della frode ricada nel loro "tratto di competenza" della catena del pagamento e non in quella dei PSP, potrebbe eliminare questa grave asimmetria. Sempre nell'ambito delle frodi, sussistono ancora altri punti lacunosi che pongono i PSP in una situazione di difficoltà e asimmetria nell'attività di contrasto e prevenzione delle frodi e che non sono stati debitamente affrontati nell'ambito della proposta di regolamento. Per fornire un esempio, è ancora viva la necessità di agevolare la cooperazione tra PSP nell'ottica di contrasto alle frodi; sarebbe importante garantire la possibilità di scambio di informazioni e dati utili all'individuazione e blocco di attori fraudolenti che minano la sicurezza degli utenti e danneggiano il mercato. Misure più ampie, quindi, di quelle attualmente previste ai sensi dell'art. 51 sui limiti e il blocco dell'uso dello strumento di pagamento e dell'art. 83 sui meccanismi di monitoraggio delle operazioni e condivisione dei dati sulle frodi.

Sarebbe stato inoltre auspicabile che il regolamento prevedesse la possibilità per il prestatore di servizi di pagamento del beneficiario di poter bloccare un conto di pagamento se, su notifica del PSP del pagatore, il beneficiario della transazione e detentore del conto è sospettato di essere destinatario di una transazione fraudolenta e quindi di essere egli stesso un frodatore. Naturalmente, questo dovrebbe essere stabilito sempre tenendo in debita considerazione la necessità di bilanciare il rispetto della *privacy* del beneficiario e dei suoi diritti, ai sensi della GDPR, con l'interesse dell'ordinante e del prestatore di servizi di pagamento dell'ordinante ad avvalersi dei dati personali del beneficiario.

Tanto nel caso della cooperazione tra PSP e fornitori di servizi di telecomunicazione quanto nel caso della cooperazione tra PSP del pagatore e PSP del beneficiario di un pagamento, si nota una asimmetria tra ciò che si richiede di fare ai PSP (cioè, individuare, prevenire e risolvere possibili casi di frode a tutela del pagatore) e gli strumenti a loro disposizione, non sufficienti per adempiere ai doveri previsti.

Infine, un'ulteriore asimmetria emerge nell'ambito dell'equa ripartizione delle responsabilità tra il PSP e l'utente/cliente in caso di frode. Il "pacchetto" PSD3/PSR avrebbe dovuto introdurre una definizione di negligenza grave ed uniforme tra i vari Paesi e chiarire le relative responsabilità in capo anche ai consumatori, ma così non è stato. Il "pacchetto" ha invece introdotto l'obbligo generale di rimborso da parte dei PSP in caso di frode per impersonificazione. Tale misura sembra essere contraria agli sforzi europei per garantire transazioni di pagamento efficienti e convenienti, potrebbe essere foriera di un ulteriore aumento delle truffe, poiché non sa-

rebbe interesse del cliente prestare attenzione a potenziali tentativi di raggiro e potrebbe incidere negativamente sulla sicurezza delle operazioni nonché, in ultima analisi sulla stabilità dei PSP che potrebbero essere chiamati a rispondere di importi estremamente elevati.

A questo si collega anche la mancanza di una chiara ripartizione delle responsabilità tra PSP e clienti, dovuta all'assenza di una definizione di "negligenza grave" uniforme tra i vari Paesi e delle relative responsabilità del cliente/utente. Pertanto, nell'ottica di sanare almeno in parte questa asimmetria, potrebbe essere utile chiarire a livello europeo i parametri per definire i casi specifici di negligenza grave e introdurre criteri per sua la valutazione.

Da ultimo, ma non ultimo, appare interamente incongruo porre su un operatore economico la responsabilità per azioni che sono del tutto al di fuori del suo controllo, non potendo, alcun PSP contrastare una frode che fa leva su falsi convincimenti dell'utente, che è spinto dal frodatore che lo raggira, a eseguire una transazione che, dal punto di vista del PSP, è correttamente autorizzata, correttamente registrata e contabilizzata, e che non ha subito le conseguenze di guasti tecnici o altri inconvenienti del servizio fornito dal PSP, cioè è perfettamente conforme all'art. 72 della PSD2) su cui si basa l'onere della prova nel contesto vigente.

3.4. Asimmetria e inclusione

Negli ultimi anni il livello di digitalizzazione dei consumatori è notevolmente aumentato; tuttavia, è sempre necessario prestare attenzione anche a coloro i quali sono meno coinvolti in questo processo (es. anziani, persone fragili o non debitamente istruite in ambito finanziario/digitale), che sono più spesso vulnerabili e soggetti a possibili frodi. Considerando anche l'elevato numero di persone affette da disabilità o con scarsa propensione all'utilizzo di strumenti digitali, è doveroso garantire uno sviluppo delle norme inclusivo e sostenibile e supportare l'educazione digitale dei consumatori, nell'ottica di evitare possibili asimmetrie.

In tal senso, una misura utile per risolvere una possibile asimmetria è assicurare la sicurezza del consumatore e l'inclusività degli strumenti sia tramite normative – ne sono un esempio la stessa revisione della PSD2 e la direttiva sui requisiti di accessibilità dei prodotti e dei servizi (*European Accessibility Act* – EAA) – sia rendendo l'utente consapevole dei cambiamenti di mercato, degli strumenti e rischi a esso associati tramite un'attenta educazione dello stesso.

In PSR, l'inclusività delle norme è oggetto dell'art. 88 "*Requisiti di accessibilità relativi all'autenticazione forte del cliente*[19]". Tale iniziativa è molto apprezzabile, purché venga assicurato l'allineamento del testo della PSR a quello dell'EAA in termini di contenuti e di tempi di adozione e recepimento a livello nazionale.

In merito al tema dell'educazione, un passo importante nella responsabilizzazione e per la formazione del consumatore è l'aggiornamento di quest'ultimo sui nuovi pericoli e tipologie di frode, così da fornire all'utente gli strumenti per riconoscere e affrontare opportunamente situazioni di potenziale rischio. Gli utenti, soprattutto quelli più fragili o meno pratici di strumenti digitali, molto spesso cadono vittime di diverse tipologie di frode. Renderli più consapevoli tramite programmi di educazione potrebbe aiutare i consumatori ad individuare possibili situazioni di rischio. Queste iniziative info/educative, condotte sia dai singoli PSP sulla propria clientela, sia a livello nazionale, aiuterebbero i consumatori ad usare maggior cautela sia nell'ambito digitale che reale, rivolti al comune obiettivo di contrasto e prevenzione delle frodi. Queste misure sono in parte incluse nella nuova PSR, dove si prevede che i PSP, nel portare avanti iniziative di questo genere, si rivolgano anche ai propri impiegati così da tenerli costantemente aggiornati e vigili sulle nuove "trovate" dei frodatori[20].

In aggiunta a questo, però, il Regolatore dovrebbe anche riconoscere e valutare il ruolo della negligenza grave da parte del consumatore nel caso in cui questo incorra in una frode, nonostante sia stato informato correttamente dal proprio PSP. Questo è doveroso al fine di evitare asimmetrie nell'ambito della sicurezza e del regime di responsabilità. L'approccio alla "educazione del consumatore" dovrebbe essere infatti bilanciato con una chiara e corretta formulazione del concetto di negligenza grave, come argomentato nel precedente paragrafo.

Un ulteriore passo dovrebbe essere una maggiore informazione resa al consumatore su cosa sono e come funzionano/quali servizi offrono gli AISP/PISP. Infatti, un ostacolo alla diffusione dei servizi AIS/PIS è rintracciabile nella scarsa conoscenza che i consumatori hanno di questi servizi innovativi. Per sopperire a questa scarsa conoscenza dei servizi, potreb-

---

[19] COMMISSIONE EUROPEA, *Payment Services Regulation*, art. 88.

[20] COMMISSIONE EUROPEA, *Payment Services Regulation*, art. 84, comma 2: "*I prestatori di servizi di pagamento organizzano almeno una volta all'anno programmi di formazione per i dipendenti sui rischi e sulle tendenze in materia di frodi nei pagamenti e assicurano che i dipendenti siano adeguatamente formati per assumere i loro compiti e le loro responsabilità conformemente alle pertinenti politiche e procedure di sicurezza volte a mitigare e gestire i rischi di frode nei pagamenti.*".

bero essere promosse iniziative su vari livelli, con il coinvolgimento anche degli stessi AISP/PISP.

4. Conclusioni

Il *Payments Package*, nell'ottica di migliorare quanto è già stato fatto con la PSD2, è ben accolto per diversi aspetti quali il mantenimento del servizio informativo sui conti (AIS) nell'ambito del perimetro della PSR e dei servizi di *Open Banking*, per la fusione operata tra PSD2 e EMD2, e anche per l'impostazione nell'affrontare nuove tipologie di frode.

Ciononostante, esistono ancora alcuni punti aperti, che non dipanano le asimmetrie esistenti che dovrebbero essere tenute in considerazione e sanate per un corretto funzionamento del mercato. Queste asimmetrie hanno a che fare con l'allineamento con altre normative europee, la sicurezza, il tema della remunerazione e l'inclusione digitale dei consumatori. Nel dettaglio, sono emerse la necessità di garantire un allineamento chiaro con altre normative europee (es. GDPR, FiDA, *Data Act*, MiCAR, IPR, etc.), di includere tutti i fornitori di servizi a vario titolo coinvolti nella catena di pagamento all'interno del regime di responsabilità, di prevedere la possibilità di cooperazione tra PSP nell'ambito di contrasto e prevenzione delle frodi, di poter bloccare non solo lo strumento di pagamento ma anche un conto sospettato come fraudolento, nel rispetto delle disposizioni del GDPR, di riallineare le responsabilità tra PSP e utente/cliente, di promuovere progetti per l'educazione e l'inclusione digitale a beneficio del mercato e dei consumatori stessi.

Una delle asimmetrie più gravi è la mancata introduzione della possibilità di remunerazione per i servizi di *Open Banking* e condivisione dei dati, che si discosta da quanto previsto da altre normative, come FiDA e *Data Act*. Queste asimmetrie, e in particolare quest'ultima citata, inerente alla remunerazione del servizio, possono causare disallineamenti e malfunzionamenti all'interno del mercato, creando delle vere e proprie distorsioni.

Stefano Firpo e Maddalena Rabitti

Digital financial strategy tra regole e mercato

SOMMARIO: 1. Il *framework* normativo e l'*Open Finance*. – 2. Il ruolo di consumatori e imprese. – 3. L'ipertrofia normativa europea. – 4. Rischi e opportunità del mercato: l'esigenza di una legislazione per principi.

1. Il *framework* normativo e l'*Open Finance*

Creare uno spazio comune di dati finanziari è un obiettivo prioritario della *Digital Financial Strategy* [1], la politica della Commissione volta a promuovere l'innovazione guidata dai dati nel settore finanziario, che trova espressione nel pacchetto di provvedimenti del 28 giugno 2023 [2]. In particolare, il legislatore europeo, da un lato, ha intenzione di introdurre *modifiche all'attuale framework normativo sui servizi di pagamento digitale* tramite due atti legislativi distinti, volti ad allineare la normativa alla transizione digitale in atto: si tratta della *proposta di direttiva (PSD 3)* che introduce norme in materia di autorizzazione e vigilanza degli istituti di pagamento e della *proposta di regolamento (PSR)* sulle norme per i prestatori di servizi di pagamento. Dall'altro lato, a completamento del *framework* esistente, ha scelto di introdurre *ex novo* una disciplina sull'accesso "aperto" ai dati finanziari delle persone, per promuovere l'offerta di prodotti e servizi finanziari innovativi in modo sicuro. Questa terza *proposta di regolamento sull'accesso ai dati relativi alle informazioni finanziarie* ("*financial in-*

[1] COMMISSIONE EUROPEA, *Strategia in materia di finanza digitale per la UE*, COM(2020)591 fnal, 24 settembre 2020.

[2] Il 28 giugno 2023, la Commissione europea ha pubblicato il testo della proposta di direttiva PSD3 (COM(2023)366 final) insieme alla proposta di regolamento PSR (*Payment Services Regulation*) (COM(2023)367 final) e la proposta di regolamento FIDA (*Financial Data Access*) (COM(2023)360 final) che insieme costituiscono il Payments Package.

formation data access" o "FIDA")[3], che estende l'obbligo di fornire accesso ai dati finanziari al di là dei dati dei conti di pagamento è certamente la più interessante, perché *affianca all'Open Banking*[4] *il nuovo regime dell'Open Finance*[5].

A spingere il legislatore europeo in questa direzione è l'idea che un solido quadro normativo per la condivisione dei dati finanziari sia fondamentale per rendere *l'Europa leader nell'offerta di servizi bancari e finanziari innovativi, con beneficio dei consumatori* a cui è data, *via* controllo dei propri dati finanziari, la possibilità di incidere in modo significativo non solo dal lato della domanda ma anche dell'offerta di servizi finanziari innovativi e personalizzati; nonché *con beneficio delle imprese, anche PMI*, che possono con i dati a disposizione essere maggiormente competitive nell'offerta di servizi e prodotti finanziari innovativi. Questa architettura dovrebbe infatti favorire l'ingresso di nuovi attori finanziari che si affiancano a, o sostituiscono gli intermediari tradizionali. *L'obiettivo finale è quello di avere imprese finanziarie europee che possano essere competitive a livello globale*[6]. La disponibilità di dati condivisi dal settore, inoltre, può influenzare positivamente gli *investimenti in Europa*, poiché le imprese possono trarre vantaggio dall'entrare in un sistema basato sulla condivisione dei dati finanziari.

Quanto detto spiega la scelta di passare da un modello di *Open Banking*, introdotto con la PSD2[7] e ora, in chiave evolutiva, con la PSD3, che già impone la condivisione dei dati ma nel solo settore dei sistemi dei pagamenti, a quello di *Open Finance*, che si applicherà a una serie più ampia di attori del settore finanziario e che amplia la gamma di dati finanziari disponibili da condividere. Ciò si realizza consentendo l'accesso anche agli operatori "Terze Parti" (TPP) all'intera gamma di dati del cliente provenienti da svariate fonti e linee di prodotti finanziari come, ad esempio, mutui, crediti al

---

[3] Proposta di regolamento relativo a un quadro per l'accesso di dati finanziari, 28 giugno 2023 COM(2023)360 final.

[4] Cfr. R. PELLITTIERI, R. PARRINI, C. CAFAROTTI, B.A. DE VENDICTIS, *Mercati, infrastrutture, sistemi di pagamento. L'Open Banking nel sistema dei pagamenti: evoluzione infrastrutturale, innovazione e sicurezza, prassi di vigilanza e sorveglianza*, in *Quaderno Banca d'Italia*, n. 31, marzo 2023.

[5] Cfr. OECD, *Shifting from Open Banking to Open Finance: Results from the 2022 OECD survey on data sharing frameworks*, in *OECD Business and Finance Policy Papers*, 2023.

[6] Sull'interazione tra tecnologia e concorrenza v. G. COLANGELO, *Data, Innovation and Competition in Finance: The Case of the Access to Account Rule*, in *European Business Law Review*, 2020 31(4), p. 573.

[7] Direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio del 25 novembre 2015 relativa ai servizi di pagamento nel mercato interno.

consumo, investimenti, pensioni, assicurazioni, servizi di consulenza, ecc.

Il modello dell'*Open Banking* che si va ad esportare – per la verità ad oggi più vincente sulla carta che nella prassi – è infatti fondato su un *obbligo giuridico di condivisione di dati imposto agli istituti finanziari titolari di dati storici*, garantendo *l'interoperabilità* sul piano tecnologico mediante il ricorso alle cd. API che devono essere efficienti, sicure, con costi accessibili [8]. Questo modello, quando applicato all'*Open Finance*, porta a una maggiore condivisione, riutilizzo e valorizzazione dei dati finanziari della clientela nell'ottica della creazione di un ecosistema finanziario aperto guidato dalla digitalizzazione e dai dati. In questo ecosistema, si assiste alla disaggregazione della fornitura di servizi finanziari in più segmenti di mercato. Come si è detto, infatti, le imprese, in particolare le PMI, godrebbero di un accesso più ampio a prodotti e servizi finanziari.

La promessa dell'*Open Finance* deriva dal suo potenziale di ridurre drasticamente le barriere legali e tecnologiche che storicamente hanno reso difficile per i clienti accedere alle proprie informazioni, impedendo loro di condividerle facilmente con terze parti e quindi dissuadendoli dal passare da un prodotto all'altro e da un servizio all'altro offerti da diverse istituzioni finanziarie. Riducendo queste barriere, l'*Open Finance* cerca di livellare il campo di gioco informativo, promuovendo così una maggiore concorrenza non solo tra le istituzioni finanziarie tradizionali, ma anche tra questi operatori storici e una nuova generazione di innovatori fintech [9].

Questa evoluzione costituisce certamente un passaggio naturale in un'economia che mette al centro i dati.

Si tratta di un cambiamento che impatta sulla configurazione attuale del sistema finanziario in modo importante [10].

Per adeguarsi, agli intermediari finanziari, vecchi e nuovi, è richiesto un *onere di compliance* molto gravoso in termini di conformità sia legale sia organizzativa.

---

[8] Sul tema, tra gli altri, F. CIRAOLO, *Open Banking, Open Problems. Aspetti controversi del nuovo modello dei "sistemi bancari aperti",* in *Riv. dir. banc.*, 4, 2020, p. 611 ss.; M. RABITTI, S. 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*, Cedam, Padova, 2019, p. 711 ss.; OECD, *Data Portability in Open Banking. Privacy and The Other Cross-Cutting Issues*, in *OECD Digital Economy Papers*, p. 348, February 2023, in *oecd-ilibrary.org*.

[9] D. AWREY, J. MACEY, *The Promise and Perils of Open Finance (February 28, 2022). European Corporate Governance Institute*, in *Law Working Paper* No. 632/2022.

[10] D.A. ZETZSCHE, R.P. BUCKLEY, D.W. ARNER, *Open Banking, Open Data and Open Finance: Lessons from the European Union*, in L. JENG (ed.), *Open Banking*, Oxford University Press, Oxford, 2022, p. 147 ss.

Quindi, da un lato, gli intermediari tradizionali fino ad oggi oligopolisti, perdono il vantaggio di posizione rappresentato dalla disponibilità in via esclusiva dei dati e sono tenuti a effettuare importanti investimenti sulla tecnologia e sulla sicurezza, necessari per rimanere sul mercato e per garantire che l'accesso ai dati sia sicuro. D'altro lato, i nuovi intermediari, cd. terze parti, devono garantire un adeguato livello di tutela degli utenti e del mercato. La sicurezza dei dati è forse uno dei punti più spinosi, per il passaggio di dati da un sistema ad un altro che potrebbe amplificare i rischi di cybercrime e di utilizzo illecito di dati.

Inoltre, più si condividono dati, più i rischi possono assumere rilevanza sistemica, con sfide anche per la vigilanza prudenziale. Ai rischi operativi cerca di rispondere anche il *regolamento Dora*[11] sulla resilienza operativa digitale del settore finanziario, che è stato adottato in attuazione del Pacchetto 2020 sulla strategia digitale. In questa prospettiva FIDA dovrà essere attuata nel rispetto dei principi e delle regole stabilite da DORA, in quanto applicabili. Infine, vi è un rischio specifico legato all'ecosistema e alla conformità alle normative generali che regolano il mercato. Se, infatti, uno dei soggetti interessati non riuscisse a rispettare queste norme, l'ecosistema potrebbe esporre tutti i membri del progetto di *Open Finance* al rischio di danni finanziari o reputazionali. Come osservato in dottrina, le norme sull'*Open Banking* previste dalla PSD2, così come la prossima disciplina sull'*Open Finance*, «sono destinate ad alimentare le interazioni tra diverse istituzioni, anche di natura non regolamentata. La disponibilità e la libera circolazione dei dati tra imprese finanziarie è tesa a stimolare lo sviluppo di nuove tecnologie finanziarie, compresi i sistemi di IA, e la loro circolazione attraverso accordi di *outsourcing*. Ciò amplificherà molto probabilmente i rischi legati alla tecnologia e quindi l'urgenza di gestirli adeguatamente»[12].

Il tema dell'adeguatezza della normativa esistente e in via di approvazione a gestire il passaggio all'*Open Finance*, induce alcune riflessioni sull'idoneità del *framework* normativo europeo ad affrontare la sfida di regolare la finanza digitale. La prospettiva è quella di considerare i rischi e le opportunità offerti dalla normativa europea nell'interesse delle imprese e dei consumatori.

---

[11] Regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativo alla resilienza operativa digitale per il settore finanziario.

[12] G. SCHNEIDER, *La proposta di Regolamento europeo sull'intelligenza artificiale alla prova dei mercati finanziari: limiti e prospettive (di vigilanza)*, in *Resp. civ. prev.*, marzo 2023, p. 1014 ss.

2. Il ruolo di consumatori e imprese

I *consumatori e le imprese* a cui i dati si riferiscono sono, infatti, in questo nuovo contesto, *i veri attori del mercato*, poiché sono chiamati a decidere a chi fornire i propri dati e per quali fini. Ad essi è attribuito un enorme potere di scelta, con conseguente responsabilizzazione.

Si prevede infatti la creazione di una *dashboard* a cui i consumatori accedono direttamente e prestano il consenso alla circolazione e condivisione dei propri dati [13].

Sono evidenti i vantaggi offerti da queste nuove opportunità in termini di personalizzazione dell'offerta, efficienza e risparmio di costi. Tra tutti i vantaggi, il più significativo è quello della potenziale maggiore *inclusione* finanziaria che la tecnologia può realizzare proprio perché apre il mercato a nuovi operatori e a servizi meno costosi, nonché a offerte più mirate e calibrate sulle esigenze della clientela. Se i soli dati provenienti dalla banca o dalle centrali rischi posso dare una rappresentazione parziale della capacità di adempimento di una persona, il complesso dei dati finanziari disponibili e condivisi può meglio fotografare il profilo del cliente e consentire ad esempio un maggior accesso al credito o a prodotti finanziari più adatti [14].

---

[13] FIDA prevede che al fine di consentire l'interazione contrattuale e tecnica necessaria per attuare l'accesso ai dati tra più enti finanziari, i titolari dei dati e gli utenti dei dati dovrebbero essere tenuti ad aderire a sistemi di condivisione dei dati finanziari. Tali sistemi dovrebbero elaborare norme in materia di dati e interfacce, quadri contrattuali standardizzati comuni che disciplinino l'accesso a specifiche serie di dati e norme di governance relative alla condivisione dei dati. Un sistema di condivisione dei dati finanziari dovrebbe consistere in un accordo contrattuale collettivo tra i titolari dei dati e gli utenti dei dati con l'obiettivo di promuovere l'efficienza e l'innovazione tecnica nella condivisione dei dati finanziari a vantaggio dei clienti. Al fine di garantire che abbiano un interesse nel fornire interfacce di elevata qualità per mettere i dati a disposizione degli utenti dei dati, i titolari dei dati dovrebbero poter chiedere un compenso ragionevole agli utenti dei dati per la realizzazione di interfacce di programmazione delle applicazioni. I membri del sistema di condivisione dei dati finanziari, compresi i titolari dei dati e gli utenti dei dati, dovrebbero essere tenuti a concordare la responsabilità contrattuale per le violazioni dei dati nonché le modalità di risoluzione di eventuali controversie tra i titolari dei dati e gli utenti dei dati in materia di responsabilità per determinare la responsabilità tra il titolare dei dati e l'utente dei dati.

[14] D'altro canto vi è anche il rischio che se si dovesse ricorrere a strumenti di intelligenza artificiale per effettuare ad esempio valutazioni di merito creditizio, si ricadrebbe nella principale se non unica ipotesi di sistema ad alto rischio contemplato dall'AI ACT. Sul tema M. RABITTI, *Credit scoring via machine learning e prestito responsabile*, in *Riv. dir. banc.*, 2023, p. 175 ss. Nelle more della pubblicazione di questo contributo, la Corte di Giustizia si è pronunciata sul tema del rapporto tra credit scoring machine learning e GDPR, con la sentenza del 7 dicembre 2023 su cui si veda ASSONIME, *Credit scoring e processo decisionale automatizzato ai sensi del GDPR: i chiarimenti della Corte di giustizia nel caso Schufa*, in *il Caso*, n. 1/24.

La Proposta Fida presuppone tuttavia che i consumatori sappiano usare in modo consapevole i propri dati: si tratterebbe dunque di *consumatori avveduti e responsabili*[15]. Al riguardo, il dubbio è che il legislatore europeo non faccia però i conti con l'esperienza del reale che vede ancora, specie in questo ambito finanziario, *consumatori vulnerabili*[16] o non adeguatamente preparati in materia finanziaria e sui rischi che possono conseguire alle scelte di utilizzo e condivisione dei propri dati finanziari[17]. La complessità dei modelli di business di *Fintech*, delle pratiche di raccolta dei dati, dei rapporti venditore-cliente o delle applicazioni tecnologiche possono cioè rendere difficile in concreto la corretta *autodeterminazione del consumatore*. Ci si può chiedere, ad esempio, come nell'ecosistema *Open Finance* i clienti possano individuare e riconoscere i dati necessari alla fornitura del servizio e come evitare che questi vengano usati per sviluppare modelli di business diversi da quelli richiesti. La mancanza di strumenti di controllo sui propri dati porta con sé, inevitabilmente, anche la ritrosia a condividere i propri dati per timore di violazione della privacy. Inoltre, la selezione dei dati da parte del consumatore può non essere corretta per l'operare di *biases*, come ci insegna l'economia comportamentale.

3. L'ipertrofia normativa europea

Inquadrato il tema a grandi linee, occorre chiedersi se il bilanciamento che l'UE persegue tra l'obiettivo di promuovere l'innovazione e l'adeguata

---

[15] Osserva M.T. PARACAMPO, *Trasformazione digitale del settore finanziario e Open Finance: quali prospettive per un credito "sostenibile"? Prime riflessioni*, in https://www.astridonline.it/static/upload/para/paracampo_medialaws_14_06_2023.pdf che il tema dell'*Open Finance* diviene punto di raccordo con quelli, altrettanto attenzionati e convergenti verso finalità inclusive e sostenibili, rappresentati dal nuovo piano d'azione per la *Capital Markets Union* e dalla *Strategia europea per gli investimenti retail*. Entrambi si completano, dal momento che in quest'ultima la finanza aperta adotta la prospettiva dell'investitore per coinvolgerlo maggiormente nel processo di investimento, rafforzando nel contempo il quadro normativo di tutela.

[16] Per un approfondimento del tema del consumatore vulnerabile nella finanza digitale si veda, tra gli altri, M.C. PAGLIETTI, M. RABITTI, *A Matter of Time. Digital-Financial Consumers' Vulnerability in the Retail Payments Market*, 33, in *European Business Law Review,* Issue 4, 2022, pp. 581-606; M.C. PAGLIETTI, *The Vulnerable Digital Payment Systems Consumer. A New Normative Standard?*, in *Competition and payments services*, Quaderni di ricerca giuridica della Consulenza legale della Banca d'Italia, dicembre 2022, p. 30 ss.

[17] Su questo tema v. F. FERRETTI, *L'Open Finance: Quali prospettive regolatorie per una strategia UE in materia di protezione dei consumatori nella finanza digitale?*, in *BIS*, 2023, p. 277 ss.

protezione ai diritti delle persone sia effettuato correttamente dal legislatore europeo in questo nuovo quadro regolatorio.

Quanto fin qui rilevato induce anche a interrogarsi sull'adeguatezza di tutto il disegno normativo a prevenire realmente i rischi per i consumatori e i rischi tecnologici che derivano dall'*Open Access*.

Quanto al primo aspetto, si può osservare che tutta la *legislazione europea recente promuove l'innovazione* con una normativa che favorisce il mercato purché esso si allinei ai *valori europei*[18]: si definisce così una sorta di limite di "ordine pubblico europeo" di direzione per il mercato e di protezione per le persone, volto a impedire che i diritti fondamentali possano essere pregiudicati nell'esercizio di attività economiche.

Cercare questo equilibrio in concreto significa tuttavia misurarsi costantemente con norme e principi che, in un *sistema di fonti articolato e multilivello* quale quello europeo, si pongono su piani diversi e hanno efficacia variabile e che, soprattutto, finiscono per delineare una architettura così complessa da essere un freno per lo sviluppo del mercato dei servizi innovativi finanziari.

Basti pensare che tutte le proposte del "Digital Financial Strategy" devono essere compatibili e devono coordinarsi oltre che tra loro, anche con il regolamento Dora e le altre normative settoriali che si applicano al sistema dei pagamenti.

Questi 'silos verticali' poi devono rispettare comunque i principi fissati da una serie di provvedimenti normativi di carattere orizzontale e generale, i silos orizzontali quali, ad esempio, il GDPR[19], il DSA[20], DMA[21], il DATA ACT[22], nonché con l'ormai compiuto regolamento sull'AI ACT, che a breve sarà definitivamente approvato[23].

Si determina così un sistema di regole a geometria variabile, poco idoneo a gestire la complessità, che forse anzi concorrono a creare.

---

[18] Si veda V. FALCE, *Piattaforme di ecosistemi digitali. Scelte proconcorrenziali*, in *Riv. dir. industriale*, 2022, p. 172 ss.

[19] Regolamento generale in materia di protezione dei dati personali (UE) 2016/679.

[20] Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali (*Digital Services Act-DSA*).

[21] Regolamento (UE) 2022/1925 del Parlamento europeo e del Consiglio del 14 settembre 2022 relativo a mercati equi e contendibili nel settore digitale (cd. Digital Markets Act o DMA).

[22] Regolamento (UE) 2023/2854 del Parlamento europeo e del Consiglio, del 13 dicembre 2023 (cd. "Data Act"), riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo.

[23] Proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (Legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione, 2021/0106 (COD).

All'interprete di oggi è richiesta la capacità di districarsi tra fonti che sembrano una tela di ragno e che impongono uno sforzo di coordinamento significativo, con un ampio margine di incertezza sulla corretta applicazione delle regole che mette in gioco il principio di certezza del diritto e rischia di pregiudicare proprio l'obiettivo da salvaguardare: la fiducia del mercato e l'interesse ad investire in Europa.

Risulta evidente che una *normativa non fondata su principi generali e non ispirata a principi di proporzionalità e di semplificazione rischia di essere inefficiente.*

A volte il conflitto tra disposizioni è tanto evidente da essere venuto già all'attenzione di dottrina e regolatori, come è accaduto nel coordinare PSD2 e GDPR[24]; altre volte invece la convivenza tra norme si risolve in termini di rapporto di specialità, come sembra accadere tra Fida e DATA ACT[25]. Il *Data Act* prevede le regole essenziali per tutti i settori quanto ai diritti di utilizzo dei dati, ma lascia alla legislazione di settore (verticale) la definizione di regole più dettagliate per il raggiungimento di obiettivi normativi specifici di settore.

Anche sul tema del ***profiling***, caratteristica imprescindibile per la fornitu-

---

[24] Posto che i dati finanziari non sono considerati di natura sensibile, per l'*Open Banking* le basi giuridiche pertinenti per un trattamento legittimo ai sensi dell'art. 6 del GDPR sono: il consenso inequivocabile dell'interessato, oppure il fatto che il trattamento dei dati sia necessario per l'esecuzione di un contratto di cui l'interessato è parte o per prendere misure precontrattuali su richiesta dell'interessato prima della stipula. I *TPP Fintech* fanno spesso un ampio uso di tecniche di profilazione, costituendone il più delle volte il modello di business. In caso di profilazione, il GDPR richiede un ulteriore livello di controllo. Stabilisce che una persona abbia il diritto di non essere sottoposta a una decisione basata *esclusivamente* su un trattamento automatizzato che possa produrre effetti giuridici che la riguardano o che, in modo analogo, incida significativamente sulla sua persona. È ammesso che la profilazione possa essere utilizzata se necessaria per esigenze contrattuali, se autorizzata dal diritto dell'UE o nazionale o se fondata sul consenso esplicito dell'interessato. Nel caso di decisioni automatizzate fondate sul consenso esplicito o sull'adempimento contrattuale, i titolari del trattamento devono rispettare il diritto degli interessati a ottenere l'intervento umano, esprimere il proprio punto di vista e poterne contestare le decisioni. Il Comitato europeo per la Protezione dei Dati (*European Data Protection Board – EDPB*), in una lettera indirizzata a un membro del Parlamento europeo, considera il «consenso esplicito» dell'art. 94, par. 2, della PSD2 come un consenso contrattuale, che non interferisce quindi con la necessità contrattuale del GDPR. La nuova proposta della Commissione mira a chiarire meglio l'interazione tra i servizi di pagamento e il GDPR. Sul punto cfr. lo Studio redatto su richiesta del Parlamento europeo e condotto da A. LEHMANN, J.S. MARCUS, *Open Finance. What can an enabling framework look like?*, October 2023, https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2023)754188.

[25] Il Data Act affronta il tema della concentrazione dei dati nel mercato e ha l'obiettivo di garantire equità nell'allocazione del valore dei dati stessi e promuoverne l'accesso e l'uso, creando un quadro di governance orizzontale e intersettoriale.

ra di servizi di *Open Finance*, sembra trovare trattamenti assai diversi e spesso non del tutto sintonici fra DSA, FIDA, GDPR e regolamento sull'IA.

Ci si trova quindi in una fase in cui il rischio è che la complessità del quadro normativo finisca da un lato per frenare l'innovazione e, per l'effetto, il mercato, e dall'altro per essere una normativa disapplicata a favore delle soluzioni di mercato offerte direttamente dalle piattaforme tecnologiche o da ordinamenti meno ingessati dalle regole stringenti.

Da più parti inoltre si solleva il *dubbio della crisi del cd. Brussels Effect* [26], in quanto la posizione assunta dall'UE di *driver* nella regolamentazione della tecnologia sta divenendo controproducente proprio per l'ipertrofia normativa che la caratterizza.

4. Rischi e opportunità del mercato: l'esigenza di una legislazione per principi

Lo spirito del tempo induce a ritenere *preferibile limitare la normazione di primo livello a principi generali*, e consentire poi al mercato di individuare, all'interno del perimetro regolatorio così definito, le regole del gioco, mediante *best practices* che poi diventano *standard*, con strumenti di co-regolazione [27], mediante ad esempio la creazione di Linee Guida elaborate insieme dalle imprese, dagli stakeholders e dalle autorità di settore.

Ciò che è soprattutto davvero auspicabile, in altri termini, è che la normativa di rango primario europeo stabilisca *poche regole di condotta certe,* per mettere il settore dei servizi finanziari nella condizione di attenersi ad adeguati standard di protezione dei consumatori in un regime di concorrenza paritario, valevole per tutti gli operatori. Da questo fattore può dipendere anche lo sviluppo dell'*Open Finance*.

In questo 'progetto regolatorio' c'è però un convitato di pietra, che consiste in quella che una volta si chiamava 'politica industriale', che solo ora inizia a svilupparsi in modo compiuto nell'Unione europea, almeno in alcuni settori. Aprire i mercati alla concorrenza, nelle nuove tecnologie, alimenta infatti, in una fase iniziale, un numero ampio di operatori, che si riducono però velocemente, nella fase di consolidamento. In assenza di controlli adeguati da un lato, e di un *sostegno vigoroso alle imprese europee*

[26] Sul significato del Brussels Effect cfr. A. BRADFORD, *The Brussel Effect: How the European Union Rules the World*, Oxford University Press, Oxford, 2020.

[27] F. BASSAN, *Digital Platforms and Blockchains: The Age of Participated Regulation*, in *European Business Law Review*, vol. 34(7), 2023, p. 1103 ss.

dall'altro, anche questo nuovo mercato rischia di diventare appannaggio di imprese extra-europee, nei confronti delle quali lo scudo del golden power europeo rischia di essere un'arma spuntata.

Le regole rischiano di avere un effetto controproducente, come ci insegna, in Europa, la discriminazione a rovescio del mutuo riconoscimento, se non sono accompagnate da una politica coerente, che spetta però agli Stati, in coordinamento tra loro.

Applicato al tema dell'*Open Finance* tutto ciò amplifica i rischi cui si è fatto cenno, legati ad un uso illegittimo dei dati, a violazioni del GDPR, a rischi di discriminazione di soggetti appartenenti a categorie vulnerabili e, soprattutto, concorre a fare perdere la *fiducia del mercato*.

Sara Landini

Circolazione dei dati, *data analytics* e tool di intelligenza artificiale nel settore assicurativo

SOMMARIO: 1. Governare la complessità attraverso le nuove tecnologie. – 2. Le diverse declinazioni di InsurTech. – 3. Conclusioni.

1. Governare la complessità attraverso le nuove tecnologie

La realtà contemporanea pone nuove sfide per la produzione e distribuzione assicurativa, per complessità normativa non solo per numerosità delle norme ma per la difficoltà di dar loro applicazione nella multiformità della domanda. Pone sfide anche per il cliente assicurativo per complessità dei prodotti e dei mercati non risolta da mere compensazioni attraverso informative abbondanti e talvolta ridondanti.

La complessità, e conseguente incertezza, è una delle parole chiave nella protezione degli interessi delle parti e la complessità trova una risposta nelle nuove tecnologie che consentono di semplificare attraverso clusterizzazioni il momento applicativo della normativa individuando accurate correlazione tra prodotti offerti e interessi degli investitori, di automatizzare processi, di rilevare difformità e inadeguatezze. Le nuove tecnologie risolvono i problemi di complessità evidenziati sia attraverso processi di semplificazione della applicazione delle regole si rendendo più effettivi i risultati che la normativa pone.

Nel 2007, Zigmut Bauman ha osservato nel suo libro *Liquid Modernity: Living in an Age of Uncertainty* [1] che il passaggio dalla modernità "solida" a quella "liquida" ha creato nuove sfide mai incontrate prima. Le forme sociali, le norme e le istituzioni non hanno avuto abbastanza tempo per

[1] Z. BAUMAN, *Liquid Modernity*, Polity, Cambridge, 2000.

consolidarsi e non possono servire come quadri di riferimento per le azioni umane e i piani di vita a lungo termine, quindi gli individui devono trovare altri modi per organizzare la propria vita attraverso una serie infinita di progetti a breve termine e episodi. Questa situazione richiede che gli individui siano flessibili e adattabili, pronti e disposti a cambiare tattica con breve preavviso, in condizioni di incertezza endemica. L'analisi predittiva può aiutare? Qual è l'impatto sulla distribuzione del rischio nei contratti e nel contratto di assicurazione che è "il" contratto del trasferimento del rischio? In che modo l'analisi dei dati può cambiare il concetto di asimmetria informativa nel settore assicurativo (l'assicuratore è meno informato dell'assicurato sul rischio, quindi l'assicurato ha il dovere di informazione) e il concetto stesso di assicurazione?

2. Le diverse declinazioni di InsurTech

Il termine *Insurtech* si riferisce all'applicazione delle tecnologie digitali al mondo assicurativo. In particolare l'*Insurtech* si caratterizza per un uso innovativo dei big data e dell'analisi predittiva. Gli ambiti di applicazione spaziano dalla produzione, alla distribuzione, fino alla stessa governance assicurativa.

Dal punto di vista della produzione, le tecnologie digitali hanno investito il mondo assicurativo a causa delle nuove esigenze di copertura dovute principalmente alla sicurezza dei dati. Lato della produzione, la vera novità riguarda l'applicazione della tecnologia blockchain ai contratti assicurativi. Una frontiera innovativa sul versante della produzione potrebbe essere rappresentata dalla *open insurance* come riproduzione nel mercato assicurativo del *Open Banking* da tempo nota nel settore bancario. Con il termine *Open Banking*, come noto, si intende un ecosistema aperto e digitale che consente, anche senza la presenza di accordi prestabiliti, lo scambio di dati e informazioni, non solo finanziarie, tra gli operatori (bancari, finanziari e non) che ne fanno parte. Si tratta di un sistema che ha consentito lo sviluppo di sistemi di pagamento a distanza.

Nel settore assicurativo, la digitalizzazione ha consentito di sfruttare i dati raccolti dai clienti insieme ai big data per effettuare operazioni di clustering in grado di profilare i clienti e migliorare l'aderenza dei prodotti alle loro esigenze assicurative.

L'utilizzo dei big data diventa importante nel settore assicurativo. Come è noto, con il termine "big data" si indica un complesso di dati enorme-

mente vasto che può essere utilizzato per formare nuova conoscenza attraverso le relazioni tra dati conoscibili. Si tratta di un'informazione che, per la sua dimensione e velocità di acquisizione, ha un valore euristico in quanto rappresenta il punto di partenza per individuare correlazioni che potrebbero essere rilevanti per sviluppi futuri [2].

Le tecniche utilizzate sono diverse:

1. Il "data mining" è il processo di analisi dei dati da diversi punti di vista al fine di ottenere informazioni utili. È il processo di ricerca di correlazioni o modelli tra i dati raccolti nei database relazionali.

2. La "data fusion" è il processo di integrazione di più dati e conoscenze. L'aspettativa è che i dati "uniti" contengano informazioni superiori ai dati originali.

3. La procedura di "clustering" ha lo scopo di raggruppare i dati e di organizzarli in gruppi in modo che i dati contenuti nello stesso cluster siano più simili tra loro rispetto a quelli contenuti in "cluster" diversi.

4. L'"analisi di regressione" viene utilizzata per stimare la forza e la direzione della relazione tra le variabili che sono in relazione lineare tra loro [3].

EIOPA (Autorità europea dei fondi assicurativi e pensionistici) nel suo Rapporto "Report on Best Practices on Licensing Requisiti, Peer-to-Peer Insurance and the Principle of Proportionality in an Insurtech Context" (Lussemburgo 2019) ha sottolineato nelle sue conclusioni che "Insurtech ha un impatto lungo tutte le fasi della catena del valore nei settori assicurativo e pensionistico, anche attraverso l'emergere di start-up, spesso nell'ambito di accordi di cooperazione con le imprese storiche".

EIOPA si concentra sull'importanza della regolamentazione poiché facilitare l'innovazione non significa deregolamentare. Una parola chiave nella regolamentazione è neutralità tecnologica nella legislazione. Il principio della neutralità tecnologica è stato attuato ed è uno dei principi chiave del quadro normativo europeo per le comunicazioni elettroniche, introdotto per la prima volta nel 2002 e rafforzato nel pacchetto telecomunicazioni del 2009.

---

[2] ASHTON, *That 'internet of things' thing*, in *RFID Journal*, 2009; L. ATZORI, A. IERA, G. MORABITO, *The internet of things: A survey*, in *Computer networks*, 2010; A.C. NAZZARO, *L'utilizzo dei Big data e i problemi di tutela della persona*, in *Rass. dir. civ*., 2018, p. 1239 ss.

[3] J. MANYIKA, M. CHUI, B. BROWN, J. BUGHIN, R. DOBBS, C. ROXBURGH, A. BYERS, *Big data: The next frontier for innovation, competition, and productivity*, The McKinsey Global Institute, New York, 2011; A. MCAFEE, E. BRYNJOLFSSON, *Big Data: The Management Revolution*, in *Harvard Business Review*, 2012, p. 13.

Secondo il Quadro europeo per le comunicazioni elettroniche, gli Stati membri hanno assicurato che le autorità nazionali di regolamentazione tengano nella massima considerazione l'opportunità di rendere la regolamentazione tecnologicamente neutra, vale a dire che non imponga né discrimini a favore dell'uso di un particolare tipo di comunicazione tecnologia.

Altra parola chiave è approccio proporzionato nella valutazione della conformità alle condizioni di autorizzazione (ad esempio in termini di aspettative relative ai processi di governance, ai sistemi e ai requisiti di controllo, che tengano conto delle specificità e dei rischi inerenti all'Insurtech).

Per questi motivi è importante l'utilizzo delle migliori pratiche. Nel suo rapporto l'EIOPA mappa alcune buone pratiche: "1. Le autorità di vigilanza, tenendo conto del loro preciso mandato, sono incoraggiate a utilizzare le misure disponibili per facilitare la consapevolezza generale dei consumatori (ad esempio attraverso la pubblicazione di lettere circolari e l'emissione di avvisi o avvertenze, ecc.) sui soggetti non vigilati Piattaforme assicurative P2P, ove possibile. 2. Le Autorità potrebbero incoraggiare i fornitori di piattaforme assicurative puramente P2P a comunicare ai consumatori in modo chiaro ed evidente che non forniscono o vendono alcuna copertura assicurativa e che quindi non sono soggetti alla regolamentazione assicurativa e a comunicare chiaramente ai consumatori la loro mancanza di accesso alle consuete tutele dei consumatori come un sistema indipendente di risoluzione delle controversie e di protezione, se applicabile. 3. Le Autorità si scambiano opinioni sul trattamento dei diversi modelli di business P2P e sugli approcci nazionali in materia di licenze a tali modelli di business".

Gli effetti positivi dell'applicazione della tecnologia blockchain al contratto assicurativo sono molteplici [4].

Tra i principali effetti positivi ricordiamo:

1. una possibile riduzione dei costi e dei possibili errori legati alla gestione umana e manuale delle richieste di risarcimento;

---

[4] La dottrina si interroga sull'impatto della tecnologia rispetto alle categorie del contratto in generale T.J. DE GRAAF, *From old to new: from internet to smart contracts and from people to smart contracts*, in *Computer Law & Security Review*, 35, 2019, p. 9. M. CINQUE, *La Blockchain smart contract-cripto attvità – applicazioni pratiche*, Pacini, Pisa, 2022; G. GITTI, *La disciplina contrattuale del mercato, dall'autonomia all'automazione*, in *Riv. dir. comm*., 2021, p. 28; A. GORASSINI, *Il valore della cultura giuridica nell'era digitale*, in *Tech. dir*., 2021, p. 49; S. A. CERRATO, *Appunti su smart contract e diritto dei contratti*, in *Banca borsa*, 2020, II, p. 370 ss.; F. LONGOBUCCO, *Utopia di un'automa. Lex Criptgraphi(c)a e responsabilità del giurista*, ESI, Napoli, 2023 in particolare pp. 71-72 per il quale le categorie civilistiche esistenti già consentono di risolvere i problemi che le nuove tecnologie pongono.

2. la maggiore trasparenza dei contratti che consentirebbe una migliore comparabilità tra le offerte delle diverse aziende, la possibilità di creare profili unici di clienti;

3. la lotta alle frodi;

4. un migliore flusso informativo anche al fine di dare attuazione alla procedura di governance del prodotto, come richiesto dall'art. 25 della direttiva IDD n. 97/2016.

Particolari applicazioni della *blockchain* possono verificarsi in fase di liquidazione dei sinistri nel caso di polizze indicizzate che consentono di correlare l'importo dell'indennizzo a determinati indici. Il concetto base delle soluzioni parametriche è: invece di risarcire l'effettiva perdita subita, l'assicurazione parametrica copre la probabilità che si verifichi un evento predefinito e paga secondo uno schema predefinito.

La distribuzione assicurativa vede una progressione di passaggi procedurali scanditi da obblighi di documentazione, informazione, registrazione e comunicazione ordinati all'idoneità dei contratti assicurativi rispetto alla richiesta e alle esigenze dell'assicurato. L'adempimento di tali obblighi potrebbe essere guidato e registrato, anche ai fini della conservazione e della prova della corretta esecuzione, mediante l'utilizzo di *blockchain*[5].

La *blockchain* potrebbe anche facilitare la ricerca dei prodotti più adatti sul mercato.

Nell'art. 20 dell'IDD (direttiva n. 97/2016 sulla distribuzione assicurativa) prevede che "qualsiasi proposta contrattuale deve essere coerente con le richieste ed esigenze assicurative del cliente".

Si legge nei considerando nn. 42-44 premesse direttiva IDD UE/2016/97: "Gli intermediari assicurativi e le imprese di assicurazione sono soggetti a requisiti uniformi quando distribuiscono prodotti di investimento assicurativi, come stabilito nel Regolamento (UE) n. 1286/2014 del Parlamento Europeo e del Consiglio. Oltre alle informazioni che devono essere fornite sotto forma di documento contenente le informazioni chiave, i distributori di prodotti di investimento assicurativi dovrebbero fornire informazioni aggiuntive che dettaglino eventuali costi di distribuzione che non siano già inclusi nei costi specificati nel documento contenente le informazioni chiave, in modo che in modo da consentire al cliente di comprendere l'effetto cumulativo che tali costi aggregati hanno sul ritorno dell'investimento. La presente direttiva dovrebbe pertanto stabilire norme sulla fornitura di in-

[5] K. NOUSSIA, *The IDD and Its Impact on the Life Insurance Industry*, in P. MARANO, K. NOUSSIA (eds.), *Insurance Distribution Directive*, in *AIDA Europe Research Series on Insurance Law and Regulation*, vol. 3, Springer, Berlin, p. 140.

formazioni sui costi del servizio di distribuzione connesso ai prodotti di investimento assicurativi in questione.

Per evitare casi di mis-selling, la vendita di prodotti assicurativi dovrebbe sempre essere accompagnata da un test delle domande e dei bisogni sulla base delle informazioni ottenute dal cliente. Qualsiasi prodotto assicurativo proposto al cliente dovrebbe sempre essere coerente con le sue richieste e necessità ed essere presentato in una forma comprensibile per consentire al cliente di prendere una decisione informata".

Come accennato in precedenza, la *blockchain* funziona come un registro decentralizzato e crittografato, nel quale, in tempo reale, vengono registrate innumerevoli operazioni senza che nessuno possa modificare quanto scritto centralmente, ma qualsiasi modifica o aggiornamento può avvenire solo dopo aver ricevuto il consenso da parte di tutte le parti coinvolte nella transazione devono essere registrate o modificate.

La *blockchain* potrebbe quindi essere considerata come un terzo attore, potenzialmente sostitutivo delle funzioni che oggi siamo soliti attribuire ai notai che da tempo stanno individuando modalità di utilizzo ai fini dell'esercizio della professione notarile. La *blockchain* ci permette di raccogliere, verificare e condividere dati di varia natura in modo sicuro e trasparente.

Questi dati possono includere le richieste e le esigenze dei clienti, i risultati della loro profilazione e dati di prodotto.

Per quanto riguarda la profilazione della clientela e l'adeguatezza del prodotto determinata attraverso processi algoritmici, è necessario distinguere: nel ramo vita l'adeguatezza è più misurabile. Nel mercato finanziario sono già in atto metriche che consentono di quantificare l'aderenza del prodotto a profili di adeguatezza e appropriatezza rispetto al profilo del cliente; nel ramo danni non esistono ancora metriche, l'adeguatezza trova ancora una determinazione non quantitativa. Si tratta di pensare a possibili misurazioni anche in questo ambito [6].

Poiché la direttiva *distribution* mira a rafforzare la tutela dei clienti retail e non i clienti nelle coperture grandi rischi, alcune delle sue disposizioni sono applicabili solo nei rapporti tra imprese e persone fisiche, in particolare quelle che regolano le norme di comportamento degli intermediari assicurativi o di altri venditori di prodotti assicurativi.

Qui la tutela del cliente assicurativo si lega al tema della *Data Protection* ed è necessario che l'applicazione del GDPR consideri gli effetti benefici

[6] Vedi P. PERLINGIERI, *Mifid II. Innovazione finanziaria e rapporti con la clientela*, in *DIMAF*, 2019, pp. 1-7.

delle nuove tecnologie nella protezione degli interessi degli assicurati [7].

Dal punto di vista del settore assicurativo, il maggiore scambio di dati attraverso *Open Insurance* può facilitare l'innovazione, l'apertura e la collaborazione a livello di settore e probabilmente consentirà al settore assicurativo di abbracciare l'innovazione basata sui dati, la creazione di prodotti innovativi per i consumatori e aumentare l'efficienza e l'interazione con terze parti (ad esempio una migliore interazione con le piattaforme assicurative e gli ecosistemi). Inoltre, potrebbe facilitare l'emergere di una maggiore concorrenza all'interno della catena del valore, come nuovi attori, nuovi modelli di business, forse riducendo alcuni costi attraverso l'efficienza.

Nella prospettiva del settore, va considerata anche l'interazione tra banche e assicuratori considerando il ruolo del fenomeno Banca-Assicurativo.

Un'altra prospettiva da considerare dovrebbe essere il punto di vista delle organizzazioni internazionali interessate ad ottenere dati, provenienti dal mercato assicurativo, per scopi sociali, come nel caso dei dati sanitari.

Esistono altri possibili usi delle "assicurazioni aperte" non considerati nel documento dell'EIOPA:

1. Indennizzo basato sull'indice (*index based insurance*).

L'assicurazione aperta può avere un ruolo importante nell'assicurazione danni nelle procedure di valutazione del danno. La determinazione delle perdite può richiedere lunghi periodi di tempo e potrebbe essere costosa sia per l'assicuratore che per l'assicurato. L'assicurazione basata sull'indice può rappresentare una valida alternativa alla determinazione del quantum in via esclusivamente peritale. Con l'assicurazione basata sull'indice, i pagamenti sono legati a un "indice" e il rapido flusso di informazioni tra assicuratori, assicurati, distributori facilita tutto questo [8].

Lo sviluppo dell'assicurazione basata su indici dipende dalla raccolta di dati che consentano di facilitare la determinazione dell'importo dell'indennizzo assicurativo grazie ad un indice predeterminato correlato all'importo dell'indennizzo.

I vantaggi dell'assicurazione basata su indici sono:

– riduzione dei costi di liquidazione;

---

[7] S. LANDINI, *Privacy, rischio informatico e assicurazioni*, in E. TOSI, *Privacy Digitale*, Feltrinelli, Milano, 2019, pp. 347-367. GDPR viene comunque applicato anche alle piccole imprese, ai professionisti, agli enti del terzo settore.

[8] B. COLLIER, J. SKEES, B. BARNETT, *Weather Index Insurance and Climate Change: Opportunities and Challenges in Lower Income Countries*, in *Geneva Pap Risk Insur Issues* Pract 34, 2009, pp. 401-424.

– maggiore possibilità di predeterminazione dei danni e quindi migliore capacità riassicurativa;

– correzione dei problemi di selezione avversa;

– tutti gli assicurati sono soggetti agli stessi termini, condizioni e vincite, il che elimina virtualmente il problema della selezione avversa per gli assicuratori.

2. Migliore mappatura dei rischi e misure preventive.

La copertura assicurativa può svolgere un ruolo rilevante nella mitigazione del rischio. Le esclusioni assicurative sono disposizioni di polizza che escludono la copertura per determinati tipi di eventi. Costituiscono uno strumento importante per introdurre norme di condotta prudenziale per gli assicurati. Ad esempio, i contratti assicurativi di solito prevedono esclusioni che escludono l'indennizzo se l'assicurato sta tentando di recuperare le perdite derivanti da comportamenti illegali o azioni criminali. È importante mappare il rischio comportamentale dell'assicurato al fine di introdurre nel contratto regole di condotta ordinate ad evitare l'evento coperto.

3. Assicurazione sull'intelligenza artificiale e macchine per l'apprendimento.

L'intelligenza artificiale può ridurre gli errori umani ma non può escludere i danni. Si discute su chi potrebbe essere responsabile in caso di danni causati dall'intelligenza artificiale: l'utente, il proprietario, il produttore, il programmatore.

Dal lato dell'assicurazione della responsabilità civile, per mitigare il rischio, è importante migliorare gli algoritmi per ridurre gli errori della macchina e le perdite in caso di azioni dell'IA [9].

La condivisione dei dati sulle richieste di indennizzo può aiutare nei processi di *self learning machine.*

3. Conclusioni

Abbiamo visto l'impatto delle nuove tecnologie nel settore assicurativo: grazie al *data analytics* è possibile effettuare una valutazione del rischio più precisa che permette di individuare il prodotto che meglio soddisfa le ri-

[9] D.C. VLADECK, *Machines Without Principals: Liability Rules and Artificial Intelligence*, in 89 *Washington Law Review*, 2014, p. 130.

chieste del cliente. È anche possibile determinare il livello di assicurabilità riequilibrando l'ordinaria asimmetria informativa nei contratti assicurativi: l'assicuratore solitamente ha meno informazioni del cliente sullo stato del rischio. Per questo motivo il legislatore introduce obblighi informativi a carico del cliente. Grazie ai big data gli assicuratori possono riequilibrare il gap informativo e addirittura ottenere più informazioni di quante ne abbia il cliente sul proprio stato di rischio.

Lato produzione, è possibile costruire contratti assicurativi più "tailor made" che considerino anche strumenti di mitigazione del rischio che il cliente deve adottare per ridurre o prevenire il verificarsi dell'evento, come nel caso delle assicurazioni agricole. La copertura assicurativa diventa così una sorta di ultima istanza laddove il danno si verifica al di fuori delle previsioni nonostante l'adozione delle misure di prevenzione previste dal contratto.

Gli stessi processi di determinazione del danno attraverso polizze parametriche, da un lato rendono più rapido il risarcimento, dall'altro rendono meglio prevedibile e quantificabile il risarcimento in caso di sinistro.

L'incertezza non può essere eliminata, ma può essere ridotta. I contratti assicurativi sono sempre più contratti per la fornitura di servizi di gestione del rischio piuttosto che per la sua copertura. Occorre poi considerare l'impatto dell'uso dell'intelligenza artificiale e di sistemi di open insurance sul rischio cyber per approntare gli opportuni presidi.

La domanda è: sono ancora contratti assicurativi? Forse vale la pena ricordare ciò che disse Ernst Bruck negli anni '30.

Ernst Bruck era figlio di un commerciante. Ha studiato giurisprudenza all'Università di Heidelberg e all'Università di Strasburgo. Nel 1916 gli fu offerta una cattedra presso l'Istituto di Amburgo, dove insegnò scienze assicurative.

Ernst Bruck pose le basi per la cd. "Scuola di Amburgo", che si ritrova nella concezione dei contratti assicurativi e nel diritto dell'intermediazione assicurativa. Bruck ha inoltre fondato la teoria dell'unione di assicurati simili in una comunità di rischio e la teoria dell'assunzione del rischio, che regola gli obblighi dell'assicuratore [10].

[10] Wolfgang Poppelbaum: Bruck, Ernst. In: Franklin Kopitzsch, Dirk Brietzke (Hrsg.): Hamburgische Biografie. Band 2. Christians, Hamburg 2003, ISBN 3-7672-1366-4, S. 70-71; Bruck, Ernst, in: Joseph Walk (Hrsg.): Kurzbiographien zur Geschichte der Juden 1918-1945. Saur, München 1988, ISBN 3-598-10477-4, S. 48.

Andrea Stazi

Open Banking: sistemi, modelli, criticità e opportunità

SOMMARIO: 1. Introduzione. – 2. La prospettiva normativa. – 3. I vantaggi dei sistemi di *Open Banking.* – 4. I modelli di *Open Banking*. – 5. Criticità e opportunità di sviluppo. – 6. Conclusioni.

1. Introduzione

Sin dal principio, l'introduzione dell'*Open Banking* ha costituito una rivoluzione nell'ambito del mercato dei servizi di pagamento e, più in generale, nei sistemi finanziari mondiali, anche grazie alle innovazioni tecnologiche che ne hanno permesso una diffusione sempre più capillare e ai recenti interventi normativi, specialmente europei, in materia.

2. La prospettiva normativa

Lo sviluppo tecnologico sperimentato negli ultimi anni ha stimolato il consumatore a cercare nuove modalità di pagamento da affiancare alle forme più tradizionali, così come gli istituti bancari, finanziari e di fintech hanno aumentato esponenzialmente la loro offerta di prodotti digitali.

Per delineare una cornice normativa più adeguata al contesto digitale, l'Unione europea ha approvato la direttiva cd. PSD2 (*Payment Services Directive* 2), entrata in vigore il 13 gennaio 2018 allo scopo di contribuire allo sviluppo del settore dei pagamenti digitali.

Tra le principali novità previste dalla PSD2 rientrano alcuni requisiti di sicurezza ai fini dell'accesso ai conti correnti online e dell'autorizzazione ai pagamenti elettronici. Nel dettaglio, sono stati adottati standard informati-

vi e di comunicazione sicuri e aperti e introdotto l'obbligo di autenticazione del cliente, con il quale sono state previste diverse modalità di accesso al sistema, tra cui l'utilizzazione del riconoscimento biometrico.

Attraverso la PSD2, il mercato dei pagamenti digitali europei è cresciuto significativamente negli ultimi anni in termini di transazioni effettuate: dai circa 885 miliardi di euro nel 2017, ai quasi 2.000 miliardi nel 2023 [1].

Tuttavia, a fronte delle evoluzioni e delle innovazioni tecnologiche che di volta in volta investono il settore in parola, anche tale direttiva presenta la necessità di un aggiornamento, in coerenza con i tempi e con le sempre più stringenti aspettative in materia di sicurezza e tutela della privacy. Inoltre, occorre ricordare che gli ultimi sviluppi tecnologici, come l'intelligenza artificiale generativa e la blockchain, non erano pienamente previste e, quindi, disciplinate nella legislazione corrente.

Per tali ragioni, nel mese di giugno del 2023 la Commissione europea ha presentato un nuovo pacchetto di revisione normativa, con lo scopo di porre le basi per la terza direttiva sui Servizi di Pagamento (PSD3 – *Payment Services Directive*) e un nuovo regolamento per i Servizi di Pagamento (PSR – *Payment Services Regulation*).

Attraverso tali iniziative legislative, si intendono unificare all'interno di un'unica disciplina le disposizioni in materia di servizi di pagamento e di moneta elettronica [2]. Tra le priorità della proposta rientrano: i) maggiore trasparenza e comunicazione tra operatori al fine di garantire la sicurezza e la consapevolezza contro frodi informatiche e finanziarie; ii) rafforzamento dei diritti dei consumatori e del loro controllo sui propri dati finanziari; iii) rimozione di ulteriori barriere di mercato e promozione della concorrenza.

Ancora più rilevante per il rafforzamento dell'Open Banking, e, in senso più ampio, per l'intero ecosistema del fintech, poi, è la proposta quadro *Financial Data Access* (FIDA), che, con nuovi obblighi di trasparenza per gli enti finanziari e una maggiore condivisione dei dati tra utenti e istituti fintech, ha l'obiettivo di espandere ulteriormente il mercato attraverso l'offerta di nuovi servizi digitali.

Contestualmente, tale proposta mira a migliorare il regime di responsabilità e di sicurezza in caso di *data breach* di dati finanziari e sensibili, oltre

[1] *Statista Market Insights*, gennaio 2024: https://www.statista.com/outlook/dmo/fintech/digital-payments/europe#transaction-value.

[2] F. CASCINELLI, L. BETTINELLI, *Verso la PSD3 e il nuovo Regolamento sui Servizi di Pagamento*, in *dirittobancario.it*: https://www.dirittobancario.it/art/verso-la-psd3-e-il-nuovo-regolamento-sui-servizi-di-pagamento.

che prevedere un migliore allineamento alle ultime normative in materia di tutela dei dati personali [3].

Tuttavia, la presentazione di queste legislazioni a pochi mesi dalla fine della legislatura europea e dal rinnovo della Commissione causerà un inevitabile prolungamento dei tempi di approvazione.

3. I vantaggi dei sistemi di *Open Banking*

Oggi, attraverso l'*Open Banking*, un titolare di un conto corrente online può liberamente accedervi, visionare lo stato del patrimonio personale o anche effettuare pagamenti attraverso servizi digitali offerti da terze parti autorizzate. Si tratta dei cd. TPPs (*Third Party Providers*) o provider di terze parti [4], che fungono da intermediari tra gli istituti di credito e i correntisti.

I TPPs possono essere di duplice natura, dove i primi sono Account Information Service Providers (AIS), che hanno accesso ai conti online per la fornitura di servizi informativi aggregati sui conti correnti; i secondi i *Payment Initiation Service Providers* (PIS), che hanno accesso ai conti per fornire servizi di pagamento.

In conformità con i principi di sicurezza, riservatezza ed efficienza, attraverso l'utilizzo di API aperte, enti terzi possono utilizzare e fornire servizi utili senza essere partner di un istituto di credito.

In ragione del fatto che la quasi totalità delle banche utilizza le API, il sistema dei pagamenti è cresciuto in modo significativo. Da qui, anche le diverse tipologie di servizi da offrire a una più vasta platea di clienti. Sul punto, avendo a disposizione una consistente mole di dati, gli istituti di credito possono fornire un portafoglio di prodotti e servizi di qualità, nonché ricavare informazioni sui loro stessi clienti, che, allo stesso tempo, a fronte delle maggiori garanzie a loro riservate, esercitano un maggiore controllo sui dati rispetto al passato, potendo prestare il consenso al trattamento dei loro dati personali e patrimoniali o invocare il diritto di revoca.

Tra gli ulteriori benefici, rientra certamente l'allargamento della gamma di prodotti e servizi forniti. Così la clientela è in grado di scegliere le soluzioni più coerenti con i propri bisogni e necessità, con la piena capacità di

---

[3] COMMISSIONE EUROPEA, *Financial data access and payments package*: https://finance.ec.europa.eu/publications/financial-data-access-and-payments-package_en.

[4] GOOGLE, *Real-Time Payments Systems & Third Party Access. A perspective from Google Payments*, 2019: https://static.googleusercontent.com/media/pay.google.com/en//about/business/static/data/gpay-rtp-2019-whitepaper.pdf.

gestirle in totale autonomia. Quindi, l'*Open Banking* ha il potenziale di promuovere l'innovazione, stimolare la concorrenza tra gli ecosistemi digitali e garantire elevati standard di sicurezza[5], in coerenza con il diritto dei consumatori e le disposizioni in materia di tutela dei dati personali. Nei Paesi in cui è stato implementato, l'*Open Banking* sta guidando l'offerta di prodotti e servizi innovativi, che consentono una scelta crescente e garantiscono le migliori soluzioni per consumatori e piccole imprese.

4. I modelli di *Open Banking*

L'*Open Banking* è presente nei principali mercati in forme diverse. L'Interfaccia Unificata di Pagamento (UPI) in India[6], attraverso cui vengono avviati pagamenti da terze parti (PIS) mediante un'infrastruttura API centralizzata, è stata utilizzata per guidare e orientare la digitalizzazione dei pagamenti e il trasferimento di capitali, ottenendo uno straordinario successo[7].

Quando, nel 2016, l'UPI è stata lanciata in India, ha condotto all'introduzione di una vasta gamma di prodotti e servizi da parte dei fornitori di terze parti. Nel solo 2019 si è registrato un aumento di valore di dieci volte e dei volumi delle transazioni di otto[8]. Si prevede che, entro il 2025, le transazioni digitali in India assumeranno un valore di un trilione di dollari l'anno, con quattro transazioni su cinque effettuate digitalmente[9].

Attualmente, il volume delle transazioni UPI rappresenta il 22% di tutti i pagamenti per un valore equivalente al 10% del PIL indiano[10]. Il numero di banche aderenti al sistema in parola è costantemente cresciuto nel tempo: dagli ultimi dati disponibili ne risultano quasi 500, con una crescita del 35% circa sull'anno scorso in termini di volumi di transazioni effettuate.

---

[5] GOOGLE, *Real-Time Payments Systems & Third Party Access. A perspective from Google Payments*, 2019: https://static.googleusercontent.com/media/pay.google.com/en//about/business/static/data/gpay-rtp-2019-whitepaper.pdf.

[6] JJ GEEWAX, *Design Principles for Third-party Initiation in Real-time Payment Systems*, 2021, https://research.google/pubs/design-principles-for-third-party-initiation-in-real-time-payment-systems/.

[7] *Ibidem*.

[8] FIS GLOBAL, *Flavors of Fast Report 2019*.

[9] ACI WORLDWIDE, *AGSTTL and ACI Highlight Key Megatrends Megatrends Shaping India's Digital Payments Revolution*, 2018: https://investor.aciworldwide.com/news-releases/news-release-details/agsttl-and-aci-highlight-key-megatrends-shaping-indias-digital.

[10] STATISTA, *Share of payment systems across India in FY 2019*: https://www.statista.com/statistics/1028157/india-payment-systems-share-by-volume/.

Nell'Unione europea e nel Regno Unito l'*Open Banking* è stato implementato attraverso API decentralizzate, con l'effetto di aver favorito la concorrenza e l'innovazione nel settore dei servizi finanziari nel continente europeo. Ad oggi, oltre 500 entità si sono registrate come provider di terze parti.

Nel continente europeo l'*Open Banking* ha portato a una rapida crescita di questi ultimi e catalizzato un'innovazione che si concentra sul rapporto con i consumatori. Infatti, il 45% degli istituti finanziari ha investito oltre 100 milioni di euro in *Open Banking* e il 44% degli *executives* ha fatto sapere che la *customer experience* rappresenta il principale motore per gli investimenti [11].

5. Criticità e opportunità di sviluppo

L'*Open Banking* ha contribuito a stimolare l'innovazione e la creazione di nuovi servizi destinati a correntisti e imprese. Un ecosistema finanziario moderno e innovativo deve innanzitutto garantire che i regolamenti e la normativa tecnica in materia riflettano le concrete esigenze degli sviluppatori di tecnologie ed evitino di inibire la partecipazione all'ecosistema stesso.

È opportuno promuovere l'accessibilità e la semplificazione dei processi, grazie ai quali si offrono soluzioni che riducono gli ostacoli, sia dal lato degli utenti che utilizzano sistemi di portafoglio digitale, sia da quello degli altri sviluppatori che intendono connettersi all'infrastruttura comune.

Occorre anche fare riferimento a quattro importanti aree critiche, su cui è opportuno che banche centrali, autorità di regolamentazione e operatori del mercato concentrino i loro sforzi.

La prima area critica riguarda l'ambito API. Avendo un impatto diretto sul grado di innovazione e di concorrenza nell'ecosistema, è opportuno implementare sia i servizi di informazioni sul conto (AIS) sia i servizi di ordine di pagamento (PIS) sin dall'inizio. Attraverso tale integrazione, si contribuisce a estendere ulteriormente l'offerta di servizi e la partecipazione degli operatori, nonché accrescere l'innovazione e la concorrenza nell'ecosistema finanziario stesso.

L'ambito di applicazione degli AIS dovrebbe consentire alle terze parti di fornire servizi finanziari sulla base di una visione completa dell'attività finanziaria quotidiana degli utenti, includendo almeno i conti correnti, i

[11] TINK, *The investments and returns of Open Banking*, 2020: https://resources.tink.com/hubfs/05%20Resources/Tink%20survey%20report%20-%20The%20investments%20and%20returns%20of%20open%20banking.pdf.

conti di risparmio e le carte di credito. Per quanto riguarda i dati e la loro disponibilità, dovrebbero almeno corrispondere a quanto risulta accessibile tramite sito web e applicazione mobile del fornitore di servizi finanziari o tramite soluzioni basate sullo *scraping* dello schermo dell'operatore.

Di rilievo anche il tema dell'infrastruttura API. A fronte dell'impatto diretto sul costo di adesione all'ecosistema dell'*Open Banking* sostenuto dai nuovi fornitori e incidendo, quindi, sul grado di concorrenza e di innovazione dello stesso, occorre adottare un sistema centralizzato al fine di minimizzare la frammentazione dell'implementazione e dei costi associati, fenomeno tipico dei modelli decentralizzati.

Tale approccio promuove la parità di accesso degli operatori finanziari e alle terze parti di tutte le dimensioni ai sistemi di pagamento in tempo reale. Inoltre, garantisce maggiore trasparenza e un ulteriore controllo sul fronte della *compliance* e delle prestazioni delle API, oltre che una più rapida identificazione e correzione dei bug.

Anche se un modello centralizzato richiede un ente indipendente deputato allo sviluppo dell'infrastruttura e alla verifica della conformità allo standard, è stato provato che i benefici di lungo termine superano i costi, in ragione del fatto che anche le giurisdizioni che hanno adottato modelli decentralizzati necessitano di un'entità indipendente che governi l'accesso all'infrastruttura dei pagamenti e fissi gli standard API.

Di pari importanza è il tema dell'autenticazione, che riguarda la facilità con cui gli utenti accedono ai sistemi di *Open Banking*. La progettazione dei sistemi di autenticazione dovrebbe essere innovativa e caratterizzata da elevati standard di sicurezza [12]. Per questo motivo è auspicabile un modello in cui le terze parti gestiscano il consenso dell'utente direttamente attraverso le loro interfacce.

Infine, è opportuno che, nell'ambito del modello commerciale, sussistano gli adeguati incentivi finanziari per incoraggiare l'adozione, l'investimento e il mantenimento delle migliori pratiche da parte di tutti gli operatori del mercato, nonché che si prosegua nell'attività di investimento in infrastrutture critiche. In presenza di tali condizioni, sarà possibile realizzare lo sviluppo di nuovi strumenti di pagamento alternativi. A tale approccio appare necessario che si associno riduzioni sulle commissioni per le microtransazioni e le PMI. Mentre, sul fronte della sicurezza, sarebbero opportuni standard chiari nell'ambito della risoluzione delle controversie tra operatori e utenti e in caso di frodi.

---

[12] THE WORLD BANK GROUP, *G20 Digital Identity Onboarding*, 2018, https://www.gpfi.org/sites/gpfi/files/documents/G20_Digital_Identity_Onboarding.pdf.

6. Conclusioni

L'*Open Banking* ha rappresentato una frontiera che ha rivoluzionato l'attività bancaria e finanziaria, anche a seguito della crisi del 2008, a partire dalla quale la fiducia da parte dei correntisti verso istituti di credito e istituzioni finanziarie si era sensibilmente ridotta.

In futuro, dovrebbero essere introdotti ulteriori incentivi per proseguire nel percorso di sviluppo del mercato, mantenendo gli standard di sicurezza delle infrastrutture, favorendo l'ingresso di nuovi concorrenti e garantendo un accesso sempre più ampio agli utenti.

Al contempo, le Autorità di vigilanza saranno fondamentali nel perseguire, da una parte, la tutela del patrimonio informativo dei correntisti, e, dall'altra, promuovere l'innovazione e la concorrenza.

Filippo Annunziata

Open Finance e cripto-attività

SOMMARIO: 1. Introduzione; i punti di contatto tra *Open Finance* e cripto-attività. – 2. La decentralizzazione: problemi strutturali e prime risposte. – 3. L'intervento legislativo nell'Unione Europea per le cripto-attività. – 3.1. MiCAR e normative preesistenti. – 4. Il difficile rapporto tra MiCAR e la De-Fi. – 5. Cenni alle risposte regolatorie negli Stati Uniti. – 6. Quali regole per la De-Fi? Il Rapporto IOSCO. – 7. Conclusione.

1. Introduzione; i punti di contatto tra *Open Finance* e cripto-attività

A prima vista cripto-attività e *Open Finance* possono sembrare fenomeni che non hanno molto in comune. Mentre le prime hanno a che fare con le tecnologie a registro distribuito, il secondo fenomeno – seppur variamente definito, in mancanza di una precisa nozione legislativa – guarda, in via prevalente, ai meccanismi di condivisione e distribuzione dei dati, per migliorare l'efficienza nei processi di fornitura dei servizi, rendendoli, al contempo, più accessibili e meno onerosi.

Tuttavia, cripto-attività e *Open Finance* hanno punti di contatto. Quello più significativo è rappresentato dal ricorso alle *Application Program Interface* (API), strumenti che consentono ad una data applicazione di accedere a funzionalità e a dati di altre applicazioni, o più in generale, di altri servizi digitali. Una API accessibile a chiunque è detta "aperta" e, nel gergo del settore, viene definita appunto *Open* API: essa rappresenta, ad oggi, un significativo punto di sviluppo di sistemi di dati condivisibili e utilizzabili attraverso una molteplicità di applicazioni e servizi.

Negli ultimi tempi, il fenomeno delle API è cresciuto notevolmente, anche in virtù delle disposizioni introdotte, nell'Unione europea, dalla PSD2.

In base a quest'ultima, gli intermediari devono rendere obbligatoriamente le API accessibili anche ad attori esterni: l'obbligo riguarda la condivisione di alcuni dati, tipicamente le informazioni sui conti e la possibilità di disporre pagamenti. I servizi di *Open* API che la disciplina richiede di rendere accessibili sono fondamentalmente di tre tipi: (i) *Account Information*, utili per accedere a conti correnti tramite applicazioni diverse da quelle bancarie; (ii) *Payment Initiation*, al fine di disporre ordini di pagamento dal conto corrente di un utente, utilizzando altre applicazioni; (iii) *Funds Checking*, ossia sistemi che consentono, tramite TPP (*Third Party Payment Services Provider*) di verificare la disponibilità di fondi sul conto corrente di un utente acceso presso un altro istituto, e di finalizzare un pagamento. Così come le API dell'*Open Banking* consentono agli sviluppatori di accedere ai dati finanziari, le API delle cripto-attività permettono agli sviluppatori di accedere ai dati della *blockchain* e di integrarli nelle loro applicazioni. Ciò apre una serie di possibilità per gli sviluppatori che vogliono creare servizi e prodotti finanziari innovativi sfruttando la tecnologia *blockchain*.

Crittografia e *Open Finance* si intersecano anche nel campo della sicurezza. Entrambi i fenomeni si basano su misure di sicurezza avanzate per proteggere i dati degli utenti e prevenire le frodi. Nell'*Open Finance*, per proteggere i dati finanziari vengono impiegate misure di sicurezza come l'autenticazione a due fattori e la crittografia. Nel caso delle cripto-attività, la tecnologia *blockchain* fornisce un elevato livello di sicurezza, in quanto tutte le transazioni sono registrate su un sistema decentralizzato e non modificabile *ex post*.

L'*Open Finance* può anche contribuire a ricondurre il fenomeno delle cripto-attività, in particolare quelle che assolvono a funzioni di pagamento, nell'alveo dei sistemi finanziari tradizionali. Questo, oltre a rendere più agevole l'utilizzo delle cripto-attività, tende a "normalizzarle" nel contesto finanziario, in specie in un momento (come quello attuale) in cui i legislatori di molti sistemi, in primis quello europeo, stanno introducendo le prime, robuste discipline per regolare e vigilare sulle cripto-attività stesse. L'integrazione tra *Open Finance* e cripto-attività può rendere più facili le transazioni tra cripto-attività e valute ufficiali: attraverso le API si può immaginare, ad esempio, di collegare portafogli di cripto-attività con conti bancari o di pagamento, e trasferire più agevolmente fondi tra i due, senza soluzione di continuità.

Sul piano più concettuale, cripto-attività e *Open Finance* pongono poi, entrambe, l'accento sul controllo dei propri dati, specificamente quelli finanziari (anche se, ovviamente, il tema non si esaurisce certo nel contesto del mercato finanziario, ma tocca questioni ben più vaste, sino a quelle che

attengono alla c.d. "identità digitale" delle persone e finanche ai diritti fondamentali). Con l'*Open Banking*, gli utenti possono concedere a sviluppatori terzi l'accesso ai loro dati finanziari, ma solo se decidono di farlo. Similarmente, con le criptovalute, gli individui hanno il pieno controllo sui loro beni digitali e possono scegliere di condividerli, o meno, con altri.

Le cripto-attività utilizzano l'*Open Banking* per consentire nuove forme di pagamento, prestito e investimento, ad esempio con le *stablecoin* (o, per utilizzare la nomenclatura del legislatore europeo, con gli *asset referenced tokens* – ART – o gli *e-money tokens* – EMT). Per utilizzare le *stablecoin*, gli utenti devono essere in grado di convertire la loro valuta ufficiale in token di pagamento. Utilizzando le API bancarie aperte, i fornitori di *stablecoin* possono consentire agli utenti di trasferire fondi dal loro conto bancario al portafoglio di *stablecoin*.

Un altro caso di utilizzo dell'*Open Finance* nel contesto delle cripto-attività riguarda i prestiti: molte piattaforme che negoziano cripto-attività consentono agli utenti di chiedere, o concedere in prestito, cripto-attività. Per poter prestare questi servizi, le piattaforme devono essere in grado di verificare l'identità e l'affidabilità creditizia dell'utente. È in questo contesto che rilevano le API bancarie aperte: accedendo ai dati bancari e finanziari dell'utente, detenuti presso altri intermediari, la piattaforma di prestito può valutare la sua affidabilità creditizia e offrirgli un prestito.

2. La decentralizzazione: problemi strutturali e prime risposte

Se quanto precede evoca alcuni punti di contatto tra i due fenomeni più sul piano tecnico ed applicativo, cripto-attività e *Open Finance* condividono un medesimo messaggio di fondo, una stessa filosofia che guarda alla decentralizzazione, alla diffusione dei dati e, dunque, alla costruzione di un sistema finanziario più aperto e condiviso.

Questo messaggio è stato, in vero, sin dalle origini alla base dello sviluppo delle cripto-attività. La nascita del fenomeno è notoriamente ricondotta all'affacciarsi sul mercato di bitcoin nel 2009, che, all'epoca, si presentava come un progetto non soltanto innovativo dal punto di vista tecnologico, ma anche sul piano delle finalità e degli obiettivi: nel *white paper* pubblicato dal promotore di bitcoin – l'ormai mitico Satoshi Nakamoto, di incerte origini e, forse, anche esistenza [1] – esso venne rappresentato come

[1] Non è stato, infatti, possibile stabilire chi fosse Nakamoto, se tale personaggio esistesse effetti-

uno strumento avente l'obiettivo principale di disintermediare le valute ufficiali, in quanto emesso e gestito in via del tutto decentralizzata. Da qui, anche, la tendenza ad esaurire l'intero fenomeno in quello delle c.d. "cripto-valute" o "*crypto-currencies*", secondo una prospettiva ormai del tutto sfuocata, posto che il fenomeno stesso non si esaurisce certo nell'ambito dei mezzi o strumenti di pagamento "tokenizzati" [2].

Sullo sfondo di un messaggio ideologico di democratizzazione del mondo della finanza globale, l'idea fu che le cripto-attività – non soltanto bitcoin, ma tutte quelle create emulando quello schema – avrebbero liberato il mercato finanziario dall'onere e dal peso dell'intermediazione, dando luogo a mercati assai più efficienti di quelli tradizionali, meno costosi, e senza Autorità centrali. Siffatta idea, accompagnata dalle teorizzazioni in materia di *smart contract* ai quali, inizialmente, si affidava la missione "taumaturgica" di sostituire il codice informatico al diritto applicabile, preconizzava, in sostanza, un mondo finanziario globale, libero, capace di autoregolarsi e di raggiungere livelli elevatissimi di efficienza, in virtù dell'impiego delle tecnologie *Distributed Ledger*: una finanza, per l'appunto, decentralizzata (*Decentralised Finance* – DeFi).

Nonostante le utopie iniziali, sono però ben presto emersi rischi e problemi nient'affatto lontani da quelli che connotano la più tradizionale industria finanziaria: opacità informativa; esigenze di tutela delle controparti più deboli; asimmetrie; inefficienza dei mercati e rischi di manipolazione; rischi di instabilità finanziaria, finanche a livello sistemico; frodi e, come noto, rischi elevati di riciclaggio [3]. I clamorosi *default* del *crypto win-*

---

vamente, se fossero un gruppo di soggetti tra loro collegati, o comunque ricavare informazioni precise sull'identità degli sviluppatori del progetto bitcoin. Sul rapporto tra tecnologia ed evoluzione degli strumenti monetari v. R. MOTRONI, *I pagamenti non monetari nella finanza digitale europea. La prospettiva italiana*, Cacucci, Bari, 2023; F. MATTASSOGLIO, *Moneta e tecnologia. Come intelligenza artificiale e DLT stanno trasformando lo strumento monetario*, Giappichelli, Torino, 2022.

[2] Il termine "criptovaluta" in uno con i suoi sinonimi è tuttavia duro a morire, ed è ancora utilizzato in letteratura, anche in contributi recenti: v. l'ampia prospettiva storico economica di M. LORENZINI, M. ZULBERTI, C. IMBROSCIANO (a cura di), *Criptovalute. Profili storico-economici e giuridici*, Giappichelli, Torino, 2023; cui adde M. PASSARETTA, *La valuta virtuale nel sistema dei servizi di pagamento e di investimento*, Giappichelli, Torino, 2023.

[3] Anche su questo punto il legislatore UE è intervenuto, mediante l'approvazione di un apposito regolamento collegato a MiCAR: regolamento (UE) 2023/1113 del Parlamento europeo e del Consiglio del 31 maggio 2023 riguardante i dati informativi che accompagnano i trasferimenti di fondi e determinate cripto-attività e che modifica la direttiva (UE) 2015/849. Non è possibile, stanti i limiti di questo contributo, dare peraltro conto né dell'amplissima letteratura sul punto, né dei vari regimi, sia nazionali sia UE, collegati al profilo del rapporto tra cripto-attività e antiriciclaggio. Sulla progressiva "finanziarizzazione" della disciplina delle cripto-attività v. D.W. AR-

ter[4], culminati nel fallimento dell'*exchange* "FTX"[5], sono stati soltanto gli esempi più evidenti di una lunga serie di fenomeni patologici che, da subito, avrebbero dovuto sollecitare una risposta regolatoria sia in Europa, sia altrove.

Le clamorose, ma non del tutto inattese, crisi registrate a cavallo tra il 2021 e il 2023 hanno, così, chiaramente mostrato la fragilità di un sistema che – in netto contrasto con la declamata autonomia della tecnologia (il noto adagio, coniato da Lawrence Lessing nel 1999, *code is law*[6]) e con l'asserita capacità dei mercati di autoregolarsi (un abbaglio ricorrente nelle dinamiche storiche dei mercati finanziari) – non è in grado di svilupparsi in modo ordinato in assenza di uno strutturato, robusto quadro regolatorio e di vigilanza. Si è dunque coniata l'espressione di "*crypto winter*"[7], per riferirsi ad una fase particolarmente buia dello sviluppo di questi mercati, a fronte della quale l'unica possibile soluzione, ormai, è una risposta legislativa quanto più decisa e coordinata, possibilmente anche a livello transnazionale.

Con il regolamento sul mercato delle cripto-attività (*Markets in Crypto-Assets Regulation*[8] – MiCAR o, anche MiCA secondo l'acronimo ormai diffusissimo in letteratura)[9], l'Europa si è mossa in anticipo rispetto ad al-

---

NER, D.A. ZETZSCHE, R.P. BUCKLEY, J.M. KIRKWOOD, *The Financialisation of Crypto*, in *EBI Working Paper*, n. 148, reperibile in https://ebi-europa.eu/publications/working-paper-series/.

[4] AA.VV., *Making it through the (crypto) winter: facts, figures and policy issues*, in *Quaderno Banca d'Italia, Mercati, infrastrutture e sistemi di pagamento*, n. 23/2003, reperibile in https://www.bancaditalia.it/pubblicazioni/mercati-infrastrutture-e-sistemi-di-pagamento/approfondimenti/2023-038/N.38-MISP.pdf.

[5] F. FUBINI, *Crollo di Ftx, è la fine delle criptovalute?*, in *Corriere della Sera*, 18 novembre 2022, reperibile in https://www.corriere.it/economia/finanza/22_novembre_18/crollo-ftx-fine-criptovalute-8f48feb2-6716-11ed-b05a-06c1012dfe21.shtml.

[6] L. LESSIG, *Code: And Other Laws of Cyberspace, Version 2.0*, Basic Books, New York, 2006.

[7] D.A. ZETZSCHE, R. BUCKLEY, D. ARNER, M. VAN EK, *Remaining Regulatory Challenges in Digital Finance and Crypto-Assets after MiCA*, in *Committee on Economic and Monetary Affairs* (ECON), Paper No. 23-27, 2023, reperibile in https://ssrn.com/abstract=4487516.

[8] Regolamento UE 2023/1114 del Parlamento europeo e del Consiglio, del 31 maggio 2023, relativo ai mercati delle cripto-attività e che modifica i regolamenti (UE) n. 1093/2010 e (UE) n. 1095/2010 e le direttive 2013/36/UE e (UE) 2019/1937.

[9] Per una prima disamina, v. M. LEHMANN, *MiCAR – Gold Standard or Regulatory Poison for the Crypto Industry? (January 12, 2024)*, in *European Banking Institute Working Paper Series 160*, reperibile in https://ssrn.com/abstract=4692743. Altri spunti, anche se meno puntuali, in P. MAUME, *The Regulation on Markets in Crypto-Assets (MiCAR): Landmark Codification, or First Step of Many, or Both?*, in *ECFR*, 2023, p. 265; T. VAN DER LINDEN, T. SHIRAZI, *Markets in crypto-assets regulation: Does it provide legal certainty and increase adoption of crypto-assets?*, in *Financial Innovation*, 2023, p. 22; R. LENER, *Criptoattività e cripto valute alla luce degli ultimi orientamenti comunitari*, in *Giur. comm*., 2023, I, p. 376; S. L. FURNARI, R.A. LENER, *Contributo alla Qualificazione Giuridica dell'Offerta al Pubblico di Utility Token (Anche) alla Luce della Proposta di regola-*

tri sistemi. Essa costituisce, ad oggi, l'unica area geografica multi-Stato dotata di una disciplina uniforme (in quanto direttamente applicabile negli Stati membri) di questi nuovi fenomeni.

In ciò, si legge, da un lato, l'attenzione e la cura che le Istituzioni europee hanno voluto dedicare ad un fenomeno che rischia di incidere seriamente sugli interessi, e dunque sulle tutele, di utenti e consumatori – definiti, nel MiCAR, con il termine "detentori al dettaglio" [10] – nonché sulla stessa stabilità finanziaria; dall'altro, l'intendimento dell'Unione di divenire lo *standard-setter* delle regole sulle cripto-attività a livello globale: insomma, un *Brussels effect* nel settore di cui si discute.

Con la nuova disciplina – destinata ad esplicare i propri effetti nel 2025 – viene così a determinarsi una scissione tra il profilo tecnologico, e quello regolatorio e di mercato: la tecnologia che sottende le cripto-attività che rientrano nell'ambito di applicazione del regolamento è, per l'appunto, di tipo *distribuito*, anche se con diversi possibili gradi o livelli, dovendosi quantomeno distinguere tra reti *permissioned* o *permissionless*. Tuttavia, l'approccio regolatorio e di vigilanza adotta, nei riguardi delle cripto-attività, approcci e metodi tipici della regolazione finanziaria tradizionale, improntata a modelli centralizzati. Ciò, come avremo modo di osservare è dovuto al fatto che ancora non è chiaro come si possa, eventualmente, affrontare il nodo di sottoporre a regolamentazione e vigilanza prodotti e/o servizi svolti in modo effettivamente, e compiutamente, decentralizzati, nel contesto dei quali difetta un centro di imputazione di interessi ben identificabili.

---

mento europeo sulle Cripto-Attività, in *Bocconi Legal Papers* 63, 2023; N. CIOCCA, *Servizi di custodia, negoziazione e regolamento di cripto-attività*, in *ODCC*, 2022, p. 79; S. CAPACCIOLI, M.T. GIORDANO (a cura di), *Crypto-asset: Regolamento MiCA e DLT Pilot Regime. Analisi ragionata su token, stablecoin, CASP*, Giuffrè, Milano, 2023, p. 193 ss.; T. TOMCZAK, *Crypto-assets and crypto-assets' subcategories under MiCA Regulation*, in *Capital Markets Law Journal*, 2022, p. 365; C. GORTSOS, *The Commission's 2020 Proposal for a Markets in Crypto-Assets Regulation ('MiCAR'): A Brief Introductory Overview (May 7, 2021)*, reperibile in https://ssrn.com/abstract=3842824. Più specifico, e dedicato ai profili di accesso all'attività, M.T. PARACAMPO, *I prestatori di servizi su cripto-attività. Tra mifidizzazione della MICA e tokenizzazione della Mifid*, Giappichelli, Torino, 2023. Sulle "mancanze" del regolamento, D.A. ZETZSCHE et al. (nt. 7).

[10] Ai sensi dell'art. 3, par. 1, n. 37, per "detentore al dettaglio", si intende – secondo una definizione modellata su quella di "consumatore" – "qualsiasi persona fisica che agisce per scopi estranei alla propria attività commerciale, imprenditoriale, artigianale o professionale". Indipendentemente dalle definizioni, la nozione del MiCAR pone delicati problemi di coordinamento con la disciplina a tutela dei consumatori: v. M. MAUGERI, *Proposta di Regolamento MiCA (Markets in Crypto-Assets) e tutela del consumatore nella commercializzazione a distanza*, in *ODCC*, 2022, p. 229 ss.; F. DELFINI, *Le discipline a tutela del consumatore e il coordinamento con la proposta di Regolamento MiCA*, *ibid*., p. 269 ss.; P. SIRENA, *La tutela del consumatore nella commercializzazione a distanza di cripto-attività*, *ibid*., p. 315.

Queste ambiguità e difficoltà sono ben riflesse nel recente regolamento UE n. 1114/2023 sulle cripto-attività (il c.d. *Markets in Crypto-Assets Regulation* – MiCA, approvato il 31 maggio 2023).

3. L'intervento legislativo nell'Unione Europea per le cripto-attività

L'idea di muovere verso una disciplina europea del mercato delle cripto-attività si affaccia in Europa, per la prima volta, nell'ambito dell'ambizioso progetto della Commissione EU sulla *Digital Finance Strategy* [11]. In quel contesto, il 24 settembre del 2020, la Commissione formula la prima proposta del regolamento sulle cripto-attività [12] alla quale si collegano due altri regolamenti apparentemente minori, ma altrettanto importanti: da un lato, la proposta satellite "*Pilot-Regime for DLT-based Market Infrastructures*", destinata al mercato di capitali che intende utilizzare soluzioni basate sulla *Distributed Ledger Technology*; dall'altro, il "*Digital Operational Resilience Act*" (cd. "DORA") in materia di "robustezza" operativa digitale per il settore finanziario [13]. Dopo un articolato dibattito, e – nel-

[11] Si veda https://finance.ec.europa.eu/publications/digital-finance-package_en#digital.

[12] Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive 2019/1937/UE" COM(2020)593 final, sulla quale v. D. ZETZSCHE, F. ANNUNZIATA, D.W. ARNER, R.P. BUCKLEY, *The Markets in Crypto-Assets regulation (MiCA) and the EU digital finance strategy*, in *Capital Markets Law Journal*, 16, 2021, p. 206 ss.

[13] Regolamento (UE) 2022/858 del Parlamento europeo e del Consiglio del 30 maggio 2022 relativo a un regime pilota per le infrastrutture di mercato basate sulla tecnologia a registro distribuito e che modifica i regolamenti (UE) n. 600/2014 e (UE) n. 909/2014 e la direttiva 2014/65/UE; regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio del 14 dicembre 2022 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, (UE) n. 909/2014 e (UE) 2016/1011. Per prime considerazioni, P. MAUME, F. KESPER, *The EU DLT Pilot Regime for Digital Assets*, in *European Company Law Journal*, 2023, 1; F. ANNUNZIATA, A.C. CHISARI, P.R. AMENDOLA, *DLT-Based Trading Venues and EU Capital Markets Legislation: State of the Art and Perspectives Under the DLT Pilot Regime*, in *Italian Law Journal*, 2023, p. 141; A. GENOVESE, *La circolazione dei valori mobiliari su blockchain*, in *Riv. dir. comm.*, 2023, p. 197 ss.; D.A. ZETZSCHE, J. WOXHOLTH, *The DLT sandbox under the Pilot-Regulation*, in 17 *Capital Markets Law Journal*, 17, 2022, p. 212 ss.; J. MCCARTHY, *A Distributed ledger technology and financial market infrastructures: an EU pilot regulatory regime*, *ibid.*, p. 288 ss.; A. TINA, *Mercati centralizzati, decentralizzati. Prospettive di inquadramento della DeFi nell'attuale orizzonte MiFID*, in *ODCC*, 2022, p. 41 ss.; F. MATTASOGLIO, *Le proposte europee in tema di crypto-assets e DLT. Prime prove di regolazione del mondo crypto o tentativo di tokenizzazione del mercato finanziario (ignorando bitcoin)?*, in *Riv. dir. banc.*, 2021, p. 413.

le more – l'approvazione dei regolamenti DLT Pilot Regime e DORA, in un contesto agitato dai clamorosi fallimenti di mercato a livello globale, dalla pandemia, da uno sfondo geopolitico a dir poco instabile, a tratti drammatico, il testo definitivo del regolamento viene pubblicato in Gazzetta Ufficiale il 9 giugno 2023. Esso, come già detto, è destinato ad esplicare i propri effetti (con alcune, limitate – ma importanti – eccezioni) a decorrere dal 30 dicembre 2024.

Le ragioni che giustificano questo massiccio intervento regolatorio da parte dell'Unione europea sono tutte ben descritte ed esposte nei Considerando, e spesso riprese nel corpo del testo del MiCAR: certezza del diritto, supporto all'innovazione, protezione degli utenti, integrità del mercato, stabilità finanziaria, mitigazione dei rischi anche sotto il profilo dei canali di trasmissione della politica monetaria e della sovranità monetaria. Un mix, insomma, di obiettivi macro e micro-prudenziali, ma anche di efficienza informativa dei mercati e di tutela degli utenti, in uno con l'obiettivo di non precludere lo sviluppo di una tecnologia che, invece, può essere foriera di sviluppi in senso positivo: aspetti, questi, che, in misura variabile, connotano anche alcuni interessanti, ma ormai transeunti, esperimenti nazionali in Europa: *inter alia* Malta, Francia, Singapore, Lussemburgo, Germania [14].

Come già ben messo in luce in numerosi contributi, il regolamento MiCA non è certo scevro da mancanze e da incertezze: vi si ritrovano le tipiche *grandi lacune* [15] che spesso connotano i testi che compongono la galassia della legislazione finanziaria dell'Unione; si leggono bene i compromessi, le scelte di breve periodo, la tendenza a rinviare, più in là, la definitiva soluzione di grandi questioni (come il confine tra il regolamento e la finanza decentralizzata). Tutto ciò non toglie il fatto che il MiCAR costituisce, ad oggi, la più compiuta, articolata e completa disciplina al mondo del

[14] Le discipline nazionali, introdotte in ordine sparso in alcuni ordinamenti UE, sono destinate a scomparire con la piena in vigore del MiCAR. Anche in Italia la Consob aveva immaginato, prima di MiCAR, un qualche intervento regolatorio, anche se poi il progetto fu di fatto abbandonato: cfr. su questi profili P. CARRIÈRE, *Possibili approcci regolatori al fenomeno dei crypto-asset; note a margine del documento di consultazione della Consob*, in *Dir. banc.*, Approfondimenti, maggio 2019. Per un altro, timido intervento a livello italiano (anch'esso destinato al tramonto, per effetto di MiCAR), volto quantomeno a realizzare un censimento degli operatori in cripto-attività, v. il d.m. 13 gennaio 2022, che introduce l'obbligo di iscrizione degli operatori del settore in un apposito registro tenuto dall'OAM.

[15] L'espressione è presa in prestito dal pensiero di Gino Gorla (1906-1992) che la utilizzò per segnalare la carenza di riflessioni e studi sul "dialogo" tra i Tribunali Supremi e le professioni legali, nei sistemi e ordinamenti della Storia del diritto europeo. V. a riguardo, anche per una sintesi, M. D'ALBERTI, *Comparazione giuridica tra storia e esperienza*, in *Riv. it. sc. giur.*, 2019, p. 67.

mercato delle cripto-attività, che dà luogo a un sistema assai più avanzato degli approcci incerti e casistici che connotano gli stessi mercati dai quali ha preso avvio il fenomeno, a partire dagli Stati Uniti, dove si pretende ancora di governare il fenomeno attraverso una forma di balbuziente *regulation by enforcement*.

3.1. MiCAR e normative preesistenti

Sia consentita una notazione preliminare, anche al fine di sgombrare il campo da equivoci. Il Regolamento *non* è in grado di disciplinare *tutti* i profili che gravitano attorno all'universo delle cripto-attività e, men che meno, delle nuove tecnologie.

In primo luogo, nonostante quanto, a prima vista, si potrebbe ritenere, il Regolamento MiCA *non* disciplina le cripto-attività *in quanto tali*, ma soltanto il loro *mercato*, ossia il fenomeno che consiste nella loro offerta, negoziazione e scambio, e nella prestazione dei servizi connessi a quanto precede [16]. Neppure si ritrova, nel MiCAR, una disciplina degli *smart contract*, che pure costituiscono lo strumento che consente la conclusione delle transazioni sulla DLT e che costituisce, per così dire, la *linfa vitale* delle contrattazioni su questi sistemi [17].

---

[16] Sulla qualificazione civilistica dei *token*, e sul tema, strettamente connesso, del rapporto tra cripto-attività e diritto societario, v. AA.VV., *Tokenizzazione di azioni e azioni token*, Consob, Quaderni di ricerca giuridica, n. 25, 2023, reperibile in https://www.consob.it/documents/1912911/1916538/qg25.pdf/0cc70f0f-49ac-7ee4-f8cc-c07f7affbf35; S. OMLOR, *Blockchain-Token im Zivilrecht*, in *Juristische Ausbildung*, 2023, p. 661 ss. Relativamente a Bitcoin, che presenta tratti del tutto peculiari, M. LEHMANN, *Who Owns Bitcoin: Private Law Facing the Blockchain, in Minnesota Journal of Law*, in *Science & Technology*, 21, 2020, p. 93 ss.

[17] Sul tema, *ex multis*, F. BASSAN, M. RABITTI, *Recenti evoluzioni dei contratti sulla blockchain. Dagli smart legal contracts ai 'contracts on chain'*, in *Riv. dir. banc.*, 2023, p. 561 ss.; G. GRECO, *Gli smart contract nel settore bancario e finanziario*, in R. Giordano *et al.* (a cura di), *Il diritto nell'era digitale*, Giuffrè, Milano, 2022, p. 189; A. STAZI, *Smart Contracts and Comparative Law. A Western Perspective*, Springer, New York, 2021; M. MAUGERI, *Smart Contracts e disciplina dei contratti*, il Mulino, Bologna, 2021; P. GALLO, *DLT, Blockchain e Smart Contract*, in M. CIAN, C. SANDEI (a cura di), *Diritto del Fintech*, Cedam, Milano, 2020, p. 146; S.A. CERRATO, *Appunti su smart contract e diritto dei contratti*, in *BBTC*, 2020, p. 370; G. LEMME, *Gli «smart contract» e le tre leggi della robotica*, in *AGE*, 2019, pp. 129-152; I. DI SARZANA, F.M. NICOTRA, *Diritto della Blockchain, Intelligenza Artificiale e IoT*, Ipsoa, Milano, 2018, p. 90; M. RASKIN, *The Law and Legality of Smart Contracts*, in *Georgetown Law Technology Review*, 1:304, 2017, p. 306, reperibile in https://ssrn.com/abstract=2959166; K. WERBACH, N. CORNELL, *Contracts Ex Machina*, in *Duke Law Journal*, 67:313, 2017, p. 102, reperibile in https://ssrn.com/abstract=2936294.

La disciplina di tutti questi aspetti è, dunque, rimessa ai legislatori nazionali, essendo, peraltro, strettamente connessa a profili che esulano per lo più dalle competenze del legislatore europeo, primo fra tutti il diritto privato, dei contratti, il diritto societario, o della crisi d'impresa, a tacer d'altri. In questo senso, il MiCAR costituisce un (quasi perfetto) omologo, nell'ambito di cui si discute, della disciplina MiFID e, non a caso, mostra di avere affinità con quest'ultima nel suo stesso titolo (e acronimo): entrambe, in vero, guardano direttamente alla disciplina non già degli *oggetti* ma dei relativi *mercati*. In definitiva, così come non ci si aspetta di rinvenire, nella MiFID, una disciplina dei singoli strumenti finanziari – *in primis*, azioni, obbligazioni, strumenti finanziari partecipativi, quote di OICR, quote di emissione, derivati [18], etc. – allo stesso modo non si rinviene nel MiCAR una disciplina delle cripto-attività in quanto tali. Come già nel contesto di MiFID, questo approccio rischia, naturalmente, di condurre a disallineamenti e frammentazioni tra le legislazioni nazionali, accentuando anche – stante la natura globale del fenomeno delle cripto-attività – i problemi di diritto internazionale privato [19]: si tratta, tuttavia, di limiti che, in verità, tagliano trasversalmente pressoché tutti gli ambiti regolazione finanziaria dell'Unione, e che non devono stupire, anche se è pur doveroso, per l'interprete, segnalare le relative manchevolezze.

Al contempo, il regolamento MiCA costituisce un esperimento di notevole interesse, non soltanto in quanto disciplina un mercato nuovo, di fatto scaturito (prodotto, verrebbe da dire) dalle nuove tecnologie, ma in quanto, nel far ciò, esso fa uso, nelle sue varie aree, del vasto armamentario di concetti, nozioni, approcci e metodi rinvenibili nel contesto dell'intera disciplina finanziaria dell'Unione. A seconda dei diversi ambiti, nel MiCAR si ritrova, così, una sorta di condensato delle principali discipline del diritto finanziario dell'UE, a partire da quella degli enti creditizi, dei prestatori di servizi di investimento, e di molti altri settori. Un vero e proprio esercizio di *cross-sectoral regulation* (seppur precipitato in un uni-

[18] Su queste questioni, in particolare sugli strumenti derivati, v. E. CALLENS, *Derivative Contracts in EU Law: Never Mind the Definition (April 29, 2022)*, in *Journal of Corporate Law Studies*, European Banking Institute Working Paper Series 2022 – no. 121, reperibile in https://ssrn.com/abstract=4096694.

[19] J. DRÖGEMÜLLER, *Blockchain-Netzwerke und Krypto-Token im Internationalen Privatrecht (Deutsches, Europäisches und Vergleichendes Wirtschaftsrecht)*, Nomos, Baden-Baden, 2023; A. BONOMI, M. LEHMANN, *Blockchain and Private International Law*, Brill Publishers (Martinus Nijhoff), Leida, 2023; C. VILLATA, *Il Regolamento (UE) 2023/1114 relativo ai mercati delle crypto-attività: prime note nella prospettiva del diritto internazionale privato*, in *Riv. dir. intern. priv. e proc.*, 2023, p. 745.

co ambito) che non ha eguali nel diritto finanziario UE[20]. Ad esempio, con riguardo alla *emissione* di cripto-attività e alla loro offerta sul mercato, il modello seguito da MiCAR è quello delle offerte al pubblico e della disciplina del prospetto informativo, seppure adattato e semplificato per tener conto di una prassi già consolidata di mercato (il c.d. *white paper*). Per quanto riguarda la disciplina applicabile ai *soggetti che forniscono servizi relativi a cripto-attività*, il modello di riferimento più evidente è, invece, la MiFID, dalla quale vengono importati schemi, nozioni, approcci regolatori e di vigilanza.

Con riferimento alle *piattaforme di scambio*, il modello è, nuovamente MiFID (relativamente ai sistemi di negoziazione), al quale si aggiunge la disciplina degli abusi di mercato prevista nel regolamento sugli abusi di mercato (*Market Abuse Regulation* o MAR) e replicata, con alcune modifiche, nel MiCAR. Infine, con riguardo alle cripto-attività con funzione di *pagamento* (ossia, come si vedrà, gli *asset-referenced token* e gli *e-money token*), il riferimento è (nuovamente) rappresentato dalla disciplina prudenziale degli enti creditizi e della moneta elettronica[21]. Tutti questi approcci ora convergono in un unico testo, talvolta applicandosi anche in via cumulativa, come ad esempio nel caso dei soggetti che emettono sul mercato token di pagamento (ARTs e EMTs) ed offrono i servizi ad essi collegati.

4. Il difficile rapporto tra MiCAR e la De-Fi

Nel contesto testé richiamato, l'impostazione del MiCAR contempla, in sostanza, modelli di servizio e di offerta sul mercato tipicamente incentrati sull'identificazione di uno o più soggetti: offerenti, prestatori di servizi, emittenti, ecc. La tecnologia, dunque, è "aperta", la disciplina è, invece, modellata su impianti tradizionali e centralizzati.

Questa scissione, tra tecnologia, da un lato, e servizi, dall'altro, conduce il MiCA a chiarire, espressamente, che esso non disciplina – *rectius*: non è

---

[20] Ampia è la letteratura che, in generale, si è occupato di cripto-attività e disciplina finanziaria: v., ad esempio, S. JOHNSTONE, *Rethinking the Regulation of Cryptoassets. Cryptographic Consensus Technology and the New Prospect*, Edward Elgar Publishing, Chelthenham-Northampton, 2021, p. 83; P. DE FILIPPI, A. WRIGHT, *Blockchain and the Law. The Rule of Code*, Harvard University Press, Cambridge (MA), 2018.

[21] F. CIRAOLO, *La disciplina degli e-money tokens tra proposta di Regolamento MiCA e normativa sui servizi di pagamento. Problematiche regolatorie e possibili soluzioni*, in *Riv. reg. mer.*, 2022, p. 239 ss.

in grado di disciplinare – i fenomeni [22] che rientrano nell'ambito della vera e propria finanza decentralizzata [23]: la ragione è da individuarsi nel fatto che, in tali contesti [24], non è possibile individuare un soggetto, o eventualmente un insieme di soggetti, che, nella veste di "emittente" o di "prestatori di servizi" possa essere destinatario delle regole appena introdotte [25].

---

[22] Incluse le piattaforme di scambio, ammesso che presentino i tratti della decentralizzazione: tema molto arduo, su cui v. V. MOHAN, *Automated Market Makers and Decentralized Exchanges: a DeFi Primer*, in *Financial Innovation*, 2022, p. 3, reperibile in https://ssrn.com/abstract=3722714; A. CAPPONI, R. JIA, *The Adoption of Blockchain-based Decentralized Exchanges*, 2021, reperibile in https://ssrn.com/abstract=3805095; A. ASPRIS, S. FOLEY, J. SVEC, L. WANG, *Decentralized Exchanges: The 'Wild West' of Cryptocurrency Trading*, in *International Review of Financial Analysis*, 2021. Sui profili di qualificazione A. MINTO, *The Legal Characterization of Crypto Exchange Platforms*, in *22 Global Jurist*, 2022, p. 137 ss., spec. p. 152 ss.

[23] V. da ultimo I.H-Y. CHIU, *The Application of the EU Markets in Crypto-asset Regulation to Decentralised Finance*, in *Journal of International Banking Law and Regulation*, 2023, forthcoming, reperibile in https://ssrn.com/abstract=4599277; I. MAKAROV, A. SCHOAR, *Cryptocurrencies and Decentralized Finance (DeFi), in Brookings Papers on Economic Activity*, 2022. Per un tentativo "istituzionale" di definizione e di inquadramento del fenomeno, v. COMMISSIONE EUROPEA (Directorate-General for Financial Stability, Financial Services and Capital Markets), *Decentralized Finance: information frictions and public policies, Approaching the regulation and supervision of decentralized finance*, reperibile in https://finance.ec.europa.eu/system/files/2022-10/finance-events-221021-report_en.pdf; BANCA D'ITALIA, *Comunicazione in materia di tecnologie decentralizzate nella finanza e cripto-attività*, 2 giugno 2022; AA.VV., *Defi and the Future of Finance*, John Wiley & Sons Inc, Hoboken, 2021. Per ulteriori riferimenti, v. S.L. FURNARI, *La Finanza Decentralizzata. Cripto-attività, protocolli, questioni giuridiche aperte*, Minerva Bancaria, Roma, 2023; E. PRANDIN, *Decentralized Finance: A new challenge for Regulators, Bocconi Legal Papers*, n. 16, 2021, pp. 51-62; S. BOYKEY SIDLEY, S. DINGLE, *Beyond Bitcoin*, Icon Books, Londra, 2022; L. ANKER-SØRENSEN, D. ZETZSCHE, *From Centralized to Decentralized Finance: The Issue of 'Fake-DeFi',* 2021, reperibile in https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3978815; S. ARAMONTE, W. HUANG, A. SCHRIMPF, *DeFi risks and the decentralisation illusion*, in *BIS Quarterly Review*, 2021. Da ultimo sull'argomento si veda il report della BANK FOR INTERNATIONAL SETTLEMENTS, *The crypto ecosystem: key elements and risks*, luglio 2023, p. 9, reperibile in https://www.bis.org/publ/othp72.htm.

[24] Sussistono, infatti, tanti modi di intendere la nozione di "decentralizzazione" e anche diversi livelli e gradi di decentralizzazione: il rapporto tra MiCA e DeFI andrà dunque meglio focalizzato man mano che, da un lato, il mercato evolve e, dall'altro, la nuova disciplina è chiamata a confrontarsi con un numero crescente di casi concreti. V.A. WALCH, *Deconstructing 'Decentralization': Exploring the Core Claim of Crypto Systems*, in *Cryptoassets. Legal, Regulatory, and Monetary Perspectives*, a cura di C. Brummer, Oxford University Press, Oxford, 2019. In un recente rapporto, ESMA ha peraltro registrato, quantomeno in Europa, un grado di sviluppo ancora modesto di modelli di servizio decentralizzati: v. ESMA, *Decentralised Finance in the EU: Developments and Risks*, 11 ottobre 2023, ESMA50-2085271018-3349.

[25] Ciò non toglie che, in alcuni casi, sia possibile ipotizzare la sussistenza, in capo ai gestori delle piattaforme o sistemi decentralizzati, doveri di diligenza e anche di natura fiduciaria verso gli utenti. Il dibattito sul punto è aperto. Si segnala, in proposito, un importante caso, ancora *in fieri* nel Regno Unito, nel quale la Court of Appeal ha ritenuto che sussistono "*realistic argu-*

Manca, dunque, il riferimento che, da sempre, connota l'approccio regolatorio in materia finanziaria, pur sempre rivolto ad un soggetto (o gruppo di soggetti) individuato, al quale indirizzare regolazione, da un lato, e vigilanza, dall'altro. Questa presa di distanza dalla *decentralised finance*, tuttavia, rischia di creare difficoltà là dove, di fatto, porterebbe talune organizzazioni a offrire servizi relativi a cripto-attività sul mercato senza essere autorizzate e per il solo fatto di essere, per l'appunto decentralizzata. A riguardo, il regolamento prevede però una norma di chiusura: l'art. 59, par. 3 dispone che "Ai fini del paragrafo 1, lettera a), altre imprese[26] che non sono persone giuridiche prestano servizi per le cripto-attività se la loro forma giuridica garantisce un livello di tutela degli interessi dei terzi equivalente a quello offerto dalle persone giuridiche nonché se sono soggette a una vigilanza prudenziale equivalente adeguata alla loro forma giuridica". È evidente che la questione, rimessa poi all'azione delle Autorità di vigilanza, si gioca tutta attorno alla nozione di "*undertaking*/impresa" che andrà meglio precisata, sia da parte delle Autorità di supervisione sia, eventualmente, dalle Corti, tenuto conto del concreto grado di effettiva decentralizzazione del fenomeno[27].

5. Cenni alle risposte regolatorie negli Stati Uniti

Può essere utile volgere brevemente lo sguardo agli Stati Uniti, in quanto utile termine di raffronto per valutare le diverse strategie regolatorie al fenomeno delle cripto-attività. A differenza dell'UE, negli USA è assente uno statuto federale sulle cripto-attività. Ferme alcune iniziative specifiche promulgate in alcuni Stati[28], non è stata ancora adottata una legislazione univoca a livello federale, anche se il già menzionato "*crypto winter*" po-

ments" per ritenere che gli sviluppatori siano soggetti a doveri fiduciari: v. Tulip Trading Ltd v Bitcoin Association For BSV [2023] EWCA Civ 83; (2023) 4 WLR 16.

[26] Nella versione in inglese "*undertakings*": sul punto, v. D. ZETSCHE *et al*., (nt. 7).

[27] E, anche, degli approcci nazionali su questi temi. V., ad esempio, per l'Italia, R. LENER, S. FURNARI, *Modelli organizzativi alla prova delle nuove tecnologie. Prime riflessioni su DAO e i principi generali del diritto dell'impresa*, XII Convegno annuale dell'Associazione Italiana dei Professori Universitari di Diritto Commerciale "Orizzonti del Diritto Commerciale", Roma, 2021, reperibile in https://art.torvergata.it/handle/2108/279396; S. FURNARI, *La finanza decentralizzata* (nt. 23), cui *adde*, I.H-Y. CHIU, *The Application of the EU Markets in Crypto-asset Regulation to Decentralised Finance* (nt. 23).

[28] Ad es., il Dipartimento dei Servizi Finanziari di New York ha una "BitLicense" speciale per le 'attività di valuta virtuale', promulgata ai sensi dei §§ 200.1-200.22 del NYCRR.

trebbe aprire la strada a una regolamentazione diretta, come sembrano indicare alcune recenti proposte in discussione al Congresso [29].

Tuttavia, negli ultimi anni le cripto-attività sono state sottoposte ad una (a tratti ondivaga) vigilanza da parte della *Commodity Futures Trading Commission* ("CFTC") e della *Securities Exchange Commission* ("SEC") [30]. Notoriamente, la legislazione statunitense alloca la supervisione finanziaria in capo alla SEC e/o alla CFTC seguendo un criterio che guarda alla natura dei prodotti e dei servizi: mentre la SEC è responsabile della salvaguardia degli interessi degli investitori e della garanzia di un funzionamento equo ed efficiente dei mercati dei capitali per quanto riguarda le "*securities*", la CFTC si occupa delle "commodities" e dei relativi prodotti derivati che sono soggetti al *Commodity Exchange Act* ("CEA") [31].

A causa della natura fluida delle cripto-attività e delle ampie definizioni di "securities" e "commodities" [32], negli Stati Uniti si è però assistito a un trattamento legale dualistico delle cripto-attività, in base al quale diverse attività di vigilanza ed *enforcement* sono svolte contemporaneamente o alternativamente dalla SEC e dalla CTFC [33], come nei casi *Winklevoss* [34] e

---

[29] E.g., la proposta di legge n. H.R. 4763 relativo al *Financial Innovation and Technology for the 21st Century Act (Financial Services Committee)*, sponsorizzato dal Rappresentante French Hill; Proposta di legge n. H.R. 4766 sul *Clarity for Payment Stablecoins Act of 2023*, sponsorizzata dal Rappresentante Patrick McHenry. Recentemente, nel dicembre 2023, la proposta di legge n. H.R. 6572, denominata *Deploying American Blockchains Act*, sponsorizzata dal Rappresentante Larry Bucshon, è stata approvata all'unanimità dal Comitato della Camera degli Stati Uniti.

[30] Si veda, inter alia, Y, GUSEVA, *Regulatory fragmentation: Investor Reaction to SEC and CFTC Enforcement in Crypto Markets*, in 64 *Boston College Law Review* 1555, 2023.

[31] V. M. DELL'ERBA, *§22. United States of America*, in P. MAUME, L. MAUTE, M. FROMBERGER (ed.), *The Law of Crypto Assets: A Handbook*, Monaco di Baviera, 2022.

[32] Si veda l'art. 1(a)(9) CEA. Si veda anche Board of Trade of City of Chicago contro SEC, 677 F. 2d 1137, 1142 (7a Cir. 1982) per una discussione del concetto.

[33] Il doppio trattamento normativo attualmente in vigore per le cripto-attività negli Stati Uniti è stato confermato anche a livello giudiziario. Cfr. Tribunale distrettuale degli Stati Uniti 6 marzo 2018 – Commodity Futures Trading Comission v McDonnel, 287 F. Supp. 3d 213, p. 228 (E.D.N.Y. 2018): "[f]ederal agencies may have concurrent or overlapping jurisdiction over a particular issue" e "[u]ntil Congress clarifies the matter, the CFTC has concurrent authority, along with other state and federal administrative agencies, and civil and criminal courts, over dealings in virtual currency" (18-CV-361, 3).

[34] Cfr. SEC, *Order Disapproving a Proposed Rule Change, Exchange Act Release No. 34-80206*, marzo 2017, reperibile in https://www.sec.gov/files/rules/sro/batsbzx/2017/34-80206.pdf; SEC, *Order Setting Aside Action by Delegated Authority & Disapproving a Proposed Rule Change, Exchange Act Release No. 34-83723*, luglio 2018, https://www.sec.gov/files/rules/other/2018/34-83723.pdf. Si veda anche SEC, *Order Disapproving a Proposed Rule Change to*

Coinflip [35]. Se alcune cripto-attività – quali *Ether* e *Litecoin* – sono state classificate come "*commodities*" dalla CFTC [36], altre sono state qualificate come "*securities*" e sono quindi rientrate nell'ambito della supervisione della SEC [37], sulla base del cd. "*Howey test*" [38].

Senza alcuna pretesa di esaurire l'analisi in materia, è sufficiente osservare che l'applicazione dello standard *Howey* da parte della Corte Suprema degli Stati Uniti si basa sulla nozione di "*investment contract*" [39], che richiede un investimento di denaro in un'impresa comune con l'aspettativa di un profitto derivante dagli sforzi di altri. Applicando questi criteri, e seguendo il principio della prevalenza della sostanza sulla forma [40], la SEC ha effettivamente concluso che molti – se non la maggior parte – dei token offerti al pubblico possono entrare in ultima analisi nel concetto di "*securities*". Tuttavia, anche l'autorità di vigilanza americana ha ritenuto che alcune cripto-attività in realtà non possono essere considerate "*securities*" e quindi esulano interamente dall'ambito della legislazione finanziaria.

List and Trade the Shares of the ProShares Bitcoin ETF and the ProShares Short Bitcoin ETF, Exchange Act Release No. 34-83904, agosto 2018, https://www.sec.gov/files/rules/sro/nysearca/2018/34-83904.pdf.

[35] La CFTC definisce 'digital assets' come 'anything that can be stored and transmitted electronically, and has associated ownership rights' (cfr. CFTC, *Digital Assets Primer*, dicembre 2020, reperibile in https://www.cftc.gov/PressRoom/PressReleases/8336-20). Una 'virtual currency' viene descritta come 'a digital representation of value that functions as a medium of exchange, a unit of account, and/or a store of value' (LabCFTC, *A CFTC Primer on Virtual Currencies*, ottobre 2017, reperibile in https://www.cftc.gov/sites/default/files/idc/groups/public/documents/file/labcftc_primercurrencies100417.pdf). La SEC, a sua volta, ha definito 'virtual currency' come 'a digital representation of value that can be digitally traded and functions as a medium of exchange, unit of account, or store of value' (cfr. SEC, *Investor Bulletin: Initial Coin Offerings*, 25 luglio, 2017, reperibile in https://www.sec.gov/oiea/investor-alerts-and-bulletins/ib_coinofferings).

[36] Cfr. Order, *In Re* Infex Inc., CFTC *Docket* No. 22-05 (15.10.2021), n. 2: "Bitcoin, Ether, Litecoin, and Tether tokens, along with other digital assets, are encompassed within the broad definition of 'commodity' under Section 1a(9) of the [Commodity Exchange] Act".

[37] V., *ex multis*, S. FITZGIBBON, *What is a Security? A Redefinition Based on Eligibility to Participate in the Financial Markets*, in 64 *Minn.L.Rev.* 893, 1980, pp. 912-918; J.D. COX, R.W. HILLMAN, D.C. LANGEVOORT, A.M. LIPTON, *Securities Regulation, Cases and Materials*, 10ª ed., Aspen Publishing, Burlington, 2021.

[38] Cfr. *SEC v W J Howey Co* 328 U.S. 293 (1946).

[39] V., *ex multis*, J. BEATTY, *Corporations: Securities Regulation: Investment Contracts under Securities Act of 1933*, in 53 *Michigan Law Review* 140, 1954; L. CROCKER, *Investment Contracts under Federal and State Law*, in 17 *W. Rsrv. L. Rev.* 1108, 1966.

[40] Il c.d. "economic realities test". Per l'applicazione del principio sulle cripto-attività, si veda la posizione ufficiale dell'autorità di vigilanza, cfr. SEC, *Release No. 81207 – Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO* (July 2017), reperibile in https://www.sec.gov/files/litigation/investreport/34-81207.pdf.

Secondo la SEC[41], ad esempio, nel caso in cui la rete su cui il token è emesso è sufficientemente decentralizzata le cripto-attività non rappresentano un contratto di investimento. Così, la SEC ha constatato che bitcoin in effetti non si affida a una terza parte centrale, i cui sforzi costituiscono un fattore determinante per il suo funzionamento[42]. E di conseguenza, al pari dell'UE, anche gli Stati Uniti hanno – almeno per il momento – lasciato il Bitcoin fuori dall'ambito della legislazione sui mercati di capitali.

6. Quali regole per la De-Fi? Il Rapporto IOSCO

Nell'ambito delle incompiutezze del regolamento MiCAR, quella che attiene all'esclusione, dal suo ambito di applicazione, della vera e propria finanzia decentralizzata spicca per il suo rilievo, anche solo intellettuale. Proprio il "fascino" dei modelli centralizzati riporta, per così dire, alle origini stesse del fenomeno delle cripto-attività: al progetto fondatore di bitcoin, e a quello che avrebbero dovuto essere i suoi sviluppi, poi in parte disattesi.

L'aver modellato MiCA sugli schemi della regolazione finanziaria tradizionale lo rende, allo stato, del tutto inadatto ad affrontare il fenomeno della DeFi: per la verità, in tutti i consessi nei quali si discute del problema della finanza decentralizzata, regna sovrana l'incertezza circa il modo in cui quello stesso problema andrebbe affrontato e risolto. Se, da un lato, si riconosce la specialità della DeFi, dall'altro, la tendenza che spesso si registra è proprio quella di tentare di regolarla seguendo approcci tradizionali, ossia quelli che si rinvengono, tipicamente, nella disciplina delle attività finanziarie svolte in via centralizzata. Questa tendenza, seppur suggestiva, suscita a sua volta questioni di difficile soluzione, stante il fatto che gli schemi tradizionali faticano ad applicarsi al nuovo fenomeno, con la conseguenza, ed il rischio, di dar luogo a ragionamenti essenzialmente circolari.

Ad ogni modo, il dibattito è intenso, anche a livello sovranazionale. Tra le riflessioni più interessanti non si può mancare di segnalare, in questa sede, gli orientamenti recentemente formulati nel Rapporto IOSCO (il

[41] Cfr. W. HINMAN, *Digital Asset Transactions: When Howey Met Gary (Plastic)*, SEC, 15 giugno 2018, reperibile in https://www.sec.gov/news/speech/speech-hinman-061418#_ftnref6.

[42] V. SEC, *Investor Alert: Bitcoin and Other Virtual Currency-Related Investments*, reperibile in https://www.investor.gov/introduction-investing/general-resources/news-alerts/alerts-bulletins/investor-alerts/investor-39.

"Rapporto"), in quanto rappresentativi di un approccio che, in futuro, potrebbe fornire un'utile *road map* per i regolatori nel mondo sul tema della DeFi.

Il Rapporto, peraltro, conferma l'approccio misto al quale si è fatto cenno: la DeFi viene a collocarsi in una zona ibrida, in parte già raggiungibile con le attuali tecniche regolatorie e di vigilanza, in parte del tutto nuova. In proposito, e significativamente, il Rapporto osserva che le raccomandazioni ivi formulate dovrebbero essere prese in considerazione dai membri dello stesso IOSCO nel momento in cui applicano regimi normativi esistenti, o nel momento in cui vengono formulati nuovi poteri o quadri regolatori proprio per cogliere le specificità del nuovo fenomeno.

In effetti, questo approccio muove proprio dal presupposto che prodotti e servizi DeFi possono rientrare nelle definizioni di prodotti o servizi già coperti dal quadro normativo vigente. Tuttavia, là dove questo non sia il caso, IOSCO invita le autorità degli Stati ad analizzare l'applicabilità e l'adeguatezza dei loro quadri normativi, e la misura in cui i prodotti e gli accordi DeFi richiedano interventi diversi da quelli tradizionali.

Il Rapporto include nove raccomandazioni, in un continuo oscillare tra prospettive nuove, e tentativi di estensione della portata e dell'ambito di applicazione dei regimi esistenti. Di seguito, un'estrema sintesi delle singole raccomandazioni, essenzialmente finalizzata ad evocarne la portata:

– Raccomandazione 1: le autorità dovrebbero analizzare i prodotti, i servizi, gli accordi e le attività DeFi che si verificano all'interno della propria giurisdizione, al fine di applicare, a seconda dei casi, i propri metodi operativi o nuovi metodi in conformità con il principio di neutralità tecnologica, che viene esplicitamente richiamato dal Rapporto.

– Raccomandazione 2: le autorità di vigilanza dovrebbero mirare a identificare le persone fisiche e giuridiche di un sistema DeFi che potrebbero essere soggette al quadro normativo applicabile (cc.dd. "soggetti responsabili"). I soggetti responsabili includono coloro che esercitano il controllo o un'influenza sufficiente su un accordo o un'attività di DeFi. Essi sono generalmente persone ed entità che forniscono o facilitano attivamente la fornitura di prodotti o servizi. I regolatori possono prendere in considerazione, ad esempio, coloro che hanno il controllo della progettazione e della manutenzione, il controllo economico-finanziario, e/o il controllo legale.

– Raccomandazione 3: secondo il Rapporto, le autorità di regolamentazione dovrebbero utilizzare gli schemi regolatori esistenti – o crearne di

nuovi – per disciplinare, supervisionare, sorvegliare e affrontare i rischi derivanti da prodotti, servizi, accordi e attività della DeFi in modo coerente con gli standard proposti. I prodotti, i servizi, gli accordi e le attività della DeFi che coinvolgono strumenti finanziari regolamentati in una particolare giurisdizione dovrebbero essere soggetti alle leggi già applicabili. Le autorità dovrebbero, quindi, valutare il modo migliore per applicare i rispettivi quadri normativi esistenti o, in alternativa, creare nuovi quadri normativi.

– Raccomandazione 4: nell'applicare la normativa esistente, le autorità dovrebbero richiedere ai fornitori di prodotti e servizi DeFi e agli altri soggetti responsabili di identificare e risolvere i conflitti di interesse. I regolatori dovrebbero valutare se alcuni conflitti siano talmente strutturali da non poter essere efficacemente attenuati, ad esempio attraverso controlli, divieti o dichiarazioni.

– Raccomandazione 5: le autorità dovrebbero impegnarsi nell'identificazione e nella gestione dei rischi rilevanti, compresi i rischi operativi e tecnologici, connessi alla DeFi. Nell'applicare le regole esistenti, o nuove regole, le Autorità dovrebbero richiedere ai fornitori di prodotti e servizi DeFi e agli altri soggetti responsabili di identificare e affrontare i rischi rilevanti. Le autorità dovrebbero valutare se alcuni dei rischi individuati siano a tal punto gravi da non poter essere efficacemente mitigati. In tal caso, dovrebbero essere nella posizione di applicare misure più incisive per la loro risoluzione.

– Raccomandazione 6: le autorità di regolamentazione dovrebbero richiedere ai fornitori di prodotti e servizi DeFi e agli altri soggetti responsabili di comunicare agli utenti e agli investitori informazioni complete e chiare sui prodotti e servizi offerti, al fine di promuovere la protezione degli investitori e l'integrità del mercato. Il Rapporto osserva che le informazioni relative ai prodotti, ai servizi, agli accordi e alle attività della DeFi sono spesso tecnologicamente complesse e/o opache. Ciò può determinare la presenza di asimmetrie informative, per effetto delle quali utenti e investitori potrebbero non essere pienamente consapevoli della natura dei prodotti e dei servizi offerti.

– Raccomandazione 7: le autorità di regolamentazione dovrebbero essere dotate di ampi poteri di autorizzazione, ispezione e indagine. In ogni caso, si dovrebbe prendere in considerazione di quali conoscenze tecnologiche, dati e strumenti abbia bisogno ciascuna autorità per svolgere efficacemente i propri compiti.

– Raccomandazione 8: le autorità di regolamentazione, in considerazione della natura transfrontaliera dei prodotti, dei servizi, degli accordi e delle attività della DeFi, dovrebbero avere la possibilità di condividere le informazioni a livello transnazionale con le autorità di altre giurisdizioni, anche tramite l'istituzione di accordi di cooperazione strutturati.

– Raccomandazione 9: il Rapporto indica la necessità di valutare le interconnessioni tra il mercato della DeFi, il più ampio mercato delle cripto-attività e i mercati finanziari tradizionali, ai fini di una compiuta analisi di prodotti, servizi, accordi e attività coinvolti nella DeFi.

7. Conclusione

Un tratto comune a molte delle più recenti manifestazioni dell'evoluzione tecnologica nel settore finanziario è rappresentato dallo sviluppo di modelli e sistemi che puntano a individuare soluzioni informatiche per la condivisione e la decentralizzazione dei dati e dei servizi. *Open Finance* e cripto-attività sono fenomeni diversi, ma, come si è cercato di mostrare, interagiscono tra di loro e, soprattutto, condividono una impostazione di fondo non dissimile sul piano degli obiettivi e dei fattori che li ispirano. In un certo senso, la più grande novità degli ultimi anni di evoluzione dei mercati è proprio il tentativo di superare gli schemi tradizionalmente incentrati su modelli bilaterali cliente-intermediario, costruiti su architetture chiuse e proprietarie. Lo sviluppo dell'*Open Finance*, molto significativo soprattutto nel settore dei pagamenti, e quello delle tecnologie a registro distribuito rappresentano modelli nuovi, che puntano alla costruzione di sistemi orizzontali e aperti, se non addirittura condivisi. Le sfide che la legislazione deve affrontare in questo contesto sono molteplici: da un lato, non compromettere lo sviluppo dei mercati e delle innovazioni tecnologiche; dall'altro, adattare i propri schemi e approcci tradizionali per far sì che le innovazioni non si traducano in pericolose lacune sul piano della tutela, della gestione dei rischi e della stabilità del sistema. In questo senso, il pendolo ancora oscilla tra, da un lato, l'incerta estensione di soluzioni derivanti dal passato ai nuovi modelli e, dall'altro, il tentativo di immaginare nuovi approcci, ancora però in fase di studio e di sviluppo. Il legislatore dell'Unione, a partire dalle innovazioni introdotte con la PSD2, sino al più recente regolamento MiCA, pare comunque ben posizionato, avendo compiuto scelte normative spesso coraggiose ed anticipatorie, anche se, per certi versi, già da aggiornare alla luce delle continue evoluzioni dei mercati.

Liliana Fratini Passi e Biancamaria Raganelli *

Open Finance e innovazione finanziaria: opportunità, questioni e sfide

SOMMARIO: 1. Rivoluzione tecnologica e implicazioni per i servizi finanziari. – 2. I c.d. ecosistemi open e i soggetti coinvolti. – 3. Iniziative collaborative. – 4. Tentativi di regolamentazione del settore. – 5. Accesso ai dati finanziari. – 6. Gestione dei dati e questioni aperte. – 7. Trasparenza e lotta alle frodi.

1. Rivoluzione tecnologica e implicazioni per i servizi finanziari

L'innovazione tecnologica degli ultimi anni ha innescato un processo evolutivo che ha prodotto un impatto rilevante in vari settori.

Nel settore dei servizi finanziari, l'accelerazione tecnologica ha fornito nuovi strumenti per lo sviluppo di prodotti e servizi e modificato significativamente l'attività degli attori sul mercato.

Questi ultimi, banche e Fintech, sono stati chiamati ad affrontare nuove sfide e confrontarsi con l'esigenza di reinventare i propri modelli operativi: modelli di business «aperti», basati sulla condivisione dei dati dei clienti e sull'interoperabilità di un eco-sistema aperto e competitivo.

Ciò ha posto nuove opportunità e nuove questioni aumentando la competitività nell'offerta dei servizi offerti.

In questo contesto, il termine *Open Banking* si riferisce alla possibilità che terze parti accedano a dati e informazioni relativi ai conti correnti tenuti presso le banche dai clienti, con l'assenso di questi ultimi, al fine di fornire loro nuovi servizi e applicazioni [1].

---

* Ogni opinione qui espressa è imputabile agli autori e non alle Istituzioni di appartenenza.

[1] Https://www.bancaditalia.it/pubblicazioni/mercati-infrastrutture-e-sistemi-di-pagamento/questioni-istituzionali/2023-031/N.31-MISP.pdf.

L'*Open Finance*, evoluzione dell'*Open Banking* offre una condivisione più ampia di dati finanziari tra i player del mercato e rappresenta una straordinaria opportunità per consumatori e imprese di accedere/offrire servizi/prodotti più adeguati e vicini alle specifiche esigenze ed aspettative dei singoli. Nuove opportunità e modalità per una più accurata modellazione di prodotti e servizi.

Si supera il tradizionale modello di utilizzo del dato all'interno del singolo intermediario bancario e si ampliano le dimensioni del sistema, incrementando sia il numero di punti di accesso sia la platea dei soggetti che possono accedere, utilizzare e, nei limiti imposti dalla normativa, rielaborare i dati dei conti di pagamento per offrire nuovi servizi.

È necessario che la normativa fornisca indicazioni che mantengano l'ecosistema stabile, consentendo a tutti i soggetti coinvolti di operare con sicurezza ed efficienza. L'Autorità di regolamentazione e controllo dal canto suo è chiamata a rimodulare le proprie prassi nel duplice obiettivo da un lato di favorire l'offerta dei nuovi servizi da parte del mercato e dall'altro di adattare le tradizionali metodologie di sorveglianza/vigilanza ai peculiari rischi connessi con il nuovo ambiente e alle specificità di nuovi sistemi e infrastrutture.

La rivoluzione tecnologica ha prodotto e continua a produrre evidenti implicazioni sociali e ricadute su molti aspetti della vita quotidiana degli individui, ponendo temi rilevanti anche da un punto di vista economico e giuridico, tra cui quello della sicurezza informatica, degli attacchi cyber e dei relativi rischi connessi, nonché quello della trasparenza e delle frodi in senso lato. La finanza digitale può rendere più impegnativo salvaguardare la stabilità finanziaria, la protezione dei consumatori, l'integrità del mercato, la concorrenza leale e la sicurezza, ponendo all'attenzione di regolatori e vigilanza nuovi rischi da affrontare e mitigare.

In Italia, a seguito dell'applicazione della normativa dettata dalla direttiva PSD2[2], le interfacce predisposte dai prestatori di servizi di pagamento per consentire l'accesso di terze parti fanno prevalentemente leva su soluzioni di sistema, infrastrutture tecniche che realizzano un unico punto di accesso per una pluralità di intermediari. L'Autorità di vigilanza e supervisione ha sviluppato un sistema dei controlli che tengono conto delle nuove caratteristiche del mercato, fortemente innovative. Si prevede inoltre la raccolta di dati statistici per il monitoraggio dei profili di efficienza, affidabilità, sicurezza e

[2] Https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015L2366.

conformità delle soluzioni di sistema, consentendo l'elaborazione di indicatori utili per valutare l'evoluzione del mercato nazionale [3].

Si pongono temi e questioni delicate che non possono essere affrontate in una prospettiva esclusivamente domestica. Come recentemente affermato anche dalla Vigilanza, al fine di rendere più efficienti i pagamenti transfrontalieri, è «necessario promuovere la cooperazione e analizzare nuove soluzioni tecniche, allineando gli obiettivi e le politiche dei diversi paesi in materia di pagamenti». Si tratta di «una sfida complessa, che richiede un lavoro coordinato da parte di soggetti sia pubblici sia privati» [4].

2. I c.d. ecosistemi open e i soggetti coinvolti

La "*condivisione e sfruttamento dei dati autorizzata dai clienti da parte delle banche con sviluppatori e aziende di terze parti per costruire nuovi servizi e applicazioni, come quelli che offrono pagamenti in tempo reale, maggiori possibilità di trasparenza finanziaria per i titolari di conti e opportunità di marketing e cross-selling*", consente a privati e imprese di ottenere, tra gli altri servizi, anche un maggiore controllo della propria situazione finanziaria, sia pur limitata ai dati dei pagamenti (*Bank of International Settlements*, BIS).

Con l'ampliamento del *set* di dati finanziari a disposizione non più relativi soltanto ai pagamenti, l'evoluzione all'*Open Finance* consente l'accesso ad un modello in cui i provider terzi autorizzati hanno accesso ad informazioni diverse (contratti di risparmio, mutui, pensioni, assicurazioni, prestiti, investimenti, azioni ed altro ancora). Ciò consente loro di sviluppare prodotti e servizi finanziari personalizzati e intuitivi, progettati su misura per soddisfare le esigenze e le aspettative dei consumatori. In questo modo l'*Open Finance* diviene uno dei driver, insieme alle valute digitali delle Banche centrali e alle criptovalute del settore privato, che possono determinare un impatto significativo sul settore finanziario internazionale nei prossimi anni.

Secondo un recente studio Banca d'Italia, il mercato italiano dell'*Open Banking* conta 377 ASPSP e 85 operatori attivi in qualità di terza parte (di cui 39 italiani), che per la maggior parte hanno integrato soluzioni di tipo *Personal Finance Management* (PFM).

---

[3] Https://www.bancaditalia.it/compiti/vigilanza/analisi-sistema/approfondimenti-banche-int/2021-PSD2-Open-Banking.pdf.

[4] Https://www.bancaditalia.it/media/notizia/fabio-panetta-sul-financial-times-in-tema-di-pagamenti-cross-border.

Sul lato degli attori, si osserva una proliferazione di start-up innovative nel campo della finanza e del mondo assicurativo. Il fenomeno sta assumendo dimensioni rilevanti che impattano notevolmente sul business di tradizionali attori del mercato. Considerando le sole realtà che hanno ricevuto funding pari almeno a 1 milione di dollari, a livello europeo si contano 1.392 startup (+81% rispetto al 2020) che hanno raccolto complessivamente 35 miliardi di dollari negli ultimi 5 anni (+73% rispetto al 2020), con una media di 25 milioni di dollari ciascuna. In Europa nel 2022 il numero di *Third party provider* registrati, ovvero le società di servizi che forniscono funzionalità aggiuntive rispetto a quelle dell'istituto di credito presso cui è stato aperto il conto corrente, è cresciuto del 12% arrivando a quota 535 (dato che include anche le Terze parti inglesi). Sul fronte dei servizi lo studio rileva poi che il 55% del totale dell'offerta è focalizzata su AIS (*Account information services*, i servizi di informazione sui conti) e su PIS (*Payment initiation services*, i servizi di disposizione di un ordine di pagamento), ma stanno crescendo le soluzioni nell'ambito degli investimenti (10%) e in quello dei prestiti e delle assicurazioni (2%). Altre funzionalità "premium" su cui si stanno concentrando gli operatori riguardano servizi di statistiche e informazioni (11%) e sicurezza (8%).

Il Regno Unito si conferma la culla del fintech in Europa, con il 38% delle startup, seguito da Francia (11%) e Germania (9%), ed è in vetta anche per entità del funding raccolto (17,4 miliardi di dollari), seguito a distanza da Francia (3,2 miliardi) e Germania (3 miliardi)[5].

L'Italia presenta un ritardo rispetto al resto del Vecchio Continente: l'internet banking ha registrato un moderato tasso di adozione tra i clienti (circa il 50%), mentre i servizi di *Open Banking* e *Open Finance* sono utilizzati da una minoranza di clientela digitale. Questo trend, secondo gli intermediari bancari, è riconducibile ad un problema di sensibilizzazione e comunicazione, insieme ad un livello di investimenti che rimane sostanzialmente invariato rispetto all'anno precedente. Sono invece triplicate (51 milioni) rispetto al 2020 le chiamate Api (*application programming interfaces*, le interfacce di accesso), principalmente legate ai servizi AIS e PIS. Dal 2021, inoltre, sono iniziati a crescere gli investimenti per i servizi oltre la compliance alla Psd2, ovvero l'offerta commerciale delle banche, ed è prevista una crescita nel prossimo futuro.

[5] *The global Open Finance report*, realizzato da Cbi in collaborazione PwC (https://www.cbi-org.eu/Media-e-Eventi/Report-e-Ricerche).

3. Iniziative collaborative

Promuovere l'innovazione attraverso iniziative collaborative è oramai determinante per abilitare il successo delle iniziative che comportino l'adozione di nuovi prodotti e servizi da parte di aziende e consumatori. I gruppi multistakeholder dell'area pan-europea stanno fornendo il loro contributo allo sviluppo di modelli "open", svolgendo un ruolo chiave nel sostenere lo sviluppo di servizi innovativi e consentire una connessione agevole tra gli attori. Ad esempio, in ambito *European Payments Council* – Associazione internazionale senza scopo di lucro formata da 77 PSP (*Payment Service Providers*) o associazioni di PSP con lo scopo di sostenere e promuovere l'integrazione e la crescita dei pagamenti europei – è in fase di sviluppo uno schema, denominato SPAA (*Sepa Payment Account Access*), che consente, attraverso un insieme di regole, pratiche e standard, lo scambio di dati relativi ai conti di pagamento, facilitando l'avvio di transazioni di pagamento nel contesto dei servizi API (*Application Programming Interface*) "a valore aggiunto".

Al momento, secondo i dati del *Global Open Finance Report*, l'offerta API – dal punto di vista tecnico un'API è una modalità utilizzata da due sistemi software (applicazioni), presenti o meno sullo stesso computer, per scambiare dati degli attori del mercato UE – rimane fortemente focalizzata sui servizi di *Account Information* (AIS: *Account Information Service* (Servizio di informazione sui conti) e *Payment Initiation* (PIS: *Payment Initiation Service* – Servizio di disposizione di ordini di pagamento), obbligatori per la PSD2, che rappresentano il 55% delle API monitorate. Si stanno consolidando le API di *Open Finance* in particolare per i servizi di investimento che rappresentano il 10% del totale, mentre quelle relative ad esempio a Prestiti e Assicurazioni sono ancora in ritardo. L'analisi evidenzia come gli operatori di mercato si concentrino su API del tipo Statistiche & Informazione (11%) e Sicurezza (8%), suggerendo quindi il rafforzamento e arricchimento della loro offerta "Open", con l'inclusione di servizi accessori insieme a quelli core offerti principalmente da banche tradizionali.

In Italia risulta che il mercato si stia polarizzando attorno ai servizi di "informazioni di conto", con l'85% (+55% vs '21) degli intervistati che include nella propria proposta un'offerta commerciale legata all'*Account Aggregation*, mentre una percentuale minore ha sviluppato anche servizi PFM/BFM. Si registra, tuttavia, anche la crescita di nuovi servizi a valore aggiunto, tra cui il "Check Iban" (oltre il 60%).

Tra le varie piattaforme, CBI Globe, sviluppata da CBI S.c.p.a. Società Benefit già nel 2019, rappresenta un ecosistema *Open Banking* e *Open Finance* internazionale che ha fortemente semplificato la connessione tra i Prestatori di Servizi di Pagamento (PSP) in tutta Europa tramite API, abilitando il recente sviluppo di servizi fintech avanzati in risposta alle crescenti esigenze dei clienti corporate e retail, quali Check IBAN, CBI GO, Name Check e il servizio Database Controllo Fatture, noto come Safe Trade, che peraltro è stato ammesso alla sperimentazione della Sandbox Regolamentare di Banca d'Italia. Nel 2023 CBI Globe, a cui aderisce l'80% dell'industria finanziaria italiana, ha registrato circa 800 milioni di invocazioni (+150% rispetto al 2022) effettuate da oltre 500 Prestatori di Servizi di Pagamento in tutta Europa operanti a vario titolo sulla piattaforma.

L'innovazione collaborativa è un processo costante. È necessario estendere ulteriormente la prospettiva, ampliando i soggetti che operano sulla funzionalità attiva delle piattaforme, consentendo ai PSP di rafforzare la propria posizione commerciale nei confronti di aziende e clienti finali, e facendo leva su partnership strategiche con gli attori dell'UE.

Occorre continuare a promuovere l'innovazione nel settore, sviluppando servizi a valore aggiunto (VAS), come il "Check IBAN Cross Border", che consente di verificare in tempo reale la corretta associazione tra codice IBAN e Partita IVA del beneficiario del pagamento, riducendo il rischio di frode. Tra gli altri servizi in grado di incrementare la sicurezza dei pagamenti, il Name Check, noto anche come VoP "*Verification of Payee*", consente di verificare in tempo reale la corretta associazione tra l'IBAN e il nome del beneficiario forniti dall'utente debitore al proprio Intermediario di riferimento e consente di rispondere al recente Regolamento sugli *Instant Payments*[6]. Inoltre, il servizio *Safe Trade* (Database Controllo Fatture), raccoglie le informazioni sulle fatture anticipate in ottica multi-banca e multicanale, al fine di aumentare la stabilità e l'efficienza del settore finanziario e di mitigare il rischio derivante dall'uso fraudolento delle fatture e dell'erogazione del credito da parte degli intermediari. Infine, con lo *Smart Onboarding* – CBI GO – i PSP (*Payment Service Providers*) possono consentire alle Corporate di recuperare real-time le informazioni di un utente finale mediante il dialogo telematico con la banca di riferimento di quest'ultimo.

[6] Https://www.consilium.europa.eu/it/press/press-releases/2024/02/26/council-adopts-regulation-on-instant-payments/#:~:text=Il%20regolamento%20sui%20pagamenti%20istantanei,altro%20Stato%20membro%20dell%27UE.

Per supportare l'industria finanziaria nel percorso di evoluzione verso modelli sempre più open è necessario garantire il corretto equilibrio tra innovazione e sicurezza per l'offerta di nuovi servizi. Per questo è fondamentale che il sistema sia retto da un'architettura evoluta, CBI Hub Cloud, che consenta il passaggio delle infrastrutture, che gestiscono oggi tutte le transazioni di pagamento e incasso multi-banca tra le aziende italiane e verso la P.A., su tecnologia Cloud privata e dedicata. Gli istituti di credito potranno così offrire, alla Pubblica Amministrazione e ai propri clienti corporate e retail, servizi transazionali e di *Open Finance* più evoluti e in tempo reale, ampliando notevolmente i livelli di efficienza, di sicurezza e di integrazione nel mercato dei pagamenti tra tutti gli attori del nostro Paese. Ciò auspicabilmente deve condurre ad una visione europea e globale che possa varcare i confini tipici tra Stati e allungare lo sguardo di regole e vigilanza oltre la siepe degli ordinamenti domestici.

Per gli intermediari bancari si delinea dunque la possibilità di mettere a frutto un patrimonio esperienziale importante, basato sulla collaborazione per una migliore competizione, per trasformare le dinamiche della nuova arena altamente competitiva in un successo sostenibile nel tempo. Tuttavia è auspicabile che l'ambizione si spinga oltre i confini dell'attività delle banche in senso stretto e si estenda all'intero mercato finanziario come macro insieme più ampio nel quale operano vari tipi di intermediari, per assicurare ai clienti servizi e tutele adeguate.

4. Tentativi di regolamentazione del settore

I Paesi che hanno adottato iniziative nell'ambito dell'*Open Banking* e/o dell'*Open Finance*, a livello mondiale, sono oltre 40 ed hanno seguito approcci diversi.

L'Europa, con la direttiva 2015/2366 sui servizi di pagamento (PSD2 – 2015/2366), è stata una precorritrice nell'offrire una prima regolamentazione del settore. Lo scopo della direttiva è quello di rafforzare la tutela degli utenti dei servizi di pagamento, aumentare la trasparenza e la sicurezza, implementando efficienza e innovazione in questo ambito, che essendo in costante crescita, spesso si rivela privo di adeguata tutela normativa. Con la PSD2 si vuole, quindi, promuovere una maggiore concorrenza sul mercato dei pagamenti e dare maggiore apertura alle informazioni dei conti correnti bancari. L'esigenza di integrare la normativa PSD1 del 2007, relativa ai servizi di pagamento nel mercato interno e il recepimento della PSD2 è stata soddisfatta in Italia con il d.lgs. n. 218/2017.

A differenza delle esperienze di altre giurisdizioni, il legislatore europeo ha adottato un approccio prescrittivo, imponendo a tutti i prestatori di servizi di pagamento che gestiscono conti per la clientela di consentire l'accesso a terze parti per l'avvio di pagamenti o per l'elaborazione di informazioni aggregate[7]. Si è inteso promuovere maggiore concorrenza in un mercato dei pagamenti e degli altri servizi finanziari on-line fortemente concentrato su un limitato numero di prodotti e di operatori, come quelli del mondo delle carte, e nel contempo prendere atto dell'esistenza di servizi tecnologicamente evoluti, ormai diffusi anche in campi diversi da quello dei pagamenti, che dovevano essere opportunamente regolamentati per garantire una migliore protezione del consumatore, nonché valorizzati per un migliore sviluppo del settore. Si promuovono in tal modo innovazione, concorrenza e tutele in un settore, quello dei pagamenti, per sua natura tendenzialmente oligopolistico.

Il sistema in esame genera, tuttavia, anche nuove complessità da gestire. Sovrappone infatti all'architettura esistente un nuovo strato di offerta di servizi e forme di interazione obbligatorie tra terze parti e prestatori di servizi di pagamento di radicamento del conto, in assenza di procedure e regole operative concordate e di un quadro di standardizzazione consolidato[8]. Le banche sono tenute ad accettare le richieste di accesso di tali soggetti terzi autorizzati, salvo che vi siano ragioni oggettive per non farlo (ad es. rischio di frode).

Si dice prescrittivo l'approccio seguito in Canada, Brasile e Sud Africa, dove le autorità istituzionali prevedono l'emanazione di framework normativi e/o tecnologici di riferimento per determinate categorie di Player. Un approccio cd. facilitatore è quello seguito da Paesi quali le Filippine, dove la Banca Centrale (BSP) ha emesso delle specifiche linee guida per stimolare la collaborazione tra gli attori e sostenere l'inclusione finanziaria. Un approccio cd. *market-driven*, infine, è quello nel quale i Player di mercato definiscono gli standard e i servizi, senza interventi delle autorità.

In Europa, la Commissione UE sta ora lavorando ad un ampliamento delle previsioni contenute nella direttiva sui servizi di pagamento (PSD2) nel settore dell'*Open Banking* spingendo nella direzione dell'*Open Finance*, lanciando importanti iniziative tra cui il *Digital Finance Package*, un insieme di misure legislative che definiscono il modo in cui l'UE possa sostene-

[7] Per una prima disamina delle molteplici novità introdotte dall'*Open Banking* nell'Unione europea, in una prospettiva interdisciplinare tra diritto, economia e finanza, si veda l'introduzione curata da Maimeri e Mancini (2019) a una raccolta di saggi di esperti della Banca d'Italia e dell'accademia.

[8] BANCA D'ITALIA, *Mercati, infrastrutture, sistemi di pagamento*, marzo 2023.

re la trasformazione digitale e l'innovazione del settore finanziario, includendo azioni significative nei settori della *Digital Identity*, dell'*Open Finance*, dei Crypto-assets, della *Digital Resilience*, della *Blockchain* e della tutela dei consumatori.

Il *Digital Finance Package* ha lo scopo di rendere i servizi finanziari più digitalizzati, stimolando l'innovazione responsabile e la concorrenza tra i diversi competitors nell'Unione europea. La strategia mira a garantire parità di condizioni tra i fornitori di servizi finanziari, siano essi banche tradizionali o fintech (principio *stessa attività, stessi rischi, stesse regole*).

I principali obiettivi sono: ridurre la frammentazione del mercato unico digitale, in modo che i consumatori possano avere accesso ai servizi cross-border, e consentire alle start-up di svilupparsi e crescere; garantire che il quadro normativo dell'UE favorisca l'innovazione digitale nell'interesse dei consumatori e dell'efficienza del mercato[9]; creare uno spazio europeo dei dati finanziari per promuovere l'innovazione nel contesto dell'*Open Finance*; affrontare le nuove sfide e i rischi associati alla trasformazione digitale.

I servizi finanziari finiscono così per migrare verso ambienti digitali con ecosistemi frammentati, che comprendono fornitori di servizi digitali spesso operanti nell'attuale regime di deroga previsto dalla regolamentazione di settore.

La finanza digitale può rendere più impegnativo salvaguardare la stabilità finanziaria, la protezione dei consumatori, l'integrità del mercato, la concorrenza leale e la sicurezza, ponendo all'attenzione dei regolatori in senso lato a diversi livelli – nazionale, europeo e globale –, ma anche di diversa tipologia – legislatore, autorità indipendenti di regolazione e vigilanza – nuovi temi. È auspicabile che quantomeno in Europa si veicoli la riflessione verso una prospettiva di regolazione e vigilanza accentrata, che garantisca uniformità di impostazione e che concili il disegno top down con un adeguato dialogo dal basso.

Con l'obiettivo di abilitare la progettazione di servizi in una più ampia visione europea di "open asset sharing economy", gli sviluppi avviati già con la PSD2 nella direzione dell'*Open Banking* saranno ulteriormente consolidati ed estesi, nel rispetto delle norme sulla protezione dei dati e della concorrenza.

---

[9] Le innovazioni basate su DLT (Distributed Ledger Technology), fra cui la **blockchain**, o sull'**intelligenza artificiale** hanno il potenziale di migliorare i servizi finanziari per i consumatori e le imprese. Il quadro normativo dovrebbe garantire che essi siano utilizzati in modo responsabile, in linea con i valori dell'Unione europea.

5. Accesso ai dati finanziari

La disciplina europea dei servizi di accesso ai conti è articolata su più livelli: la PSD2 e le fonti di recepimento nazionali; i RTS (Regulatory Technical Standards) e le altre regole attuative di secondo livello definite dall'EBA (European Banking Association); le interpretazioni fornite sia dalla Commissione sia dall'EBA nell'ambito del tool "Questions and Answers". Il fulcro dell'innovazione sottostante è la condivisione del patrimonio informativo del cliente: un modello nuovo che si discosta nettamente da quello classico basato su un rapporto bilaterale banca-cliente.

La seconda direttiva sui servizi di pagamento, 2015/2366/UE ha abilitato nuovi modelli di servizio di *Open Banking* con i quali il cliente di un prestatore di servizi di pagamento presso cui è aperto un conto on-line – c.d. Account Servicing Payment System Provider – ASPSP - può utilizzare una terza parte autorizzata – c.d. Third Party Provider – TPP, che può operare come fornitore di servizi di disposizione di ordini di pagamento – c.d. Payment Initiation Services Provider – PISP). Ciò al fine di avviare pagamenti a valere sul proprio conto on-line oppure come fornitore di servizi di informazioni sui conti on-line detti Account Information Services Provider – AISP, che sono detenuti presso più prestatori di servizi di pagamento (ASPSP). Accanto alla direttiva si pongono le fonti di recepimento nazionali; i RTS e le altre regole attuative di secondo livello definite dall'EBA; le interpretazioni fornite sia dalla Commissione sia dall'EBA nell'ambito del tool "Questions and Answers".

Un complesso di regole provenienti da fonti normative diverse, ma anche di tipologia diversa: alle norme contenute nella direttiva si aggiungono quelle elaborate dalla Europen Banking Authority, una delle tre Financial Supervisory Authorities connesse alle autorità nazionali secondo un modello di network multilivello tra autorità. La normativa attuativa è contenuta nei c.d. Regulatory Technical Standards (RTS), predisposti dalla European Banking Authority (EBA) e adottati dalla Commissione Europea. La Commissione Europea ha dettagliato, nel Regolamento delegato del 27 novembre 2017, tutte le norme tecniche per l'autenticazione del cliente e gli standard di comunicazione [10].

È così emersa l'esigenza di contemperare gli interessi contrapposti delle banche, delle terze parti e dei rispettivi utenti, che non trovano composi-

[10] R. PELLITTERI, RAVENIO PARRINI, C. CAFAROTTI, B.A. DE VENDICTIS, *Mercati, infrastrutture, sistemi di pagamento (Markets, Infrastructures, Payment Systems)*, marzo 2023, Banca d'Italia.

zione in una spontanea disciplina di mercato e in forme di autoregolamentazione strutturate. In assenza di un rapporto contrattuale diretto, si disciplinano i diritti e gli obblighi che connotano il rapporto tra la terza parte e la banca (artt. da 64 a 67 della PSD2). Il servizio offerto alla clientela può essere sviluppato nel rispetto dei vincoli stabiliti da queste norme ed è dunque ad esse che devono conformarsi i relativi contratti.

Alcune specifiche norme si occupano di definire il regime delle responsabilità che gravano solitamente sulla banca nel caso di operazioni svolte con l'intermediazione della terza parte. Si occupano della corretta autenticazione ed esecuzione dei pagamenti, della gestione del consenso dell'utente, del riparto di responsabilità in caso di operazioni non autorizzate.

Altre previsioni normative riguardano l'interazione operativa tra la banca e la terza parte: regole di secondo livello, definite dall'EBA con cui sono fissati i requisiti tecnici per l'identificazione reciproca e la comunicazione sicura, le modalità di accesso tramite apposite interfacce e le misure per assicurare la continuità di servizio dei canali di colloquio. Il buon funzionamento dell'intero sistema dipende dalla corretta e uniforme applicazione di "standard normativi". L'EBA attraverso le proprie linee guida e le opinioni ha disciplinato gli aspetti di dettaglio e ridotto i margini di interpretazione.

La disciplina, recepita in Italia con il Decreto legislativo del 15 dicembre 2017, ha modificato il Testo Unico Bancario (TUB). Si è ricercata una convergenza su standard tecnici comuni per la realizzazione di interfacce dedicate ed è stato adottato lo standard "NextGenPSD2 Framework". Successivamente, il sistema bancario nazionale si è organizzato per definire soluzioni applicative "di sistema" per la realizzazione dell'interfaccia dedicata. Un ruolo centrale è stato quindi assunto dalle cd. "piattaforme di sistema" di cui si è detto, che sia affiancano alle banche e terze parti.

Il 28 giugno 2023 la Commissione europea ha pubblicato una proposta per l'adozione di un regolamento volto a definire un quadro normativo armonizzato in materia di accesso ai dati finanziari: cd. "*Financial Data Access*" o "FIDA".

Si mira a promuovere la creazione di un sistema di cd. *Open Finance*, che consenta la condivisione dei dati degli utenti tra i soggetti operanti nel settore bancario, dei servizi di investimento, assicurativi, di pagamento e finanziari, partendo dalle norme della direttiva PSD2, ma garantendo elevati *standard* di sicurezza e riservatezza da parte degli operatori. Si intende quindi promuovere lo sviluppo di prodotti finanziari personalizzati in base alle esigenze della clientela, agevolare la creazione di modelli di *business* innovativi basati sull'accesso ai dati degli utenti, assicurando che l'utilizzo dei dati avvenga soltanto con il consenso dell'utente. Un sistema che po-

trebbe avvicinare l'Europa a paesi come il Brasile, Hong Kong, Australia consentendo uno sviluppo dell'*Open Finance*.

La *European Data Strategy* della Commissione europea condivide l'impostazione di fondo della proposta di cd. *Data Act* del 23 febbraio 2023. La proposta di regolamento FIDA si inserisce in un gruppo di proposte o provvedimenti di riforma della disciplina applicabile in materia di servizi finanziari e gestione dei dati degli utenti a livello europeo: nuovo regolamento sui servizi di pagamento (PSR) e nuova direttiva sui servizi di pagamento e di moneta elettronica (PSD3). Un unico "*Financial Data Access and Payments Package*" con una disciplina dell'*Open Finance* e dell'*Open Banking.*

Il regolamento FIDA dovrebbe applicarsi a tutti i soggetti sottoposti a vigilanza ai sensi del diritto dell'Unione, con alcune limitate eccezioni con riferimento ai gestori sotto-soglia, agli intermediari assicurativi qualificabili come le PMI. Dovrebbe disciplinare la condivisione dei dati del cliente (cd. "*customer data*") di natura personale ("*personal data*") o non personale ("*non-personal data*"), che siano forniti dai clienti stessi o generati dall'interazione del cliente con l'intermediario e raccolti, conservati o trattati ad altro titolo da un intermediario nell'ambito della propria attività ordinaria con i clienti.

Sono coinvolte diverse tipologie di dati, tra cui prestiti, mutui, risparmi, investimenti, pensioni, assicurazioni non vita, merito creditizio, prodotti pensionistici, valutazione d'idoneità ed adeguatezza finanziaria. Più precisamente, è previsto siano resi accessibili i dati inerenti a crediti ipotecari, finanziamenti e conti (fatta eccezione per i conti di pagamento di cui alla PSD2); risparmi, investimenti in strumenti finanziari, prodotti di investimento assicurativi (IBIPs), cripto-attività, immobili e altre attività finanziarie, nonché i benefici economici derivanti da tali attività, ivi inclusi i dati raccolti per effettuare le valutazioni di adeguatezza e appropriatezza; prodotti pensionistici; prodotti assicurativi del ramo danni, fatta eccezione per i prodotti che coprono il rischio salute e malattia, ivi incluse le informazioni raccolte per effettuare la valutazione di coerenza (cd. "*demands and needs test*") e di appropriatezza/adeguatezza del prodotto assicurativo; i dati che fanno parte della valutazione del merito creditizio di un'impresa che siano raccolti nell'ambito di una richiesta di erogazione di un finanziamento o di una richiesta di assegnazione di un *rating*.

Viene prevista una nuova figura, i *Financial Information Service Providers* (FISP), che corrispondono agli *Account Information Service Providers* (AISP) previsti in ambito PSD2, che potranno accedere ai dati dei clienti previa autorizzazione a operare rilasciata dall'Autorità competente del loro Stato membro d'origine. Potranno essere autorizzati a operare come FISP

anche i soggetti stabiliti in Paesi terzi, senza necessità di stabilire una società o una succursale nel territorio dell'Unione, a condizione che sia nominato un rappresentante legale in uno degli Stati membri da cui il FISP intende avere accesso ai dati finanziari, responsabile della *compliance* con il quadro normativo europeo.

Il Regolamento FIDA individua due tipologie di soggetti che agiscono rispettivamente in qualità di titolari del dato ed utilizzatori del dato. Entrambi saranno chiamati a richiesta del cliente, alla condivisione di informazioni attraverso interfacce dedicate (API) realizzate in accordo a standard di mercato ampiamente diffusi. L'ambito di applicazione soggettivo riguarda pertanto i soggetti che agiscono in qualità di titolare dei dati, cd. *data holder*, qualsiasi intermediario che raccolga, conservi o tratti ad altro titolo i dati finanziari del cliente, ovvero di utilizzatore dei dati, cd. *data user*, qualsiasi intermediario o FISP che, in forza del consenso dato dal cliente, abbia legittimo accesso ai dati finanziari di quest'ultimo.

I *data holders* devono mettere a disposizione i dati finanziari del cliente in favore del cliente stesso e del *data user*. Questi sono tenuti a rendere disponibili i dati finanziari senza ritardo, su base continuativa e in tempo reale; utilizzare un formato basato su modelli *standard* generalmente riconosciuti e con una qualità non inferiore a quella caratterizzante i dati posseduti dal *data holder*; comunicare con il *data user* garantendo la sicurezza e la riservatezza del trattamento e della trasmissione dei dati; chiedere la prova dell'avvenuta prestazione del consenso del cliente rilasciato al *data user*; mettere a disposizione del cliente una *permission dashboard*. Potranno chiedere il pagamento di un compenso per la condivisione dei dati entro i limiti massimi identificati dai cd. *Financial data sharing scheme* (FDSS). Il compenso non potrà essere chiesto qualora i dati vengano messi a disposizione direttamente su richiesta del cliente; in caso di richiesta di accesso da parte di PMI, inoltre, il compenso non potrà superare i costi sostenuti dal *data holde*r per rispondere alla richiesta stessa.

I *data holders* dovranno mettere a disposizione del cliente la cd. *permission dashboard*, una particolare interfaccia informatica da utilizzare per monitorare e gestire i consensi dati dal cliente al *data user*. Con la *permission dashboard* si potrà fornire al cliente una panoramica su ciascun consenso attivo che è stato dato ai *data users* e consentire la revoca o la ri-attivazione del consenso, oltre che fornire un registro dei consensi revocati o scaduti in un termine massimo di due anni.

I *data users*, dal canto loro, sono tenuti a non trattare i dati dei clienti per finalità differenti rispetto a quelle attinenti alla prestazione del servizio espressamente richiesto dal cliente; rispettare la riservatezza dei segreti in-

dustriali e i diritti di proprietà intellettuale in sede di accesso ai dati; adottare le misure necessarie per assicurare che vi sia un adeguato livello di sicurezza attinente al profilo della conservazione, trattamento e trasmissione dei dati non personali; non trattare i dati dei clienti per finalità di mero *marketing*, salvo per il *marketing.*

6. Gestione dei dati e questioni aperte

La condivisione dei dati è previsto avvenga attraverso i cd. *Financial data sharing schemes* (FDSS). Si tratta di organismi di autoregolamentazione costituiti da *data holders* e *data users*, nonché da organizzazioni e associazioni rappresentative dei clienti e dei consumatori, cui è affidata la gestione di numerosi profili applicativi della normativa in questione. Ciascuna data holder e *data user* deve diventare membro di almeno un FDSS e condividere i dati dei clienti secondo le regole e le modalità previste dal FDSS stesso. Ove non venisse istituito alcun FDSS per una o più categorie di dati, la Commissione potrà adottare atti delegati per disciplinare i profili di rilievo concernenti la condivisione dei dati.

I *data users* potranno avere accesso ai dati finanziari del cliente anche in via transfrontaliera in regime di libera prestazione di servizi o di stabilimento. Nel caso dei FISP, l'accesso transfrontaliero ai dati finanziari dei clienti richiederà il completamento di una procedura di notifica tra le autorità competenti, sulla falsariga di quanto previsto per l'attivazione del cd. "passaporto" negli altri settori dell'ordinamento finanziario europeo.

L'EBA dovrà istituire e gestire un registro elettronico centrale che contenga le informazioni relative ai FISP autorizzati dalle autorità nazionali competenti, ai FISP che hanno notificato l'intenzione di accedere ai dati in altri Stati membri e ai FDSS che sono stati costituiti.

La proposta si inserisce nella più ampia Data Strategy dell'UE e si affianca al *Data Act* e al *Digital Operational Resilience Act* (DORA), cercando di superare l'esperienza dell'*Open Banking* e di aprire il mercato a operatori e modelli innovativi. La proposta della Commissione cerca di potenziare le opportunità per gli operatori, consentendo la prestazione di servizi di aggregazione delle informazioni relative all'intero patrimonio del cliente e facilitando l'offerta di servizi a valore aggiunto, in uno spetto più ampio dei servizi di consulenza offerti al cliente sul suo patrimonio.

L'accesso ai dati finanziari presenta tuttavia delle complessità e dei profili di delicatezza significativamente maggiori rispetto all'accesso ai conti di pagamento.

A differenza dei dati concernenti le operazioni di pagamento, i dati finanziari possono rivelare informazioni di rilevanza strategica sui prodotti e i servizi offerti dagli intermediari e sul *know-how* alla base dell'elaborazione e gestione degli stessi, con particolare riferimento ai servizi di investimento, di gestione collettiva del risparmio e assicurativi.

La proposta della Commissione lascia aperti diversi dubbi in ordine all'effettivo bilanciamento tra le esigenze di innovazione e gli interessi alla riservatezza delle informazioni proprietarie degli intermediari. Si inserisce in un contesto giuridico particolarmente vulnerabile oltre che dibattuto che riguarda la ricerca di una condivisione sicura delle informazioni che garantisca adeguatamente la privacy.

Riguarda tra le altre cose la definizione e tutela dei consumatori, la c.d. *cyber resilience*, il coordinamento e la cooperazione tra le autorità organizzate in un sistema multilivello nella produzione di regole del gioco uniformi, supportate da un enforcement adeguato, l'organizzazione e gestione di una adeguata vigilanza sugli operatori di mercato, la definizione e applicazione di un adeguato meccanismo sanzionatorio basato su procedure e sanzioni amministrative efficaci.

La proposta prevede che la condivisione dei dati avvenga attraverso i cosiddetti *Financial data sharing schemes* (FDSS). Si tratta di organismi di autoregolamentazione costituiti da *Data Holder* e *Data User*, nonché da organizzazioni e associazioni rappresentative dei clienti e dei consumatori, cui è affidata la gestione di numerosi profili, tra cui la definizione di linee guida legate al modello di remunerazione, il disegno di standard tecnici per il colloquio e l'identificazione dei partecipanti, la standardizzazione di processi.

Attraverso i *Financial Data Sharing Schemes*, la FIDA demanda ai player di mercato il disegno dell'ecosistema di *Open Finance* attraverso cui abilitare lo scambio di dati, di modo che la collaborazione diventi un elemento cardine per l'implementazione di sistemi virtuosi di scambio dei dati. Tuttavia, il disegno può lasciare alimentare delle questioni. La definizione di regole tecniche di condivisione dei dati affidata ad una molteplicità di soggetti può di fatto tradursi in un gravame eccessivo per i soggetti vigilati e incrementare i costi di *compliance* degli intermediari, costringendoli ad adottare differenti *standard* per la condivisione dei dati, oltre che alimentare distorsioni e forme di arbitraggio regolamentare.

Opportunità ed incognite accompagnano la proposta. La proposta costituisce senza dubbio un'interessante novità per gli operatori di mercato ed apre significative opportunità in un settore in cui l'elaborazione dei dati resa possibile dal rapido sviluppo dell'intelligenza artificiale, potrebbe ef-

fettivamente consentire un importante miglioramento della qualità del servizio reso alla clientela. Restano comunque da mettere a punto alcuni aspetti che meritano attenzione e cautela, tra cui, oltre a quanto già detto, il metodo di identificazione degli operatori, l'autenticazione del cliente, le regole alla base della remunerazione. Profili che saranno auspicabilmente meglio definiti prima della formale adozione del regolamento.

7. Trasparenza e lotta alle frodi

Se da un lato la digitalizzazione del settore finanziario ha portato a una crescente disponibilità di servizi innovativi facilmente accessibili a costi ridotti dall'altro ha posto temi di gestione dei dati e determinato un incrementato della vulnerabilità complessiva del sistema, rendendolo un obiettivo per la criminalità informatica.

L'innovazione tecnologica, come detto, è uno dei pilastri su cui si fonda il percorso di evoluzione verso modelli sempre più open. Questa sfida, tuttavia, presenta oggi molte insidie, soprattutto in termini di sicurezza dei dati condivisi. Il sistema finanziario risulta infatti particolarmente esposto alla minaccia del cyber crime, che si evolve adottando strumenti e tecniche sempre più sofisticati. La digitalizzazione del settore ha, da un lato, garantito lo sviluppo e l'offerta di servizi innovativi di facile accesso e a costi decrescenti, ma, dall'altro, ne ha anche aumentato la vulnerabilità. Per rimanere competitive sul mercato, le banche devono dunque ricercare, come precondizione per l'offerta di nuovi servizi, il corretto equilibrio tra innovazione e sicurezza.

Il mercato sta cercando di far fronte alle rinnovate esigenze attraverso strumenti di preventiva verifica che consentono ai clienti di controllare i dettagli del conto del beneficiario prima dell'invio di un'istruzione di pagamento; identificatori di entità giuridica, quali ad esempio il codice LEI (*Legal Entity Identifier*), che permette l'identificazione di qualsiasi ordinante o beneficiario di un pagamento in modo preciso, istantaneo e automatico a livello transfrontaliero; l'Intelligenza artificiale (AI) e il *Machine Learning* (ML), che consentono di identificare i casi di frode in un elevato volume di transazioni; la tecnologia *Blockchain*, che rende la condivisione delle informazioni tra i soggetti coinvolti nelle transazioni molto più sicura rispetto alle transazioni tradizionali.

Un tema è rappresentato dalla frammentazione tra normative dei vari paesi coinvolti, da cui la necessità di una maggiore armonizzazione, sempre con un approccio che tenga conto degli orientamenti del mercato e degli strumenti proprietari già sviluppati e sperimentati con successo a livello corporate.

In Europa, il *Payment Service Regulation*, assieme alla *Payment Service Directive* 3 e alla *Financial Data Access Regulation*, intende migliorare l'esperienza di pagamento dei consumatori e delle imprese, nonché garantire la protezione dei dati e la sicurezza delle transazioni. Il regolamento sugli *Instant Payments*, recentemente approvato, modifica e modernizza il regolamento del 2012 sul regolamento unico sui pagamenti in euro (Sepa), al fine di migliorare la disponibilità di opzioni di pagamento istantaneo in euro, che consentono il trasferimento di denaro entro dieci secondi, per i consumatori e le imprese nell'UE e nei paesi del See. La direttiva PSD3 è finalizzata a rafforzare la regolamentazione degli istituti di pagamento nell'Unione europea operanti quali Prestatori di Servizi di Pagamento vigilati. Essa introduce nuove normative riguardanti i servizi di prelievo di contanti, richiede l'elaborazione di un piano di liquidazione come parte del processo di richiesta di autorizzazione e amplia le possibilità di protezione dei fondi; si propone di potenziare la trasparenza e l'efficienza nel settore dei pagamenti con l'obiettivo di mantenere registri sempre aggiornati delle istituzioni autorizzate e stabilire un quadro per la cooperazione transfrontaliera.

Sia il *Payment Service Regulation* che la proposta normativa sugli *Instant Payments* prevedono l'obbligo da parte dei prestatori di servizi di pagamento di adottare schemi di prevalidazione per verificare la corretta associazione tra il nome del beneficiario di un pagamento e il codice Iban di cui è titolare. Tali strumenti sono già presenti e operativi sul mercato.

Sul solco dell'importanza della verifica del soggetto beneficiario, anche per contrastare le frodi, nel 2020 in Italia Cbi aveva implementato il servizio Check Iban, che consente – come già evidenziato (infra par. 3) -la verifica della corretta associazione tra codice Iban e codice fiscale/partita Iva del beneficiario di un pagamento, prima a supporto della Pubblica amministrazione, poi delle corporate anche nella sua declinazione *cross-border*. Il successo del servizio è dimostrato dagli elevati tassi di crescita (+120% su base annua, con una previsione di oltre 5,5M di operazioni nell'anno 2023).

Inoltre, il servizio Name Check consente di verificare in tempo reale la corrispondenza tra il nominativo del beneficiario di un pagamento e il codice Iban a esso associato, consentendo agli utenti (sia Corporate che Retail) di evitare pagamenti accidentali e indirizzati al titolare di un conto corrente sbagliato e fornendo un ulteriore livello di protezione nella lotta contro le frodi e le truffe. Per espandere il servizio Name Check a livello europeo, e non solo, Cbi ha attivato varie interlocuzioni con partner internazionali, avviando in particolare una collaborazione con Swift per l'utilizzo della sua funzionalità *Pre-Validation Account*. Questa collaborazione

consentirà a entrambi gli operatori di ampliare i rispettivi mercati, costituendo una rete di verifica più ampia e un maggiore livello di sicurezza per gli utenti dei servizi finanziari. In particolare, nei prossimi mesi, le banche italiane potranno effettuare verifiche all'estero attraverso Cbi, implementando una soluzione unica a livello nazionale e transfrontaliero.

Servizi come Name Check e Check Iban, peraltro, rappresentano importanti strumenti antifrode in linea con alcuni dei target specifici dei *Sustainable Development Goals* delle Nazioni Unite, in quanto consentono risparmi in termini di costi, maggiore efficienza, ridotto impatto ambientale dei servizi finanziari, maggiore innovazione attraverso un ecosistema collaborativo tra i player del mercato [11].

[11] Https://uncefact.unece.org/display/uncefactpublic/CHECK+IBAN+OPEN+FINANCE+USE+CASE.

Marco Cassese

Open Banking e profilazione dei dati nei servizi di pagamento

SOMMARIO: 1. Introduzione. – 2. La profilazione dei dati nell'*Open Banking* – 2.1. Definizione normativa e profilazione dei dati da parte dei TPPs. – 2.2. Le basi giuridiche del trattamento da parte dei TPPs. – 2.3. La profilazione: titolarità del trattamento e disciplina vigente. – 2.4. ... (segue): il trattamento automatizzato. – 3. Conclusioni preliminari e prospettive future.

1. Introduzione

Con l'introduzione del modello *Open Banking*, la direttiva UE n. 2015/2366 (PSD2) ha reso i dati bancari e di pagamento dei clienti delle banche accessibili a nuove categorie di soggetti, i c.d. *Third-Party Providers* (TPPs), permettendo a questi ultimi di accedere al mercato e di erogare nuove tipologie di servizi nel settore dei pagamenti digitali [1].

Nell'ambito delle operazioni di pagamento digitale così disintermediate, i TPPs svolgono un'attività strumentale, ma significativa, in quanto rendono più complesso il procedimento di pagamento, frammentandolo, e impongono ai fini del successo di ciascuna operazione una collaborazione tra

[1] Per una panoramica generale sull'*Open Banking* si vedano, *inter alia*: BANCA D'ITALIA, *PSD2 e Open Banking: nuovi modelli di business e rischi emergenti*, 2021; BANCA D'ITALIA, *Occasional papers: questioni di economia e finanza "intelligenza artificiale nel credit scoring"*, n. 721/2022; Banca d'Italia, *L'Open Banking nel sistema dei pagamenti: evoluzione infrastrutturale, innovazione e sicurezza, prassi di vigilanza e sorveglianza*, n. 31/2023; D. GAMMALDI, C. IACOMINI, *Mutamenti del mercato dopo la PSD2*, in F. MAIMERI, M. MANCINI (a cura di), *Le nuove frontiere dei servizi bancari e di pagamento fra PSD2, criptovalute e rivoluzione digitale*, Banca d'Italia, Quaderni di ricerca giuridica, n. 87, settembre 2019; THE BERLIN GROUP (2021), *NextGenPSD2 XS2A Framework Implementation Guidelines*, settembre 2021; EBA, Orientamenti in materia di esternalizzazione, (EBA/GL/2019/02), 25 febbraio 2019.

i diversi intermediari, che svolgono attività distinte, ma dipendenti l'una dall'altra, connesse dal necessario scambio di dati e informazioni [2].

La mole delle informazioni scambiate e raccolte dai PSP di radicamento di conto e dai TPPs compongono il modello in esame, che ha negli anni dischiuso, quale corollario, l'*Open Finance*, oggi sotto evidenza specie in seguito all'adozione della proposta legislativa del 28 giugno 2023 che prende il nome di *Financial Data Access and Payments Package* [3] che include, oltre alla revisione della PSD2, proprio la instaurazione di un quadro giuridico embrionale di condivisione dei dati finanziari, sulla falsa riga e sulla base delle lezioni apprese dall'applicazione della PSD2 in materia di condivisione dei dati relativi ai conti di pagamento [4]. La rapida successione dal modello «banking» a quello «finance» si deve specialmente alle politiche europee, che nonostante abbiano registrato tutt'oggi scarsi risultati in materia di *Open Banking*, si sono orientate alzando la posta in gioco promuovendo la instaurazione di un vero e proprio spazio europeo di dati finanziari.

In genere, i dati dell'utente-interessato oggetto di condivisione non configurano esclusivamente come dati finanziari o para-finanziari ma, come successivamente esaminato, anche come dati personali. Da tale

---

[2] F. MARASÀ, *Il trattamento dei dati personali dell'utente dei servizi di pagamento tra PSD2 e GDPR,* in *Riv. ODC,* n. 2/2020, p. 632. L'incisività è data dalla instaurazione del nuovo modello di *Open Banking* e dal fatto che sono entrati nuovi attori in un mercato da sempre "monopolistico". Sul tema si veda: BANCA D'ITALIA, *L'Open Banking nel sistema dei pagamenti: evoluzione infrastrutturale, innovazione e sicurezza, prassi di vigilanza e sorveglianza*, n. 31/2023; E. BANI, E. MACCHIAVELLO, *"Il diritto alla portabilità dei dati nell'ambito della nuova economia dei dati"*, 2021, p. 155, ove si sottolinea come tradizionalmente le banche sono sempre state le uniche depositarie di un ingente mole di dati dei clienti, proprio per la loro natura di "operatore universale", l'unico in grado di offrire qualsiasi tipo di servizio finanziario. Tuttavia, per effetto della PSD2, la riserva dei suddetti dati è stata aperta anche ai nuovi operatori; F. CIRAOLO, *Open Banking, Open Problems. Aspetti controversi del nuovo modello dei "sistemi bancari aperti"*, in *Riv. diritto bancario*, anno 2020 – fascicolo IV – sezione I, ove si evidenzia come le banche, con l'entrata in vigore della PSD2 abbiano effettivamente perso il monopolio sui dati dei propri utenti per effetto dell'obbligo normativo, la c.d. access to account rule, che impone loro "*di condividerli con altri soggetti, in nome dell'innovazione, dell'efficienza e dello sviluppo competitivo del mercato dei servizi di pagamento*", p. 612.

[3] Il pacchetto è composto dalle seguenti proposte normative: *Financial Data Access Regulation*, Bruxelles, 28 giugno 2023 COM(2023) 360 final; *Payment Services Directive III*, Bruxelles, 28 giugno 2023 COM(2023) 366 final; *Payment Services Regulation*, Bruxelles, 28 giugno 2023 COM(2023) 367 final.

[4] A seguito della emanazione della PSD2, si è effettuata una valutazione di impatto. Si veda: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13331-Payment-services-review-of-EU-rules/public-consultation_it.

configurazione ne discendono, principalmente, due effetti. In primo luogo, dal punto di vista degli operatori, si rende altamente appetibile l'attività di profilazione dei dati per finalità diverse da quelle strettamente connesse all'esecuzione dei propri servizi di pagamento; detti operatori, invero, facendo propri gli odierni progressi tecnologici e le capacità in materia di analisi dei megadati (*big data*), specie se *FinTech* e, in misura ancor più marcata, se *BigTech* [5], sono in grado di ottenere a mezzo della profilazione risultanze che gli consentono di praticare, nei confronti della propria utenza e dei *competitors*, logiche commerciali ad alta redditività [6].

In secondo luogo, dal punto di vista degli utenti, occorre tenere conto che la qualificazione dei dati come personali implica potenziali ripercussioni significative sui propri diritti e libertà [7]. Sia chiaro. L'attività di profilazione dei dati raccolti non costituisce l'attività principale svolta dagli operatori bancari ed è, anzi, un'attività eventuale e accessoria, ad eccezione dei casi in cui risulta obbligatoria con riguardo a determinate finalità di rilevanza pubblicistica [8]. Ciò però non toglie che gli utenti-interessati, nel godere loro stessi degli effetti benefici derivanti dalla profilazione dei propri dati, ricevendo – essenzialmente – offerte personalizzate di prodotti e servizi a costi più contenuti, corrono seri rischi di essere parallelamente soggetti a pratiche che comportano discriminazione ingiustificata, stereoti-

---

[5] BANCA D'ITALIA, *PSD2 e Open Banking: nuovi modelli di business e rischi emergenti*, *ibidem*, p. 7 ss.

[6] Ad esempio, le banche utilizzano il *credit scoring* automatizzato per prendere decisioni relative alla concessione di prestiti ai clienti, utilizzando come base i dati relativi a operazioni di pagamento e dati aggiuntivi come quelli ricavati da social media. Sul punto, si veda BANCA D'ITALIA, *Occasional papers: questioni di economia e finanza "intelligenza artificiale nel credit scoring"*, n. 721/2022, p. 25; F. BAGNI, *Uso degli algoritmi nel mercato del credito: dimensione nazionale ed europea*, in *Riv. OSF,* n. 2/021, p. 3; BANCA D'ITALIA, *PSD2 e Open Banking: nuovi modelli di business e rischi emergenti*, 2021*,* ove si afferma che: "*I dati ceduti potrebbero essere utilizzati dagli intermediari per l'offerta di prodotti personalizzati e maggiormente rispondenti alle esigenze finanziarie della clientela ma anche per la proposta di servizi accessori di natura non finanziaria, ovvero per la costruzione di nuovi servizi da destinare a soggetti terzi*", p. 27 ss.

[7] Da ultimo, si veda EDPB, Opinion n. 39 sulla Proposta di Regolamento sui Servizi di pagamento e sulla Proposta di direttiva sui Servizi di Pagamento III, del 22 agosto 2023, in cui si indica che "*I servizi di pagamento spesso comportano il trattamento di dati personali che possono rivelare informazioni sensibili su un singolo interessato*", p. 1.

[8] Tutti i PISP e gli AISP sono soggetti obbligati ai sensi della direttiva (UE) 2015/849 del Parlamento europeo e del Consiglio relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo. Tali soggetti sono obbligati ad applicare misure di adeguata verifica della clientela specificate nella direttiva.

pizzazione, segregazione sociale e frode [9], specie quando l'attività di profilazione medesima sia svolta senza adeguate garanzie.

I confini normativi della profilazione dei dati nei servizi di pagamento sono stati solo in parte esplorati e sono ancora in evoluzione [10]. Per mettere ordine si impone dunque una preliminare (e breve) ricognizione della normativa vigente in materia, per poi analizzare la recente sentenza della Corte di giustizia europea [11], di significativa utilità per l'interprete ai fini di un corretto inquadramento dell'attività di profilazione nell'ambito dei servizi di pagamento e, infine, riflettere se la normativa recentemente proposta, ove adottata, comporti in tale ambito conseguenze giuridiche e/o fattuali degne di rilievo. Il tutto con una precisazione: le considerazioni che saranno svolte sono applicabili a tutti gli operatori bancari, ma affrontare l'analisi dall'ottica dei TPPs appare di indubbia utilità trattandosi di operatori di settore, di diversa entità, che mai prima d'ora hanno avuto accesso ai dati finanziari in questione e che certamente contribuiranno ad accrescere ulteriormente il ruolo rivestito dall'attività di profilazione nel settore. Tra questi, invero, figurano *BigTech* ed altre entità dotate di tecnologie di elaborazione dei dati

[9] Tra le pratiche più note che hanno ingenerato elevati rischi di violazione della privacy e di frode sono lo *Screen Scraping* e il *Reverse Engeneering*. Il primo, consiste in una forma di intercettazione dei dati dai siti web, che nacque inizialmente come copia/incolla manuale, evolvendo poi in processi software automatizzati in grado di emulare le modalità di accesso del cliente. Per accedere ai conti on-line i metodi di *screen scraping* richiedono che il cliente inserisca le credenziali di accesso al sito di internet banking della propria banca (ad es. nome utente e password) nella pagina web, o nell'APP, che la terza parte utilizza per i servizi di pagamento; la terza parte effettua così l'accesso al sito di on-line banking simulando, tramite appositi software, la navigazione del cliente ed eseguendo operazioni dispositive e/o informative al posto del cliente stesso. Quanto alla pratica del *Reverse Engineering*, essa consiste invece nella ricostruzione del codice delle applicazioni di mobile banking per capire quali informazioni sono scambiate tra l'applicazione del cliente e i server delle banche, realizzando successivamente una versione "reverse engineered" dell'applicazione in grado di instaurare direttamente la comunicazione da/verso i server delle banche, senza possibilità di rilevamento e consapevolezza da parte di queste ultime. Come anticipato, entrambe le tecniche presentano diversi fattori di rischio in termini di sicurezza e di conservazione dei dati. Ciò, in particolare, dal momento che il Third Party, memorizzando le credenziali del cliente e avendo pieno accesso al conto del cliente ha, ad esempio, la possibilità di accedere a ulteriori informazioni rispetto a quelle per le quali ha ottenuto l'autorizzazione; il medesimo Third Party potrebbe inoltre eseguire transazioni finanziarie non autorizzate e modificare, in maniera autonoma e senza consenso, le stesse credenziali di accesso ai dati e ad altre operazioni bancarie del cliente.

[10] Al groviglio normativo generatosi dalla molteplicità delle normative interessate, quali principalmente il regolamento UE 2016/679 (GDPR) e la PSD2, occorre tenere presente che il panorama assumerà ulteriori sfumature nel caso in cui siano adottate le recenti proposte normative già menzionate

[11] Corte giust. UE, sez. I, Sent., 7 dicembre 2023, C-634/21.

all'avanguardia, che non guardano *ab origine* alla profilazione come un'attività meramente eventuale e accessoria, ma principale, specie qualora si tratti di dati di un elevato grado di affidabilità, come quelli finanziari.

2. La profilazione dei dati nell'*Open Banking*

2.1. Definizione normativa e profilazione dei dati da parte dei TPPs

La profilazione [12] dei dati si inserisce tra le tecniche aziendali che consentono, mediante la realizzazione di un insieme di attività, di raccogliere ed elaborare dati inerenti agli utenti di un servizio, al fine di suddividerli in gruppi a seconda del loro comportamento e di analizzare o prevedere aspetti della loro vita.

Nell'economia digitale la profilazione dei dati ricorre a tecniche ad alta intensità tecnologica completamente distinte da quelle tradizionali. Diverse e variegate sono le sue composizioni, le sue componenti, le sue funzionalità e finalità; diversità di elementi i quali, senza dubbio, rendono assai arduo offrirne una ricostruzione tecnica unitaria e generalizzata. Tuttavia, con un certo grado di approssimazione, può affermarsi che la profilazione espletata nel nuovo contesto tecnologico è scomponibile in tre distinte fasi: i) la raccolta dei dati; ii) l'analisi degli stessi, di regola in forma automatizzata e mediante l'impiego di algoritmi, per individuare correlazioni ed elaborare un profilo; iii) l'applicazione del profilo così ricavato a una persona fisica per individuare caratteristiche di comportamento presenti o future.

---

[12] Per un approfondimento sulla profilazione in generale si rinvia a: F. MARASÀ, *Il trattamento dei dati personali dell'utente dei servizi di pagamento tra PSD2 e GDPR*, *ibidem*; G. GOMETZ, *Intelligenza artificiale, profilazione e nuove forme di discriminazione*, in *Riv. teoria e storia del diritto privato*, 2022; F. BAGNI, *Uso degli algoritmi nel mercato del credito: dimensione nazionale ed europea*, in *Riv. OSF*, n. 2/2021; M. DE MARI, *La profilatura finanziaria algoritmica*, in *Riv. ODC*, n. 1/2021; M. ZAPPATORE, *Big Data, Profilazione e Mercati Finanziari: utilizzo e tutela*, in *Riv. giur. civ.*, 2019, 4 (ISSN 2532-201X); F. Mattassoglio, *La profilazione dell'investitore nell'era dei Big Data. I rischi dell'estremizzazione della regola del "Know your Customer"*, in *Riv. trim. dir. econ.*, 4/2016 supplemento n. 1. Sul piano istituzionale, si richiamano inoltre: Linee guida dell'EDPB sul trattamento di dati personali ai sensi dell'art. 6, par. 1, lett. b), del regolamento generale sulla protezione dei dati nel contesto della fornitura di servizi online agli interessati, n. 2, adottate il 8 ottobre 2019; Linee guida dell'EDPB sull'interazione tra la seconda direttiva sui servizi di pagamento e il GDPR, n. 6, adottate il 15 dicembre 2020; Linee guida del Gruppo di Lavoro articolo 29 per la protezione die dati sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679, adottate il 3 ottobre 2017, versione emendata e adottata in data 6 febbraio 2018.

L'attività di profilazione dei dati può essere, poi, pura o complessa. Si parla di profilazione pura quando l'attività è priva di processi decisionali, componendosi della semplice raccolta di dati mediante modalità non necessariamente automatizzate. La profilazione è invece complessa quando rispetto ad essa si pone, a monte e/o a valle, un processo decisionale che può essere automatizzato o esclusivamente automatizzato, non prevedendo alcun intervento umano [13].

Oggetto dell'attività di profilazione sono generalmente i dati personali. Ogni volta che viene espletata, specie se il soggetto che svolge l'attività di profilazione ha accumulato una ingente quantità di tali dati, si configura pertanto "*un rischio elevato per i diritti e le liberà delle persone fisiche* [14]" che vedono incrementare significativamente i rischi di incorrere nei diversi fenomeni di discriminazione ingiustificata [15], di stereotipizzazione e di segregazione sociale, da parte dei gestori dei dati, nonché di frode e di furto di identità, da parte degli *hacker*. Ciò si palesa in maniera ancor più marcata quando l'attività di profilazione è espletata da un *BigTech* o una *FinTech*, nella veste di TPP, in quanto sono agglomerati, sotto un unico titolare, enormi quantità di dati di alta qualità (come quelli finanziari-personali) unitamente ad altri dati di qualità ed affidabilità variabile (dati reperiti dai *social* [16]).

---

[13] Le Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679 del 2018, forniscono un esempio per comprendere tale differenza. Si ricorre all'ipotesi del soggetto richiedente un prestito online: "*un essere umano decide se accordare il prestito sulla base di un profilo prodotto con mezzi unicamente automatizzati – punto ii); un algoritmo decide se il prestito viene accordato e la decisione viene trasmessa automaticamente alla persona, senza alcuna previa valutazione significativa da parte di un essere umano – punto iii)*".

[14] Art. 35, par 1, del GDPR.

[15] Si veda, tra i vari: A. AZZUTTI, W.-G. RINGE, H. S. STIEHL, *Machine Learning, Market Manipulation and Collusion on Capital Markets: Why the "Black Box" Matters*, in *European Banking Institute*, 2021, Working Paper 84; K. JOHNSON, F. PASQUALE, J. CHAPMAN, *Artificial Intelligence, Machine Learning, and Bias in Finance: Toward Responsible Innovation Symposium: Rise of the Machines: Artificial Intelligence, Robotics, and the Reprogramming of Law*, in (2019) *88 Fordham L Rev* 499; S. KELLEY *et al.*, *Antidiscrimination Laws, Artificial Intelligence, and Gender Bias: A Case Study in Nonmortgage Fintech Lending*, in (2022) *24 M&SOM* 3039.

[16] Il fatto, tutt'altro che residuale, per il quale i BigTech e le FinTech, nella veste di TPP, profilano i dati finanziari unitamente ai dati personali, e non, raccolti negli altri settori in cui operano rappresenta un punto cruciale ed è determinante con riguardo alla tematica della c.d. combinazione dei dati. Gli utilizzatori dei dati possono in pratica scegliere di combinare fonti di dati tradizionali con "nuove" fonti di dati, che possono portare a un'analisi più sofisticata o completa di alcuni segmenti vulnerabili di consumatori, come le persone a basso reddito, o possono aumentare il rischio di condizioni sleali o di pratiche tariffarie differenziate, come l'applicazione di premi differenziati.

Facendo un passo indietro e nel limitare l'indagine della presente trattazione alla profilazione dei dati raccolti nell'ambito dell'*Open Banking*[17], è da evidenziarsi come, di fatto, una certa attività di profilazione risulti quasi necessaria tanto per i *Payment Initiation Service Providers* (PISPs) quanto per gli *Account Information Service Providers* (AISPs). Nell'ipotesi di servizi erogati dai PISPs, veri e propri intermediari di pagamento abilitati dall'utente ad eseguire transazioni a loro nome collegandosi direttamente al conto bancario per trasferire i fondi al beneficiario, gli operatori hanno, di regola, accesso alle seguenti tipologie di dati: dati inerenti all'ordine di pagamento (a titolo esemplificativo, l'importo del pagamento, la valuta, la data e l'ora della transazione, il beneficiario), essenziali per processare la transazione, che sono generalmente forniti dal commerciante o dallo stesso sistema di pagamento; dati sul conto bancario (a titolo esemplificativo, la banca mittente, la proprietà del conto bancario, il numero dello stesso, l'origine dei fondi e il saldo del conto al momento del pagamento); dati di autenticazione (a titolo esemplificativo, password, codici OTP, dati biometrici); dati sul tipo e la frequenza delle transazioni passate; dati identificativi (a titolo esemplificativo, nome e cognome, indirizzo di residenza, numero telefonico, indirizzo mail, data di nascita, nazionalità e cittadinanza), di regola fornite direttamente dall'utente. Dal punto di vista degli AISPs, la cui attività principale è, al contrario, meramente informativa, avendo l'incarico di fornire all'utente, in un'unica interfaccia, tutte le informazioni – quali principalmente transazioni e saldi – relative ai suoi conti online detenuti presso i diversi ASPSP, il prestatore del servizio svolge invece un'attività esclusiva di raccolta e di gestione di alcuni dei dati finanziari sopraindicati degli utenti, ma relativi ad ogni istituto bancario aggregato.

Ebbene, la grande maggioranza dei dati sopra indicati non sono solo finanziari, ma consentono l'identificazione degli utenti del servizio di pagamento (del pagatore e del beneficiario[18]) e quindi rientrano a pieno titolo

---

[17] La sede non consente una disamina di tutte le ipotesi plausibili. Tuttavia, vista l'importanza rivesta dalle pratiche di combinazione dei dati, specie da quando sono entrati i nuovi *players* nel settore, nella parte dedicata all'analisi della disciplina applicabile si svolgeranno alcune considerazioni sul quadro normativo applicabile a tali pratiche.

[18] Il riferimento è al trattamento dei dati dei taciti interessati, c.d. *silent parties*, i quali, per l'appunto, non hanno rilasciato alcun'autorizzazione a trattare i propri dati da un prestatore di servizi di pagamento ai fini dell'esecuzione di un contratto stipulato con l'utente di tale servizio. Per un approfondimento sul tema, si vedano: Linee guida 06/2020 sull'interazione tra la seconda direttiva sui servizi di pagamento e il GDPR; F. MARASÀ, *Il trattamento dei dati personali dell'utente dei servizi di pagamento tra PSD2 e GDPR*, in *Riv. ODC*, n. 2/2020.

nella definizione di dati personali. A titolo esemplificativo, costituiscono dati personali raccolti dai TPPs nell'ambito della prestazione di un servizio di pagamento o di informazione su conti non solo i dati non direttamente inerenti al servizio medesimo, come il nome, il numero di telefono, la residenza, l'indirizzo di posta elettronica, etc., del pagatore e del beneficiario, ma anche i dati specificamente attinenti allo stesso [19], come l'identificativo unico bancario ovvero la combinazione di lettere, numeri o simboli che il prestatore del servizio indica all'utente e che quest'ultimo deve fornire per identificare con chiarezza un altro utente del servizio e/o il conto di pagamento dell'altro utente del servizio per una determinata operazione di pagamento [20].

La necessità di acquisire e archiviare le diverse tipologie dei dati sopraindicati per erogare il proprio servizio di pagamento o di informazione su conti è la conferma che i servizi erogati, rispettivamente, dai PISPs e dagli AISPs, risultano parzialmente inscindibili da una certa attività di profilazione dei dati medesimi: la conoscenza di dette informazioni consente invero, e inevitabilmente, di ottenere un certo grado di visione delle spese dell'utente-interessato, delle sue operazioni di pagamento, dei suoi acquisti, etc. [21]. Alla luce di quanto detto non sorprende dunque che la definizione normativa di profilazione prevista dal legislatore europeo sia contenuta nella disciplina dedicata alla protezione dei dati personali, e precisamente nel GDPR [22], che la definisce come una "*qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica*".

---

[19] F. MARASÀ, *Il trattamento dei dati personali dell'utente dei servizi di pagamento tra PSD2 e GDPR*, *ibidem*, p. 650.

[20] Art. 4, par. 1, n. 33, PSD2. I dati relativi ai pagamenti sono stati ritenuti dati personali dalla giurisprudenza ben prima dell'entrata in vigore del GDPR: si veda, *inter alia*, F. MARASÀ, *Il trattamento dei dati personali dell'utente dei servizi di pagamento tra PSD2 e GDPR*, *ibidem*, p. 651.

[21] La definizione normativa di profilazione contenuta nel GDPR risulterebbe in tali casi integrata in quanto "*... trattamento ... consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare ... aspetti riguardanti il rendimento professionale, la situazione economica, ... il comportamento, ... di detta persona fisica*".

[22] L'art. 4, par. 1, n. 4, del GDPR si ispira alla definizione di profilazione di cui alla raccomandazione CM/Rec (2010)13.

Non sussiste, invece, una definizione specifica di profilazione dei dati da parte degli operatori bancari che, in linea generale, devono trattare i dati raccolti nel limite di quanto necessario per l'esecuzione del contratto stipulato tra i medesimi e l'utente-interessato, avente ad oggetto la prestazione di un servizio di pagamento [23].

La principale ragione di questa impostazione normativa sta, verosimilmente, nelle logiche fatte proprie dall'Unione europea nelle politiche legislative degli ultimi anni in materia di Strategia per il mercato unico digitale [24], in generale, e delle Strategie per la finanza digitale [25] e per i pagamenti al dettaglio [26], con riguardo al settore finanziario. Logiche che, in breve, conducono in materia di economia digitale ad una disciplina verticale e specifica dei singoli settori di riferimento, quanto al loro funzionamento, servizi e peculiarità, e ad una disciplina orizzontale delle attività e degli strumenti tecnologici generalmente utilizzati, come proprio la profilazione, applicabile in via trasversale in tutti i settori.

Le considerazioni svolte, seppur sommarie, consentono di collocare l'attività di profilazione dei dati acquisiti da parte dei TPPs durante la prestazione del proprio servizio nell'alveo applicativo del GDPR, che per l'appunto definisce l'attività di profilazione come l'"*... utilizzo di [tali] dati personali per valutare determinati aspetti personali relativi a una persona fisica ...*". Ciò trova ulteriore conferma guardando all'ipotesi in cui l'attività di profilazione viene svolta dai TPPs su più categorie di dati, in combinazione tra loro [27], per fini diversi dall'esecuzione del servizio principale richiesto dall'utente, e precisamente per finalità di analisi della clientela e di creazione di profili personali, con eventuale suddivisione in *clusters* da analizzare e valutare [28], per fare previsioni in relazione ad aspetti quali la capa-

[23] Inserisci meglio spiegazione più analitica degli artt. 66, 67 e 94 PSD2.

[24] Bruxelles, 6 maggio 2015, COM(2015)192 final.

[25] Bruxelles, 24 settembre 2020, COM(2020) 591 final.

[26] Bruxelles, 24 settembre 2020, COM(2020) 592 final.

[27] La PSD2 vieta di usare i dati per fini diversi ma non sembra "vietare" la combinazione di dati che può essere effettuata dalle BigTech e dalle FinTech tra i dati acquisiti nello svolgimento dei servizi di pagamento e altre informazioni relative agli utenti (ad es., dati ricavati da internet) ai fini anche di una maggiore personalizzazione e qualità dei servizi.

[28] Sul punto si richiama l'ordinanza della Corte di Cassazione n. 32411, del 8 novembre 2021. Nel caso di specie una società aveva predisposto, sul proprio sito, offerte personalizzate, ricorrendo ad un algoritmo, sulla base di informazioni ulteriori e specifiche rilasciate dal cliente con la compilazione di una scheda. La Cassazione ha specificato che il trattamento di dati personali posto in essere con modalità automatizzate al fine di analizzare abitudini o scelte di con-

cità di compiere determinate attività, gli interessi in merito a prodotti e servizi, l'affidabilità creditizia ed eventuali altre caratteristiche legate alla sfera personale [29].

2.2. Le basi giuridiche del trattamento da parte dei TPPs

La profilazione dei dati svolta dai TPPs risulta, dunque, soggetta prevalentemente alla disciplina contenuta nel GDPR, oltreché a quella contenuta nella PSD2. Assumono inoltre rilievo le linee guida in materia elaborate dall'EDPB, che "*sono pienamente pertinenti nel contesto dei servizi di pagamento e dovrebbero pertanto essere prese in debita considerazione*" [30].

Procedendo con ordine, è bene osservare che l'attività di profilazione di dati personali nient'altro è che una forma di trattamento degli stessi [31]. Il medesimo GDPR, tra l'altro, esordisce definendo l'attività di profila-

---

sumo, sebbene non comporti l'identificazione precisa di un individuo e sia diretta ad offrire un'offerta commerciale adeguata alle caratteristiche dell'interessato, "*non può che essere una manifestazione della profilazione del cliente*". Rilevante, infatti, è l'attività di screening dei dati personali attraverso un algoritmo, "*al fine di analizzare o prevedere le specifiche esigenze dell'utente fruitore, in vista di un vantaggi economico*".

[29] Linee Guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679: "*In generale, la profilazione consiste nella raccolta di informazioni su una persona (o un gruppo di persone) e nella valutazione delle loro caratteristiche o dei loro modelli di comportamento al fine di includerli in una determinata categoria o gruppo, in particolare per analizzare e/o fare previsioni, ad esempio, in merito a: capacità di eseguire un compito; interessi, o comportamento probabile*". Sul tema, si veda: I risultati dell'indagine conoscitiva interdisciplinare sui Big Data, deliberata congiuntamente dall'AGCOM (delibera n. 217/17/CONS), dall'AGCM e dal Garante per la privacy. 10 febbraio 2020), ove si precisa che "*La funzione predittiva della profilazione, volta ad anticipare i bisogni degli individui, avviene ricorrendo a tecniche di organizzazione e modellizzazione dei dati raccolti, con l'obiettivo di incidere sulle scelte dei singoli individui, adattandole alla realtà che si vive in un determinato periodo di tempo*", p. 23.

[30] Linee guida 06/2020 sull'interazione tra la PSD2 e il GDPR, p. 28.

[31] La PSD2 menziona il trattamento dei dati personali al Considerando n. 89 e all'art. 94. In particolare, è specificato che il GDPR si applica al trattamento dei dati personali effettuato nell'ambito dei servizi di pagamento. Infatti, il Considerando n. 89 della PSD2 dispone che: "*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*".

zione come "*qualsiasi forma di trattamento automatizzato di dati personali …*". A tal riguardo, sembrano potersi distinguere tre distinte circostanze in cui i TPPs trattano i dati personali dei propri clienti: (i) quando il trattamento risulta necessario per l'esecuzione di un contratto di cui l'interessato è parte [32]; (ii) quando il trattamento risulta necessario per prevenire, indagare ed individuare casi di frode nei pagamenti [33]; e (iii) quando il trattamento viene svolto, dietro consenso dell'interessato, per finalità diverse da quelle strettamente connesse all'esecuzione del servizio di pagamento.

In materia, impianto cardine del GDPR è la sussistenza di una base giuridica che legittimi il trattamento (e, quindi, la profilazione) dei dati da parte dei TPPs in ognuna delle dette circostanze. Con riguardo alla prima circostanza, che rappresenta l'ipotesi più ricorrente in materia di prestazione di servizi di pagamento, v'è da precisare che i dati personali sono lecitamente trattati dai vari attori coinvolti nell'erogazione del servizio di pagamento (TPP e ASPSP) in favore dell'utente-interessato sulla base, ciascuno, di distinte basi giuridiche di trattamento, che sono tutte rinvenibili nel GDPR e il cui elenco è da considerarsi tassativo ed esaustivo [34].

Come generalmente condiviso, nemmeno l'art. 94, par. 2, della PSD2 può considerarsi propriamente una base giuridica di trattamento supplementare, seppur lo stesso preveda che la raccolta, il trattamento e la conservazione dei dati personali da parte dei prestatori dei servizi di pagamento sia legittima nel solo caso in cui i dati personali risultino necessari alla prestazione dei rispettivi servizi di pagamento e l'utente del servizio abbia prestato apposito consenso esplicito [35]. Detto consenso, invero, è da considerarsi piuttosto come un requisito aggiuntivo di natura negoziale (più precisamente, una autorizzazione del cliente), non assimilabile al consenso (esplicito) ai sensi del GDPR [36], e non passibile di essere

---

[32] Art. 6, par. 1, lett. b), GDPR.

[33] Art. 94, par. 1, PSD2.

[34] Si veda, tra l'altro, la sentenza della Corte di giustizia (C-252/21) sul caso *Meta Platforms Inc. c. Bundeskartellamt*, del 4.07.2023; Linee Guida 06/2020 *dell'European Data Protection Board (EDPB) sull'interazione tra la seconda direttiva sui servizi di pagamento e il GDPR*.

[35] Art. 94, par. 2, PSD2.

[36] Sul punto è da evidenziarsi come anche l'EDPB, nelle recenti Opinion n. 38 e 39, sottolinei come entrambe le proposte PSR e FIDA dovrebbero specificare che la concessione di "autorizzazioni" per accedere ai dati finanziari non equivale a dare il consenso ai sensi del GDPR. Di conseguenza, l'EDPB precisa che tutti i trattamenti di dati personali a seguito di una richie-

soggetto ad alcuna verifica da parte dell'ASPSPs, di volta in volta coinvolto, per espressa previsione normativa, attualmente presente anche nella recentemente proposta di cui al pacchetto *Financial Data Access and Payments Package*[37].

Guardando ora alla prima circostanza, a monte, vi sono un contratto stipulato tra il TPP e l'utente-interessato, avente ad oggetto la prestazione di un servizio di pagamento o di informazione su conti e la necessità per il medesimo TPP di richiedere all'ASPSP l'accesso ai dati personali dell'utente-interessato relativi al conto corrente da utilizzarsi per l'esecuzione del servizio richiesto. L'ASPSP, di regola, già svolge un generico trattamento dei dati dell'utente-interessato in qualità di istituto presso cui è radicato il conto corrente da cui sarà disposto il pagamento in forza di una propria base giuridica di trattamento, che però non assume in questo contesto rilevanza dirimente; assume, invece, interesse lo specifico trattamento dei dati dallo stesso espletato, dietro richiesta del TPP, per l'esecuzione del servizio richiesto dall'utente-interessato, consistente nel concedere l'accesso ai dati del conto di pagamento. La legittimazione del trattamento qui esposto si basa su un preciso obbligo di legge[38], noto come la "*access to account rule*", che rappresenta proprio una norma cardine per l'intero impianto *Open Banking* prevedendo l'obbligo, a carico delle banche presso cui sono radicati i conti, di dare accesso ai PISPs e agli AISPs che forniscono de-

sta di accesso ai dati finanziari di un individuo devono avere una base giuridica adeguata ai sensi del GDPR. Si veda, in particolare: EDPB, Opinion n. 39, *ibidem*, nn. 1 e 2, e EDPB, Opinion n. 38 sulla Proposta di Regolamento sull'accesso ai dati finanziari, n. 4, 22 agosto 2023. In tali Opinions l'EDPB raccomanda tra l'altro di chiarire che la concessione dell'autorizzazione non deve pregiudicare gli obblighi dei PISP e AISP in relazione all'art. 6 e 9 del GDPR, e spiega brevemente che il termine "esclusivamente", presente nel Considerando n. 69 della proposta, introduce un certo grado di incertezza e non consente di distinguere chiaramente tra permesso (riferito accettazione del servizio commerciale da parte del consumatore), da un lato, e consenso (ai sensi dell'art. 6, par. 1, lett. a), GDPR) o consenso esplicito (ai sensi dell'art. 9, par. 2, lett. a), GDPR), dall'altro.

[37] In un'ottica di rafforzamento della sicurezza degli utenti l'EDPB ad oggi raccomanda di eliminare il divieto imposto agli ASPSP di verificare l'autorizzazione all'accesso ai dati o, in alternativa, di introdurre garanzie per proteggere gli utenti dai rischi di condivisione illecita di dati personali. Tale rischio potrebbe avere come effetto il venir meno della fiducia degli utenti nei servizi di pagamento e aumentare anche il rischio di frodi. Si veda: EDPB, Opinion n. 39, ibidem, n. 3; nella medesima Opinion, l'EDPB inoltre sottolinea che il divieto in questione indurrebbe "*gli ASPSP a condividere i dati personali con terzi che non si sono assicurati un motivo legittimo adeguato ai sensi del GDPR (o a condividere più dati personali di quelli previsti dall'utente)*", par 17.

[38] Art. 6, par. 1, lett. c), GDPR.

terminati servizi di pagamento o informazione su conti relativamente ai dati relativi ai conti di pagamento degli utenti-interessati [39]. Accesso che, allo stato, come anticipato, deve essere concesso da parte dell'ASPSP senza poter fare previamente alcuna verifica.

Di regola, i TPPs ottengono i dati mediante l'impiego di API [40] ovverosia "*di interfacce che permettano a provider e programmi diversi di interagire in maniera sicura e predefinita, secondo le indicazioni tecniche fornite dall'European Banking Authority*" [41], predisposte dagli ASPSPs [42], iniziando così a svolgere il proprio trattamento su di essi. La base giuridica che legittima il trattamento in esame è diversa da quella relativa al trattamento degli ASPSPs sopra illustrata. In particolare, essa si ravvisa nella necessità di eseguire il contratto di prestazione di servizi di pagamento o di informazione su conti stipulato a monte tra il TPP e l'utente-interessato [43] e in questo caso l'ambito oggettivo dell'intero trattamento è li-

---

[39] Art. 36, direttiva PSD2. Sul tema si veda: E. BANI, E. MACCHIAVELLO, "*Il diritto alla portabilità dei dati nell'ambito della nuova economia dei dati*", 2021, p. 19.

[40] A dire il vero, le terze parti, prima che i servizi di *Open Banking* venissero regolati, utilizzavano diverse tecniche per accedere ai conti disponibili on-line dei clienti che avevano concesso il permesso di accedere alle proprie informazioni bancarie, tra cui lo *Screen Scraping* e il *Reverse Engineerd*, già precedentemente illustrate. Si veda: BANCA D'ITALIA, *L'Open Banking nel sistema dei pagamenti: evoluzione infrastrutturale, innovazione e sicurezza, prassi di vigilanza e sorveglianza*, *ibidem*, p. 36 ss., in cui si illustra tra l'altro che l'offerta dei servizi di *Open Banking* non può prescindere dall'utilizzo di una tecnologia che garantisca l'accesso sicuro a parti del patrimonio informativo dei correntisti detenuto dal mondo bancario da parte di attori esterni, quali, ad esempio, le società *fintech* o altri operatori attivi in campo finanziario; le API, in particolare, dovrebbero i) permettere la segregazione dei dati a cui si ha accesso, ii) consentire modalità di interazione sicure e iii) limitare la complessità tecnica necessaria all'integrazione tra il tradizionale mondo dei pagamenti e i nuovi soggetti. La questione è cruciale ai fini della efficienza del settore e della tutela degli interessati e invero anche l'EDPB se ne occupa nelle sue recenti Opinion nn. 38 e 39 relative alle normative proposte nell'ambito del Financial Data Access e Payments Package accogliendo positivamente le previsioni, ivi contenute, concernenti in particolare l'art. 43 del PSR che impone agli ASPSPs di mettere a disposizione dei TPP cruscotti standardizzati nelle forme di cui al regolamento medesimo e alle future norme tecniche da adottarsi.

[41] BANCA D'ITALIA, *L'Open Banking nel sistema dei pagamenti: evoluzione infrastrutturale, innovazione e sicurezza, prassi di vigilanza e sorveglianza*, *ibidem*, p. 20.

[42] Di regola, sono gli ASPSPs che realizzano interfacce dedicate. Oltre a queste, si precisa che gli ASPSP hanno anche l'obbligo di implementare e rendere operativa un'interfaccia alternativa (cd. interfaccia di *fall-back*), da utilizzarsi nel caso di indisponibilità dell'interfaccia principale. Gli ASPSP possono richiedere alle autorità competenti di essere esentati dalla realizzazione di detta interfaccia (c.d. *fall-back exemption*) dimostrando che l'interfaccia principale dedicata rispetti i requisiti di performance e robustezza definiti nella normativa.

[43] Linee guida 06/2020 sull'interazione tra la PSD2 e il GDPR, dalle quali si evince che i servizi di pagamento sono prestati sulla base di un contratto tra l'utente di servizi di pagamento

mitato solo ed esclusivamente ai dati necessari all'esecuzione del contratto medesimo. Non possono dunque prevedersi eventuali clausole che subordinano l'erogazione del servizio di pagamento (o di altri servizi, diversi e/o accessori) a talune attività di trattamento che di fatto non sono necessarie ai fini dell'esecuzione del contratto [44], non possono ampliarsi artificiosamente le categorie dei dati personali o le tipologie di trattamenti che il titolare necessita di effettuare per l'esecuzione del contratto e, del pari, non sono ammissibili le clausole che subordinano l'erogazione di un servizio alla richiesta di prestazione di un ulteriore servizio per il quale occorre trattare diversi e rilevanti dati personali, creando di fatto situazioni in cui gli utenti-interessati sono costretti ad accettare, o rifiutare, tutti i distinti servizi raggruppati in un unico contratto [45]. In breve, tracciando un minimo comune denominatore alle ipotesi indicate, si può affermare che il TPP deve essere sempre in grado dimostrare che il trattamento e la profilazione dei dati personali relativi al conto di pagamento è oggettivamente necessario per la prestazione di ciascun distinto servizio prestato [46].

---

e il prestatore di servizi di pagamento, e nelle quali si precisa, con riguardo al quadro normativo applicabile, che l'esecuzione di un contratto di cui all'art. 6 par. 1, lett. b), GDPR, rappresenta, nella maggior parte dei casi, la principale base giuridica per il trattamento dei dati personali nell'ambito della prestazione dei servizi di pagamento, p. 10.

[44] Art. 7, par. 4, GDPR. Sul punto assume rilievo il principio di minimizzazione e l'ordinanza della Corte di Cassazione, del 21 ottobre 2019, n. 26778, avente ad oggetto il trattamento di dati particolari da parte di una banca. In tale provvedimento il Supremo consesso chiarisce che "*la clausola con cui la banca ha subordinato l'esecuzione delle proprie operazioni al rilascio del consenso al trattamento dei dati sensibili contrasta indubitabilmente con i principi informatori della legge sulla privacy, la quale ha natura di norma imperativa, contenendo tale normativa precetti che non possono essere derogati dall'autonomia privata in quanto posti a tutela di interessi generali, di valori morali e sociali pregnanti nel nostro ordinamento, finalizzati al rispetto dei diritti e delle libertà fondamentali, quali la dignità, la riservatezza, l'identità personale, la protezione dei dati personali*". Nel caso di specie, quindi, emerge la violazione del principio di "minimizzazione dei dati personali", che impone il trattamento dei soli dati adeguati, pertinenti e limitati a quanto necessario per il perseguimento delle finalità per le quali sono trattati.

[45] EDPB, Linea guida 2/2019 sul trattamento di dati personali ai sensi dell'art. 6, par. 1, lett. b), del regolamento generale sulla protezione dei dati nel contesto della fornitura di servizi online agli interessati, p. 18.

[46] La Corte di giustizia, nel caso *Meta Platforms Inc. c. Bundeskartellamt*, ha chiarito come, nel caso dell'art. 6 par. 1, lett. b), il trattamento dei dati, per essere considerato necessario deve essere oggettivamente indispensabile per realizzare una finalità che costituisce parte integrante della prestazione contrattuale destinata a quegli stessi utenti, cosicché l'oggetto principale del contratto non potrebbe essere conseguito in assenza di tale trattamento.

Venendo ora alla seconda circostanza, ovverosia l'ipotesi in cui i TPPs trattano e profilano i dati personali per prevenire, indagare e individuare casi di frode nei pagamenti, è da evidenziarsi come questa sia generalmente occasionata dalla prestazione di un servizio di pagamento o di informazione su conti richiesto dall'utente-interessato. Le basi giuridiche che legittimano tale tipo di attività [47] sono, in base al caso, l'adempimento di un obbligo giuridico [48], ovvero il perseguimento di un interesse legittimo [49]. La loro peculiarità risiede nella rilevanza pubblicistica che assume la finalità di contrastare pratiche di rilevanza criminosa, quali ad esempio le frodi. Finalità che, nel delimitare di per sé le tipologie di dati personali suscettibili di formare lecitamente oggetto di trattamento, può persino comportare per il TPP la possibilità di dover profilare, lecitamente, un maggior numero di dati personali rispetto a quelli necessari per l'esecuzione del contratto di servizi concluso con l'utente-interessato.

Con riferimento all'ultima circostanza, infine, occorre tenere presente che il trattamento e la profilazione dei dati da parte dei TPPs per finalità diverse da quelle sin qui esaminate sono circoscritti in modo più significativo. Gli artt. 66, par. 3, lett. g) e 67, par. 2, lett. f), della PSD2, invero, richiedono espressamente che l'interessato abbia prestato il proprio consenso a norma dell'art. 6, par. 1, lett. a), del GDPR o che, in alternativa, il trattamento in oggetto sia previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, a norma dell'art. 6, par. 4, del GDPR. Tra le finalità in esame maggiormente perseguite si annovera lo scopo di proporre pubblicità mirata a un pubblico di soggetti aventi carat-

---

[47] L'art. 94, par. 1, PSD2 infatti prevede 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.*".

[48] Art. 6, par. 1, lett. c), GDPR.

[49] Art. 6, par. 1, lett. f), GDPR. In aggiunta, si veda il Considerando n. 47 del GDPR, che considera legittimo interesse di un titolare del trattamento – quale base giuridica ai sensi dell'art. 6, par 1, lett. f) – la prevenzione delle frodi. In riferimento a tale condizione di liceità del trattamento, occorre, ancora una volta, richiamare la sopracitata sentenza della Corte di giustizia nel caso *Meta Platforms*, ove il Supremo Consesso ha chiarito, ulteriormente, come il trattamento dei dati può considerarsi necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, solo a condizione che il suddetto operatore abbia indicato agli utenti presso i quali i dati sono stati raccolti un legittimo interesse perseguito dal loro trattamento, che tale trattamento sia effettuato entro i limiti di quanto strettamente necessario alla realizzazione di tale legittimo interesse e che dal contemperamento dei contrapposti interessi, alla luce di tutte le circostanze pertinenti, risulti che le libertà e i diritti fondamentali e gli interessi di tali utenti non prevalgono su detto legittimo interesse del titolare del trattamento o di terzi.

teristiche simili, che non può essere svolto sulla base dell'art. 6, par. 1, lett. b), in quanto non si può affermare che tracciare e confrontare le caratteristiche e i comportamenti dell'utente per finalità correlate alla pubblicità rivolta ad altre persone sia oggettivamente necessario all'esecuzione del contratto stipulato con l'utente medesimo.

2.3. La profilazione: titolarità del trattamento e disciplina vigente

A prescindere dalla base giuridica del trattamento dei dati personali di volta in volta applicabile, v'è da rimarcare come la definizione contenuta nell'art. 4, par. 4, del GDPR richieda che la profilazione implichi necessariamente una "*qualche forma di trattamento automatizzato*". Tale elemento comporta diverse considerazioni aventi conseguenze di non poco rilievo. In primo luogo, che va tenuto distinto dal concetto di profilazione quello relativo al processo decisionale totalmente automatizzato, che può condurre all'adozione di una decisione inerente all'interessato senza intervento dell'essere umano. Resta inteso che i due piani non sono totalmente distinti tra di loro e, in determinate circostanze, i processi decisionali automatizzati si pongono a valle dell'attività di profilazione ovvero vi si sovrappongono[50]. In secondo luogo[51], che l'attività di profilazione rientra sempre nella disciplina del GDPR, anche se espletata con coinvolgimento umano, purché sussista una qualche forma di trattamento automatizzato[52].

Ora, nell'ambito del trattamento (di profilazione) automatizzato o semi-automatizzato ci si deve chiedere se i PSP di radicamento di conto e i TPPs assumano effettivamente la qualifica di titolare del trattamento dei

[50] Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679, adottate il 3 ottobre 2017, versione emendata e adottata il 6 febbraio 2018 "*Il processo decisionale automatizzato ha una portata diversa da quella della profilazione, a cui può sovrapporsi parzialmente o da cui può derivare. Il processo decisionale esclusivamente automatizzato consiste nella capacità di prendere decisioni impiegando mezzi tecnologici senza coinvolgimento umano. Le decisioni automatizzate possono essere prese ricorrendo o meno alla profilazione, la quale a sua volta può essere svolta senza che vengano prese decisioni automatizzate*", p. 8.

[51] Nel settore finanziario quest'ultimo elemento non appare dirimente in quanto l'attività di profilazione è ormai svolta quasi esclusivamente con trattamenti automatizzati o semi-automatizzati.

[52] CONSIGLIO D'EUROPA, "*La protezione delle persone fisiche con riguardo al trattamento automatizzato di dati personali nel contesto di attività di profilazione*". Si veda inoltre la Raccomandazione CM/Rec (2010)13.

dati personali dei propri utenti. La risposta positiva a tale quesito assume notevole rilievo in quanto comporterebbe l'applicazione, nei confronti dei TPPs, di diversi obblighi, generali e specifici, tra cui il rispetto dei principi di cui all'art. 5 del GDPR (di liceità, trasparenza e correttezza; di limitazione; di conservazione; di integrità e riservatezza; di responsabilizzazione) e gli obblighi di comunicazione e di informazione, specie in materia di trasparenza, come previsto dall'art. 12 del GDPR, di adozione di misure adeguate[53] a fornire tutte le informazioni prescritte dagli artt. 13-14 del GDPR e di sicurezza.

Quanto ai PSP di radicamento di conto si deve preliminarmente illustrare come l'assunzione della qualifica di titolare di trattamento dei dati è indiscutibile allorquando l'utente apra, presso gli stessi, un conto corrente o un conto di pagamento[54]. Diversa è invece l'attività (strumentale) espletata dai TPPs nell'ambito del servizio di pagamento, e si discute se essi possano qualificarsi alla stregua di veri e propri titolari o responsabili del trattamento[55]. La risposta al quesito non è univoca, ma prevale nettamente l'idea per cui la collaborazione (necessaria) tra gli intermediari in virtù della legge e della volontà dell'utente che ha richiesto il servizio ad un determinato TPP impone di per sé la sua qualificazione di titolare del trattamento in quanto non sussiste alcun rapporto contrattuale tra il TPP e i PSP di radicamento del conto. Ad ogni modo, la questione non appare avere una risposta certa in quanto la qualifica del TPP come titolare o co-

---

[53] Sul punto, in base al soggetto che fornisce i dati al TPP, che può essere l'utente stesso o l'ASPSP, si applicherà la disciplina riguardante l'obbligo di informativa gravante sul TPP (titolare) contenuta, rispettivamente, negli artt. 13-14 GDPR. Ciò è confermato anche nelle stesse linee guida sulla interazione tra PSD2 e GDPR che al par. 75 affermano che "*per i servizi di cui alla PSD2, l'articolo 13 del GDPR si applica ai dati personali raccolti presso l'interessato, mentre l'articolo 14 si applica qualora i dati personali non siano stati ottenuti presso l'interessato*".

[54] Occorre infine considerare che, in caso di *data breach*, ove il PSP di radicamento del conto sia il titolare del trattamento, questo risponderà di tutte le violazioni del GDPR comprese quelle derivanti dai comportamenti del responsabile del trattamento, salvo che dimostri di non essere in alcun modo responsabile. Considerando n. 146 del GDPR e art. 82, par. 3, GDPR.

[55] Cass., sez. I, ordinanza 23 luglio 2021, n. 21234; tale considerazione è altresì confermata dal GDPR che all'art. 28, par. 10 dispone che: "*Fatti salvi gli articoli 82, 83 e 84, se un responsabile del trattamento viola il presente regolamento, determinando le finalità e i mezzi del trattamento, è considerato un titolare del trattamento in questione*". Sul punto occorre inoltre considerare che se il responsabile non osserva tutte le istruzioni impartite dal titolare, può essere in concreto considerato esso stesso titolare del trattamento "in ragione dell'autonomia decisionale e gestionale manifestata nell'aver disatteso le disposizioni impartite dal titolare".

me responsabile del trattamento può variare a seconda delle circostanze fattuali e di eventuali accordi stipulati tra gli operatori coinvolti. Si ricorda in tal senso che, tra l'altro, gli stessi accordi intervenuti tra le parti potrebbero dare luogo ad un rapporto di contitolarità ai sensi dell'art. 26 del GDPR che, si genera esclusivamente quando entrambi i soggetti determinano congiuntamente, almeno in parte, le finalità e i mezzi del trattamento dei dati dell'utente e circoscrivono[56] le responsabilità di ciascuno relativamente alle attività di trattamento. Rapporti di contitolarità che, ove sussistenti, come generalmente condiviso, hanno efficacia meramente interna senza produrre alcuna rilevanza nei confronti dell'interessato. Tale considerazione trova conferma nel par. 3 dell'art. 26 del GDPR, che non sposta l'asse delle responsabilità riconoscendo la possibilità all'interessato di esercitare i propri diritti nei confronti di ciascun titolare, indipendentemente da quanto disposto nel suddetto accordo.

Ciò chiarito, è giunto il momento di precisare che la rigida disciplina generale dettata dal GDPR, prescindendo dalla qualifica contingente rivestita dall'operatore del servizio di pagamento, trova comunque applicazione nei suoi confronti per ogni tipologia di profilazione[57]. In primo luogo, il GDPR richiede ai TPPs, titolari del trattamento, di assolvere ad una serie di obblighi per svolgere in maniera lecita l'attività di profilazione, sia se svolta con esclusivo riguardo ai dati finanziari raccolti durante il proprio servizio che se eseguita combinando[58] i medesimi dati finanziario con altri dati, personali e non, già raccolti in altra sede o settore[59].

---

[56] Si specifica, che tale accordo individua solamente gli obblighi e le responsabilità dei contitolari, non avendo la funzione di costituire un rapporto di contitolarità, che emerge da circostanze di fatto.

[57] Considerando n. 89 della PSD2.

[58] Si rileva inoltre che alcune combinazioni di dati possono già essere esplicitamente vietate dal diritto nazionale o dell'UE, come nel caso del trattamento di categorie particolari di dati e di dati personali ottenuti da reti di *social media* nel contesto della valutazione del merito di credito dei consumatori. A titolo esemplificativo, quanto ai dati ottenuti da fonti terze, come le reti *di social media* occorre considerare che la pratica è già esplicitamente vietata nella legislazione settoriale in riferimento a determinati servizi finanziari: si veda l'art. 19, par. 3-*bis*, della direttiva sui crediti al consumo, che prevede che "*i creditori e gli intermediari del credito non trattano le categorie particolari di dati di cui all'articolo 9, paragrafo 1, del regolamento (UE) 2016/679 e i dati personali trattati dai social network che possono essere contenuti nelle banche dati di cui al paragrafo 1*".

[59] Si deve invero considerare che il titolare dei dati è libero di dare il proprio consenso e di conferire al TPP mandato per un ulteriore trattamento dei propri dati. al fine di fornire servizi di diversa natura che rientrino nell'interesse dell'utente medesimo. In altre parole, il cliente deve autorizzare espressamente i TPPs ad accedere e utilizzare i dati dei conti di pagamento.

Oltre a dover sempre disporre di un'idonea base giuridica, i TPPs devono rispettare tutti i principi sanciti all'art. 5 del GDPR. Tra questi meritano preliminarmente attenzione quelli di minimizzazione [60] e conservazione dei dati. Il primo impone che i dati raccolti debbano essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati [61]. Ne consegue che i dati devono essere sufficienti, ma non eccedenti, ai fini del trattamento e quindi la quantità dei dati personali raccolti sarà considerata adeguata qualora sarà essenziale e funzionale al trattamento stesso [62]. Strettamente connesso al primo è il principio di conservazione degli stessi [63] (c.d. *data retention*) il quale impone che l'arco temporale di conservazione dei dati, individuato dal titolare del

[60] In materia di minimizzazione è da evidenziarsi come l'EDPB, nell'ambito delle proprie raccomandazioni relative al pacchetto Financial Data Access and Payments Package, accolga con favore la prescrizione, contenuta nel pacchetto medesimo, secondo cui i PISP e gli AISP dovrebbero limitarsi a richiedere solo i dati strettamente necessari per erogare il servizio. Ciò, invero, come afferma l'EDPB, ridurrebbe il rischio di esposizione dei dati e, per tale ragione, nel rilevare al par. 32 della Opinion n. 39 che "*il requisito di cui alla lettera b) dell'articolo 46, paragrafo 2, in base al quale i PISP possono richiedere all'utente dei servizi di pagamento solo i dati necessari per fornire il servizio (di avvio del pagamento), non è incluso mutatis mutandis nell'articolo 47, paragrafo 2, relativo agli obblighi degli AISP*", si raccomanda espressamente di inserire una disposizione equivalente nell'art. 47, par. 2, della proposta di PSR. Si veda, in particolare: EDPB, Opinion n. 39, *ibidem*, n. 10.

[61] Art. 5, par. 1, lett. c), GDPR. Sul tema si veda la già richiamata ordinanza della Corte di Cassazione, 21 ottobre 2019, n. 26778.

[62] Invero, emerge la necessità di circoscrivere le categorie di dati personali che i TPP possono trattare, per evitare il rischio di una eccessiva raccolta e trattamento di dati non pertinenti alle finalità perseguite; la mancanza di chiarezza e trasparenza potrebbe arginare i limiti del consenso rilasciato dall'utente. Non a caso, oltre a quanto illustrato nella nota n. 55, l'EDPB, con riferimento al pacchetto Financial Data Access and Payments Package, raccomanda pertanto anche l'esclusione esplicita dei dati creati come risultato della profilazione dalla definizione di "dati dei clienti" come modo per ridurre al minimo i rischi per i diritti e le libertà delle persone. Si veda, in particolare: EDPB, Opinions nn. 38-39.

[63] Sul tema, si vedano le recenti sentenze gemelle (C-26/22; 64/22) del 7 dicembre 2023, nel caso UF (C-26/22) AB (C-64/22) c. Land Hessen con l'intervento di SCHUFA Holding AG, con cui la Corte di giustizia ha fornito importanti indicazioni in merito al principio di conservazione dei dati. I giudici hanno sottolineato come i dati personali debbano essere conservati per un periodo di tempo determinato sia in base alla finalità del trattamento sia alla luce del principio di limitazione della conservazione, ai sensi dall'art. 5, lett. e), GDPR. Tale principio richiede che il titolare del trattamento possa dimostrare che il periodo di conservazione sia pari al tempo necessario per il conseguimento delle finalità del trattamento. Riprendendo, poi, le conclusioni dell'Avvocato Generale, il quale afferma che "*anche un trattamento lecito dei dati può, con il tempo, smettere di essere conforme al GDPR quando tali dati non sono più pertinenti o risultano eccessivi alla luce della finalità per la quale erano stati raccolti originariamente*", conclude ritenendo come la conservazione prolungata delle informazioni sull'esdebitazione è contraria al GDPR.

trattamento, deve essere proporzionato alle finalità per le quali sono trattati [64]. Pertanto, in combinazione con il principio di minimizzazione, che identifica le caratteristiche dei dati trattati, ogni TPPs che tratta i dati dei propri utenti dovrà individuare, ancor prima che il trattamento abbia inizio, i tempi di conservazione in funzione delle finalità del trattamento medesimo.

In attuazione del principio di trasparenza, risulta poi necessario che siano adottate misure adeguate a fornire agli utenti tutte le informazioni relative al trattamento dei dati, contenute nell'elenco tassativo di cui agli artt. 13 e 14 del GDPR [65], compreso l'eventuale svolgimento dell'attività di profilazione. Le informazioni fornite dai TPPs devono essere concise, trasparenti, intelligibili e facilmente accessibili [66] e devono preliminarmente consistere in una spiegazione in favore dell'interessato con cui si illustrino le finalità del trattamento cui sono destinati i dati, le basi giuridiche che lo legittimano [67], il periodo di conservazione dei dati ovvero, se non risulta possibile, i criteri utilizzati per determinare tale periodo, gli eventuali interessi legittimi perseguiti dal titolare o da terzi e, se espletata, il funzionamento della profilazione [68].

---

[64] Sul punto è interessante indicare che l'EDPB, sempre nell'ambito delle raccomandazioni relative alla proposta Financial Data Access and Payments Package, interviene anche in materia di *data retention* raccomandando di definire adeguati periodi di conservazione dei dati perché di fondamentale importanza per la protezione dell'utente e in linea con i principi del GDPR sulla limitazione della conservazione e di responsabilizzazione. Si veda, in particolare: EDPB, Opinion n. 39, *ibidem*, par. 42.

[65] Sul punto, in base al soggetto che fornisce i dati al TPP, che può essere l'utente stesso o l'ASPSP, si applicherà la disciplina riguardante l'obbligo di informativa gravante sul TPP (titolare) contenuta, rispettivamente, negli artt. 13-14 GDPR. Ciò è confermato anche nelle stesse linee guida su interazione tra PSD2 e GDPR che al par. 75 affermano che "*per i servizi di cui alla PSD2, l'articolo 13 del GDPR si applica ai dati personali raccolti presso l'interessato, mentre l'articolo 14 si applica qualora i dati personali non siano stati ottenuti presso l'interessato*".

[66] Art. 12 GDPR, che prescrive, altresì, come le informazioni siano "*fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici*". Inoltre, si veda Guida all'applicazione del regolamento europeo in materia di protezione dei dati personali, edizione 2023.

[67] Sul punto il Considerando n. 60 del GDPR esplicita come gli stessi principi di trattamento, corretto e trasparente, impongono di fornire informazioni sull'esistenza del trattamento e delle sue finalità e, in particolare, sull'esistenza della profilazione e delle sue conseguenze.

[68] L'EDPB, nell'ambito dell'Opinion del 22 agosto 2023 relativa alle proposte normative relative al pacchetto Financial Data Access and Payments Package, in materia di trasparenza, raccomanda di indicare che i TPPs devono fornire informazione all'ASPSP in merito alla base giuridica per l'accesso ai dati. Si veda in particolare: EDPB, Opinion n. 39, *ibidem*, n. 11. Tale raccomandazione si lega inscindibilmente con quella n. 3 della medesima Opinion, già meglio sopra descritta, finalizzata a eliminare il divieto imposto agli ASPSP di verificare l'autorizzazione

Nel caso in cui il trattamento dei dati avvenga sulla base del consenso, l'interessato deve essere inoltre informato del diritto di revoca ad esso spettante in qualsiasi momento. A tal riguardo, di rilievo sono proprio le informazioni relative agli altri diritti di carattere generale riconosciuti all'interessato, tra cui il diritto di ottenere la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano, il diritto di accedere ad intervalli ragionevoli ai dati personali impiegati per la profilazione, al fine di rendere l'interessato consapevole del trattamento e di verificarne la liceità[69], il diritto di ottenere la rettifica dei dati personali inesatti che lo riguardano, senza ingiustificato ritardo, e il diritto di ottenere l'integrazione dei dati personali incompleti, potendo fornire anche una dichiarazione integrativa[70].

Ulteriori, e non meno importanti, diritti spettanti all'interessato sono quelli alla cancellazione dei dati[71], alla limitazione del trattamen-

---

all'accesso ai dati o, in alternativa, di introdurre garanzie per proteggere gli utenti dai rischi di condivisione illecita di dati personali.

[69] Il diritto di accesso di cui all'art. 15 GDPR deve essere esaminato in combinazione con i Considerando nn. 63 e 64. In particolare, si specifica come il titolare del trattamento dovrebbe adottare tutte le misure idonee a verificare l'identità di un interessato che eserciti il diritto di accesso, soprattutto quando questo ricorre al contesto online e tale *diritto* "*non dovrebbe ledere i diritti e le libertà altrui, compreso il segreto industriale e aziendale e la proprietà intellettuale, segnatamente i diritti d'autore che tutelano il software*". Dunque, viene riconosciuto un certo grado di protezione al titolare in caso di segreti aziendali o proprietà intellettuale; tuttavia questi non può strumentalizzare tale protezione per negare l'accesso all'interessato.

[70] Art. 16 GDPR. Sul punto, si vedano le Linee Guida sul processo decisionale automatizzato del 2018, ove si sottolinea che in caso di profilazione, tale diritto potrebbe esercitarsi qualora l'interessato venisse inserito in una determinata categoria sulla base di informazioni errate.

[71] Art. 17 GDPR che subordina il diritto alla cancellazione dei dati al verificarsi di uno dei motivi indicati nella norma. Il diritto alla cancellazione, tuttavia non è un diritto assoluto, in quanto deve essere bilanciato con altri interessi meritevoli di protezione. Il par. 3 dell'art. 17 infatti, esclude la possibilità di esercitare tale diritto qualora il trattamento deve esser effettuato: "*a) per l'esercizio del diritto alla libertà di espressione e di informazione; b) per l'adempimento di un obbligo legale che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro 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; c) per motivi di interesse pubblico nel settore della sanità pubblica in conformità dell'articolo 9, paragrafo 2, lettere h) e i), e dell'articolo 9, paragrafo 3; d) a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1, nella misura in cui il diritto di cui al paragrafo 1 rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento; o e) per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria*". Sul tema, assumono rilevanza le sentenze della Corte di giustizia nelle cause riunite C-26/22 e C-64/22, ove, oltre a fornire importanti indicazioni in merito al principio di conservazione dei dati, come già illustrato nella nota n. 58, ha affermato che l'art. 17, par. 1, lett. d), GDPR deve essere interpretato nel senso che il titolare del trattamento è tenuto a cancellare, senza ingiustificato ritardo, i dati personali oggetto di un trattamento illecito. Invero, sottolineando la cristallina formulazione della dispo-

to[72], e di opposizione allo stesso. Anche questi diritti devono essere portati a conoscenza dell'interessato[73] da parte del titolare del trattamento, che deve presentarli in maniera chiara e separata da qualsiasi altra informazione[74]. In tema di opposizione, in particolare, l'interessato ha diritto di opporsi al trattamento, compresa la profilazione, per motivi connessi alla sua situazione particolare[75] e in tal caso il titolare deve interrompere o non iniziare l'attività di profilazione e può, altresì, essere obbligato anche alla cancellazione dei dati personali interessati[76]. Anche tale diritto, al pari di quel-

sizione *de qua*, nell'ipotesi in cui il giudice del rinvio, compiute le opportune valutazioni sulla liceità del trattamento dei dati personali, dovesse ritenere il suddetto trattamento illecito, spetterebbe alla società di valutazione del merito creditizio cancellare i dati degli interessati quanto prima. Tale situazione ricorrerebbe nel caso di un trattamento dei dati personali effettuato oltre il termine di conservazione dei dati di sei mesi nel registro pubblico fallimentare. Inoltre, ha chiarito come l'art. 17, par. 1, lett. c), GDPR, deve essere interpretato nel senso che l'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione, senza ingiustificato ritardo, dei dati personali che lo riguardano qualora si opponga al trattamento ai sensi dell'art. 21, par. 1, di tale regolamento e non sussistano motivi legittimi prevalenti che possano giustificare, in via eccezionale, il trattamento in esame. Tale disposizione prevede che la presenza di un "motivo legittimo prevalente" costituisca un'eccezione rispetto al diritto dell'interessato di opporsi al trattamento e di ottenere la cancellazione dei dati.

[72] Art. 18 GDPR, ai sensi del quale l'interessato ha il diritto a che i suoi dati siano trattati limitatamente a quanto necessario ai fini della conservazione. Sul punto, il Regolamento definisce la limitazione come "*il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro*". In particolare, ai sensi del par. 1 dell'art. 18, tale diritto può essere esercitato: i) in caso di violazione dei presupposti di liceità del trattamento; ii) se l'interessato ne contesta l'esattezza chiedendo la rettifica dei dati. La limitazione dura il periodo necessario al titolare per verificare l'esattezza dei dati; iii) i dati sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria, mentre al titolare del trattamento non servono più a fini del trattamento; iv) si oppone al trattamento ai sensi dell'art. 21 GDPR. Il Considerando n. 67, con degli esempi di carattere non tassativo, indica delle modalità di limitazione del trattamento consistenti nel trasferimento temporaneo dei dati selezionati verso un altro sistema di trattamento, nel rendere i dati personali selezionati inaccessibili agli utenti o nel rimuovere temporaneamente i dati pubblicati da un sito web. Il considerando prosegue sottolineando che "*Negli archivi automatizzati, la limitazione del trattamento dei dati personali dovrebbe in linea di massima essere assicurata mediante dispositivi tecnici in modo tale che i dati personali non siano sottoposti a ulteriori trattamenti e non possano più essere modificati. Il sistema dovrebbe indicare chiaramente che il trattamento dei dati personali è stato limitato*".

[73] Art. 21, parr. 2 e 3, GDPR.

[74] Art. 21, par. 4, GDPR.

[75] Il titolare del trattamento deve riconoscere tale diritto in tutti i casi in cui il trattamento si basi sull'art. 6, par. 1, lett. e) o f). Inoltre, ai sensi del combinato disposto degli artt. 21, par. 2, e Considerando n. 70, l'interessato può opporsi al trattamento dei dati, in qualunque momento, per finalità di marketing diretto, compresa la profilazione nella misura i cui sia connessa a tale marketing diretto.

[76] Art. 17, par. 1, lett. c), GDPR.

lo alla cancellazione, non è assoluto[77], ed è a tal fine prevista la possibilità del titolare di continuare a trattare i dati ove dimostri la sussistenza di "motivi legittimi cogenti" che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato[78].

Ogni TPP che svolge attività di profilazione deve poi adottare misure tecniche e organizzative adeguate a fornire la prova della conformità del trattamento al GDPR[79] ed è obbligato a svolgere una valutazione di impatto[80], il tutto in ossequio al noto principio di responsabilizzazione[81]. I titolari possono dunque decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali purché questi rispettino il Regolamento anche in forza della relativa valutazione d'impatto eseguita dal titolare con cui si valutano i rischi connessi al processo decisionale automatizzato ovvero alla profilazione[82].

---

[77] Combinato disposto degli artt. 21, par. 2, e Considerando n. 70 del GDPR. L'interessato, poi, può opporsi al trattamento dei dati, in qualunque momento e gratuitamente, per finalità di marketing diretto, compresa la profilazione nella misura i cui sia connessa a tale marketing diretto. In tale circostanza non è nemmeno necessario effettuare un bilanciamento degli interessi contrapposti poiché il titolare è tenuto a dare seguito alla richiesta di opposizione dell'interessato senza contestare i motivi addotti

[78] Considerando n. 69 del GDPR. Il regolamento non fornisce alcuna indicazione per poter considerare i motivi come legittimi e cogenti. Tuttavia, tale circostanza potrebbe verificarsi nel caso di profilazione posta in essere per finalità pubbliche, come quelle sanitarie, volte ad individuare la diffusione di malattie.

[79] Art. 24 GDPR.

[80] Art. 35 GDPR. In linea con un approccio basato sul rischio, che è alla base dell'intero GDPR, la valutazione di impatto rappresenta proprio uno strumento essenziale per la responsabilizzazione. Le linee guida sul processo decisionale automatizzato sottolineano come il citato articolo faccia riferimento a valutazioni, tra cui rientra la profilazione e decisioni "basate" su un trattamento automatizzato e non "basate unicamente" sullo stesso. Pertanto, si evince come l'art. 35 è applicabile sia nel caso in cui il processo decisionale comprendente la profilazione che non è interamente automatizzato, sia nell'ipotesi di decisione basata unicamente sul trattamento automatizzato, ai sensi dell'art. 22. Invero, tra le ipotesi in cui è necessario che il titolare del trattamento svolga la suddetta valutazione, si annovera il caso in cui sia coinvolta "*una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche*" (art. 35, par. 3, lett. a).

[81] La responsabilizzazione o *accountability*, è prevista all'art. 5, par. 2 e art. 24 GDPR ai sensi del quale il titolare del trattamento "deve essere in grado di dimostrare che il trattamento è effettuato conformemente" al regolamento, ovvero che tutti i diritti stabiliti dalla legge a presidio degli interessati sono adeguatamente garantiti e che sono rispettati tutti i principi e le condizioni che caratterizzano il trattamento.

[82] Infatti, sul punto, il Considerando n. 74 del GDPR precisa che le misure messe in atto dal titolare al fine di dimostrare la conformità delle attività di trattamento con il GDPR devono tenere conto "*della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche*".

Infine, merita una considerazione il fenomeno dell'esternalizzazione[83], frequente nel settore bancario e finanziario, che comporta l'insorgere di problematiche connesse all'individuazione dei soggetti destinatari degli obblighi normativi vigenti (e delle correlative responsabilità in caso di loro violazione)[84]. Anche di fronte all'esternalizzazione di una funzione non si può escludere l'applicazione di tutta la normativa finora descritta, che va però integrata dagli orientamenti non vincolanti dell'EBA in materia. In ossequio a questi ultimi, i TPPs che esternalizzano proprie funzioni devono senza dubbio predisporre politiche di esternalizzazione e rigidi procedimenti di gestione dei rischi, comunicare e segnalare alle autorità competenti determinate informazioni concernenti l'esternalizzazione medesima e, in linea più generale, rispettare il principio di proporzionalità. In virtù di questo principio, le esternalizzazioni devono essere elaborate e attuate in modo coerente con il profilo di rischio individuale, con la natura e il modello di *business* dell'ente o dell'istituto di pagamento nonché con la portata e la complessità delle loro attività[85]. Il tutto con requisiti e obblighi aggravati se ad essere esternalizzata è una funzione considerata essenziale o importante[86], qualifi-

[83] Per esternalizzazione si intende un accordo di qualsiasi forma tra un ente, un istituto di pagamento o un istituto di moneta elettronica e un fornitore di servizi in base al quale quest'ultimo svolge un processo, un servizio o un'attività che sarebbe altrimenti svolto/a dall'ente, dall'istituto di pagamento o dall'istituto di moneta elettronica stesso. Si veda: EBA, *Orientamenti in materia di esternalizzazione*, *ibidem*, par. 12.

[84] Sul punto il principio generalmente accolto è quello "*esternalizzazione si, impunità no*". Il caso di scuola, in materia finanziaria, è rappresentato dallo *scoring* effettuato da società terze, che rappresenta tra l'altro l'ipotesi in cui si è recentemente pronunciata la CGUE, come meglio illustrato nel prosieguo della trattazione e precisamente nel par. 2.4.

[85] In particolare, gli enti e gli istituti di pagamento dovrebbero tenere in considerazione la complessità delle funzioni esternalizzate, i rischi derivanti dall'accordo di esternalizzazione, l'essenzialità o l'importanza della funzione esternalizzata e l'impatto potenziale dell'esternalizzazione sulla continuità delle loro attività. Vedi: EBA, *Orientamenti in materia di esternalizzazione*, *ibidem*, par. 19.

[86] Una funzione è sempre da considerarsi come essenziale o importante nelle seguenti situazioni: a. se un'anomalia nella sua esecuzione o la sua mancata esecuzione comprometterebbero gravemente: i) il rispetto nel continuo delle condizioni della loro autorizzazione o degli altri obblighi previsti dalla direttiva 2013/36/UE, dal regolamento (UE) n. 575/2013, dalla direttiva 2014/65/UE, dalla direttiva (UE) 2015/2366 e dalla direttiva 2009/110/CE e dei loro obblighi normativi; ii) i risultati finanziari; o iii) la solidità o la continuità delle attività bancarie o dei servizi di pagamento svolti; b. quando sono esternalizzati compiti operativi delle funzioni di controllo interno, a meno che la valutazione non stabilisca che la mancata esecuzione della funzione esternalizzata o un'esecuzione inadeguata della stessa non avrebbe un impatto negativo sull'efficacia della funzione di controllo interno; c. quando intendono esternalizzare le funzioni relative ad attività bancarie o a ser-

cazione su cui incide l'impatto potenziale che ha l'esternalizzazione con riguardo ai servizi forniti ai propri clienti e la protezione dei loro dati [87].

L'esternalizzazione di determinate funzioni, inoltre, non può mai comportare una delega delle responsabilità dell'organo di amministrazione e occorre in ogni caso considerare che gli enti e gli istituti di pagamento rimangono pienamente responsabili del rispetto di tutti i loro obblighi normativi. In particolare, l'EBA ha segnalato in un proprio orientamento [88] che, in caso di esternalizzazione, da instaurare con apposito contratto, gli enti e gli istituti di pagamento dovrebbero almeno assicurare di poter prendere e attuare decisioni in relazione alle proprie attività operative e alle funzioni essenziali o importanti, incluse quelle esternalizzate, e di mantenere l'ordinato svolgimento delle proprietà attività e dei servizi bancari e di pagamento che forniscono, nonché di individuare, valutare e gestire i rischi connessi agli accordi di esternalizzazione e gli eventuali conflitti di interesse.

2.4. ... (segue): il trattamento automatizzato

L'attività di profilazione dei dati da parte dei TPPs, come visto, riguarda dati personali degli utenti – delle volte persino dati sensibili – e può riguardare anche altre categorie eterogenee di dati, anche combinati tra loro. L'attività è, inoltre, generalmente svolta in una forma unicamente automatizzata: i dati personali vengono analizzati ed elaborati, sempre più spesso, grazie al ricorso alle tecniche algoritmiche, che portano ad un trattamento automatizzato degli stessi che può configurare, per l'appunto, una profilazione e/o un processo decisionale automatizzato, con completa esclusione del coinvolgimento umano.

Ora, si deve tenere conto che l'attività di profilazione svolta in forma

---

vizi di pagamento in misura tale da richiedere l'autorizzazione di un'autorità competente, come indicato nella sezione 12.1.

[87] Infatti, nel valutare se un accordo di esternalizzazione riguarda una funzione essenziale o importante, gli enti e gli istituti di pagamento dovrebbero considerare, insieme all'esito della valutazione del rischio di cui alla sezione 12.2, almeno i seguenti fattori: d. l'impatto potenziale sui servizi forniti ai propri clienti; e j. la protezione dei dati e l'impatto potenziale di una violazione dell'obbligo di riservatezza o della mancata disponibilità e integrità dei dati relativi all'ente o all'istituto di pagamento e ai suoi clienti, compreso tra l'altro il rispetto del regolamento (UE) 2016/679. Vedi: EBA, *Orientamenti in materia di esternalizzazione*, *ibidem*, par. 31.

[88] Vedi: EBA, *Orientamenti in materia di esternalizzazione*, *ibidem*, parr. 39-40 e 74.

unicamente automatizzata [89] è vietata [90] qualora dalla stessa derivino effetti giuridici per l'interessato o quando questo ne risulti inciso [91] in modo analogo [92]. Il divieto è derogato in tre circostanze applicabili a prescindere dalla natura del soggetto che svolge la profilazione. In particolare, l'attività di profilazione automatizzata è consentita quando i) la decisione risulta necessaria per la conclusione o l'esecuzione di un contratto tra il titolare e l'interessato, ii) il trattamento è previsto dalla legge [93], o iii) l'interessato abbia prestato il proprio consenso esplicito.

In presenza di una di queste eccezioni, la profilazione realizzata dai TPPs in forma automatizzata risulta quindi senza alcun dubbio lecita [94], ma occorre subito precisare che in tal caso risulta necessario il rispetto di ulteriori obblighi prescritti dal GDPR. In primo luogo, il TPP dovrà rispettare determinati obblighi informativi aggiuntivi rispetto a quelli ordinari, con

---

[89] Ciò implica che, ove la decisione sia presa ricorrendo a sistemi tecnologici sia soltanto un elemento di un procedimento più ampio che prevede l'intervento umano al fine di modificare la decisione automatizzata, non troverà applicazione l'art. 22 GDPR.

[90] Tale divieto si pone in linea con il principio dell'*accountability*, che impone al titolare del trattamento di adottare misure adeguate al trattamento dei dati da porre in essere. Inoltre, interpretare l'art. 22 come divieto, anziché come diritto, implica che gli utenti siano automaticamente tutelati dai potenziali effetti di tale trattamento, senza la necessità di invocare la suddetta tutela. L'interpretazione è confermata anche dal combinato disposto dell'art. 22, par. 2 e del Considerando n. 71 che prevedono l'adozione di una decisione automatizzata e della profilazione al ricorrere di determinate condizioni.

[91] La categoria degli effetti diversi che "incidono in modo analogo significativamente" sull'interessato, sembrerebbe ricomprendere tutte quelle ripercussioni che non portano ad una modifica nei diritti dell'interessato. Il Considerando n. 71 cita come esempi tipici "*rifiuto automatico di una domanda di credito online*" o "*pratiche di assunzione elettronica senza interventi umani*".

[92] L'art. 22, par. 1, GDPR prevede espressamente che "*l'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona*"; si tratta, in particolare, di un divieto generale.

[93] Considerando n. 71. Tale eccezione ricorre solitamente nell'ipotesi in cui sia autorizzata dal diritto dell'Unione o dello Stato per fini di monitoraggio e prevenzione delle frodi e dell'evasione fiscale o a garanzia della sicurezza e dell'affidabilità di un servizio fornito dal titolare del trattamento.

[94] L'art. 9 GDPR considera come dati particolari quelli "*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*". Tale eccezione rappresenta, come detto, l'ipotesi più frequente in cui il TPP procede alla profilazione dei dati. Certamente, in applicazione del principio di responsabilizzazione, il titolare deve dimostrare che il trattamento sia necessario per perseguire al meglio l'obiettivo, non esistendo altri mezzi idonei. Art. 22, par. 4, GDPR.

particolare riguardo a quelli concernenti le logiche su cui si basa la profilazione, l'importanza e le conseguenze di tale tipologia di trattamento per l'interessato medesimo [95]. Il TPP, poi, dovrà necessariamente dotarsi di misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi degli interessati, tra cui si devono annoverare, almeno, il diritto di ottenere l'intervento umano nonché il diritto di esprimere la propria opinione e di contestare la decisione [96], che deve essere inoltre spiegata, dopo la valutazione, e sempre dietro apposita richiesta dell'interessato [97].

Il più penetrate quadro regolatorio applicabile all'attività di profilazione automatizzata trova giustificazione nel fatto che essa rappresenta l'operazione che più mette a repentaglio i diritti e le libertà degli interessati. Si pensi, in particolare, alla profilazione automatizzata che ricorre all'intelligenza artificiale, la quale, come noto, può comportare diverse discriminazioni algoritmiche [98].

Ciò detto, l'applicazione dell'art. 22 del GDPR rappresenta dunque una norma cardine in materia di profilazione automatizzata, che però non è stata ad oggi di facile e pronta applicazione, specie di fronte a varie fattispecie riconducibili all'*Open Banking* ed al settore finanziario, in cui *unbundling* e esternalizzazione di determinate fasi dell'attività d'impresa sembrano essere comuni denominatori anche, come già accennato, con riguardo alla stessa attività di profilazione [99]. Non è raro, infatti, che la profilazione sia commissionata a terzi e che le modalità con cui vengono

---

[95] Art. 13, par. 2, lett. f), art. 14, par. 2, lett. g), e Considerando n. 60 del GDPR. Analogamente, l'art. 15, par. 1, lett. h), GDPR riconosce all'interessato il diritto di ottenere dal titolare del trattamento le medesime informazioni previste dagli artt. 13 e 14. Sul tema, il Considerando n. 63 del GDPR ribadisce che l'interessato deve avere il diritto di accesso al fine di ottenere le informazioni in merito al trattamento automatizzato e "*almeno quando è basato sulla profilazione, alle possibili conseguenze di tale trattamento*".

[96] Art. 22, par. 3, GDPR, nei casi previsti dal par. 2, lett. a) e lett. c).

[97] Considerando n. 71 del GDPR, che afferma che gli interessati devono aver diritto "*di ottenere una spiegazione della decisione conseguita dopo tale valutazione*". In aggiunta, il Considerando n. 71 prescrive che il titolare dovrebbe utilizzare "*procedure matematiche o statistiche appropriate per la profilazione*" e porre in essere "*misure tecniche e organizzative adeguate al fine di garantire, in particolare, che siano rettificati i fattori che comportano inesattezze dei dati e sia minimizzato il rischio di errori, […]*".

[98] Per una approfondita analisi delle discriminazioni algoritmiche si veda F. MANCUSO, V. GIORDANO, *Intelligenza artificiale, profilazione e nuove forme di discriminazione*, in *Teoria e storia del diritto privato*, numero speciale, anno 2022.

[99] Conclusioni dell'Avvocato Generale già richiamate in cui si rinviene come sia "*evidente che, benché un istituto finanziario possa occuparsi di tale processo, nulla gli impedisce di delegare taluni compiti, in via contrattuale, a un'agenzia di valutazione del credito, ad esempio la profilazione*".

ripartite le singole attività di raccolta dei dati, di profilazione e di decisione, comportino una certa difficoltà a considerare integrati diversi requisiti normativi tra cui, in materia, rilevano quelli richiesti ai fini dell'applicazione dell'art. 22 del GDPR, ora per il committente ora per l'appaltatore (che ben può essere un TPP), con la diretta conseguenza dell'instaurazione di un clima di incertezza in ordine alla individuazione degli addebiti delle responsabilità.

Tra i singoli servizi finanziari in cui si registrano tali pratiche, emblematico è quello della concessione del credito bancario, per il quale le banche ricorrono con una certa frequenza a consulenze esterne – svolte da terzi in forma automatizzata – ai fini dell'ottenimento del *credit scoring* di un determinato utente [100]. Ad una di tali pratiche è invero recentemente conseguita una nota pronuncia giurisprudenziale della Corte di giustizia [101], che ha affrontato due questioni interpretative di non poco rilievo, offrendo una ricostruzione orientata a dare effettività alle tutele normative predisposte per gli interessati in materia di profilazione automatizzata dei loro dati. La prima, in breve, consistente nel vagliare la possibilità, o meno, di qualificare come decisioni le risultanze derivanti dall'attività di profilazione commissionata a terzi dal momento che né l'art. 22 del GDPR né l'intero regolamento offrono all'interprete una definizione del concetto di decisione. La seconda, invece, riguardante l'interpretazione normativa da dare all'articolo in commento nella parte in cui richiede che la decisione abbia effetti giuridici nei confronti dell'interessato o incida, sul medesimo, "in modo analogo".

Con riguardo alla prima questione, la Corte sembra aver colto l'occasione per fornire chiarimenti in merito al processo decisionale unicamente automatizzato, svolgendo una serie di considerazioni che permettono in generale di affermare come al termine "decisione", di cui al suddetto articolo, deve essere riconosciuta portata ampia [102]. In particolare, la Corte af-

[100] Nel caso di specie, la Corte ha affrontato il caso di una persona fisica, che si era vista negare la concessione di un mutuo da una banca a causa di un *credit scoring* negativo, predittivo della sua incapacità di ripagarlo, svolto da un prestatore di servizio di informazione in materia di credito. La Corte si è in particolare interrogata se l'attività di profilazione, svolta dalla società di valutazione del credito, consistente nel "calcolo automatizzato di un tasso di probabilità relativo alla capacità di un interessato di saldare in futuro un debito" costituisca essa stessa una decisione automatizzata.

[101] Corte giust. UE, sez. I, Sent., 7 dicembre 2023, C-634/21.

[102] Nella sentenza, è fondamentale il richiamo al Considerando n. 71 del GDPR che conferma la portata ampia della nozione di decisione; in particolare, nel suddetto considerando viene chiarito che una decisione può implicare una valutazione (profilazione) di aspetti personali del singolo ovvero includere una misura che incide notevolmente sulla sua sfera personale.

ferma che il termine "decisione" e, più in generale, l'art. 22, par. 1, del GDPR deve essere interpretato nel senso che il calcolo automatizzato, da parte di una società che fornisce informazioni commerciali, di un tasso di probabilità basato su dati personali di una persona (relativi alla capacità di adempiere in futuro agli obblighi di pagamento), "*costituisce un processo decisionale automatizzato relativo alle persone fisiche, ai sensi di tale disposizione, qualora da tale tasso di probabilità dipenda in modo decisivo la stipula, l'esecuzione o la cessazione di un rapporto contrattuale con tale persona da parte di un terzo, al quale è comunicato tale tasso di probabilità*" [103]. Così facendo [104], la nozione ricomprenderebbe l'attività di *scoring* effettuata dalla società in questione [105], che si limitava a fornire alla banca le risultanze della profilazione, ricoprendo un ruolo decisivo nella concessione del finanziamento da parte di quest'ultima.

L'interpretazione data dalla Corte può applicarsi a qualunque fattispecie in cui l'attività di profilazione e quella di decisione assumano confini incerti, ed è dunque significativa. Questa, unitamente ai principi generali di proporzionalità e di responsabilizzazione, come anche sopra investigati, consente invero di evitare che qualunque parcellizzazione delle attività di raccolta dati, profilazione e decisione possa comportare una elusione della normativa di cui al GDPR. Secondo la CGUE, in materia, occorre sempre effettuare una valutazione – caso per caso – se le risultanze derivanti dall'attività di profilazione svolta da un terzo ricoprano, o meno, un ruolo determinante per la decisione. In altre parole, così come anche indicato dall'Avvocato Generale [106], occorre fare riferimento al concetto di predeterminazione della decisione indagando se questo risulti integrato o meno nel procedimento di volta in volta analizzato,

---

[103] Par. 73 della sentenza. Lo stesso Avvocato Generale nelle sue conclusioni ha specificato come il fattore determinate è l'impatto che la decisione ha nei confronti dell'interessato. Dunque, un punteggio di *scoring* negativo può essere considerato una decisione ai fini dell'art. 22 GDPR "*quando un istituto finanziario gli attribuisce un'importanza fondamentale nel processo decisionale*".

[104] Invero, sia la Corte che l'Avvocato Generale ritengono che sia pacifico che l'attività in questione rientra nella definizione di profilazione di cui all'art. 4, par. 4, GDPR, in quanto lo scoring effettuato dalla società "*utilizza dati personali per valutare determinati aspetti relativi alle persone fisiche per analizzare o prevedere aspetti riguardanti la situazione economica, l'affidabilità e il probabile comportamento di dette persone*", permettendo, per l'effetto, di trarre conclusioni sulla solvibilità dell'interessato.

[105] Par. 46 della sentenza.

[106] Par. 42 delle conclusioni dell'Avvocato Generale.

superando ogni tipo di rigido formalismo che comporterebbe l'elusione della normativa qualora la decisione finale sia presa da un altro soggetto [107]. In definitiva, seguendo i ragionamenti della Corte e dell'Avvocato Generale, l'esternalizzazione, attività generalmente lecita e incentivata, deve essere (e rimanere) solo uno strumento per accedere a competenze di cui terzi sono specializzati e mai un costituire un presupposto per l'esonero dalle responsabilità.

D'altro canto, guardando al caso specifico, qualora la Corte avesse proceduto a dare un'interpretazione restrittiva (ovverosia considerare l'attività di calcolo un atto preparatorio), è di immediata evidenza che si sarebbe assistito ad un'elusione della tutela prevista dell'art. 22 del GDPR non potendosi richiedere, per un verso, all'agenzia di valutazione del credito le informazioni di cui all'art. 15, par. 1, lett. h) del GDPR, perché non soggetto a tale normativa e, per altro verso, all'istituto finanziario che ha adottato la decisione in quanto, anche se collaborativo, non ha in possesso alcuna informazione rilevante. Proprio grazie all'approccio seguito in tale pronuncia, pertanto, si è riconosciuta effettiva tutela all'interessato, potendo questi far valere i propri diritti direttamente nei confronti dell'agenzia di valutazione del credito, l'unica in grado di rispondere alle sue richieste [108].

La seconda questione interpretativa su cui si pronuncia la Corte è invece relativa al significato della norma in esame nella parte in cui richiede che la decisione abbia effetti giuridici nei confronti dell'interessato o incida, sul medesimo, "in modo analogo".

Sul punto viene espresso, in particolare, il principio per cui la "decisione", per essere rilevante ai sensi dell'art. 22 del GDPR, può non avere un impatto di natura giuridica, ma è sufficiente che questo abbia natura economica e sociale. Le ripercussioni per l'interessato devono ovviamente es-

[107] Il giudice del rinvio spiega altresì che, benché il terzo non sia tenuto a prendere la sua decisione in base al punteggio di *scoring*, resta il fatto che "di solito lo fa ampiamente". Esso aggiunge che, "benché un prestito possa essere rifiutato malgrado un punteggio di scoring in linea di principio sufficiente (per altre ragioni, come l'assenza di garanzie o dubbi sull'esito positivo di un investimento da finanziare), un punteggio di *scoring* insufficiente porterà al rifiuto di un prestito *in quasi tutti i casi*, almeno nell'area dei prestiti al consumo, ancorché un investimento sembri altrimenti proficuo". Infine, detto giudice osserva che "il fatto che i punteggi di scoring abbiano un *peso decisivo* nella concessione dei prestiti e nella formulazione delle loro condizioni è dimostrato dalle esperienze delle autorità di controllo della protezione dei dati".

[108] Par. 50 delle conclusioni dell'Avvocato Generale.

sere poi dotate di un certo grado di gravità della quale dovrà tenersi conto caso per caso facendo riferimento tanto al singolo individuo quanto alla normativa vigente [109]. La pronuncia sembra quindi confermare sul punto quanto già anticipato dalla dottrina, ovverosia come la soluzione più idonea sia proprio un ritorno al ragionamento per principi da applicare al caso concreto, poiché le diverse discipline, generali e di settore, per quanto dettagliate, risulteranno sempre "anacronistiche" rispetto al rapido sviluppo che interessa i vari settori influenzato sempre più dall'innovazione tecnologica.

3. Conclusioni preliminari e prospettive future

A prescindere dal settore di riferimento e dal soggetto che la esercita, la profilazione soggiace alla disciplina del GDPR e, specie se svolta in forma automatizzata, comporta per i titolari di trattamento l'osservanza di diversi e rigidi obblighi posti a presidio degli individui. La collocazione della disciplina in una normativa a carattere orizzontale e trasversale è la naturale conseguenza delle politiche legislative dell'Unione europea in materia di mercato unico digitale, che si preordina di disciplinare l'attività sulla base del noto principio "stessa attività, stessi rischi, stesse regole e supervisione" e, in definitiva, sui principi di responsabilizzazione e di proporzionalità [110].

Ciò però non toglie, come visto nel corso della trattazione, che la normativa speciale (e verticale) non abbia ripercussioni, giuridiche e fattuali. Già la PSD2, disinnescando l'*Open Banking*, ha instaurato un nuovo paradigma di interazione per i pagamenti al dettaglio, basato essenzialmente sulla tecnologia API, e predisposto norme specifiche, da applicare unitamente a quelle contenute nel GDPR, che hanno di fatto incentivato le attività di profilazione dei dati dei conti di pagamento degli interessati even-

---

[109] A tal proposito, occorre osservare anzitutto che il Considerando n. 71 del GDPR cita esplicitamente "il rifiuto automatico di una domanda di credito online" come esempio tipico di una decisione che incide «significativamente» sull'interessato.

[110] BANCA D'ITALIA, *L'Open Banking nel sistema dei pagamenti: evoluzione infrastrutturale, innovazione e sicurezza, prassi di vigilanza e sorveglianza*, *ibidem*, secondo la quale "*A questo fine, gli sviluppi di mercato dovranno essere accompagnati e indirizzati da una evoluzione dell'impianto normativo che, nel rispetto degli interessi delle varie parti coinvolte e secondo un criterio di proporzionalità, continui a favorire la diffusione di nuovi servizi nell'ambito di un sistema finanziario solido, inclusivo e aperto all'innovazione*".

tualmente (o verosimilmente) in combinazione con altri dati, finanziari e non finanziari [111].

Ora, ove adottata, la recente proposta normativa di cui al pacchetto Financial Data Access and Payments Package comporterà la nascita di un quadro embrionale di condivisione di tutti i dati finanziari e un nuovo e importante attore: il Financial Information Service Provider [112]. Dal momento che è toccato l'intero settore finanziario nel suo complesso occorre probabilmente aspettarsi, in tema di profilazione, un impatto ancor più significativo di quanto non lo sia stato quello conseguente all'adozione della PSD2. L'aumento dei flussi dei dati e delle possibili combinazioni tra gli stessi, unitamente all'entrata in campo di nuovi attori (i FiSP), comporterà inevitabilmente un ulteriore spostamento del baricentro dai servizi di pagamento e servizi finanziari in favore dell'attività di profilazione in sé. In altre parole, l'attività di profilazione nel settore finanziario, seppur accessoria ed eventuale, rivestirà sempre più un ruolo centrale per ciascun modello di *business*, così confortando la nota filosofia di Umberto Galimberti, per il quale la tecnologia, per natura, da mezzo diventa fine.

Servirà dunque riflettere su nuovi e ulteriori interventi normativi in futuro in tema di profilazione? Ebbene, seppur non possa a priori escludersi la necessità di ulteriori interventi normativi in materia, elaborati sulla base di ciò che solo l'esperienza insegna, allo stato, occorre considerare che l'alluvione normativa a cui si assiste già da diversi anni porta più incertezze che benefici. Ciò deve portare a serie riflessioni e indurre probabilmente a ritenere che sia più conveniente mettere da parte l'intensa attività legislativa di dettaglio per lasciar spazio, sul piano legislativo, alla normazione per principi e, sui piani operativo e giudiziario, alle (giuste) raccomandazioni e interpretazioni. Su quest'ultimo aspetto, un insegnamento può trarsi dalla recente pronuncia della CGUE che risolve diverse problematiche sorte in occasione delle attività di profilazione automatizzate commissionate a terzi offrendo, appunto, virtuose ricostruzioni interpretative. Almeno nell'ambito del trattamento dei dati personali, inclusa la profilazione, dunque, il

[111] Sul punto è da evidenziare come l'Opinion n. 38 dell'EDPB, relativa al nuovo pacchetto Financial Data Access and Payments Package, precisi che sia opportuno elaborare orientamenti specifici in materia di combinazione dei dati. Vedi EDPB, Opinion n. 38, *ibidem*, par. 34.

[112] Il Financial Information Service Provider (FiSP) è ai sensi dell'art. 3, n. 7, della proposta di regolamento FiDA: "*un utente dei dati autorizzato ai sensi dell'articolo 14 ad accedere ai dati del cliente di cui all'articolo 2, paragrafo 1, per prestare servizi di informazione finanziaria*".

GDPR appare una normativa esaustiva [113], enunciativa di principi generali chiari e solidi, da poter utilizzare per risolvere di volta in volta le problematiche contingenti poste dalla transizione digitale, unitamente ai pareri e alle raccomandazioni di volta in volta emessi dalle autorità di settore competenti.

[113] Occorre considerare che, oltre al GDPR, in materia di profilazione automatizzata che ricorre ad algoritmi assumerà rilievo anche il regolamento sull'IA, attualmente in fase di adozione perché proposto COM/2021/206 final.

Tommaso Edoardo Frosini

Conclusioni

1. Più che delle conclusioni farò delle riflessioni. Innanzitutto sul tema oggetto di questo libro: *Open Banking* e *Open Finance*, e quindi l'accesso aperto ai servizi bancari e finanziari. Può sembrare un argomento per specialisti e invece riguarda tutti noi, come cittadini e consumatori. Perché si tratta di regolazione delle piattaforme digitali e quindi di dati informatici, che oggi sono il modo attraverso il quale la persona si manifesta, è conosciuta e opera (anche) nel mercato finanziario. Noi siamo dei dati sempre tracciabili: lasciamo impronte "digitali" ogniqualvolta facciamo un prelievo dal bancomat, usiamo la carta di credito oppure gestiamo operazioni sul conto attraverso l'*e-banking*. Non ci sono solo rischi per la nostra *privacy*, che può essere violata dall'accesso ai nostri dati, che hanno una loro natura sensibile in quanto collegate a situazioni private. Il problema, più in generale, attiene alla tenuta del sistema bancario, oggi gestito attraverso la tecnologia. Ci sono stati diversi casi di accesso nei sistemi informatici delle banche, al fine di svuotare i conti dei clienti o fare delle truffe utilizzando la modalità dei bonifici elettronici. Così come si sono potuti rendere pubblici i conti bancari di un cliente, come nel recente caso di un senatore della repubblica che si è visto pubblicare sui giornali e *online* l'estratto conto della propria movimentazione bancaria. Pertanto, il trattamento dei dati personali dei clienti richiede delle garanzie supplementari, per impedire che l'*Open Banking* degeneri in una licenza di abuso o in un'occasione di agevolazione delle frodi informatiche. Proteggere i dati, vuol dire assicurare la sicurezza informatica e la corretta gestione delle informazioni bancarie e dei servizi di pagamento. Che hanno financo una loro esplicita tutela costituzionale *ex* art. 47 Cost.: "*La Repubblica incoraggia e tutela il risparmio in tutte le sue forme: disciplina, coordina e controlla l'esercizio del credito*". Una norma che andrebbe osservata e applicata di più e meglio di quanto finora è stato fatto. Certo, la costituzione riproduce uno schema del sistema creditizio bancario che non è più soltanto quello del luogo del

deposito dei propri averi finanziari. Il risparmio dei cittadini ha dei costi, affinché possa essere tutelato e conservato, se non addirittura forzosamente prelevato come fu con l'anatocismo bancario. E le banche non sono più casse di risparmio, perché hanno intrapreso attività imprenditoriali con investimenti e quotazioni in borsa, che impongono continue operazioni economiche, volte a impedire le oscillazioni al ribasso delle azioni.

L'ordine giuridico del digitale sviluppa nuovi servizi in forme nuove, come la gestione automatizzata dei conti o alle cripto-valute organizzate su registri *blockchain*. Oppure, le piattaforme di *peer to peer (P2P) lending* e di *crowfunding*, quali canali di raccolta del capitale alternativi a quello bancario o anche ai nuovi servizi di pagamento digitali. In questo scenario digitale del sistema bancario e finanziario è intervenuta, ancora una volta, l'Unione europea, da ultimo con la direttiva PSD2, che intende promuovere la concorrenza nei servizi di pagamento, sollecitando una nuova forma di competitività e disarticolando il potere nel contesto dell'economia delle piattaforme digitali. Norma fondamentale, per così dire, della direttiva PSD2 è l'art. 36, il quale prevede che «*Gli Stati membri provvedono affinché gli istituti di pagamento abbiano accesso ai servizi relativi ai conti di pagamento degli enti creditizi in maniera obiettiva, proporzionata e non discriminatoria. L'accesso è sufficientemente ampio da consentire all'istituto di pagamento di fornire servizi di pagamento in modo agevole ed efficiente*».

Alla citata direttiva va aggiunto l'annunciato pacchetto sulla finanza digitale, con le proposte di Regolamento *Open Finance* o – *Financial Data Access Framework* – (FIDA), relativo ai servizi di pagamento nel mercato interno (PSR) e di Direttiva PSD3, che modifica la PSD2, attraverso la quale si vuole fornire una regolamentazione organica delle implicazioni che la digitalizzazione ha sul settore finanziario. Si tratta di proposte – come emerge nei contributi presenti in questo volume, in particolare quello di Valeria Falce – con le quali prende corpo la Strategia europea per la finanza digitale, nella direzione anzitutto dell'estensione del paradigma dell'*Open Banking* a tutto il settore finanziario. Queste proposte normative, presentate dalla Commissione a giugno 2023, vorrebbero valorizzare i dati del cliente promuovendone la condivisione e il riutilizzo per la personalizzazione di prodotti e servizi finanziari, per i consumatori e per le piccole e medie imprese. Se fosse davvero così, allora andrebbero salutate con favore. Bisognerà vedere l'interpretazione e l'applicazione, che spesso va ben oltre la letteralità della norma.

In punto di dati digitali, bancari e non, bisogna tenere conto del rovescio della medaglia, per così dire. E cioè che i dati hanno un valore economico e sono soggetti alla loro commercializzazione. Infatti, chi viene in

possesso dei dati bancari di clienti facoltosi, può commercializzarli ovvero venderli a quelle società interessate a proporre l'acquisto di una serie di prodotti finanziari, da veicolare nel mercato attraverso la tecnica della profilazione. Di fatto questo già avviene, anche attraverso le dichiarazioni dei redditi che, in nome della trasparenza amministrativa, devono essere messi *on line*, specie quando si svolgono incarichi pubblici. Trasparenza vs. *privacy*, che può voler dire altrimenti: controllo statale e sociale contro libertà individuale e riservatezza dei propri dati. Chi scrive si schiera, senza se e senza ma, per la seconda soluzione.

2. Il tema dello *Open Banking* che si fa *Open Finance*, può essere altresì declinato come problema dell'organizzazione di un ordinamento giuridico, occhiuto o liberale. Fin dove si deve controllare il cliente-consumatore? L'unico vera forma di controllo è quella dei dati a vocazione sensibile, altrimenti "particolari" come usa dire adesso. La cui conoscibilità verso terzi può determinare danni economici e morali nei confronti dell'individuo. Il fenomeno dei *social network*, sia pure vietati per determinati servizi finanziari, è una pericolosa deriva che può alimentare una situazione di rischi e disagi nei confronti del cittadino – utente, consumatore o cliente che sia. Quindi, ben venga un ordine giuridico che regola il sistema del digitale sebbene, a mio avviso, dovrebbe essere organizzato sulla base di norme di principio anziché di dettaglio, su norme a prevalenza promozionali anziché sanzionatorie. Come invece sembra essersi avviata l'Unione europea, attraverso una continua produzione di regolamenti e direttive, con i quali ha iniziato a normare il mercato e i servizi delle piattaforme digitali e financo a contenere l'espansione dell'intelligenza artificiale. Nell'illusione di volere "plasmare il futuro digitale dell'Europa", per dirla con uno *slogan* coniato dalla stessa UE, mentre invece rischia di determinare un disordine giuridico del mercato digitale, generato da un eccesso farraginoso di norme, che complicano il quadro regolatorio e rendono assai difficile l'applicazione delle stesse, sia da parte del cittadino-consumatore-utente delle piattaforme digitali, sia da parte delle aziende che operano nel settore della tecnologia industriale. Una prova di ciò è già verificabile nei regolamenti che sono stati varati dalla UE, che si distribuiscono per numerosi articoli e paragrafi: si prenda, a esempio, il regolamento sull'intelligenza artificiale (*AI act*), che si spalma su 89 "considerando", 85 articoli (di cui, almeno uno, il 4, di 44 paragrafi) e 9 allegati. Non è facile districarsi nella boscaglia normativa nemmeno per l'intelligenza umana, anche quella di un giurista avvezzo alla interpretazione delle norme. Invece: un regolamento su una materia davvero strategica per la UE e non solo (posto che la AI si andrà a

usare e applicare, da cittadini e imprese europee, in giro per il mondo, quindi oltre la perimetrazione normativa eurounitaria) dovrebbe, a mio avviso, essere sorretto da una disciplina normativa "sostenibile", con l'intento di riuscire a bilanciare interessi e concezioni diversificate, ponendosi quale primario obiettivo quello di non inibire la ricerca e lo sviluppo della AI, tenuto conto della sua importanza per la crescita economica e per l'implementazione della ricerca scientifica, a cominciare da quella medica, dove l'impatto della AI si sta rivelando determinante per la diagnosi e la terapia di una serie di patologie. La normativa europea dovrebbe essere altresì flessibile e adattabile ai cambiamenti; con l'obiettivo di creare e formare un diritto della AI *stable but not still*. In tal modo, si potrà giungere a una sorta di ordine giuridico del digitale: ordine da intendersi non come comando piuttosto come precetto, che dispone di compiere (o di non compiere) un certo tipo di azioni. Pertanto, il problema va impostato e risolto sul terreno pratico dell'esperienza giuridica; si deve cioè esaminare, se si tratta o no di un fatto, che si verifica nel mondo delle azioni degli uomini in società, dove è dato constatare l'esistenza del diritto. Come scrive e conclude Valeria Falce il suo contributo: «Rimangono ferme le linee di indirizzo e i principi generali che ispirano la Strategia digitale soprattutto in relazione ai profili soggettivi e agli ambiti di esternazionalizzazione. Indipendentemente, quindi, dai soggetti, sono attività e rischi ad attrarre responsabilità e regole».

Questo libro ci aiuta a riflettere anche su questo.

Gli Autori

Valeria Falce, Titolare della Cattedra Jean Monnet in politica europea dell'innovazione, Titolare della Cattedra Jean Monnet in Digital Transformation and AI Policy e Professore ordinario di Diritto dell'economia presso l'Università Europea di Roma.

Umberto Morera, Professore ordinario di Diritto dell'economia presso il Dipartimento di Management e Diritto dell'Università di Roma Tor Vergata.

* * *

Filippo Annunziata, Professore associato di Diritto dei mercati finanziari presso l'Università Luigi Bocconi di Milano; Docente esterno presso l'Università Ca' Foscari di Venezia; Visiting Scholar presso la Katholieke Universiteit di Leuven (Belgio).

Magda Bianco, Capo del Dipartimento Tutela della Clientela ed Educazione Finanziaria di Banca d'Italia.

Rita Camporeale, Responsabile Servizio Sistemi di Pagamento presso l'Associazione Bancaria Italiana (ABI).

Marco Cassese, Team Member del progetto Digital Markets and Competition Policy (DiCo) e Ricercatore dell'Innovation, Regulation and Competition Policy Centre (ICPC) presso l'Università Europea di Roma.

Giuseppe Colangelo, Professore associato di Diritto dell'economia presso l'Università della Basilicata, Jean Monnet Professor of European Innovation Policy e Transatlantic Technology Law Fellow presso la Stanford University.

Stefano Firpo, Direttore Generale di Assonime.

Liliana Fratini Passi, Direttore Generale del CBI S.c.p.a. e VICE-CHAIR – United Nations Centre For Trade Facilitation and Electronic Business (UN/CEFACT).

Tommaso Edoardo Frosini, Professore ordinario di Diritto pubblico comparato e Direttore del Dipartimento di Giurisprudenza dell'Università Suor Orsola Benincasa di Napoli.

Sara Landini, Professore ordinario di Diritto dell'economia presso l'Università di Firenze.

Marino Ottavio Perassi, Avvocato Generale presso Banca d'Italia.

Maddalena Rabitti, Professore ordinario in Diritto dell'Economia presso l'Università degli Studi Roma Tre.

Biancamaria Raganelli, Professore di Diritto dell'economia presso l'Università di Roma Tor Vergata.

Pasquale Stanzione, Presidente del Garante per la protezione dei dati personali.

Andrea Stazi, Regulatory Affairs Lead per il Sud Europa presso Google e Professore ordinario di Diritto privato comparato presso l'Università Telematica San Raffaele di Roma.

Maria Iride Vangelisti, Direttore nel Servizio di Educazione finanziaria in Banca d'Italia.

Finito di stampare nel mese di giugno 2024
nella Stampatre s.r.l. di Torino
Via Bologna 220

UNIVERSITÀ EUROPEA DI ROMA

Volumi pubblicati

Sezione Giuridica – MANUALI

1. A.M. GAMBINO-A. STAZI-D. MULA, *Diritto dell'informatica e della comunicazione. Terza edizione*, 2019, pp. XVI-288.

Sezione Giuridica – SAGGI

1. A. MERONE, *Il tribunale arbitrale dello sport*, 2009, pp. X-266.
2. F. TESTA, *La funzione negoziale nell'azione sindacale. Seconda edizione. Contributo per una teoria unificante del riconoscimento giuridico dell'azione sindacale*, 2010, pp. XVI-228.
3. P. RIVELLO, *Il processo penale di fronte alle problematiche dell'età contemporanea. Logiche processuali e paradigmi scientifici*, 2010, pp. VIII-188.
4. V. FALCE, *La modernizzazione del diritto d'autore. Seconda edizione*, 2012, pp. VI-274.
5. T. SCANDROGLIO, *La Teoria Neoclassica sulla legge naturale di Germain Grisez e John Finnis*, 2012, pp. XII-516.
6. F. TESTA, *Il diritto alle ferie del lavoratore subordinato*, 2012, pp. XVIII-142.
7. E. BILOTTI, *Separazione dei beni del defunto e tutela dei creditori*, 2012, pp. X-222.
8. F. SANTAGADA, *La mediazione*, 2012, pp. X-190.
9. M. PALMARO, *Eutanasia: diritto o delitto? Il conflitto tra i principi di autonomia e di indisponibilità della vita umana*, 2012, pp. XII-116.
10. A. STAZI, *Innovazioni biotecnologiche e brevettabilità del vivente. Questioni giuridiche e profili bioetici nei modelli statunitense ed europeo*, 2012, pp. X-302.
11. I. GARACI, *Nuovi beni e tutela della persona. Lo sfruttamento commerciale della notorietà*, 2012, pp. XIV-106.
12. C. LONGARI, *Le cause di estinzione del reato*, 2012, pp. XIV-218.

13. G. NAVA, *Regolamentazione e contenzioso tra operatori nelle comunicazioni elettroniche*, 2012, pp. VIII-224.
14. E. PROSPERETTI, *L'opera digitale tra regole e mercato*, 2013, pp. VIII-280.
15. F. TOZZI, *La circolazione dei diritti della persona*, 2013, pp. X-214.
16. F. VARI, *L'affermazione del principio d'eguaglianza nei rapporti tra privati. Profili costituzionali*. Seconda edizione, 2016, pp. X-142.
17. W. WALDSTEIN, *Scritto nel cuore. Il diritto naturale come fondamento di una società umana,* traduzione italiana a cura di Filippo Vari, 2014, pp. XIV-146.
18. V. OCCORSIO, *La clientela professionale come bene giuridico,* 2016, pp. VIII-240.
19. A. MERONE, *Il disconoscimento delle prove documentali,* 2018, pp. XXIV-328.
20. A. STAZI, *Automazione contrattuale e "contratti intelligenti". Gli* smart contracts *nel diritto comparato*, 2019, pp. XII-196.
21. M.L. BIXIO, *Modelli di gestione collettiva a tutela dei diritti d'autore. Itinerari tra dinamiche concorrenziali ed interferenze di diritto sovranazionale*, 2020, pp. XX-260.

Sezione Giuridica – MATERIALI

1. *Codice civile applicato. Casi scelti a cura di* A.M. GAMBINO-E. BILOTTI-E. SQUINTANI, 2011, pp. VIII-284.
2. F. DONATO-SEMINARA, *La speciale disciplina delle banche popolari cooperative*, 2011, pp. VIII-224.
3. *Rimedi e tecniche di protezione del consumatore a cura di* A.M. GAMBINO, 2011, pp. X-450.
4. F. VARI, *La fecondazione eterologa tra costituzione italiana e convenzione europea dei diritti dell'uomo*, 2012, pp. VIII-194.
5. V. FALCE, Fairness e *innovazione nel mercato digitale*, 2020, pp. XIV-210.
6. V. FALCE (a cura di), Financial Innovation *tra disintermediazione e mercato*, 2021, pp. XXVIII-212.
7. V. FALCE (a cura di), *Digital Markets and Competition Law*, 2021, pp. VIII-334.

8. V. FALCE (a cura di), *Strategia dei dati e intelligenza artificiale. Verso un nuovo ordine giuridico del mercato*, 2023, pp. X-326.
9. V. FALCE (a cura di), *Digital Ecosystems. Market challengers and pro-competitive solutions*, 2024, pp. VIII-312.
10. V. FALCE (a cura di), *Dall'Open Banking all'Open Finance. Profili di diritto dell'economia*, 2024, pp. XIV-194.

Sezione Economica – SAGGI

1. M. PEDRANA, *Le dimensioni del capitale sociale. Un'analisi a livello regionale*, 2012, pp. XIV-178.

Sezione Economica – MATERIALI

1. A. NUZZI, *Towards year 2010. Issues in European Transport Policy - Railways and Motorways*, 2009, pp. XVI-224.

Sezione Umanistica – SAGGI

1. P. SCARAFONI, *Il Dio presente*, 2013, pp. XII-300.