A chi ha sempre creduto in me,
Anche quando io non ci credevo più.

UNIVERSITÀ DEGLI STUDI DI PADOVA
DIPARTIMENTO DI DIRITTO PRIVATO E CRITICA DEL DIRITTO
DIPARTIMENTO DI DIRITTO PUBBLICO, INTERNAZIONALE E COMUNITARIO

CORSO DI LAUREA MAGISTRALE IN GIURISPRUDENZA
A.A. 2023/2024

TESI DI LAUREA IN BANKING LAW

I SERVIZI DI PAGAMENTO ALLA LUCE DELLA PROPOSTA DI UNA PAYMENT SERVICES DIRECTIVE III

RELATORE: CHIAR.MO PROF. MATTEO DE POLI

LAUREANDO: GIADA BONALDO
MATRICOLA N. 1145948

INDICE

INTRODUZIONE

L'industria dei pagamenti è sempre più digitale e, in particolar modo, negli ultimi decenni, ha subito una evoluzione esponenziale dovuta all'innovazione tecnologica. L'emergere di nuove tecnologie e la crescita del commercio elettronico hanno di fatto rivoluzionato il modo di effettuare e ricevere pagamenti. Oggi è infatti possibile effettuare pagamenti tramite *smartphone* e *smartwatch*, e si possono ordinare trasferimenti di denaro da un conto ad un altro da qualsiasi luogo tramite *home banking* o *mobile banking*, e via dicendo.

Sicuramente questo ha da un lato facilitato le transazioni economiche ma dall'altro ha posto nuove sfide in termini di sicurezza e protezione degli utenti. È in questo contesto che è intervenuto il legislatore comunitario al fine di armonizzare a livello europeo la disciplina sui servizi di pagamento e a cercare di rispondere al rapido sviluppo delle tecnologie che investe il settore, al fine di assicurare la velocità e la sicurezza delle transazioni, percepite quale propulsore della crescita economica.

Parallelamente alle novità introdotte dal legislatore europeo, la rivoluzione digitale cui si sta assistendo negli ultimi anni ha creato prospettive di sviluppo che possono modificare radicalmente la tradizionale conformazione dei servizi di pagamento, e più in generale dei servizi bancari e finanziari. Si pensi, ad esempio, all'avvento di nuovi operatori in un contesto che prima era monopolio assoluto della banca.

Per la prima volta nel 2007, con la *Payment Services Dirrective*, l'Unione Europea ha definito un quadro giuridico comune per tutti gli Stati membri, vincolando i Paesi a modificare il proprio ordinamento per

rendere uniforme la disciplina dei servizi di pagamento. La direttiva più importante, e quella attualmente vigente, è la *Payment Services Directive 2* emanata nel 2015: essa ha rappresentato un punto di svolta nella regolamentazione del settore introducendo significative novità soprattutto con riguardo alla protezione degli utenti e al rafforzamento di un *level playing field* per gli operatori.

L'innovazione tecnologica è però incessante e imprevedibile, tanto da mostrare ben presto delle "falle" nella normativa, che necessita quindi di essere sempre aggiornata al fine di tutelare correttamente l'utente. Attraverso questa indagine si intende fornire un quadro sulle più importanti direttive europee che affrontano il tema dei servizi di pagamento, con uno sguardo alla proposta di aggiornamento avanzata dalla terza direttiva sui servizi di pagamento, e, inoltre, si intende guardare anche alla normativa interna del nostro Paese, ossia il d.lgs. 11/2010 che ha recepito la prima direttiva europea (con successive modifiche) e la modifica del Testo Unico Bancario che ne è conseguita.

CAPITOLO I

-

I SERVIZI DI PAGAMENTO

1. Inquadramento del fenomeno e della normativa rilevante

I servizi di pagamento sono tutti quei servizi prestati da un intermediario che consentono il trasferimento di denaro da un soggetto (il c.d. pagatore) ad un altro (il c.d. beneficiario) senza che il primo debba materialmente consegnare al secondo monete, banconote o titoli di credito come assegni e cambiali.[1]

Un quadro normativo comunitario armonizzato dei servizi di pagamento è essenziale per la realizzazione del "mercato unico", ossia un sistema delineato da regole base comuni per tutti i Paesi dell'Unione Europea che siano in linea con il progresso tecnologico e che consente di conseguenza il perfezionamento del mercato interno di ciascun Paese membro.[2]

---

[1] Così E. CECCHINATO, *I servizi di pagamento* in *Il diritto bancario oggi: aspetti sostanziali processuali*, F. Aratari e Guido Romano (a cura di), Wolters Kluwer, 2023, pp. 365 e ss. Si veda in tal senso anche RISPOLI FARINA, *I servizi di pagamento (con cenni alle nuove c.d. "valute virtuali")*, in Urbani (a cura di), *L'attività delle Banche*, Milano, II ed., 2020, p. 555.

[2] Per approfondimenti si veda S. MONETI, *«Mobile payments»: gli sviluppi del mercato e l'inquadramento normativo*, in Analisi Giuridica dell'Economia, n. 1, 2015, pp. 101 ss. Si veda anche M. DONNELLY, *Payments in the digital market: Evaluating the contribution of Payment Services Directive II*, Law School University College in Cork, Ireland.

A tal fine è intervenuto sul tema il legislatore europeo[3], per la prima volta nel 2007, con la c.d. *Payment Services Directive*[4] (d'ora in poi *PSD*), recepita nel nostro ordinamento all'interno del Testo Unico Bancario (TUB) e del d.lgs. 11/2010, il cui obiettivo primario era di creare un quadro legale uniforme per i servizi di pagamento in tutta l'Unione Europea e fornire il fondamento legislativo per l'area unica dei pagamenti in euro (SEPA)[5].

La cornice giuridica dei servizi di pagamento venutasi a creare nel 2007 ha però mostrato, dopo pochi anni di applicazione, la sua difficoltà nello stare al passo con i tempi, soprattutto per quanto atteneva all'innovazione tecnologica e dei modelli operativi. È per questeo che la

---

[3] Merita sottolineare che la prima Direttiva sui servizi di pagamento ha preso le mosse da un'iniziativa esterna alle istituzioni dell'Unione. L'impulso infatti proveniva direttamente dal sistema bancario, attraverso il Consiglio Europeo dei Pagamenti. Così A. SCIARRONE ALIBRANDI, *Impostazione sistematica della Direttiva PSD2*, in *Innovazione e regole nei pagamenti digitali: il bilanciamento degli interessi nella PSD2, a cura di* M. C. Paglietti e M. I. Vangelisti, Università degli Studi Roma Tre Dipartimento di Giurisprudenza, Roma Tre-Press, 2020.

[4] Direttiva 2007/64/CE sui servizi di pagamento.

[5] Acronimo di "*Single Euro Payments Area*": si tratta di un progetto promosso dall'Unione Europea al fine di rendere uniformi e dunque sviluppare servizi di pagamento comuni a tutta l'Unione. È l'area in cui cittadino, impresa, Pubblica Amministrazione e ogni altro operatore economico possono effettuare e ricevere pagamenti in euro secondo regole, procedure operative e prassi di mercato uniformi. Alla SEPA aderiscono i ventotto paesi dell'UE, inclusi quelli non euro, e anche altri paesi non appartenenti all'UE. Questa rappresenta per i pagamenti al dettaglio con strumenti diversi dal denaro contante il naturale completamente del passaggio alla moneta unica. Per un maggiore approfondimento sul tema si veda P. GAGGI, *L'apporto dell'autoregolamentazione alla realizzazione della SEPA*, in *Armonizzazione europea dei servizi di pagamento ed attuazione della direttiva 2007/64/CE*, a cura di M. Rispoli Farine, V. Santoro, A. Sciarrone Alibrandi e O. Troiano, 2009, p.243 ss.; e O. TROIANO, *La nuova disciplina privatistica comunitaria dei servizi di pagamento: realizzazioni e problemi della Single Euro Payments Area (SEPA)*, in *Il nuovo Quadro normativo comunitario dei servizi di pagamento. Prime riflessioni*, a cura di Mancini e Perassi, in *Quaderni di ricerca giuridica della consulenza legale di Banca d'Italia*, n. 63, dicembre 2008, p. 41 e ss.

PSD fu abrogata nel 2015 dalla *PSD2*[6], anch'essa recepita nel nostro ordinamento dal d.lgs. 218/2017, il quale ha contestualmente aggiornato, da un lato il TUB, nelle parti in cui esso disciplina gli istituti di pagamento (Titolo V-ter) e la trasparenza dei rapporti dei prestatori di servizi di pagamento con i clienti (Titolo VI), dall'altro il d.lgs. 11/2010, per i profili concernenti i rapporti contrattuali tra prestatori di servizi di pagamento e i clienti. Giova ricordare che, trattandosi di una direttiva di massima armonizzazione volta a garantire l'applicazione uniforme del quadro legislativo in tutta l'Unione, sono stati pochi gli spazi di discrezionalità esercitati dal legislatore nazionale.

Nello specifico, tra i motivi che hanno spinto il legislatore europeo a rivedere la *PSD* troviamo il costante innovarsi delle tecnologie utilizzate nei servizi di pagamento, tali da rendere obsoleta la direttiva precedente. Tra le novità introdotte dalla *PSD2* vi è l'allargamento delle attività e dei servizi sottoposti alla disciplina della direttiva dei pagamenti, questo perché la stessa mira a disciplinare i servizi di disposizione di ordini di pagamento nel commercio elettronico e i servizi di informazione sui conti. Altra rilevante novità introdotta da parte della *PSD2* è stata la creazione di un *level playing field* tra operatori bancari e non: infatti, sempre alla *PSD2* si deve il riconoscimento degli Istituti di Pagamento (IP), accanto ai già previsti Istituti di Moneta Elettronica (IMEL) con la conseguente erosione del monopolio bancario rispetto allo svolgimento di questo tipo di attività.[7]

---

[6] Direttiva 2015/2366/UE.

[7] Così A. SCIARRONE ALIBRANDI, *Impostazione sistematica della Direttiva PSD2*, *op. cit.*, p. 14.

Successivamente all'introduzione della *PSD2* nell'ordinamento europeo, la Commissione, nel 2022, ha svolto una valutazione in merito alla sua applicazione dove ha rilevato che la direttiva ha effettivamente conseguito alcuni degli obiettivi che si era prefissata, ma ha fatto emergere alcune criticità. Si auspicava, ad esempio, una parità tra prestatori di servizi di pagamento bancari e non bancari, ma concretamente ciò non è avvenuto, principalmente a causa della mancanza di un accesso diretto da parte di questi ultimi ai fondamentali sistemi di pagamento[8]. Quindi nonostante la *PSD2* sia stata fondamentale nel miglioramento del settore dei pagamenti, si è reso necessario un aggiornamento normativo.

Sulla scia di questa valutazione, il 28 giugno 2023 la Commissione Europea ha presentato alcune proposte legislative, tra cui la terza direttiva sui servizi di pagamento (*PSD3*)[9], il Regolamento sui Servizi di Pagamento (PSR)[10] e il "Pacchetto Moneta Unico" riguardante l'uso del contante e dell'euro digitale. Tali nuovi testi legislativi, quindi, se approvati, abrogheranno e sostituiranno la *PSD2*.[11]

[8] F. CASCINELLI e L.BETTINELLI, *Verso la PSD3 e il nuovo Regolamento sui Servizi di Pagamento,* consultabile al sito: www.dirittobancario.it

[9] Proposta di direttiva 2023/0209/COD.

[10] Proposta di regolamento 2023/0210/COD.

[11] *PSD3 e PSR: le norme sui servizi di pagamento approvate dal Parlamento Europeo*, reperibile al sito www.dirittobancario.it

2. Evoluzione della normativa che disciplina i servizi di pagamento

Delineati al paragrafo precedente per sommi capi i plessi normativi più rilevanti, pare opportuno ora approfondire più nel dettaglio come si è evoluta la disciplina della materia nel corso degli anni.

Il settore dei servizi di pagamento ha cominciato a svilupparsi a partire dagli anni '80 del secolo scorso, a seguito della diffusione dei primi strumenti di pagamento elettronici[12] e inizialmente, l'industria dei pagamenti ha potuto autoregolarsi. L'autoregolamentazione o *self-regulation*[13] nonostante talvolta, per quanto riguarda i mercati finanziari, essa anticipi il legislatore e/o il regolatore riuscendo a dare voce immediata alle esigenze di mercato, nel caso di specie non è stata in grado di assicurare la certezza del diritto, essendosi venute a creare situazioni di disomogeneità all'interno del settore dei servizi di pagamento[14].

È chiaro come le criticità dell'autoregolamentazione vanno a scapito dell'efficiente funzionamento dell'industria dei pagamenti e dei diversi mercati che fanno ricorso ad essa. Parve opportuna quindi una

[12] A tal riguardo si v. F. CIRAOLO, *I servizi di pagamento nell'era Fintech*, in *Fintech. Introduzione ai profili giuridici in un mercato unico tecnologico dei servizi finanziari*, Paracampo (a cura di), Torino, 2019, p.183 e ss.

[13] Sul punto si veda J PEGADO LIZ, *Parere del Comitato economico e sociale europeo sul tema Autoregolamentazione e co-regolamentazione nel quadro legislativo dell'UE*, INT/754, il quale afferma che «Con il termine autoregolamentazione, […] si designa genericamente, quando ci si riferisce al comportamento economico, l'adozione da parte degli attori economici di certe regole di condotta nelle relazioni reciproche oppure nei confronti di terzi sul mercato e nella società, regole il cui rispetto è frutto di un accordo tra gli stessi attori, senza meccanismi coercitivi esterni».

[14] E. CECCHINATO, *I servizi di pagamento* in *Il diritto bancario oggi: aspetti sostanziali processuali*, F. Aratari e Guido Romano (a cura di), Wolters Kluwer, 2023, pp. 365 e ss.

adeguata armonizzazione della disciplina dei servizi di pagamento, funzionale alla più generale armonizzazione del mercato interno (come recita l'art. 26 TFUE, quello «spazio senza frontiere interne, nel quale è assicurata la libera circolazione delle merci, delle persone, dei servizi e dei capitali»).

Sono quindi seguiti diversi interventi normativi che hanno affrontato la materia in modo organico: come detto al paragrafo precedente, nel 2007 è stata emanata la Direttiva 2007/64/CE sui servizi di pagamento, la cd. *Payment Services Directive*.

Tale direttiva è stata superata poi dalla *PSD2*, alla quale, invero, vanno aggiunti altri atti a completare il quadro normativo di riferimento, in particolare sull'accesso ai conti di pagamento dei consumatori (la *Payment Accounts Directive* o *PAD*)[15]; sulla moneta elettronica (la *E-Money Directive* o *EMD*)[16]; sulla commercializzazione a distanza dei

[15] Si tratta della direttiva 2014/92/UE, recepita in Italia nel Testo Unico Bancario e nelle disposizioni di trasparenzadi Banca d'italia: essa ha introdotto nuove regole finalizzate al rafforzamento della tutela della clientela, garantendo ai consumatori la possibilità di comparare le spese e i costi relativi ai conti di pagamento, di trasferire senza oneri il conto di pagamento e di ampliare le possibilità di accesso al conto di base, eliminando anche le precedenti differenziazioni basate sulla residenza del consumatore. Il conto di pagamento costituisce uno strumento fondamentale per la partecipazione delle persone all'economia e alla società moderna ma la scarsa trasparenza delle spese ad esso associate rendeva difficile ai consumatori raggiungere la piena conoscenza degli strumenti di pagamento. La *PAD* persegue l'obiettivo di garantire maggiore protezione ai consumatori, stimolandoli ad intraprendere scelte più consapevoli.

[16] Si tratta della direttiva 2009/110/CE concernente l'avvio, l'esercizio e la vigilanza prudenziale dell'attività degli istituti di moneta elettronica. Anche questa si inserisce in un processo europeo di armonizzazione dei servizi di pagamento a livello europeo. Le disposizioni di vigilanza hanno adeguato la disciplina degli istituti di moneta elettronica (IMEL) a quella degli istituti di pagamento, definendo in tal

servizi di pagamento nei confronti dei consumatori (la direttiva 2002/65/CE). Alcuni di questi atti sono "autosufficienti",[17] nel senso che esauriscono lo scopo cui sono rivolti; altri invece delegano Commissione o Autorità Bancaria Europea ad integrarne le disposizioni con norme di dettaglio, secondo il c.d. "metodo Lamfalussy".

Il processo legislativo comunitario, infatti, per il settore del diritto bancario opera su più livelli seguendo il c.d. "metodo Lamfalussy" che prende il nome dal suo ideatore, Alexandre Lamfalussy.[18] Gli atti normativi appena citati attengono al primo livello che è costituito da una direttiva od un regolamento volti a delineare un quadro generale di un determinato argomento.

Il secondo livello è composto da un regolamento delegato o da un regolamento d'esecuzione emanato dalla Commissione Europea su delega della direttiva o del regolamento di primo livello. Questi atti contengono regole dettagliate e tecniche frutto della collaborazione tra la Commissione e l'Autorità Bancaria Europea in ragione della sua competenza in materia.

Il terzo livello è dato dagli orientamenti dell'Autorità Bancaria Europea, emanati su delega della normativa di primo livello, questi raccolgono *standard* e *best practice* con riferimento a determinati aspetti della materia che qui ci occupa. Tali orientamenti non sono vincolanti e

---

modo un regime prudenziale omogeneo per tutti gli intermediari che operano nel settore dei pagamenti e rispondente all'esigenza di eliminare le barriere all'ingresso del mercato dei servizi di pagamento e dell'emissione di moneta elettronica.

[17] Ad esempio, lo è la direttiva 2002/65/CE.

[18] Per approfondimenti in merito si v. M. DE POLI, *Fundamentals of Banking Law*, CEDAM, II ed., 2020; pp. 55-58.

pertanto vengono ricompresi nella materia della cd. *soft law*.[19] Anche se non vincolanti si precisa comunque che «Le autorità e gli istituti finanziari competenti compiono ogni sforzo per conformarsi agli orientamenti e alle raccomandazioni» (così il comma 3 dell'art. 16 del regolamento 1093/2010 che istituisce l'Autorità europea di vigilanza).

Il quarto livello impegna la Commissione a monitorare la corretta applicazione negli Stati membri della normativa di cui ai tre livelli precedenti e, qualora fosse necessario, ad intervenire avviando una procedura di infrazione[20].

Obiettivo del metodo Lamfalussy è chiaramente l'armonizzazione del diritto bancario degli Stati membri, e risponde a una esigenza di certezza del diritto. Allo stesso tempo però si tratta di un settore, quello dei pagamenti, in continuo divenire, dinamico e che subisce influenze dovute all'innovazione tecnologica; ad avviso di chi scrive, un metodo normativo così rigoroso, e anche capillare, rischia di rallentare i ritmi del mercato nel tentativo di rispettare la moltitudine di regole cui è soggetto.

Così decritto si nota come il quadro normativo europeo presenta diverse criticità in materia di servizi di pagamento, che meglio saranno esaminate in seguito; inoltre, è necessario

---

[19] La *soft law* consiste in atti non vincolanti come *standards* e *best-practices* emanati da Autorità pubbliche come *EBA* o Istituzioni internazionali come il *Basel Committee on Banking Supervision* o Organizzazioni private come *UK Finance*.

[20] Per quanto riguarda primo, secondo, terzo e quarto livello si veda E. CECCHINATO, *I servizi di pagamento* in *Il diritto bancario oggi: aspetti sostanziali processuali*, F. Aratari e Guido Romano (a cura di), Wolters Kluwer, 2023, p. 365 e ss. e anche M. DE POLI, *Diritto della finanza etica e sostenibile*, anno accademico 2023/2024.

ricordare che esso è composto in prevalenza da direttive e che, in quanto tali, non sono direttamente applicabili ma necessitano di essere recepite dagli Stati membri e quindi, di conseguenza, non c'è massima armonizzazione.

2.1 PSD, PSD2 e PSD3: un primo sguardo d'insieme

La *PSD* è stata recepita dall'ordinamento italiano con il decreto legislativo n. 11 del 2010[21].

Essa aveva come principale obiettivo quello di realizzare una piena armonizzazione del comparto dei servizi di pagamento *retail*, introducendo significative novità: sui soggetti che possono prestare servizi di pagamento; sulle forme di tutela della clientela, mirando a prevedere regole uniformi in tutta l'UE al fine di garantire livelli elevati di chiarezza delle informazioni fornite dai prestatori sui contratti e sulle operazioni di pagamento;[22] sui diritti e gli obblighi delle parti nell'esecuzione di

[21] L'Italia, è un Paese in cui la propensione all'uso del contante è ancora molto alta, stando infatti a UNIMPRESA: «L'Italia è il Paese della zona euro in cui si fanno meno pagamenti digitali. Gli italiani, infatti, nel 2023 hanno prelevato in media un miliardo in contanti al giorno; è, tra i Paesi che adottano l'euro, quello con meno transazioni digitali con una media di 200 transazioni digitali pro-capite contro la media europea di 370 transazioni. Il motivo è la presenza ancora massiccia del contante: in Italia nel 2023 sono stati prelevati 360 miliardi di euro, 10 miliardi in più del 2022 e 18 miliardi in più rispetto al 2021.» Questo primo tentativo di uniformazione della disciplina è stato una condizione essenziale per incentivare l'utilizzo di strumenti elettronici e una spinta alla modernizzazione dell'industria dei pagamenti. Sul punto si v. per approfondimenti A. ENRIA, Commissione VI della Camera dei deputati sul "*Recepimento della direttiva sui servizi di pagamento*" in data 1° dicembre 2009.

[22] A. ENRIA, Commissione VI della Camera dei deputati sul "*Recepimento della direttiva sui servizi di pagamento*", in data 1° dicembre 2009

operazioni di pagamento, sulla struttura delle operazioni e sull'assetto delle responsabilità delle parti.[23]

Dal riesame del quadro europeo e dalla consultazione pubblica della Commissione del 2012[24] è emersa concretamente la necessità di apportare degli adeguamenti alla normativa sui servizi di pagamento per rispondere meglio alle esigenze emparse. L'incalzare della tecnologia e i rapidi cambiamenti del mercato, tra gli altri, hanno rappresentato elementi ostativi alla completa armonizzazione della normativa di riferimento.[25]

In conseguenza di tali considerazioni è stata adottata la *PSD2* che ha revisionato la precedente direttiva per promuovere lo sviluppo del mercato interno dei pagamenti al fine di renderlo sicuro, efficiente e competitivo.[26]

Le principali finalità perseguite dalle istituzioni europee sono state le seguenti:

---

[23] In tal senso la direttiva si poneva in linea stretta di continuità con gli obiettivi propri del progetto di realizzazione di un'area unica dei pagamenti in euro (SEPA), la quale mira ad armonizzare le modalità operative di offerta dei principali servizi di pagamento relativamente alla loro componente più efficiente e cioè gli strumenti elettronici intesi come bonifici, addebiti diretti e carte.

[24] Sulla promozione di pagamenti elettronici sicuri, efficienti e competitivi v. libro verde della Commissione europea "Verso un mercato europeo integrato dei pagamenti tramite carte, internet e telefono mobile" dell'11.1.2012, il quale sul tema afferma che «La diffusione dei pagamenti elettronici si muove di pari passo con quella dei dispositivi mobili (smartphone, tablet, mobile internet device (MID) che possono collegarsi wireless alla rete internet, permettendo di realizzare una delle moderne forme di cd. mobile payments». Sul tema v. S. Moneti, Mobile payments: gli sviluppi del mercato e l'inquadramento normativo, in Analisi giuridica dell'economia, 2015, 101.

[25] Così F. PORTA, *Obiettivi e strumenti della PSD2*, in *Le nuove frontiere dei servizi bancari e di pagamento fra PSD", Criptovalute e Rivoluzione Digitale,* a cura di F. MAIMERI e M. MANCINI, Quaderni di Ricerca Giuridica della Consulenza Legale di Banca d'Italia, n. 87, 2019, p. 28.

[26] Atti del Governo, *Servizi di pagamento nel mercato interno,* 20 gennaio 2020.

- garantire una maggiore tutela dei clienti in generale;
- uniformare le commissioni bancarie tra i diversi Stati membri dell'UE;
- allargare il mercato dei pagamenti *on line*, prevedendo nuovi operatori e servizi alternativi.[27]

Uno degli aspetti innovativi della *PSD2* è l'aumento della concorrenza nel settore finanziario: a partire dal 14 settembre 2019 Banche e Poste Italiane hanno dovuto obbligatoriamente condividere le informazioni relative ai propri clienti con terze parti autorizzate (i cd. *Third Party Providers - TPP*). Questi sono dei soggetti terzi rispetto a quello presso il quale l'utente detiene il proprio conto, e offrono servizi quali disposizione di ordine di pagamento e servizi di informazione sui conti[28].

Vengono inoltre previsti dalla *PSD2* nuovi tipi di prestatori di servizi e nuovi tipi di servizi che possono essere prestati. Per poter utilizzare i servizi prestati dai nuovi *player*, è l'utente stesso a doverne autorizzare l'accesso e il segnale di autorizzazione è trasmesso alla banca del cliente mediante meccanismi rinforzati di sicurezza. [29]

Considerando che le banche non traggono nessun vantaggio dal condividere i dati dei propri clienti con altre imprese innovative in grado di fornire ulteriori servizi, l'introduzione di un obbligo di accesso mira ad

---

[27] I. D'AMBROSIO, *La tutela del consumatore nei pagamenti elettronici e la nuova direttiva europea PSD2*, NLCC 6/2019.

[28] Si rimanda al capitolo seguente per un maggiore approfondimento su tali soggetti, e si v. per quanto riguarda la definzione V. PROFETA, *I third Party Provider: profili soggettivi e oggettivi,* in *Le nuove frontiere dei servizi bancari e di pagamento fra PSD", Criptovalute e Rivoluzione Digitale, op. cit.,* pp. 49 e ss.

[29] Per approfondimenti in tema si v. B. RUSSO*, L'evoluzione dei sistemi e dei servizi di pagamento nell'era del digitale*, CEDAM, 2020.

assicurare una maggiore competizione nel mercato dei servizi di pagamento; bisogna comunque tenere presente che i *TPP* non hanno pieno accesso ai dati dei clienti bancari ma l'accesso è autorizzato solamente per lo scopo specifico «esplicitamente richiesto dal cliente».[30]

In tale contesto sembra utile, a parere di chi scrive, introdurre un altro concetto chiave che sta travolgendo la materia dei servizi di pagamento: le *Fintech*. Con tale espressione viene generalmente indicata l'innovazione finanziaria resa possibile dall'innovazione tecnologica, che può tradursi in nuovi modelli di business, processi o prodotti, ed anche in nuovi operatori di mercato. Il *Fintech* sta investendo totalmente i mercati dei servizi bancari e finanziari, modificandone anche la struttura[31]. Attraverso le nuove tecnologie dell'informazione e delle telecomunicazioni nuove imprese operanti nel settore *Fintech* hanno potuto offrire servizi che in precedenza erano parte del monopolio del sistema bancario.

In questo senso, quindi, imprese che in passato non avrebbero potuto affermarsi in un sistema bancario "tradizionale", stanno invece assumendo ruoli nuovi e aggressivi, cambiando radicalmente la fisionomia del mercato "tradizionale"[32]. La nuova normativa ha aperto le porte a società

---

[30] Così S. VEZZOSO, *Fintech, access to data, and the role of competition policy*, consultabile all'indirizzo www.ssrn.com/abstract=3106594

[31] In tal senso v. R. MENZELLA, *Il ruolo dei big data e il mobile payment,* in *Le nuove frontiere dei servizi bancari e di pagamento fra PSD", Criptovalute e Rivoluzione Digitale, op. cit.*, pp. 148 e ss.

[32] Di nuovo si v. R. MENZELLA, *Il ruolo dei big data e il mobile payment,* in *Le nuove frontiere dei servizi bancari e di pagamento fra PSD", Criptovalute e Rivoluzione Digitale, op. cit., pp. 148 e ss.*; in tal senso anche A. ARGENTATI, *Le banche nel nuovo scenario*

Fintech e a colossi dell'*e-commerce*, come Apple o Amazon, affinché possano gestire in modo completo i processi di pagamento dei propri utenti. L'impatto di simili cambiamenti sulla configurazione del sistema bancario è imprevedibile e, come si vedrà più specificamente nel capitolo successivo, ci sono due differenti visioni sul prossimo futuro: chi presagisce la definitiva scomparsa della banca tradizionale che è destinata a soccombere di fronte ai nuovi competitors e chi ritiene invece che le imprese *Fintech* giungeranno ad un naturale esaurimento, nel momento in cui gli intermediari storici saranno in grado di rispondere positivamente alle innovazioni tecnologiche anche creando alleanze strategiche con i nuovi operatori.[33]

In questo contesto le autorità pubbliche sono chiamate, pertanto, a una attenta analisi delle conseguenze dell'innovazione, al fine di individuare un giusto equilibrio tra rischi e benefici e di predisporre norme in grado di salvaguardare l'interesse pubblico in maniera da garantire la parità di condizioni tra operatori tradizionali e nuovi operatori per stimolare una concorrenza sana.[34]

Un'altra disposizione di rilievo introdotta dalla *PSD2* riguarda l'auteticazione forte del cliente (*Strong Customer Authentication* o *SCA*)[35], che prevede un rafforzamento della sicurezza per la clientela con particolare riferimento alle operazioni di pagamento elettronico. Questo

competitivo. Fintech, il paradigma Open banking e la minaccia delle big tech companies, Fascicolo 3, dicembre 2018, pp. 441-465.

[33] In tal senso F. CIRAOLO, *Open Banking, Open Problems*, in *Riv. Dir. Banc.*, n. 4/2020.

[34] F. PANETTA, *L'innovazione digitale nell'industria finanziaria italiana*, Milano, 26 settembre 2017, reperibile su www.bancaditalia.it

[35] Di cui si dirà in maniera più approfondita nel secondo capitolo del presente elaborato.

aggiornamento normativo è stato considerato indispensabile per il rafforzamento della tutela in favore dei clienti che utilizzano modalità di pagamento elettronico al fine di ridurre il rischio di abusi o frodi informatiche[36]; queste norme richiedono l'adozione di strumenti per la tutela della riservatezza e l'integrità delle

[36] Sulla materia, cfr. Camera dei Deputati, VI Commissione (Finanze), Indagine conoscitiva sulle tematiche relative all'impatto della tecnologia finanziaria sul settore finanziario, creditizio e assicurativo, Audizione del Vice Direttore Generale della Banca d'Italia Fabio Panetta (Roma, 29 novembre 2017), pp. 7 e 8; si vedano anche i mandati PSD2 conferiti all'EBA in tema di sicurezza e frodi: *RTS on strong customer authentication and secure communication* (art. 98, PSD2 – Commission Delegated Regulation (EU) 2018/389), pubblicati a marzo 2018 (applicazione 14 settembre 2019); *Guidelines on fraud data reporting* (art. 96), pubblicate a luglio 2018; *Guidelines on major incident reporting* (art. 96), pubblicate a luglio 2017; *Guidelines on operational and security risk management* (art. 95), pubblicate a dicembre 2017.

credenziali degli utenti, limitando in tal modo fenomeni quali *phishing*[37], *vishing*[38], *smishing*[39], *spoofing*[40], e altre ancora.[41]

È stato evidenziato, purtroppo, che tali frodi spesso non possono essere efficacemente contrastate dalla *SCA* perché la maggior parte di queste si verificano prima della sua applicazione ed è proprio lo stesso pagatore che in buona fede autorizza l'operazione di pagamento attraverso la *SCA*[42].

---

[37] Il *phishing* è una tipologia di frode ormai diffusa effettuata tramite un'e-mail con logo contraffatto di un istituto di credito o di una qualsiasi attività commerciale, in cui il pagatore viene invitato a inserire, in appositi campi, i propri dati riservati, motivando tale richiesta con ragioni di ordine tecnico.

[38] Il termine *vishing* deriva dall'unione fra due parole: "*voice*" e "*phishing*". Un attacco di *vishing* è simile al *phishing*, ma avviene per telefono o tramite messaggio vocale.

[39] Lo *smishing* è una forma di phishing che utilizza i telefoni cellulari come piattaforma di attacco, SMS (da cui il nome "*SMiShing*") con l'intento di raccogliere informazioni personali, compresi il codice fiscale e/o il numero di carta di credito e/o i codici statici e dinamici dell'home banking delle potenziali vittime. Il contenuto dei messaggi consiste nell'attirare l'attenzione della vittima su operazione sospette o anomalie nel processo di aggiornamento relativo alla sicurezza dei dati personali, invitandola a cliccare su un collegamento ipertestuale, al fine di intervenire sulle presunte anomalie. La vittima, attraverso il reindirizzamento a pagine *web* che copiano graficamente quelle della propria banca, è tratta in inganno e indotta a inserire le proprie credenziali (statiche e dinamiche).

[40] Lo *spoofing* si verifica quando i frodatori riescono a camuffare la provenienza della e-mail o dell'sms "civetta", facendolo comparire all'interno del *thread* dei messaggi, autentici e legittimi, intercorsi con il proprio intermediario. Generalmente, tali messaggi contengono un collegamento ipertestuale che rinvia a pagine di phishing dove l'utente viene indotto ad inserire le proprie credenziali.

[41] Si v. S. BALSAMO TAGNANI, *Il mercato europeo dei servizi di pagamento si rinnova con la PSD2*, in *Contr. Impr. Eur.*, 2018 p. 609-624.

[42] Ad esempio, è questo il caso in cui l'utente ricevendo una e-mail, da un malintenzionato che si finge la banca, viene informato di un problema inerente al suo conto, viene reindirizzato ad un falso sito della banca che corrisponde esattamente a

Si deve anche sottolineare la scarsa consapevolezza degli utenti riguardo alle principali tipologie di frodi e l'importanza di una educazione del cliente in merito a queste e ai rischi ad esse associati.[43] Infatti anche il tema della responsabilità è stato centrale nelle novità introdotte dalla *PSD2*: all'art. 69 si riconosce in capo all'utente di servizi di pagamento la sussistenza dell'obbligo di tutelare le credenziali personalizzate fornite dal prestatore di servizi di pagamento utilizzate per l'accesso *on-line* ai propri conti.

La *PSD2* inoltre estende le regole di trasparenza e corretta informativa anche alle transazioni cd. "one leg", ossia quando solo uno dei due prestatori di servizi di pagamento si trova nel territorio dell'UE.

Il 13 gennaio del 2018[44] è stato pubblicato il Decreto Legislativo n. 218 del 2017, il quale recepisce la *PSD2* apportando considerevoli modifiche e integrazioni ad atti normativi vigenti, in particolare:

a) al Titolo VI del t.u.b. in materia di «trasparenza delle condizioni contrattuali e dei rapporti con i clienti» e segnatamente al Capo II bis, specificamente dedicato ai servizi di pagamento;

---

quello originale e dopo aver inserito le proprie credenziali compie anche l'autenticazione forte, approvando totalmente l'operazione che però si rivelerà ben presto fraudolenta.

[43] F. CASCINELLI e L. BETTINELLI, *Verso la PSD3 e il nuovo Regolamento sui Servizi di Pagamento, op. cit.*

[44] In forza dell'art. 115, par. 1 e 2, PSD2, tutti gli Stati membri avrebbero dovuto adottare, pubblicare ed applicare le misure necessarie per la trasposizione della direttiva nei rispettivi ordinamenti nazionali entro e non oltre il 13 gennaio 2018. Pertanto, al fine di rispettare tale prescrizione temporale, il Decreto è entrato in vigore il giorno stesso della sua pubblicazione in Gazzetta Ufficiale, senza alcun periodo di *vacatio legis*.

b) al d.lgs 27 gennaio 2010, n. 11[45].

Va sottolineato che il legislatore nazionale in sede di attuazione della *PSD2*, ha voluto mantenere separati i due blocchi normativi che insieme concorrono a disciplinare la prestazione di servizi di pagamento. Insieme, TUB e d.lgs. 11/2010, diciplinano congiuntamente i servizi di pagamento. Il TUB si occupa di individuare gli intermediari autorizzati a fornire servizi di pagamento, regola l'accesso al mercato, definisce le tipologie di servizi di pagamento, stabilisce gli obblighi di trasparenza e corretta informazione per gli utenti dei servizi di pagamento. Il d.lgs. 11/2010, invece, si occupa della definizione degli obblighi del prestatore di servizi di pagamento, della diligenza dell'utente e dei profili di colpa del pagatore, con particolare riferimento all'operazione di pagamento, le sue tempistiche, la sicurezza e l'autenticazione forte.

2.2 Definizione di servizi di pagamento

Per una migliore disamina del fenomeno sembra doveroso precisare la definizione di "servizi di pagamento". Si ricorda nuovamente che con tale espressione si intendono «tutti quei servizi prestati da un intermediario che consentono un trasferimento di denaro da un soggetto (c.d. pagatore) ad un altro (c.d. beneficiario) senza che il primo debba

[45] Nonchè al d.lgs. 18 agosto 2015, n. 135 contenente la disciplina sanzionatoria per le violazioni delle disposizioni contenute nel reg. CE 2009/924 contenenti norme sui pagamenti transfrontalieri nelle allora Comunità europee e sui requisiti tecnici e nel reg. UE 2012/260 recante le norme commerciali dei bonifici e degli addebiti diretti in euro.

materialmente consegnare al secondo monete, banconote o titoli di credito come assegni o cambiali».[46]

L'Allegato I della *PSD2* fa una elencazione di quelli che sono nello specifico i servizi di pagamento[47]:

«1. Servizi che permettono di depositare il contante su un conto di pagamento nonché tutte le operazioni richieste per la gestione di un conto di pagamento.

2. Servizi che permettono prelievi in contante da un conto di pagamento nonché tutte le operazioni richieste per la gestione di un conto di pagamento.

3. Esecuzione di operazioni di pagamento, incluso il trasferimento di fondi, su un conto di pagamento presso il prestatore di servizi di pagamento dell'utente o presso un altro prestatore di servizi di pagamento:

a) esecuzione di addebiti diretti, inclusi addebiti diretti una tantum;

b) esecuzione di operazioni di pagamento mediante carte di pagamento o analogo dispositivo;

c) esecuzione di bonifici, inclusi ordini permanenti.

4. Esecuzione di operazioni di pagamento quando i fondi rientrano in una linea di credito accordata ad un utente di servizi di pagamento:

---

[46] Così E. CECCHINATO, *I servizi di pagamento*, in *Il diritto bancario oggi: aspetti sostanziali processuali*, F. Aratari e Guido Romano (a cura di), Wolters Kluwer, 2023, p. 365 e ss.

[47] Sembra opportuno, ad opinione di chi scrive, dare la definizione di servizi di pagamento partendo dalla *PSD2* per poi fare un confronto con quella che viene data dalla *PSD3*, senza partire dalla già obsoleta definizione che veniva data dalla prima *PSD*.

a) esecuzione di addebiti diretti, inclusi addebiti diretti una tantum;
b) esecuzione di operazioni di pagamento mediante carte di pagamento o analogo dispositivo;
c) esecuzione di bonifici, inclusi ordini permanenti.

5. Emissione di strumenti di pagamento e/o convenzionamento di operazioni di pagamento.

6. Rimessa di denaro.

7. Servizi di disposizione di ordine di pagamento.

8. Servizi di informazione sui conti».

Possiamo notare come il legislatore effettua un puntuale elenco delle attività e dei singoli servizi ricompresi in questa categoria, non riuscendo a dare una definizione generale che possa adeguarsi alle nuove esigenze che possono essere dettate dall'innovazione tecnologica. Questo, ad avviso di chi scrive, risulta un limite per la materia che necessiterà di costanti aggiornamenti da parte del legislatore.

Tale categoria di servizi e la sua definizione riveste un ruolo centrale nel settore finanziario vista la crescente frequenza con cui i consumatori ricorrono ai servizi di pagamento piuttosto che all'uso di denaro contante.

Il progressivo ricorrere a servizi di pagamento alternativi al denaro contante è stato alimentato anche dalla pandemia Covid-19 che ha comportato una diminuzione dell'uso di banconote e monete per limitare la diffusione di certi tipi di malattie, inoltre la pandemia ha anche stimolato l'e-commerce, che per forza di cose non prevede l'uso del contante e ha

dimostrato l'importanza di disporre di un'infrastruttura di pagamento digitale sicura ed efficiente[48].

L'impatto dei timori di contagio sui comportamenti di famiglie e imprese ha toccato infatti anche il loro modo di effettuare i pagamenti e i risultati mostrano che l'emergenza sanitaria e le misure governative per contenere la diffusione della pandemia hanno indotto una maggiore preferenza per le carte di pagamento rispetto all'uso del contante al punto vendita fisico e, in generale, un più intenso utilizzo degli strumenti di pagamento elettronici rispetto a quelli tradizionali. Invero, bisogna riconoscere che gli effetti della pandemia sui pagamenti al dettaglio si innestano nell'ambito di tendenze che erano già in atto da tempo, e questa ne ha solamente accelerato gli sviluppi.[49]

I servizi di pagamento all'interno della direttiva non sono solo individuati in maniera positiva ma anche negativamente (cd. *negative scope*).

L'art. 3 della *PSD2* individua infatti 15 ipotesi di servizi ed operazioni di pagamento che sono escluse dall'ambito di applicazione della direttiva (elenco che, invece, sembra mancare nella nuova proposta di *PSD3*[50]); tale elencazione è parsa fondamentale visto il dibattito[51] che aveva investito la precedente

[48] E. CECCHINATO, *I servizi di pagamento in Il diritto bancario oggi: aspetti sostanziali processuali*, F. Aratari e Guido Romano (a cura di), Wolters Kluwer, 2023, p. 365 e ss.

[49] Per approfondimenti si v. G. ARDIZZI, A. GAMBINI, A. NOBILI, E. PIMPINI, G. ROCCO, *L'impatto della pandemia sull'uso degli strumenti di pagamento in Italia* in *Mercati, Infrastrutture, sistemi di pagamento*, n. 8, Luglio 2021.

[50] Proposta di direttiva 2023/0209/COD.

[51] Era emerso infatti, con riguardo al «*negative scope*», la necessità di un intervento di armonizzazione della materia, in quanto nei vari paesi membri si erano

direttiva (intendendo la *PSD*) riguardante il regime di applicazione o esenzione della stessa.

L'esclusione trova applicazione innanzitutto nei confronti di alcune operazioni di pagamento basate su determinate tipologie di documenti, con i quali viene ordinato al prestatore di servizi di pagamento di mettere dei fondi a disposizione del beneficiario; si fa qui riferimento più specificamente ad assegni bancari, titoli bancari, *etc.* [52]

Diversamente dalla precedente *PSD*, inoltre, rientrano all'interno della categoria del *negative scope* anche tutte quelle operazioni di pagamento effettuate tramite un agente commerciale il quale agisca soltanto per conto del solo pagatore o del solo beneficiario, indipendentemente dal fatto che l'agente sia o meno in possesso dei fondi dei clienti.[53] Nel caso in cui l'agente commerciale intervenga in una operazione di pagamento nell'interesse di entrambe le parti, allora si rientrerebbe nell'ambito di applicazione della disciplina solo nel momento in cui lo stesso non fosse mai entrato in possesso dei fondi dei clienti.[54]

Sono ricompresi nell'ambito d'esclusione anche i servizi di prelievo di contante erogati da prestatori tramite ATM indipendenti per conto di uno o più emittenti della carta che non siano parti del contratto quadro con il cliente che preleva denaro da un conto di pagamento[55].

---

create discordanti esenzioni con riguardo la normativa sui servizi di pagamento, determinando interpretazioni divergenti con relativi danni alla concorrenza.

[52] Cosi come indicato dall'art. 3, comma 1, lett. g), della Direttiva 2015/2366/UE.

[53] Si veda art. 3, comma 1, lett. b), della Direttiva 2015/2366/UE.

[54] S. BALSAMO TAGNANI, *Il mercato europeo dei servizi di pagamento si rinnova con la PSD2*, in Contr. Impr. Eur., 2018 pp. 609-624.

[55] Sul punto art. 3, comma 1, lett. o), della Direttiva 2015/2366/UE.

Alla luce delle continue innovazioni tecnologiche anche in campo finanziario sembra essere inevitabile che la definizione di servizi di pagamento sia in costante aggiornamento (prima con la *PSD*, poi modificata dalla *PSD2* e ora con la proposta di *PSD3*). Oggigiorno è possibile, infatti, compiere pagamenti con computer, smartphone e persino orologi digitali (*smartwatch*); il web è il punto centrale dei servizi di pagamento tanto che si cominciano ad esplorare dimensioni sempre più futuristiche come ad esempio il "metaverso", nel quale chiaramente non circolano fisicamente banconote e monete. Inoltre, è diffusa la possibilità di effettuare pagamenti tramite portafoglio eletronico (*e-wallet*), una soluzione che permette ai propri utenti di registrare in un portafoglio virtuale i propri strumenti di pagamento per poi utilizzarli quando si effettua una transazione; tra i portafogli elettronici più diffusi troviamo quelli proposti ad esempio da *Apple Pay*, *Google Pay*, etc.[56] Ed infatti, ad oggi si parla anche di "prestatori di servizi di pagamento" e non più solo di banche in quanto queste ultime non detengono più il monopolio nella prestazione dei servizi di pagamento.

Come si è potuto notare dalla disamina della definizione di servizi di pagamento, il legislatore non ne dà una definizione onnicomprensiva, ne fa invece una puntuale elencazione e successivamente il TUB poi, a livello interno, recepisce quasi alla lettera la lista contenuta nell'allegato I della *PSD2*, con la differenza che con riguardo ai servizi di pagamento non viene

[56] Sul punto, A. ARGENTATI, *Le banche nel nuovo scenario competitivo. Fintech, il paradigma Open Banking e la minaccia delle Big tech companies*, in *Mercato Concorrenza Regole*, 3/2018, pp. 441-466 e S. BALSAMO TAGNANI, *op. cit.*

menzionata la natura commerciale dei servizi. L'intento del legislatore sembrerebbe essere quello di creare una maggiore certezza del diritto elencando puntualmente ogni attività e servizio appartenente alla categoria dei servizi di pagamento in una lista tassativa.[57] Questo, come già si è detto, porta la Commissione europea a un continuo aggiornamento attraverso nuove proposte di direttiva riguardante l'elencazione, visto l'esponenziale progresso tecnologico in atto. D'altro canto, è vero che non è prevedibile fino a dove possa arrivare il progresso ed è quindi bene valutare, con le dovute attenzioni, l'inserimento o meno di determinati nuovi servizi di pagamento all'interno della disciplina di cui si discute.

Il Consiglio Europeo consapevole di ciò, pochi anni dopo la *PSD2* ha emanato nel 2020 una comunicazione in materia di pagamenti al dettaglio che auspicava la proposta di *PSD3*[58]. L'innovazione e la digitalizzazione continueranno a modificare le modalità di funzionamento dei pagamenti. I prestatori di servizi abbandoneranno sempre più i vecchi canali e gli strumenti di pagamento tradizionali e svilupperanno modalità nuove di disporre gli ordini di pagamento[59].

Secondo la Commissione il mercato dei servizi di pagamento al dettaglio ha registrato importanti cambiamenti, principalmente legati a un maggiore utilizzo di carte e altri strumenti di pagamento digitali, a una diminuzione dell'utilizzo del contante e alla presenza crescente di operatori e servizi nuovi, tra cui i portafogli digitali e i pagamenti senza

---

[57] E. CECCHINATO, *I servizi di pagamento in Il diritto bancario oggi: aspetti sostanziali processuali*, F. Aratari e Guido Romano (a cura di), Wolters Kluwer, 2023, p. 365 e ss.

[58] Proposta di direttiva 2023/0209/COD.

[59] Così la *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*, Bruxelles, 24.9.2020 reperibile al sito www.publications.europa.eu

contatto, il contributo della pandemia e conseguenti trasformazioni nei consumi e nella prassi di pagamento hanno accresciuto l'importanza di disporre di pagamenti digitali sicuri ed efficienti come evidenziato sopra.[60]

2.3 La definizione di servizio di pagamento secondo la PSD3[61] e altre questioni definitorie

Ad oggi con la proposta di *PSD3*[62] l'elenco dei servizi di pagamento – sembra – sarà modificato come segue:

«1. Servizi che permettono di depositare il contante su un conto di pagamento e/o di prelevare contante da un conto di pagamento.

2. Esecuzione di operazioni di pagamento, incluso il trasferimento di fondi da o su un conto di pagamento, anche quando i fondi rientrano in una linea di credito presso il prestatore di servizi di pagamento dell'utente o presso un altro prestatore di servizi di pagamento.

3. Emissione di strumenti di pagamento.

4. Convenzionamento di operazioni di pagamento.

5. Rimessa di denaro.

6. Servizi di disposizione di ordine di pagamento.

---

[60] Relazione della commissione europea alla proposta di Direttiva del Parlamento europeo e del Consiglio relativa 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.

[61] Proposta di direttiva 2023/0209/COD.

[62] Proposta di direttiva 2023/0209/COD.

7. Servizi di informazione sui conti»[63].

Come si può notare, rispetto alla elencazione precedente è sembrato più opportuno dissociare il servizio che permette prelievi di contante da un conto di pagamento dall'attività di prestazione di servizi di pagamento di radicamento del conto.

Si sono poi unificate tutte le esecuzioni di operazioni di pagamento di cui ai punti 2, 3 e 4 della precedente direttiva ritenendo superflua la distinzione tra di esse. Al punto 5 si è deciso che i servizi di emissione di strumenti di pagamento e di convenzionamento di operazioni di pagamento dovessero essere presentati come due diversi servizi di pagamento e non come se uno non potesse essere offerto senza l'altro.[64]

Anche la definizione di "strumento di pagamento" subirebbe una modifica con la *PSD3:* questa si è resa necessaria all'emergere di nuovi tipi di strumenti di pagamento e alla diffusa incertezza del mercato riguardo la qualificazione giuridica di tali strumenti.[65] Per tali ragioni si è reso necessario migliorare la definizione specificando cosa costituisca o non costituisca uno strumento di pagamento, tenendo presente il principio di neutralità tecnologica[66].

---

[63] Proposta di direttiva 2023/0209/UE - allegato I "servizi di pagamento" art. 2, punto 3.

[64] Considerando 7 della valutazione della Commissione Europa della proposta di direttiva 2023/0209/UE.

[65] Considerando 10 della valutazione della Commissione Europea della proposta di direttiva 2023/0209/UE.

[66] Per neutralità tecnologica si intende la libertà delle persone e delle organizzazioni di scegliere la tecnologia più adeguata ai loro bisogni, per questo motivo i prodotti, servizi o quadri normativi che tengono conto del principio della neutralità tecnologica non impongono né introducono discriminazioni a favore dell'impiego di un tipo particolare di tecnologia. Si tratta

Con la proposta di direttiva *PSD3* la definizione di "strumento di pagamento"[67] fa riferimento a dispositivi "individualizzati" anziché "personalizzati" specificando che le carte prepagate su cui non è stampato il nome del titolare dello strumento sono anch'esse strumenti di pagamento, in quanto prima non sembravano essere ricomprese perché senza nominativo stampato[68].

Anche l'emissione di moneta elettronica va considerata servizio di pagamento. Sono autorizzati ad emetterla, oltre alle banche, gli Istituti di Moneta Elettronica (*IMEL*[69]), che sono persone giuridiche, diverse

---

di un altro principio cardine già presente nella *PSD2* (e anche nel 10° considerando della *PSD3*), richiamato con sempre maggiore insistenza dal legislatore europeo. Già il 21° considerando della *PSD2* richiedeva ai legislatori nazionali, al fine di rispettare tale principio, che per tutelare ed incentivare l'innovazione, non si definiscano con rigidità le modalità tecnologiche con cui i singoli servizi di pagamento devono essere erogati, in tal modo rimanendo neutri sotto il profilo tecnologico.

[67] Secondo la *PSD2* uno «strumento di pagamento» è «un dispositivo personalizzato e/o insieme di procedure concordate tra l'utente di servizi di pagamento e il prestatore di servizi di pagamento e utilizzate per disporre un ordine di pagamento».

[68] Considerando 12 della valutazione della Commissione Europea della proposta di direttiva 2023/0209/UE

[69] Secondo BANCA D'ITALIA, *Disposizioni di vigilanza per gli istituti di pagamento e gli istituti di moneta elettronica*: «Gli IMEL, oltre ad emettere moneta elettronica, possono: a) prestare servizi operativi strettamente connessi con l'emissione di moneta elettronica; b) prestare servizi di pagamento previsti dal TUB, anche non connessi con l'emissione di moneta elettronica, nonché le relative attività accessorie; c) concedere finanziamenti relativi ai servizi di pagamento entro i limiti indicati nelle disposizioni di vigilanza applicabili; esercitare altre attività d'impresa non connesse alla prestazione dei servizi di pagamento o all'emissione di moneta elettronica; d) in questo caso la legge prevede che i servizi di pagamento e l'emissione di moneta elettronica siano svolti attraverso un patrimonio destinato che l'intermediario deve costruire.

dalle banche, autorizzate in Italia a emettere moneta elettronica, conformemente a quanto previsto dall'art. 114-quinquies del TUB.[70]

Con emissione di moneta elettronica si intende il compimento di tutte quelle operazioni attraverso le quali l'emittente riceve da parte del richiedente una somma di denaro, procede a memorizzare nel dispositivo elettronico del richiedente una disponibilità monetaria di entità non superiore alla somma previamente ricevuta e mette il titolare del dispositivo in condizioni di disporre della moneta elettronica in esso caricata.[71]

L'emissione di moneta elettronica, come si diceva sopra, è riservata a banche e *IMEL*. Tra i servizi di pagamento elettronici che costituiscono moneta elettronica o *e-money* non rientrano bancomat e carte di credito; al contrario di queste, infatti, la moneta elettronica può essere incorporata in un dispositivo materiale o in un supporto meramente virtuale. La definizione di moneta elettronica si riferisce sia a «moneta elettronica detenuta su un dispositivo di pagamento in possesso del detentore di moneta elettronica stessa, sia a moneta elettronica memorizzata a distanza su un server e gestita dal detentore tramite un conto specifico per la moneta elettronica».[72] Secondo l'articolo 114-

---

[70] In tal senso l'art. 114-quinquies1 TUB: «1. Gli istituti di moneta elettronica registrano per ciascun cliente in poste del passivo, nel rispetto delle modalità stabilite dalla Banca d'Italia, le somme di denaro ricevute dalla clientela per l'emissione di moneta elettronica (…)».

[71] I. D'AMBROSIO, *La tutela del consumatore nei pagamenti elettronici e la nuova direttiva europea PSD2, Riv.Le nuove Leggi*, NLCC 6/2019.

[72] Art. 2, n. 2 direttiva 2009/110/CE, recepito dall'ordinamento italiano con l'art. 1 TUB.

quater del TUB «Gli istituti di moneta elettronica trasformano immediatamente in moneta elettronica i fondi ricevuti dal richiedente».[73]

2.4. La controversa questione delle criptovalute

Va rilevato come alcuni concetti sottesi alle definizioni finora richiamate risultino ambigui al punto da chiedersi se nel loro perimetro rientrino anche operazioni in cripto-attività, e in criptovalute in particolare.

Le cripto-attività sono "rappresentazioni digitali basate sul distributed ledger technology (*DLT*)"[74] e sono beni oggetto di un diritto che attribuisce a chi ne ha la disponibilità giuridica di utilizzarle come: mezzo di scambio, strumento di investimento nella prospettiva che il valore si incrementi, diritto che permette di disporre di un asset virtuale o reale (*NFT*[75]) o di godere o fruire

[73] Così dispone l'art. 114-quater del TUB: «1. La Banca d'Italia iscrive in un apposito albo gli istituti di moneta elettronica autorizzati in Italia; sono altresì iscritte le succursali di istituti di moneta elettronica italiani stabilite in uno Stato comunitario diverso dall'Italia. 1-bis. La Banca d'Italia comunica senza indugio all'ABE le informazioni iscritte nell'albo e ogni relativa modifica, nonché, in caso di revoca dell'autorizzazione o dell'esenzione concessa ai sensi dell'articolo 114 quinquies 4, le ragioni che la hanno determinata. 2. Gli istituti di moneta elettronica trasformano immediatamente in moneta elettronica i fondi ricevuti dal richiedente. 3. Gli istituti di moneta elettronica possono: a) prestare servizi di pagamento e le relative attività accessorie ai sensi dell'articolo 114-octies senza necessità di apposita autorizzazione ai sensi dell'articolo 114-novies; b) prestare servizi operativi e accessori strettamente connessi all'emissione di moneta elettronica».

[74] Così M. PIERRO, *L'origine europea della nozione di cripto-attività e la scelta del legislatore nazionale* in *Corriere Tributario*, n. 4, 2024, pp. 382-387.

[75] Acronimo di *non-fungible token*. Si intendono dei certificati digitali basati sulla tecnologia blockchain, che rappresentano l'atto di proprietà e il certificato di autenticità di un bene unico.

di un bene o di un servizio virtuale o reale (*utility token*). Dapprima queste hanno trovato espressione nelle criptovalute, il Bitcoin nel 2009 è stata la prima cripto-valuta ad essere messa in circolazione, e poi in una vasta varietà di altri asset crittografati. Nella categoria delle cripto-attività si ricomprendono tutte le valute virtuali e tutti i token digitali.

La circolazione delle criptovalute è attualmente troppo ridotta perché si possa parlare di equivalenza con la moneta legale e ciò è dovuto sia all'assenza di un apparato normativo che possa regolarne la funzione di mezzo di adempimento di obbligazioni pecuniarie, sia all'assenza di una base consensuale sufficientemente ampia da favorirne la diffusione capillare, tale che, anche in assenza di una regolamentazione specifica[76], possa parificare la criptovaluta ad una moneta legale.[77]

[76] Si noti però che l'Unione Europea, in particolare la BCE, a partire dal 2020 ha pubblicato il "Report on a digital euro" riguardante la possibile emissione di una valuta digitale di banca centrale, una moneta virtuale utilizzabile da famiglie e imprese per effettuare o ricevere pagamenti al dettaglio ovunque nell'area dell'euro. L'euro digitale sarebbe quindi una valuta virtuale emessa dalla BCE che avrebbe un valore garantiro dallo Stato, ha lo stesso valore di una moneta fisica e si distingue da questa principalmente per la forma. L'euro digitale differisce dalle criptovalute, anch'esse monete virtuali in quanto il primo è emesso da un soggetto unico e ben identificato (BCE) mentre le seconde sono create attraverso procedure informatiche e non sono assistite da garanzie che ne assicurino in valore. La proposta di euro digitale fa parte del pacchetto di misure legislative (il c.d. *Single Currency Package*) che la Commissione europea ha presentato il 28 giugno 2023. Si veda per ulteriori approfondimenti sul tema F. PANETTA, *Plasmare il futuro digitale dell'Europa: il percorso verso un euro digitale*, Bruxelles, 2023; in tal senso si veda anche G. MARCHIANÓ, *Brevi riflessioni sulla proposta di creare l'euro digitale*, in Amm. E Cont., 2021.

[77] LEMME-PELUSO, *Criptomoneta e distacco dalla moneta legale: il caso bitcoin*, in *Riv. Dir. Banc.*, 2016, n. 4, sezione 1, p. 381 ss.

Alla luce di queste problematiche pare quindi difficile assoggettare il fenomeno delle operazioni in cripto-attività alla disciplina dei servizi di pagamento.

Al di là di ciò se si guarda all'elenco dei "servizi di pagamento", non si trova nessun esplicito riferimento alla criptovaluta, questa non rientra in alcuna delle categorie elencate e neppure in quella della moneta elettronica dal momento che quest'ultima rappresenta un credito pecuniario nei confronti dell'emittente.[78]

Ad oggi il mercato delle cripto-attività sembra aver fatto dei passi in avanti per quanto riguarda la sua regolamentazione: è ora normato dal Regolamento (UE) 2023/114 (Regolamento MiCa o MiCAR[79]) [80] del Parlamento Europeo e del Consiglio, che recita in apertura come sia «importante garantire che gli atti legislativi dell'Unione in materia di servizi finanziari siano adeguati all'era digitale e contribuiscano a creare una economia pronta per le sfide del futuro e al servizio delle persone, anche consentendo l'uso di tecnologie innovative. […]».[81] Come viene

[78] E. CECCHINATO, *I servizi di pagamento in Il diritto bancario oggi: aspetti sostanziali processuali*, F. Aratari e Guido Romano (a cura di), Wolters Kluwer, 2023, p. 365 e ss.

[79] Acronimo di Markets in Crypto-Assets.

[80] In merito alle norme contenute nel MiCA, cfr. N. CIOCCA, *Servizi di custodia, negoziazione e regolamento di cripto-attività*, in Oss. dir. civ. comm., 2022, p. 79 ss.; M.-T. PARACAMPO, *I prestatori di servizi per le cripto-attività. Tra mifidizzazione della MICA e tokenizzazione della Mifid*, Torino 2023, p. 27 ss.; A. PANTALEO, *I Prestatori di servizi su cripto-attività*, in S. CAPACCIOLI - M.T. GIORDANO (a cura di), Crypto-asset: Regolamento MiCA e DLT Pilot Regime. Analisi ragionata su token, stablecoin, CASP, Milano 2023, p. 193 ss. Per un inquadramento dell'attività degli exchanges da un punto di vista civilistico, v. anche A. CALONI, *Deposito di cripto attività presso una piattaforma exchange: disciplina e attività riservate*, in G. comm., 2020, p. 1073 ss.

[81] Considerano 1 del Regolamento (UE) 2023/114 del Parlamento Europeo e del Consiglio.

evidenziato, l'assenza di un quadro generale dell'Unione per i mercati delle cripto-attività potrebbe portare gli utenti a non avere fiducia in tali attività e si è reso pertanto necessario un quadro specifico e armonizzato per tali mercati. Con il regolamento MiCA[82] verranno superate per la prima volta le differenze dei singoli Paesi membri in materia di regolamentazione dell'organizzazione e della definizione dei dati informativi necessari ad accompagnare trasferimenti di cripto-attività. Sono stati individuati inoltre requisiti uniformi per la loro offerta al pubblico e l'ammissione alla negoziazione.[83]

Si tratta di un significativo intervento normativo che ha l'ambizione di porsi come un modello di disciplina a livello mondiale. [84]

La nozione di cripto attività è frutto di un complesso processo legislativo europeo che ha l'obiettivo di regolarne in maniera uniforme i mercati. La definizione si trova all'art. 3, comma 1, n. 5 il quale recita che le cripto attività sono generalmente definite come «rappresentazioni digitali di valori o di diritti che possono essere trasferite e memorizzate elettronicamente, utilizzando la tecnologia del registro distribuito o tecnologia analoga».[85]

[82] Regolamento (UE) 2023/114.

[83] I. AVEGNO, *Regolamentazione delle cripto-attività: lo scenario comunitario*, *Riv. Amministrazione & Finanza*, n. 1/2024, pp. 15-21.

[84] Così F. P. PATTI, *L'offerta al pubblico di cripto attività nel titolo II del regolamento MICA*, *Riv. Di diritto civile*, 1/2024, pp. 98.

[85] Per altre definizioni fondamentali ai sensi del regolamento si rimanda all'art. 3, comma 1 del regolamento MiCA.

Successivamente le cripto vengono definite in negativo e per differenza, nel senso che sono escluse dal perimetro di applicazione della disciplina MiCA. Nello specifico non si applica tale regolamento alle cripto-attività che sono uniche e non fungibili con altre cripto-attività che siano definibili come: strumenti finanziari, depositi, compresi i depositi strutturati; fondi, eccetto ove siano qualificabili come token di moneta elettronica; posizioni inerenti a cartolarizzazione, prodotti assicurativi non vita o vita che rientrano nelle classi di assicurazione contratti di riassicurazione e retrocessione; i prodotti pensionistici e gli schemi pensionistici aziendali o professionali riconosciuti ufficialmente. [86]

Tale regolamento stabilisce i requisiti uniformi per l'offerta al pubblico e l'ammissione alla negoziazione di cripto-attività e i requisiti per i prestatori dei relativi servizi e si applica alle persone fisiche e giuridiche e ad alcune imprese coinvolte nell'emissione, nell'offerta al pubblico e nell'ammissione alla negoziazione di cripto-attività o che prestano servizi connessi alle cripto-attività nell'unione. [87]

Il regolamento MiCA e la direttiva *PSD2*, pur avendo ambiti distinti di applicazione, possono intersecarsi in diversi punti, come ad esempio l'innovazione finanziaria e concorrenza,

[86] Per tutte le esclusioni si veda art. 2, comma 2 del regolamento MiCA

[87] I. AVEGNO, *Regolamentazione delle cripto-attività: lo scenario comunitario*, *op. cit.* Per un approfondimento si rinvia a M. PIERRO*, Contributo all'individuazione della nozione di crypto-asset e suoi riflessi nell'ordinamento tributario nazionale,* in *Rass. trib.*, n. 3/2022 pag. 574., si veda anche M. PIERRO, *L'origine europea della nozione di cripto-attività e la scelta del legislatore nazionale*, in *Corr. Tributario* 4/2024, p. 382 e ss; sul tema anche M. DEOTTO, *Per le cripto-attività una disciplina criptica e anche un po' critica*, in *il fisco*, n. 45/2023, pp. 4267.

la regolamentazione dei servizi di pagamento e delle criptovalute e la sicurezza e protezione dei consumatori.[88]

Per quanto attiene ad esempio alla innovazione e concorrenza, la *PSD2* promuove l'innovazione aprendo il mercato dei servizi di pagamento a nuovi attori tramite l'*open banking*, che consente alle terze parti di accedere ai dati bancari dei clienti con il loro consenso, questa apertura potrebbe facilitare l'integrazione di servizi legati alle criptovalute, regolamentati dal MiCA[89], nei servizi di pagamento tradizionali; il MiCA invece, sempre per quanto attiene l'innovazione e concorrenza, potrebbe influenzare i fornitori di servizi di pagamento che intendono incorporare le criptovalute nelle loro offerte, richiedendo loro di rispettare norme specifiche sugli asset digitali.

Assieme, *PSD2* e MiCA, contribuiscono a creare un quadro normativo europeo complementare che promuove l'innovazione, la sicurezza e la protezione dei consumatori. La loro integrazione potrà sicuramente essere d'aiuto a garantire che i nuovi servizi di pagamento che coinvolgono criptovalute possano operare in un ambiente che sia sicuro e regolamentato, favorendo la crescita del mercato fintech dell'UE.[90]

---

[88] P. CARRIERE, *Decreto Fintech e MICAR: il quadro normativo sulle cripto-attività*, dal sito www.dirittobancario.it, si v. anche per ulteriori approfondimenti P. CARRIERE, *Il fenomento delle cripto-attività in una prospettiva societaria*, in *Banca Imprese e Società*, 3/2020.

[89] Regolamento (UE) 2023/114

[90] T. N. POLI, *MiCA, Pilot Regime e Decreto Fintech: la regolazione del fenomeno crypto e le difficoltà di inquadramento nel sistema finanziario*, in *Dir. Bancario*, Dicembre 2023.

Le criptoattività – intese in senso ampio – non sono le uniche ad essere soggette al nuovo Regolamento MiCA, ed infatti questo ne disciplina anche alcune sottospecie:

- *utiliy token*, definiti dall'art. 3 comma 1 n. 9 come «un tipo di cripto-attività destinato unicamente a fornire l'accesso a un bene o a un servizi prestato dal suo emittente»;

- *token* di moneta elettronica (o *e-money token*), ossia quel «tipo di cripto-attività che mira a mantenere un valore stabile facendo riferimento al valore di una valuta ufficiale» (art. 3 comma 1 n. 7);

- *asset-referenced token*, ossia cripto-*asset* che non sono EMT finalizzati a mantenere un valore stabile facendo riferimento a un altro valore o diritto o una combinazione di essi, comprese una o più valute ufficiali (art. 3 comma 1 n. 6).

In particolare, sugli *e-moeny token* è da evidenziare che a differenza delle cripto-valute tradizionali, queste mantengono un valore stabile e svolgono una funzione analoga a quella della moneta elettronica fungendo da surrogati eletronici di monete e banconote. La differenza con la moneta elettronica è che il *token di moneta elettronica* è una rappresentazione digitale di un valore che può essere scambiato o utilizzato in un sistema decentralizzato e vengono emessi con una supervisione normativa molto stringente che gli impone, per la loro emissione, l'ottenimento di una specifica licenza (tale normativa è così rigorosa al fine di garantire una certa stabilità, sicurezza e trasparenza). Inoltre, l'entità che li emette deve essere autorizzata e possono essere sviluppatori privati o piattaforme *blockchain*, e i token stessi possono avere diversi scopi oltre al pagamento. Tali emittenti devono garantire che i *token* siano supportati da riserve equivalenti di asset liquidi

(che possono essere facilmente convertiti in denaro senza subire una significativa perdita di valore).[91]

3. Le interconnessioni tra normativa sui servizi di pagamento e il regolamento europeo sulla protezione dei dati (GDPR[92])

L'incessante sviluppo tecnologico fa sorgere la necessità di rendere edotte le persone su chi è in possesso dei loro dati e dell'utilizzo che ne viene fatto. È immediatamente ovvio come i servizi di pagamento coinvolgano dati della clientela.[93] La direttiva *PSD2* (datata 2015) e il *GDPR* [94] (datato 2016) sono quasi contestuali, eppure, le questioni legate alla applicazione coordinata di entrambe ha sollevato più di qualche problematica, soprattutto a seguito dell'introduzione dell'*Open Banking*,

[91] Sulle differenze tra moneta elettronica e *token* di moneta elettronica si v. E. FRANZA, *La regolamentazione dei Cripto-Asset.* MiCa un primo passo, in dirittobancario.it. Sul MiCA si v. M. PIERRO, *Contributo all'individuazione della nozione di crypto-asset e i suoi riflessi nell'ordinamento tributario nazionale*, in *Studi in memoria di Francesco Tesauro Tomo III*, M. C. FREGNI, A. GIOVANNINI, M. LOGOZZO, M. PIERRO, S. SAMMARTINO, N. SARTORI (a cura di), CEDAM, 2023.

[92] General Data Protection Regulation. Per approfondimenti su ulteriori questioni relative al rapporto tra PSD2 e GDPR: V. RABBITI e SCIARRONE ALIBRANDI, *I servizi di pagamento tra PSD2 e GDPR: Open Banking e conseguenze per la clientela*, in *Liber Amicorum Giudo Alpa*, a cura di Capriglione, Padova, Cedam, 2019, 711 e ss.

[93] Questo aspetto dell'educazione del consumatore è stato centrale sia per quanto riguarda la *PSD2* sia per quanto riguarda la *PSD3* che vuole cercare di rendere cosciente il consumatore sulla destinazione dei propri dati personali e su come questi vengono trattati.

[94] Il 27 Aprile 2016 è entrato in vigore il c.d. GDPR. La sua vigenza a far data dal 25 Maggio 2018 ha abrogato la precedente Direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 Ottobre 1995 riguardo la tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché la libera circolazione di tali dati.

uno degli aspetti più complessi e controversi nella nuova cornice normativa.

La *PSD2* prevede che i dati acquisiti nello svolgimento dei servizi dei *TPP* non possano essere utilizzati dalle terze parti per finalità diverse da quelle funzionali allo svolgimento dei servizi di pagamento, tuttavia merita notare che nonostante la *PSD2* detti regole in generale sufficientemente specifiche, con riguardi alla tutela dei dati personali le previsioni si rivelano più asciutte. Infatti, la direttiva si limita a sancire la necessità di un coordinamento con la normativa europa in tema di *data protection*.

Il regolamento è parte del "Pacchetto Protezione Dati" presentato dalla Commissione Europea nel gennaio 2012. Il diritto alla *privacy* e alla riservatezza è sempre stato percepito come fondamentale già dalla Convenzione Europea dei Diritti dell'Uomo (*CEDU*) del 1950; gradualmente al diritto alla *privacy* si è andato ad aggiungere il principio riguardante il trattamento dei dati personali. Il legislatore, quindi, è stato spinto a considerare "riservatezza" e "protezione" quali diritti fondamentali, tanto da voler superare la pregressa legislazione mediante l'emanazione di un nuovo Regolamento (679/2016/CE).

Il GDPR diventa misura di attuazione di un equilibrio tra sviluppo tecnologico e dignità umana e mette l'individuo al centro della *policy* individuando un limite alla negoziabilità di questi diritti nel campo dell'informazione.[95]

[95] Sul punto si v. B. RUSSO*, L'evoluzione dei sistemi e dei servizi di pagamento nell'era del digitale*, CEDAM, 2020.

La possibilità di raccogliere, organizzare ed analizzare grandi insiemi di dati con l'obiettivo di facilitare e velocizzare le decisioni strategiche nella gestione del business, ha spinto sempre di più le banche verso processi di *Big Data analytics*. Tale utilizzo dei dati da parte delle banche ha permesso e favorito un maggiore controllo delle abitudini dei propri clienti, l'algoritmo è infatti in grado di individuare comportamenti sospetti nelle operazioni di pagamento, nel prelievo di contanti o nella negoziazione di titoli, evitando al contempo comportamenti come il riciclaggio di denaro o altri atti illeciti. Non solo, l'analisi di *Big Data* è funzionale anche a proporre prodotti su misura per il cliente (come, ad esempio, linee di credito e investimenti).

La domanda da porsi è se si può collezionare questa grande mole di dati garantendo al tempo stesso il rispetto alla *privacy*. L'approccio legislativo del GDPR sembra bilanciare gli interessi del titolare/responsabile con quelli degli interessati garantendo, nella raccolta dei dati di grandi dimensioni, il rispetto della *privacy*. Per questo è fatto obbligo ai responsabili del trattamento di mettere in atto misure tecniche ed organizzative adeguate a garantire un livello di sicurezza coerente con il grado di rischio, supportate da procedure valutative circa la loro efficienza ed efficacia al fine di garantire la concreta tutela dei dati trattati.

Bisogna evidenziare che la diffusione di sistemi di intelligenza artificiale, l'analisi di *Big Data* e l'avvento dell'internet delle cose (*Internet of things*[96]), che è in grado di rendere tutti gli oggetti interconnessi ed in grado

[96] *Internet of Things*: espressione coniata dal ricercatore del M.I.T. Kevin Ashton nel 1999 con la quale si intende alludere all'acquisizione di nuove potenzialità funzionali da parte di oggetti in ragione del loro collegamento ad *Internet*; così A. ZANUSSI in *Internet of Things e privacy. Sicurezza e autodeterminazione informativa*, P. MORO e C. SARRA (a cura di), *Tecnodiritto: temi e problemi di informatica e robotica giuridica*, FrancoAngeli, 2017, p. 99 e ss.

di interagire, sono rivoluzioni che stanno profondamente cambiando le nostre vite.[97] Il rendere gli oggetti *smart* è senz'altro funzionale ma pone allo stesso tempo delle consistenti ricadute sulla protezione dei dati in relazione principalmente a due profili: quello della sicurezza stessa dei dati e quello della consapevolezza del mantenimento di un potere di controllo sui trattamenti relativi ai dati personali. Viviamo in un'epoca in cui le informazioni sensibili sono una risorsa preziosa per le aziende, in quanto vengono utilizzate per tracciare le abitudini di consumo, personalizzare l'esperienza dell'utente e migliorare i propri servizi, ma come si evidenziava questo comporta un rischio significativo per la privacy delle persone se non viene gestita correttamente.[98]

Il consenso dovrebbe essere espresso mediante un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione di accettare il trattamento dei dati personali che lo riguardano. Ciò può avvenire ad esempio selezionando una apposita casella in un sito web, o in altro modo simile, che indichi in modo chiaro che l'interessato accetta il trattamento proposto. Nel caso in cui il trattamento abbia più finalità, il consenso dovrebbe essere prestato per tutte queste.[99]

Fatte queste premesse, risulta difficoltoso in questo contensto individuare chi sia il responsabile del trattamento e chi

---

[97] D. RUGGIU, *Secondary use", così la Ue ribalta il Gdpr e apre all'accesso indiscriminato ai nostri dati*, Agenda Digitale EU, articolo disponibile su www.research.unipd.it

[98]Per approfondimenti si v. A. CAROBENE, M. MASTRANGELO, *La tutela dei dati personali in un mondo digitale. Il regolamento europeo sulla privacy*, *Riv. Aggiornamenti Sociali*, Giugno-Luglio 2019.

[99] Considerando 32 del GDPR.

invece il titolare, considerando che la direttiva *PSD2* fa nascere il diritto all'accesso dal consento prestato al *TPP*s del titolare del conto, senza che sia necessario un accordo diretto tra il prestatore e la banca. Quindi nel caso di un utilizzo illecito dei dati dei correntisti diviene difficile distribuire l'obbligazione risarcitoria, individuando il responsabile del danno.[100]

La questione è di importanza fondamentale se si considera quanto sono appetibili i dati finanziari e bancari che ora non sono più appannaggio esclusivo delle banche tradizionali. In particolare, le *Big Tech* essendo profondamente attratte da questi dati potrebbero decidere di subentrare anche nel mercato dei pagamenti *online*.

In ogni caso l'applicazione coordinata delle due normative risulta ancora difficile, lasciando aperte le interpretazioni.[101]

[100] In tal senso si v. C. VENANZONI , *I servizi bancari online*, in *Il diritto bancario oggi: aspetti sostanziali e processuali*, *op. cit.*, pp. 458 e ss.

[101] Sul punto criticamente si v. C. VENANZONI*, I servizi bancari online,* in *Il diritto bancario oggi: aspetti sostanziali e processuali*, *op. cit.*, pp. 458 e ss.

CAPITOLO II

-

LA PAYMENT SERVICES DIRECTIVE 2 E IL SUO RECEPIMENTO NELL'ORDINAMENTO ITALIANO

1. La PSD 2: i punti chiave della direttiva

Come si è visto nel capitolo precedente la *PSD2* cerca di porsi in un piano di continuità con la *PSD*, introducendo però delle significative novità.

Innanzitutto, riguardo agli obblighi di trasparenza vengono rafforzati i diritti degli utenti dei servizi di pagamento (siano essi il beneficiario, il pagatore o entrambi[102]) in relazione agli obblighi di informazione, esecuzione e alle condizioni economiche. Sono state poi introdotte nuove misure di sicurezza: viene introdotta l'autenticazione forte del cliente (*SCA*) per accedere ai conti, disporre ordini di pagamento sui canali online e per effettuare operazioni che implichino rischi di abuso o frode. Viene inoltre disposto l'accesso ai conti online tramite Third Party Providers (*TPP*[103]) prevedendo la possibilità di accedere alle informazioni

[102] Vengono divisi tali soggetti in tre categorie: consumatori, microimprese e soggetti che per esclusione non sono rappresentati nei punti precedenti.

[103] Per quanto attiene l'ambito soggettivo di applicazione della direttiva, questo ricomprende Banche, Istituti di Moneta Elettronica (*IMEL*), Istituti di Pagamento, nonché le imprese diverse dalle banche e dagli istituti di moneta elettronica, autorizzate a prestare i servizi di pagamento dall'Autorità di Vigilanza. I TPP rientrano nella categoria dei prestatori di servizi di pagamento e vengono pertanto assoggettati alla disciplina della *PSD2*, essi debbono essere autorizzati in via amministrativa alla stregua di istituti di pagamento, ma soggiacciono a una

relative al proprio conto corrente e alle transazioni effettuate nonché di disporre ordini di pagamento attraverso terze parti. Tali servizi preesistevano all'entrata in vigore della *PSD2* ma sfuggivano all'ambito di applicazione della precedente direttiva e in tal modo scontavano la difformità di regole fra i diversi Stati membri o addirittura non avevano una specifica regolamentazione, come in Italia[104].

Un ruolo centrale per la disciplina dei servizi di pagamento è svolto dalla Autorità Bancaria Europea (d'ora in poi *ABE*).[105] La *PSD2*

---

disciplina parizalmente differenziata rispetto alla categoria generale di intermediari in ragione della specificità del loro business. Si v. per approfondimenti S. SICA e B.M. SABATINO, *Disintermediazione finanziaria e tutela del cliente e dell'utilizzatore*, Dir. e Inf., n. 1/2021, pp. 1 e ss; in tal senso si v. anche V. PROFETA, *I third party provider: profili soggettivi e oggettivi*, in *Le nuove frontiere dei servizi bancari e di pagamento fra PSD 2, criptovalute e rivoluzione digitale*, a cura di F. MAIMERI e M. MANCINI, in *Quaderni di ricerca giuridica della consulenza legale di Banca d'Italia*, n. 87, 2019, pp. 49 e ss.

[104] Una norma, a parere di chi scrive, molto significativa è quella che sancisce la piena armonizzazione all'art. 107 par 1 del Titolo VI intitolato "Disposizioni finali" il quale prevede che: «*nella misura in cui la presente direttiva contiene disposizioni armonizzate, gli Stati membri non mantengono né introducono disposizioni diverse da quelle previste dalla presente direttiva*». L'obiettivo è quello di garantire un impianto normativo unitario e di massima armonizzazione tendenzialmente non modificabile dagli stati membri. In tal senso si v. S. VANINI, *L'attuazione in Italia della seconda direttiva sui servizi di pagamento nel mercato interno: le innovazioni introdotte dal d.lgs. 15 dicembre 2017*, in *Rivista Le nuove leggi*, NLCC 4/2018, Wolters Kluwer.

[105] Questa è stata istituita con Regolamento (UE) n. 1093/2010 ed è una delle tre autorità europee di vigilanza (*European Supervisory Authorities* o *ESA*[105]). Le *ESAs* sono autorità indipendenti dell'Unione Europea e hanno sede a Parigi (*EBA*[105] e *ESMA*) e Francoforte sul Meno (*EIOPA*). Esse sono dotate di poteri normativi (o *quasi-normativi*[105]); poteri di supervisione; altri poteri e ruoli finalizzati alla protezione della stabilità finanziaria dell'UE e dei consumatori. Le autorità di vigilanza europea inoltre contribuiscono a una applicazione coerente delle norme affinché si creino condizioni di parità concorrenziale ed hanno il compito di valutare rischi e

conferisce all'*ABE* il mandato di redigere, in stretta cooperazione con la *Banca Centrale Europea* diversi *Regulatory Technical Standards* (o *RTS),* che vengono adottati dalla commissione, sull'autenticazione forte dei clienti (una delle attività più controverse[106] affidatagli) e sui requisiti per la comunicazione comune e sicura.[107] In tutto la *PSD2* ha conferito 12 mandati all'*EBA*, tra sviluppo di *RTS* e linee guida e sono stati tutti completati.

Tra gli altri l'*ABE* ha avuto anche il compito, secondo l'art. 15 della direttiva, di sviluppare, gestire e mantenere un registro contenente le informazioni notificate dalle autorità competenti riguardo gli istituti di pagamento degli Stati Membri.

La stesura degli *RTS* ha richiesto ampie e difficili consultazioni pubbliche e un intenso dialogo con le diverse categorie di parti interessate come banche, fornitori terzi, associazioni di consumatori, *etc.*; si è dovuto cercare di bilanciare la neutralità tecnologica con la contribuzione alla creazione di un mercato unico di pagamenti dell'UE, che poteva richiedere una

---

vulnerabilità nel settore finanziario. Nello specifico l'*ABE* ha il compito di assicurare un livello di regolamentazione e di vigilanza prudenziale, efficace ed uniforme nel settore bancario europeo contribuendo alla creazione di un corpus unico di norme nel settore bancario, il c.d. *Single Rulebook*. Il *Single Rulebook* mira a costituire un'unica serie di norme prudenziali armonizzate per gli istituti finanziari, volte ad assicurare condizioni di parità e una tutela elevata dei depositanti, degli investitori e dei consumatori. Si veda per approfondimenti sul tema E. CERVONE, *Servizi di pagamento e innovazione tecnologica. Ruolo dell'Autorità bancaria europea alla luce della giurisprudenza della Corte di Giustizia*, in *Analisi Giuridica dell'Economia*, *Studi e discussioni sul diritto dell'impresa*, 2/2018, pp. 393-408.

[106] Definita controversa in quanto non sempre è agevole individuare quando deve applicarsi la SCA e quando invece intervengano le relative esenzioni.

[107] Considerando 33, 41, 42, 44, 93, 94, 107, 108 della *PSD2*.

maggiore standardizzazione di alcuni requisiti e quindi potenzialmente limitare il margine all'innovazione.

Per garantire una maggiore neutralità l'*ABE* ha rimosso diversi riferimenti agli standard tecnologici in maniera tale da potersi adattare più facilmente alle innovazioni dei sistemi di pagamento, come si diceva in maniera più approfondita nel capitolo precedente.

Gli *RTS* proposti dall'*ABE* sono stati presentati alla Commissione europea per l'adozione nel febbraio 2017, subendo poi qualche modifica, fino ad essere entrati in vigore il 14 marzo 2018[108], ricordando che gli obblighi stabiliti negli *RTS* saranno applicati dopo un periodo transitorio di 18 mesi.[109]

In data 9 gennaio 2019 Banca d'Italia ha avviato una consultazione pubblica volta a recepire nell'ordinamento nazionale alcuni orientamenti emanati da *ABE* ai sensi della *PSD2* di cui si dirà più dettagliatamente in seguito.

1.1 L'Open Banking e i Third Party Providers (TPP)

Come anticipato nel capitolo precedente, uno degli aspetti più interessanti della direttiva *PSD2* è sicuramente l'introduzione *dell'Open Banking* (in italiano servizi bancari aperti).

---

[108] Regolamento delegato (UE) 2018/389 della Commissione del 27 novembre 2017 che integra la direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione per l'autenticazione forte del cliente e gli standard aperti di comunicazione comuni e sicuri («Regolamento delegato»).

[109] E. CERVONE, *Servizi di pagamento e innovazione tecnologica*, *op. cit.*; si veda anche F. PORTA, *Obiettivi e strumenti della PSD2*, *op.cit*, pp. 13 e ss.

Tale espressione[110] si riferisce all'obbligo previsto dalla *PSD2* per le banche di aprire l'accesso ai conti di pagamento, alle transazioni bancarie e ad altri dati finanziari dei propri clienti utilizzando interfacce interoperabili a fornitori di servizi terzi (cd. *Third Party Providers* o *TPP*).[111] Si tratta della *Access to Account Rule*, in gergo tecnico indicata con la sigla XS2A rule. Questo punto è di grande rilevanza per le implicazioni che ne discendono perché testimonia la sopravvenuta modifica del tradizionale rapporto tra banche e clienti.

Abbiamo già visto che con l'accesso di specifiche categorie di soggetti (i *TPP*) ai dati dei conti di pagamento intrattenuti dagli utenti presso banche o altri enti autorizzati, si percepisce subito come le banche perdono per la prima volta il monopolio sui dati dei propri correntisti, per effetto di un obbligo normativo che impone loro di condividere tali dati con altri soggetti. [112]

Ci si chiede quindi in questo scenario quali saranno le sorti della banca tradizionale, tra chi sostiene che questa cesserà di esistere a fronte dei nuovi *competitors* e chi ritiene, invece, che la forza delle imprese *Fintech* giungerà ad un naturale esaurimento. Ma l'ipotesi più plausibile al

---

[110] L'*Open Banking* si configura come il nuovo modello bancario che garantisce a terze parti, fornitrici di servizi finanziari, un accesso aperto/libero a servizi bancari, transazioni e altri dati finanziari dei clienti tramite l'uso di interfacce tecnologiche interoperabili (*API*, dall'inglese *Application Programming Interface*).

[111] F. FERRETTI, *L'open finance. Quali prospettive regolatorie per una strategia UE in materia di protezione dei consumatori nella finanza digitale?*, in *Banca Impresa Società*, 2/2023, pp. 277-314; v. anche A. SCIARRONE ALIBRANDI, *Impostazione sistematica della Direttiva PSD2,* (a cura di) M.C. PAGLIETTI e M.I. VANGELISTI, Consumatori e Mercato, n.9, Roma Tre-Press, 2020, p. 13 e ss.

[112] A. ARGENTATI, *Le banche nel nuovo scenario competitivo. FinTech, il paradigma dell'Open banking e la minaccia delle big tech companies*, in *Mercato Concorrenza Regole*, n. 3/2018, pp. 441-466.

momento è quella di una cooperazione tra banche e imprese *Fintech*, ed infatti sono già numerosi i casi di *partnership*.[113]

La *PSD2* obbliga la banca a fornire ad un *TPP*, attraverso la creazione di una interfaccia tecnica dedicata, «tutte le informazioni in suo possesso sull'ordine di pagamento e sull'esecuzione delle operazioni»[114] e a collaborare senza ritardo, comunicando attraverso standards sicuri, che sono oggetto di regolamentazione secondaria da parte dell'*ABE*.

Nonostante sia un sistema innovativo, che spinge le banche a condividere dei dati che prima erano inaccessibili a soggetti esterni, dall'altra parte pone dei problemi sul versante della sicurezza, non essendo facilmente individuabile il soggetto responsabile in caso di violazioni, operazioni non autorizzate, furto delle credenziali e altri disservizi nel funzionamento dell'interfaccia.[115]

I *TPP* [116] sono soggetti altamente specializzati che forniscono, come parte di un contratto, un servizio o una

---

[113] F. CIRAOLO, *Open Banking, Open Problems.*, in *Riv. Dir. Banc.*, n. 4/2020, Sezione 1; M. SCHIEPPATI, *Banche, «pensare come Google»?*, in Bancaria, 2017, n. 3, 60. Anche l'ultima Indagine *FinTech* nel sistema finanziario italiano (Banca d'Italia, dicembre 2019) conferma la crescita degli investimenti *FinTech* nel settore bancario, il 14% dei quali è rappresentato da forme di cooperazione tra istituti tradizionali e imprese *FinTech*, prevalentemente secondo la modalità della partnership, sovente in combinazione con incubatori, acceleratori, distretti, o con l'acquisizione di partecipazioni. Significativa, peraltro, l'affermazione secondo la quale proprio l'*open banking* e la *PSD2* hanno dato impulso alla realizzazione di progetti innovativi e di più ampio respiro, volti alla creazione di nuovi ecosistemi digitali.

[114] Art. 6, n. 4 lett. a della *PSD2*.

[115] Si v. in questo senso C. VENANZONI , *I servizi bancari online*, in *Il diritto bancario oggi: aspetti sostanziali e processuali*, F. Aratari e Guido Romano (a cura di), Wolters Kluwer, 2023, pp. 438 e ss.

[116] Figura peraltro non nuova all'interno del mercato europeo, in quanto già prima della *PSD2* erano classificati come *players* importanti nelle transazioni e-commerce.

tecnologia specifica. Prima della *PSD2* erano privi di qualsiasi disciplina e sottratti a requisiti di autorizzazione, registrazione e vigilanza. Il loro emergere ha pertanto comportato il bisogno di disciplinare la loro attività. Questi vengono classificati dalla normativa come soggetti non bancari che possono essere autorizzati a gestire finanze e operazioni di pagamento. Le attività da loro svolte sono caratterizzate da differenze notevoli rispetto al ruolo e ai servizi offerti dagli istituti di pagamento e, benchè siano partecipi a passaggi importanti della filiera dei pagamenti con moneta scritturale, non custodiscono né gestiscono, in alcun momento, i fondi dell'operazione; questo perché il loro compito è fornire informazioni o avviare pagamenti su conti che sono radicati presso altri prestatori.[117]

Si dividono in tre categorie:

1. *PISP* (*Payment Initiation Service Providers*): prestano, dietro autorizzazione del cliente, il servizio di disposizione di ordini di pagamento; fanno da tramite tra banca e titolare del conto di pagamento accessibile online e avviano il pagamento a favore di un terzo soggetto. Questi assicurano contestualmente al beneficiario del pagamento che lo stesso è stato disposto, in tal modo il beneficiario viene incentivato a una pronta esecuzione della propria prestazione.[118]

2. *AISP* (*Account Information Services Providers*): consentono al titolare di conti accessibili online di ottenere un'informativa completa relativa sui servizi di pagamento dei rapporti a lui intestati. Servono ad avere una visione d'insieme della propria situazione finanziaria, analizzando le abitudini e le esigenze future. L'utente tramite questo servizio può ricevere una informativa completa e organizzata su tutti i

[117] Così C. VENANZONI , *I servizi bancari online*, in *Il diritto bancario oggi: aspetti sostanziali e processuali*, *op. cit.*, pp. 440 e ss.

[118] Si veda il considerando 27 e 29 della *PSD2*.

propri conti di pagamento e assumere, alla luce di questa, decisioni consapevoli in merito all'efficiente gestione delle proprie risorse.[119]

3. *CISP* (*Card Issuer Service Providers*): verificano se c'è disponibilità sul conto corrente di una persona che abbia disposto, presso un esercente, un pagamento attraverso carta.[120]

Il cliente si mostra ben predisposto a questo sistema di scambio di dati. Un'indagine di Forrester[121] rivela che il 50% dei consumatori sarebbe favorevole alla condivisione di alcuni dati personali se questo comporta un miglioramento dei servizi finanziari. Alcuni dei vantaggi più rappresentativi dell'*Open banking* sono ad esempio la possibilità di gestire conti correnti di diverse banche tramite l'app bancaria preferita o ancora la progettazione di soluzioni personalizzate per i clienti, consentita proprio grazie allo scambio di informazioni.[122]

I clienti sono tenuti a prestare il consenso agli istituti bancari per consentire l'accesso ai dati del proprio conto tramite un «consenso esplicito» che deve avvenire solo a seguito di un rapporto contrattuale.[123] Come si diceva, l'accesso ai conti di

---

[119] Per approfondimenti sul tema si rimanda alla lettura di M. CATENACCI, C. FORNASARO, *PSD2: i prestatori di servizi di informazione sui conti (AISPS)*, aprile 2018, 3-4, disponibile su www.dirittobancario.it.

[120] Si veda art 65 della *PSD2*.

[121] European Open Banking Forecast, 2022-2027 | Forrester, 2022.

[122] In argomento, D. GIROMPINI, *PSD2 e Open Banking. Nuovi modelli di business e ruolo delle banche,* in *Bancaria*, 2018, n. 1, 70 ss.

[123] Art. 27 della *PSD2* laddove dispone che «il prestatore di servizi di informazione sui conti: *a*) presta servizi unicamente sulla base del consenso esplicito dell'utente dei servizi di pagamento; (*omissis*)».

pagamento deve inoltre avvenire in modo sicuro e secondo gli standard stabiliti dall'Autorità Bancaria Europea emanati in conformità con la *PSD2*, come ad esempio il Regolamento delegato UE 2018/389 sull'autenticazione forte del cliente e comunicazione sicura, che regola anche l'accesso non discriminatorio dei *TPP*. Ciò significa che non si devono imporre barriere tecniche o condizioni di servizio peggiori ai *TPP* rispetto a quelle offerte dalla banca stessa (art. 32 Reg. UE 2018/389).

Non c'è dubbio, quindi, che tra i principali obiettivi della *PSD2* risieda anche quello di garantire maggiore concorrenzialità al mercato dei servizi di pagamento, favorendo appunto l'ingresso di nuovi operatori e migliorando il tono competitivo del settore.[124] Certamente non ci si può esimere dalla considerazione che una tale apertura a soggetti terzi nella "catena procedimentale" di ogni operazione di pagamento intermediato implica inevitabilmente un maggiore rischio di *data breach*[125], di frodi informatiche e di abusi in danno dei correntisti.[126] Per quanto riguarda gli *AISP*s, in particolare, questi si limitano a fornire un servizio a carattere informativo, quindi, i rischi sono essenzialmente limitati all'accesso abusivo a dati personali immagazzinati nei conti, ma per quanto riguarda i *PISP*s, pur non detenendo fondi dell'utente e non amministrando conti di pagamento, agiscono dando impulso a delle

[124] A. ARGENTATI, *Le banche nel nuovo scenario competitivo*, *op. cit.*, pp. 441-466.

[125] Consistente in una violazione di sicurezza che comporta - accidentalmente o in modo illecito - la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati. Una violazione dei dati personali può compromettere la loro riservatezza, l'integrità o la disponibilità.

[126] Per approfondimenti si veda v. ad es. M. ONZA, *Gli strumenti di pagamento nel contesto dei pagamenti on line*, in *Dir. banc. fin.*, 2017, p. 579.

operazioni di pagamento a valere sui conti del cliente, quindi al pericolo di accesso si somma quello di transazioni inesatte o fraudolente.

Anche gli istituti di pagamento che svolgono il ruolo di *TPP* sono soggetti alla vigilanza informativa e ispettiva delle autorità nazionali competenti, nonché alle disposizioni di *soft law* e ai provvedimenti amministrativi vincolanti emanati da queste ultime. L'autorità può adottare provvedimenti di sospensione o revoca dell'autorizzazione al ricorrere delle condizioni previste dall'art. 13 della *PSD2* (a cui si rimanda) e comminare sanzioni amministrative nei confronti di detti intermediari o di coloro che di fatto controllano l'attività degli istituti di pagamento che si sono resi colpevoli di infrazioni alle disposizioni legislative, regolamentari o amministrative in materia di vigilanza o di esercizio dell'attività di servizi di pagamento, o adottare nei loro confronti provvedimenti la cui applicazione è diretta specificamente a far cessare le infrazioni accertate o a rimuoverne le cause.[127]

Si tratterà di questo argomento più nello specifico nel capitolo 3 a cui si rimanda. Al momento basta evidenziare che, nel caso di operazioni di pagamento non autorizzate, in materia di responsabilità, la *PSD2* ricalca le medesime scelte normative operate dalla precedente dir. 2007/64/CE, proponendo un criterio di suddivisione della responsabilità fra utente e prestatore

[127] Si rimanda alla lettura del comma 2 dell'articolo 23 riportato in nota 96. Sul punto si veda V. PROFETA, *I third party provider: profili soggettivi e oggettivi*, in *Le nuove frontiere dei servizi bancari e di pagamento fra PSD 2, criptovalute e rivoluzione digitale*, a cura di F. MAIMERI e M. MANCINI, in *Quaderni di ricerca giuridica della consulenza legale di Banca d'Italia*, n. 87, 2019, pp. 49 e ss.

di servizi di pagamento, basato sulle rispettive capacità di prevenire e/o gestire determinati rischi, sostanzialmente ciascuna delle parti è tenuta a sopportare le conseguenze degli eventi che ricadono in modo più diretto nella propria sfera di controllo.[128]

1.2 L'autenticazione forte del cliente o Strong Costumer Authentication (SCA)

Un altro punto importante della normativa è stato l'introduzione di numerose disposizioni che hanno avuto l'obbiettivo di rafforzare la sicurezza dei pagamenti elettronici a fronte del crescente sviluppo delle transazioni online. In particolare, l'introduzione dell'obbligo di autenticazione forte del cliente (artt. 97-98 *PSD2*); l'adozione di misure di sicurezza adeguate a tutelare la riservatezza e l'integrità delle credenziali di sicurezza personalizzate degli utenti; l'utilizzo di standard aperti per la comunicazione sicura tra prestatori di servizi di pagamento; gli obblighi di *reporting* all'Autorità competente dei gravi incidenti di sicurezza. [129]

L'autenticazione forte viene definita come «un'autenticazione basata sull'uso di due o più elementi, classificati nelle categorie della conoscenza (qualcosa che solo l'utente conosce), del possesso (qualcosa che solo l'utente possiede) e dell'inerenza (qualcosa che caratterizza l'utente), che sono indipendenti, in quanto la violazione di uno non compromette l'affidabilità degli altri, e che è concepita in modo tale da tutelare la riservatezza dei dati di autenticazione»[130]. Le credenziali di

[128] In tal senso si v. F. CIRAOLO, *Open Banking, Open Problems*, *op. cit.*

[129] F. PORTA, *Obiettivi e strumenti della PSD2,* in *Le nuove frontiere dei servizi bancari e di pagamento fra PSD", Criptovalute e Rivoluzione Digitale* a cura di F. MAIMERI e M. MANCINI, *Quaderni di Ricerca Giuridica della Consulenza Legale di Banca d'Italia n. 87*, 2019, pp. 41 e ss.

[130] Così l'art. 4 co 30 della Direttiva (UE) 2015/2366.

sicurezza personalizzate che vengono usate per l'autenticazione sicura dall'utente del servizio di pagamento o dal prestatore di servizi di disposizione di ordine di pagamento, sono in genere quelle rilasciate dai prestatori dei servizi di pagamento di radicamento del conto.[131]

L'autenticazione si definisce forte in quanto, come enunciato dalla norma sopra citata, si richiede la corretta combinazione di almeno due elementi classificati come: «*Knowledge*», qualcosa che soltanto il cliente può conoscere come ad esempio una *password* o un PIN; «*Possession*», qualcosa che solo il cliente possiede come ad esempio una chiavetta o un token; «*Inherence*», cioè qualcosa che solo l'utente può essere come per esempio nel caso dell'impronta digitale o del riconoscimento facciale. Questi elementi devono essere indipendenti l'uno dall'altro così che la violazione di uno non comprometta l'affidabilità degli altri e l'autenticazione deve essere progettata in modo tale da tutelare la riservatezza dei dati[132].

Tale aggiornamento normativo è stato considerato indispensabile soprattutto nell'ottica di rafforzamento della tutela in favore dei clienti, utilizzatori di modalità di pagamento elettronico, in modo da ridurre il rischio di abusi o frodi informatiche. Queste nuove norme prevedono anche l'adozione

[131] Considerando 30 della Direttiva (UE) 2015/2366.

[132] Sulla riservatezza si rimanda a M. DONNELLY, *Payments in the digital market: Evaluating the contribution of Payment Services Directive II*, Computer Law and Security Review 32 (2016), pp. 827-839; si veda anche S. BALSAMO TAGNANI, *Il mercato europeo dei servizi si rinnova con la PSD2,* in Contr. Impr. Eur., 2018 p. 609-624; sul punto anche S. SICA e B.M. SABATINO, *Disintermediazione finanziaria e tutela del cliente e dell'utilizzatore*, *op. cit.*

di strumenti per la tutela della riservatezza e l'integrità delle credenziali degli utenti in modo tale da limitare il rischio di *phishing*, o altre attività di natura fraudolenta già illustrate nel capitolo I.

Centrale per questo tema è anche l'educazione del consumatore in maniera tale che sia in grado di sfruttare al meglio i servizi senza incorrere in frodi informatiche mettendo a rischio i propri dati personali; questo aspetto è stato rilevato dagli operatori come critico. Infatti, sembra che i clienti-consumatori abbiano una scarsa consapevolezza delle principali tipologie di frode e la *PSD3* ha cercato di implementare campagne di sensibilizzazione più efficaci al fine di tutelare il cliente-consumatore.[133]

Per quanto riguarda l'ambito di applicazione di questo sistema di autenticazione, si guarda al comma 1 dell'art. 97 «Gli stati membri provvedono a che un prestatore di servizi di pagamento applichi l'autenticazione forte del cliente quando il pagatore: a) accede al suo conto di pagamento *on line*; b) dispone un'operazione di pagamento elettronico; c) effettua qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o abusi».

Rispetto all'impianto generale della *strong authentication* dell'utente, la normativa tollera talune eccezioni contemplate dal par. 3 dell'art. 98 della *PSD2* in funzione del livello di rischio, dell'importo, della frequenza e del canale utilizzato per l'esecuzione dell'operazione di pagamento. Nello specifico il Reg. delegato (UE) 2018/389, all'art. 11[134], dà puntuale

[133] In tal senso F. CASCINELLI e L.BETTINELLI, *Verso la PSD3 e il nuovo Regolamento sui Servizi di Pagamento,* consultabile al sito: www.dirittobancario.it

[134] Art. 11 Reg. (UE) 2018/389, *Pagamenti senza contatto fisico al punto vendita*, «I prestatori di servizi di pagamento sono autorizzati a non applicare l'autenticazione forte del cliente, a condizione di rispettare gli obblighi di cui all'articolo 2, se il pagatore dispone

attuazione alla deroga prevista nei suoi lineamenti generali dalla *PSD2*, con specifico riguardo ai pagamenti *contactless* di importo ridotto eseguiti nell'ambito del commercio al dettaglio. Tale esenzione è operante solamente qualora il prestatore di servizio di pagamento se ne avvalga in seno al contratto-quadro, ed è condizionata a stringenti criteri legati, oltre che all'importo ridotto della singola operazione di pagamento considerata, anche ad un numero massimo di operazioni consecutive e a un determinato tetto complessivo di valore di tali operazioni.[135]

1.3 La funzione contactless nelle carte di pagamento e regime speciale di responsabilità per i Prestatori di Servizi di pagamenti contactless di importo ridotto

Come si diceva nel paragrafo precedente con riguardo alla *Strong Authentication* la normativa tollera alcune eccezioni, una di queste è con riguardo alla funzione contactless delle carte di

---

un'operazione di pagamento elettronico senza contatto, purché siano soddisfatte le seguenti condizioni: [...] l'importo individuale dell'operazione di pagamento elettronico senza contatto non supera i 50 EUR; e l'importo cumulativo delle precedenti operazioni di pagamento elettronico senza contatto disposte per mezzo di uno strumento di pagamento con una funzionalità senza contatto a partire dalla data dell'ultima applicazione dell'autenticazione forte del cliente non supera i 150 EUR; oppure il numero di operazioni consecutive di pagamento elettronico senza contatto disposte per mezzo di uno strumento di pagamento con una funzionalità senza contatto a partire dalla data dell'ultima applicazione dell'autenticazione forte del cliente non è superiore a cinque». Si veda sul punto L. MIOTTO e M. SPERANZIN, *I pagamenti elettronici*, in *Diritto del Fintech*, M. Cian e C. Sandei (a cura di), CEDAM, 2020, p. 179.

[135] G. MARINO, *Carte di pagamento con funzione contactless, uso non autorizzato e responsabilità dei prestatori di servizi di pagamento*, in *Osservatorio del diritto civile e commerciale,* 1/2021, pp. 137-178.

pagamento per quanto attiene ad operazioni di pagamento di importo ridotto.

La funzione *contactless* è una forma innovativa delle carte di pagamento: la banda magnetica è stata sostituita con microprocessori che utilizzano sistemi crittografati idonei a consentire l'autenticazione *offline* e questo aiuta a ridurre i rischi di frode e di clonazione e consentono di memorizzare dei dati in modo da trasformare le carte tradizionali in *smart card*[136]. Esse impiegano la tecnologia di comunicazione *Near Field Communication* (*NFC*)[137], senza fili, a corto raggio e ad alta frequenza, la quale consente la trasmissione quasi immediata di dati tra dispositivi e viene utilizzata in diverse applicazioni, tra cui le carte di credito e di debito e i telefoni cellulari. [138]

Riguardo all'esecuzione in modalità *offline* si deve notare che si ha l'assenza di un'autorizzazione da parte dell'emittente al momento della

---

[136] Per approfondimenti sulla evoluzione delle carte di pagamento si veda L. MIOTTO e M. SPERANZIN, *I pagamenti elettronici*, in *Diritto del Fintech*, M. Cian e C. Sandei (a cura di), CEDAM, 2020 pp. 177 e ss.

[137] Il sistema di connettività senza fili NFC è basato su onde radio: più precisamente, è una evoluzione della RFID, l'identificazione su frequenze radio. La RFID collega due tipi di dispositivi: i reader/writer, che leggono e scrivono informazioni, e i tag (o etichette elettroniche, o transponder), che memorizzano i dati e rispondono ai messaggi inviati dai reader/writer. I dispositivi che "leggono e scrivono" chiedono i dati contenuti nelle etichette e li aggiornano: una trasmissione che avviene per induzione elettromagnetica grazie alle antenne dei due tipi di dispositivi.

[138] Sull'uso degli strumenti di pagamento senza contatto si veda l'analisi della European Central Bank, *Card payments in Europe – current landscape and future prospects: A Eurosystem perspective*, 2019; e dello European Cards Stakeholders Group, *Feasibility Study on the development of open specifications for a card and mobile contactless payment application*, 2017, entrambi disponibili all'indirizzo www.ecb.europa.eu.

transazione, quindi, essa avviene successivamente alla verifica di capienza rispetto al *plafond* disponibile, invece nella modalità *online* autorizzazione e verifica avvengono contestualmente. Quindi si può comprendere come tale variante tecnologica introduca un elemento di rischio.[139]

Nell'ambito del commercio al dettaglio gli utenti hanno la possibilità di attuare il pagamento di un bene o di un servizio avvicinando la carta al POS[140], senza che occorra passarla attraverso una fessura di lettura. Tale comunicazione senza fili tra la carta dotata di *NFC* e il terminale di vendita è sufficiente per perfezionare il procedimento solutorio, consentendo l'addebito dal conto del pagatore, titolare della carta.

Innanzitutto, si deve distinguere tra l'utilizzo della funzione *contactless* per importi di somme modeste e l'utilizzo per importi più consistenti. Infatti, nel secondo caso troverà applicazione il regime generale di responsabilità degli istituti di pagamento e la regola dell'autenticazione forte, a differenza del primo caso in cui, come si è già notato, questa non opera.

In secondo luogo si deve specificare che le carte con funzione *contactless* sono sicuramente uno strumento di pagamento in base ad alcuni indici che lasciano pochi dubbi: l'Allegato I, punto 3, lett. b), *PSD2* considera servizio di

---

[139] In tal senso L. MIOTTO e M. SPERANZIN, *I pagamenti elettronici*, in *Diritto del Fintech*, M. Cian e C. Sandei (a cura di), CEDAM, 2020, p. 178.

[140] Apparecchi di accettazione elettronici utilizzati per accettare pagamenti con carta di debito, di credito o prepagate. Tale sistema permette agli utenti di effettuare acquisti verificando la disponibilità dei fondi sul conto bancario associaro alla carta e, nel caso in cui venga approvato, esegue la transazione in tempo reale.

pagamento «l'esecuzione di operazioni di pagamento mediante carte di pagamento o analogo dispositivo»; nell'ambito della normativa di dettaglio, il Reg. (UE) 2015/751 definisce la «carta di pagamento» come «una categoria di strumenti di pagamento che consente al pagatore di disporre un'operazione tramite carta di debito o carta di credito» (art. 2, punto 15); ancora, all'art. 2, punto 7, il medesimo regolamento definisce «operazione di pagamento basata su carta» il «servizio basato sull'infrastruttura e le regole commerciali di uno schema di carte di pagamento per effettuare un'operazione di pagamento tramite carta, dispositivi di telecomunicazione, digitali o informatici o software, se il risultato è un'operazione tramite carta di debito o di credito».

Si può quindi affermare che indubbiamente[141] le carte di pagamento, dotate di duplice funzionalità, debbano essere qualificate quali strumenti di pagamento alla luce della *PSD2*.[142]

In materia di responsabilità dei *Payment Services Provider* per pagamenti *contactless* di importo ridotto si guarda all'art. 63 della *PSD2*, «Deroga per gli strumenti di pagamento di importo ridotto e moneta elettronica» il quale permette ai prestatori di servizi di pagamento di derogare ad alcuni obblighi di condotta gravanti sulle parti, in seno al contratto-quadro per la prestazione di servizi di pagamento. Tale evenzienza è ammessa per una precisa categoria di strumenti di pagamento, ossia quelli che «conformemente al contratto quadro riguardano unicamente operazioni di pagamento singole per un importo non superiore a 30 EUR oppure che hanno un limite di spesa di 150 EUR,

[141] Data la combinazione di norme lette sul punto, credo di poter fare questa affermazione.

[142] Sul punto si veda G. MARINO, *Carte di pagamento con funzione contactless, uso non autorizzato e responsabilità dei prestatori di servizi di pagamento*, *op. cit.*, pp. 137 e ss.

o sono avvalorati per un importo che non supera in alcun momento 150 EUR» e in due ipotesi distinte quanto a presupposti e contenuti: qualora risulti tecnicamente impossibile il blocco[143] dello strumento utilizzato senza l'autorizzazione dell'utente che ne è titolare o in modo fraudolento (art. 63 lett a) e qualora lo strumento sia utilizzato in modo anonimo ovvero sia impossibile per il prestatore, per altri motivi intrinseci allo strumento stesso, dimostrare che l'operazione di pagamento sia stata autorizzata (art. 63, lett b).[144]

Il legislatore europeo in quest'ottica fissa un rapporto di proporzionalità diretta tra il grado di rischio sotteso allo strumento di pagamento e quello di sicurezza per l'utente che lo adopera, ciò emerge con chiarezza dai considerando n. 81, 91 e 96 della *PSD2* («le misure di sicurezza dovrebbero essere compatibili con il livello di rischio insito nel servizio di pagamento prestato»)

In definitiva, le modalità di pagamento senza contatto altro non sono che espressione peculiare di una tendenza verso la semplificazione, che si esprime tra le altre cose anche dalla liberazione degli utenti dallo sforzo di memorizzare le *password*. Si

[143] Nel linguaggio tecnico per «blocco» secondo l'art. 68, par 2 della Direttiva 2015/2366/UE si intende una misura preventiva assunta dal *Payment Service Provider* che gli permette «il diritto di bloccare lo strumento di pagamento per motivi obiettivamente giustificati legati alla sicurezza dello strumento di pagamento, al sospetto di un utilizzo non autorizzato o fraudolento dello strumento di pagamento, oppure, nel caso di uno strumento di pagamento dotato di una linea di credito, al significativo aumento del rischio che il pagatore non sia in grado di adempiere ai propri obblighi di pagamento».

[144] In argomento si veda G. MARINO, *Carte di pagamento con funzione contactless, uso non autorizzato e responsabilità dei prestatori di servizi di pagamento, op.cit.*

stanno inoltre considerando anche altri strumenti alternativi per i pagamenti *mobile* che potrebbero sostituire le carte tradizionali, andando in questo modo ad aumentare la sicurezza e la facilità delle transazioni. Sono già attualmente in uso supporti alternativi quali *smartphone*, *tablet, smartwatch*, e *smart object* in generale che processano il pagamento mediante tecnologia *contactless* o *biometrica*.[145]

2. Il Testo Unico Bancario e le disposizioni in materia di trasparenza

Il Testo Unico Bancario[146] ed il Provvedimento di Banca d'Italia del 29/07/2009[147] denominato "Trasparenza delle operazioni e dei servizi bancari e finanziari. Correttezza delle relazioni tra intermediari e clienti" disciplinano congiuntamente i servizi di pagamento in chiave di trasparenza, recependo le disposizioni della *PSD2*: il legislatore interviene al fine di ridurre la situazione di squilibrio tra intermediario e cliente, cercando di bilanciare il maggiore potere contrattuale dell'intermediario con la previsione di alcuni diritti in capo al cliente, puntando soprattutto

[145] Si v. per approfondimenti al riguardo L. MIOTTO e M. SPERANZIN, *I pagamenti elettronici*, in *Diritto del Fintech, op. cit.*, pp. 180 e ss.

[146] Il 1° settembre 1993 con d.lgs. n. 385 veniva varato il Testo Unico Bancario (*TUB*).

[147] Il provvedimento del 29 luglio 2009 ha subito due modifiche consistenti: una prima modifica è intervenuta nel 2012 con l'entrata in vigore del d.lgs. 45/2012, di recepimento della direttiva 2009/110/CE, in tema di Istituti di Moneta Elettronica;[147] la seconda modifica è intervenuta il 19 Marzo 2019, quando Banca d'Italia ha emanato un provvedimento che si è reso necessario al fine di adeguare la disciplina nazionale al nuovo quadro normativo europeo.

sulle tutele informative in maniera coerente con la disciplina comunitaria.[148]

La previsione di una regola generale di trasparenza nel comportamento dell'operatore mancava nel Codice Civile[149], ma è stata introdotta in molti settori dell'ordinamento dalla legislazione speciale, in considerazione del ruolo sempre più centrale riconosciuto all'informazione. L'espressione "trasparenza" assume diversi significati: in linea generale ci si riferisce alla chiarezza e comprensibilità nella redazione del contratto, ma si estende poi a comprendere altri vincoli di forma e obblighi di comportamento. Inoltre, in termini ancor più estesi, può riferirsi all'intero complesso della disciplina della correttezza nei rapporti contrattuali con la clientela, e in questo senso il Titolo VI del TUB e le disposizioni della Banca d'Italia paiono espliciti.

Con tale espressione, in senso lato intesa, ci si riferisce direttamente anche al controllo del contenuto del contratto e alle misure di riequilibrio delle asimmetrie non solo informative ma anche di potere contrattuale, di obblighi e diritti che scaturiscono dal contratto.[150]

---

[148] Così E. CECCHINATO, *I servizi di pagamento*, in *Il diritto bancario oggi: aspetti sostanziali processuali*, F. Aratari e Guido Romano (a cura di), Wolters Kluwer, 2023, p. 365 e ss.

[149] Dello stesso parere però non è A.A. DOLMETTA, *Trasparenza dei prodotti bancari*, Zanichelli, 2013. Egli ritiene infatti che l'art. 1337 c.c. che richiede alle parti di agire secondo buona fede durante le trattative precontrattuali fosse una norma che indirettamente richiamava la trasparenza degli istuti bancari che sono chiamati a comportarsi lealmente nei confronti dei propri utenti. L'A. in tal senso interpreta la trasparenza come una diretta applicazione del principio di buona fede nelle trattative contrattuali *ex* art. 1337 c.c.

[150] Così A. BARENGHI, *Note sulla Trasparenza Bancaria. Venticinque anni dopo,* in *Banca, Borsa, Tit. Cred.*, n. 2 del 2018, pp.163. Sulla trasparenza bancaria in generale, le più ampie trattazioni sono quelle di E. CAPOBIANCO *I contratti bancari*, in *Trattato*, M. RESCIGNO - E. GABRIELLI, Torino, 2016; MUCCIARONE, *La*

In questo quadro risulta decisivo il paragrafo 1.2 della Sezione I del provvedimento in esame, il quale ci fornisce un quadro riassuntivo degli obblighi di trasparenza imposti agli intermediari.

La predisposizione di una normativa in materia di trasparenza nasce dall'esigenza di disciplinare in maniera più incisiva i rapporti contrattuali che si instaurano in alcuni mercati, in questo caso nel mercato dei prodotti bancari e finanziari in generale, e in quello dei servizi di pagamento in particolare. È un settore in cui risultano piuttosto forti le esigenze di tutela del cliente in quanto quest'ultimo è in una posizione di svantaggio, cui risulta possibile rimediare soltanto fissando a priori le regole, qualificando l'informazione come un diritto dell'utente in modo che questi si trovi in una posizione quanto più possibile paritaria a quella del professionista.

Per quanto riguarda i servizi di pagamento, è di nostro interesse in tema di trasparenza soprattutto il capo II-*bis* del TUB di cui si dirà più specificamente nel prossimo paragrafo.

2.1. L'ambito di applicazione del capo II-bis TUB: "i servizi di pagamento"

Il capo II-*bis* del TUB è stato introdotto con il d.lgs. n. 11/2010 che ha portato all'inserimento degli artt. *126-bis – 126-octies*[151]: la modifica citata è importante in quanto stabilisce norme riguardanti la trasparenza delle condizioni contrattuali e dei rapporti con la clientela con riferimento

trasparenza bancaria, in *Trattato dei contratti*, V. ROPPO (a cura di), Milano, 2014, 663 ss.

[151] Con il D.lgs. 16 Aprile 2012, n.45 è stato inserito anche l'art. 126-*novies* che tratta delle Commissioni applicabili al rimborso della moneta elettronica.

ai servizi di pagamento. La nuova disciplina sembra «deviare dai canoni classici della trasparenza bancaria»[152], nel senso che differisce dalla disciplina dettata per la trasparenza degli altri servizi bancari nel Capo I del Titolo VI.

Si nota sin da una prima lettura del Titolo VI come il capo II-*bis* si presenti più asciutto e flessibile rispetto alla normativa generale contenuta nel capo I, questo perché si tratta di una disciplina più generale in quanto la normativa di dettaglio di questo capo in esame è poi affidata a Banca d'Italia.

Ai sensi del comma 1 dell'art. *126-bis* TUB «Il presente capo si applica ai contratti quadro[153] relativi a servizi di pagamento e alle operazioni di pagamento[154], anche se queste non rientrano in un contratto quadro, quando i servizi sono offerti sul territorio della Repubblica» specificando al secondo comma che per servizio di pagamento si intende anche l'emissione di moneta elettronica con la precisazione che «allo Stato italiano, agli altri Stati comunitari e alle pubbliche amministrazioni statali, regionali

---

[152] In tal senso E. CECCHINATO, *I servizi di pagamento*, *op. cit.*; nonché B. PIACENTINI, *La trasparenza nei servizi di pagamento: il provvedimento di Banca d'Italia 20 Giugno 2012, op. cit.*

[153] Da intendersi come «il contratto che disciplina la futura esecuzione di operazioni di pagamento singole e ricorrenti che può dettare gli obblighi e le condizioni che le parti devono rispettare per l'apertura e la gestione di un conto di pagamento» così definito al par. 2 della sez. VI del Provvedimento del 29/07/2009.

[154] Intendendosi «l'attività, posta in essere dal pagatore o dal beneficiario, di versare, trasferire o prelevare fondi, indipendentemente da eventuali obblighi sottostanti tra pagatore e beneficiario» così definito al par. 2 della sez. VI del Provvedimento del 29/07/2009.

e locali, che agendo in veste di pubblica Autorità, emettono moneta elettronica, si applica soltanto l'art. *126-nonies*[155]».

Per cominciare, le disposizioni del capo II-bis non distinguono tra consumatore e non consumatore, come invece fanno i due capi precedenti e quello successivo, questo perché i servizi di pagamento vengono ricondotti ad una disciplina unitaria, della quale possono beneficiare anche i professionisti e le imprese, in veste di utenti del servizio.[156] Per quanto riguarda l'ambito soggettivo di applicazione di questo capo, le tutele previste sono a vantaggio del "cliente" dell'intermediario o "utente" del servizio[157] ossia «la persona fisica o giuridica che

[155] Il cui testo dell'articolo 126-*nonies* afferma: «1. Il rimborso della moneta elettronica previsto dall'articolo 114 ter può essere soggetto al pagamento di una commissione adeguata e conforme ai costi effettivamente sostenuti dall'emittente, solo se previsto dal contratto e in uno dei seguenti casi: a) il rimborso è chiesto prima della scadenza del contratto; b) il detentore di moneta elettronica recede dal contratto prima della sua scadenza; c) il rimborso è chiesto più di un anno dopo la data di scadenza del contratto. 2. I soggetti, diversi da un consumatore, che accettino in pagamento moneta elettronica possono regolare in via contrattuale con l'emittente di moneta elettronica le condizioni del rimborso loro spettante nei suoi confronti, anche in deroga al comma 1. 3. L'emittente di moneta elettronica fornisce al detentore, prima che egli sia vincolato da un contratto o da un'offerta, le informazioni relative alle modalità e alle condizioni del rimborso, secondo quanto stabilito dalla Banca d'Italia. 4. Il contratto tra l'emittente e il detentore di moneta elettronica indica chiaramente ed esplicitamente le modalità e le condizioni del rimborso».

[156] In tal senso E. CECCHINATO, *I servizi di pagamento*, *op. cit.*, pp. 384 e ss.

[157] "clienti" o "clientela" sono definiti come gli utenti di servizi di pagamento dal par. 2 della sez. VI del Provvedimento del 29/07/2009.

utilizza un servizio di pagamento in veste di pagatore[158] o beneficiario o di entrambi»[159].

Una applicazione indistinta dell'intero comparto legisaltivo, che non fa differenze tra consumatori e non consumatori, potrebbe rivelarsi talvolta inefficiente, specialmente per quanto riguarda quei soggetti che possono rapportarsi con l'intermediario in un rapporto di parità. È per questo che il comma 3 dell'art. 126-*bis* precisa che le previsioni del Capo II-*bis* possono non applicarsi, in tutto o in parte, previo accordo delle parti, se l'utente del servizio di pagamento non è un consumatore o una microimpresa. Ai sensi di tale comma, quando nella trattativa sono coinvolte categorie particolari di soggetti (consumatori e microimprese), il legislatore non consente alle parti di disporre modifiche a tale disciplina, al fine di evitare situazioni che possano in qualche modo andare a scapito della parte debole e le tutele di cui al capo II-bis sembrerebbero quindi irrinunciabili solamente per il consumatore e microimpresa.

Prima di passare a una analisi del contenuto sostanziale è bene evidenziare che talvolta le disposizioni del TUB e quelle del Codice del consumo, in materia di commercializzazione a distanza di servizi finanziari, possono sovrapporsi e non sempre è semplice stabilire quale sia la normativa applicabile, ma è intervenuto il legislatore, il quale ha elaborato alcuni criteri al fine di risolvere il conflitto tra le normative.[160]

---

[158] Da intendersi «la persona fisica o giuridica detentrice di un conto di pagamento che autorizza l'ordine di pagamento a partire da detto conto di pagamento o, in mancanza di conto di pagamento, una persona fisica o giuridica che dà l'ordine di pagamento» così definito al par. 2 della sez. VI del Provvedimento del 29/07/2009.

[159] Così definito al par. 2 della sez. VI del Provvedimento del 29/07/2009.

[160] Così E. CECCHINATO, *I servizi di pagamento*, *op. cit*, pp. 384 e ss.

Al fine di coordinare le due normative in tema di obblighi informativi, il legislatore ha stabilito come regola generale l'art. *67-decies,* comma 1, Codice del Consumo «Oltre alle informazioni di cui agli articoli 67-quater, 67-quinquies, 67-sexies, 67-septies e 67-octies sono applicabili le disposizioni più rigorose previste dalla normativa di settore che disciplina l'offerta del servizio o del prodotto interessato».

2.2 Gli obblighi di informativa

Il tema in questione è sicuramente disciplinato in maniera più puntuale nel Provvedimento del 29/07/2009. L'art. 126-*quater*, comma 1, *TUB* si limita a stabilire che «le informazioni e le condizioni sono redatte in termini di facile comprensione e in forma chiara e leggibile» e continua precisando che, «in particolare, l'utilizzatore dei servizi di pagamento è informato di tutte le spese dovute al prestatore di servizi di pagamento e la loro suddivisione. Sono previsti obblighi di trasparenza semplificati nel caso di utilizzo di strumenti di pagamento che riguardino operazioni o presentino limiti di spesa o di avvaloramento inferiori a soglie fissate dalla stessa Banca d'Italia».

Tale articolo conferisce un'ampia delega a Banca d'Italia a precisare il contenuto dell'informativa cui l'intermediario è tenuto nei confronti della clientela. Si può affermare che il legislatore nazionale si è espresso in termini fin troppo generali[161] all'art. 124-*quater*, specie se si fa un confronto con i capi precedenti. Questa scelta del legislatore nazionale di recepire la disciplina comunitaria non attraverso le norme di rango

[161] Così critico sul contenuto E. CECCHINATO, *I servizi di pagamento*, *op. cit.*, p. 387.

primario, ma attraverso la regolamentazione dell'Autorità di Vigilanza, non deriva da uno scarso interesse del legislatore per la materia, bensì è data dal fatto che permette a eventuali aggiornamenti della *PSD2*[162] in materia di informativa, di non rimanere bloccati nell'iter legislativo, ma di poter essere regolamentati in maniera più celere dall'Autorità.[163]

La disciplina comunitaria non è stata quindi recepita interamente all'interno del Testo Unico, ma dalle previsioni del Provvedimento del 29/07/2009 dove alla sez. VI viene disciplinata sia l'informativa precontrattuale (par. 4), sia le comunicazioni alla clientela nel corso del rapporto (par. 6).

Per quanto riguarda l'informativa pubblicitaria, questa sembra non essere disciplinata né dalla *PSD2*, né dall'art. 124-*quater*. Tuttavia, l'Autorità di vigilanza rimedia alla lacuna assoggettando i servizi di pagamento alle disposizioni del par. 5 della sez. II sugli annunci pubblicitari. La sezione II del provvedimento si intitola «Pubblicità e informazione precontrattuale» e, quindi, trova piena applicazione anche per quanto riguarda i servizi di pagamento per quanto non diversamente disciplinato dalla sezione come dice la norma[164]. Il

---

[162] Come, tra l'altro, sta avvenendo in questo determinato momento, in quanto il 23 Aprile 2024 il Parlamento Europeo ha approvato nella plenaria i testi emendati della terza direttiva sui servizi di pagamento.

[163] Si veda B. PIACENTINI, *La trasparenza nei servizi di pagamento: il provvedimento di Banca d'Italia 20 Giugno 2012, op. cit.,* pp. 352 e ss.

[164] Sez. VI, par. 3.1 « Per quanto non diversamente disciplinato dalla presente sezione si applicano, inoltre, le disposizioni contenute nella sezione I (disposizioni di carattere generale); sezione II, paragrafi 1, 3, 4 (4), 5 (premessa, fogli informativi, offerta fuori sede, annunci pubblicitari) e 7 (documento di sintesi);

foglio informativo costituisce il vero e proprio documento dell'offerta rivolta al pubblico e viene messo dagli intermediari a disposizione dei clienti presso le filiali o sul proprio sito internet, questo sembra destinato a rendere il cliente consapevole dei termini complessivi del rapporto contrattuale che si intende instaurare con il prestatore ed in grado di operare anche raffronti con le altre offerte presenti sul mercato.[165] Bisogna evidenziare che solitamente, le condizioni offerte al pubblico sono standardizzate e non risultano in alcun modo personalizzabili.

Quando si giunge alla conclusione del contratto, il provvedimento prevede la necessità di rispettare requisiti di forma e di contenuto del medesimo. Per quanto riguarda i primi la previsione generale è quella per cui i contratti sono redatti in forma scritta *ad substantiam* e un esemplare viene consegnato al cliente[166], il quale ne attesta il ricevimento mediante apposita sottoscrizione, ulteriore rispetto alla firma del contratto ed apposta sull'esemplare custodito dall'intermediario.

Vengono poi previsti obblighi di informazione semplificati nel caso di utilizzo di strumenti di pagamento destinati a micropagamenti,

---

sezione III (contratti), secondo quanto previsto dal paragrafo 5 della presente sezione; sezione V (tecniche di comunicazione a distanza), salvo quanto previsto dal paragrafo 4.1.2 della presente sezione; sezione X (controlli). La sezione XI (requisiti organizzativi) si applica secondo quanto previsto dal paragrafo 1 della stessa sezione. Ai contratti disciplinati dalla presente sezione che incorporano una componente creditizia (carte di credito) e che sono commercializzati presso consumatori si applica la sezione VII, secondo quanto previsto dal paragrafo 7 della medesima sezione».

[165] In tal senso si v. B. PIACENTINI, *La trasparenza nei servizi di pagamento: il provvedimento di Banca d'Italia 20 Giugno 2012, op. cit.*, p. 352.

[166] La disciplina legislativa in materia di forma dei contratti relativi alla prestazione di servizi di pagamento risulta dal combinato disposto tra il testo dell'art. 126-*quinquies* ed il testo dell'art. 117 *TUB*. Nel caso di inosservanza della forma prescritta il contratto è nullo e la nullità può essere fatta valere solo dal cliente.

questo al fine di operare un effettivo bilanciamento degli interessi: infatti occorre tenere presente che l'adempimento degli obblighi di informazione e trasparenza comporta un costo per il prestatore dei servizi di pagamento, il quale finisce per essere traslato sull'utente finale del servizio medesimo: Banca d'Italia ha quindi mitigato questi obblighi informativi tenendo presente il fine ultimo, che è quello della massima efficienza del sistema dei pagamenti.[167]

Per quanto riguarda l'assolvimento degli obblighi informativi spetta all'intermediario darne dimostrazione, l'art. 126-*bis*, comma 4 stabilisce che «spetta al prestatore dei servizi di pagamento l'onere della prova di aver correttamente adempiuto agli obblighi previsti dal presente capo».[168]

2.3 Lo Ius Variandi

Il capo II-*bis* prosegue con l'art. 126-*sexies* che tratta lo *ius variandi*, un tema alquanto delicato in quanto riguarda il potere dell'intermediario di disporre unilateralmente delle modifiche del contratto.

---

[167] Ancora si v. B. PIACENTINI, *La trasparenza nei servizi di pagamento: il provvedimento di Banca d'Italia 20 Giugno 2012, op. cit.*

[168] Sul punto E. CECCHINATO, *I servizi di pagamento*, *op. cit*, pp. 384 e ss..; in argomento si veda anche A. MIRONE, *Profili evolutivi della trasparenza bancaria*, in Osservatorio del diritto civile e commerciale, n. 1 – 2018, pp. 55-58

Le modifiche alle quali ci si riferisce sono sia quelle sfavorevoli al cliente, sia le modifiche favorevoli ad esso.[169]

Al comma 1 si legge che: «Ogni modifica del contratto quadro o delle condizioni e informazioni a esso relative fornite all'utilizzatore ai sensi dell'articolo 126-*quater*, comma 1, lettera *a)*, è proposta dal prestatore dei servizi di pagamento secondo le modalità stabilite dalla Banca d'Italia, con almeno due mesi di anticipo rispetto alla data di applicazione indicata nella proposta», ciò significa che qualora alla proposta formulata dall'intermediario non seguisse l'accettazione del cliente, le modifiche effettuate sono prive di effetto. A meno che il contratto non contenga un meccanismo di silenzio-assenso come delineato dal comma 2, il quale recita che «Il contratto quadro può prevedere che la modifica delle condizioni contrattuali si ritiene accettata dall'utilizzatore a meno che questi non comunichi al prestatore dei servizi di pagamento, prima della data indicata nella proposta per l'applicazione della modifica, che non intende accettarla. In questo caso, la comunicazione di cui al comma 1, contenente la proposta di modifica, specifica che in assenza di espresso rifiuto la proposta si intende accettata e che l'utilizzatore ha diritto di recedere senza spese prima della data prevista per l'applicazione della modifica».

Questo significa che in assenza di espresso rifiuto da parte del cliente, la proposta deve intendersi accettata e qualora il cliente non intenda accettare la proposta, potrà comunque recedere dal contratto.[170]

---

[169] Per approfondimenti si veda M. ONZA, *La trasparenza dei servizi di pagamento in Italia*, in *Banca, Borsa e tit. cred.*, n. 5/2013, pp. 614-615

[170] Si rimanda ancora a E. CECCHINATO, *I servizi di pagamento*, *op. cit.*, pp. 384 e ss.

Si propone al cliente, il cui contratto è soggetto alla modifica, la possibilità di valutare l'alternativa tra più strumenti diversi: uno di adeguamento e uno risolutorio. In particolare, il cliente può espressamente rifiutare la variazione proposta e quindi conservare il contratto alle condizioni originarie o nel caso di un non rifiuto espresso (o consenso tacito) di accettare le modifiche salva la possibilità di recedere dal contratto.[171]

Questo *modus operandi* è confermato dal par. 5.2 della sez. VI del Provvedimento del 29/07/2009 di Banca d'Italia dove si legge che «il contratto può prevedere che le modifiche si ritengono accettate se il cliente non recede entro la data indicata nella proposta per la loro applicazione; in questo caso la comunicazione precisa tale circostanza e richiama l'attenzione del cliente sul suo diritto di recedere senza spese».

Ci si chiede se tale disciplina riguardi solo le "modifiche" o si intendano anche le "integrazioni" al contratto, interpretando il concetto di "modifica" in senso lato. Una circolare interna del Ministero dello Sviluppo Economico[172] sembrerebbe preferire però una interpretazione restrittiva.[173]

---

[171] Sul tema si v. M. GAMBINI, *Ius variandi bancario e finanziario,* in *Banca, Borsa e tit. cred.*, n. 4/2012, pp. 424 ss.

[172] Circolare del Ministero dello Sviluppo Economico del 21/02/2007 recante "Chiarimenti in merito all'applicazione dell'art. 10 della legge 4 agosto 2006, n. 248 in www.mise.gov.it

[173] Tale circolare fa riferimento all'art.118 *TUB* ma le considerazioni sembrano applicabili anche all'art. 126-sexies e chiarisce che «le modifiche disciplinate dal nuovo articolo 118 TUB, riguardando soltanto le fattispecie di variazioni previste dal contratto, non possono comportare l'introduzione di clausole *ex novo*».

Un trattamento di favore è previsto per il cliente consumatore al comma 4-*bis* il quale statuisce che «Se il cliente è un consumatore, il contratto quadro o le condizioni e informazioni a esso relative fornite all'utilizzatore ai sensi dell'articolo 126-*quater*, comma 1, lettera *a)*, possono essere modificate se sussiste un giustificato motivo». Possono costituire «giustificato motivo»[174] solo quelle circostanze successive alla stipula del contratto che non siano imputabili all'intermediario e che siano in grado di alterare l'originale equilibrio contrattuale.[175]

Anche se non espressamente richiamato dall' art. 126-*sexies*, si ritiene che allo *ius variandi* siano applicabili i principi di correttezza e buona fede, i quali impongono al titolare dello *ius variandi*, ad esempio, di non esercitare il suo diritto in situazioni o con modalità che, tenuto conto delle circostanze del caso concreto, si dimostrino ispirate a ragioni futili o pretestuose, di non discostarsi dal comportamento usualmente tenuto nello svolgimento dei suoi rapporti contrattuali con la clientela e così via tutti quei comportamenti che non integrano il principio generale di buona fede.[176]

---

[174] Il richiamo al requisito del giustificato motivo apre, inoltre, la strada ad un controllo giudiziale sulle ragioni del singolo atto di esercizio del potere modificativo, che consente di ampliare gli spazi di tutela delle ragioni della parte destinata a subire la variazione.

[175] La circolare del Ministero dello Sviluppo Economico richiamata poco sopra precisa che con la nozione di "giustificato motivo" «deve intendersi nel senso di ricomprendere gli eventi di comprovabile effetto sul rapporto bancario. Tali eventi possono essere sia quelli che afferiscono alla sfera del cliente, sia quelli che consistono in variazioni di condizioni economiche generali che possono riflettersi in un aumento dei costi operativi degli intermediari».

[176] Si v. M. GAMBINI, *Ius variandi bancario e finanziario, op. cit.*, pp. 424 e ss.

2.4 Il recesso

Mentre lo *ius variandi* è un istituto unilaterale a favore delle banche, il recesso è un istituto bilaterale, che regola una facoltà spettante ad entrambe le parti. *Ius variandi* e recesso sono strettamente legati tra di loro, prima di tutto perché il recesso costituisce il rimedio tipico a disposizione del cliente in caso di modificazione unilaterale delle condizioni da parte della banca, e poi perché il recesso unilaterale potrebbe costituire un modo per la banca di imporre modifiche contrattuali non gradite alla controparte. [177]

L'articolo che se ne occupa in tema di servizi di pagamento è l'art. 127-*septies* del *TUB*. Tale diritto di recesso, come detto, si presta a una duplice funzione: una difensiva, nel procedimento di modificazione del contenuto delle informazioni sul contratto quadro e l'altra tesa a liberare anticipatamente le parti dal vincolo contrattuale[178].

Il comma 1 recita: «L'utilizzatore di servizi di pagamento ha sempre la facoltà di recedere dal contratto quadro senza penalità e senza spese di chiusura». Si noti come, a differenza dell'art. 120-*bis*[179] che si occupa di una tutela del cliente più generale, non si fa qui riferimento al contratto di durata. Infatti, il cliente potrà recedere senza penalità e senza spese di chiusura sia

[177] Per approfondimenti A. MIRONE, *La rilevanza del tempo nella disciplina dei rapporti bancari*, in *Banca, Borsa e tit. cred.*, n. 4/2016, pp. 422-423.

[178] In tal senso si v. M. ONZA, *La trasparenza dei servizi di pagamento in Italia*, *op. cit.*, pp. 614-615.

[179] «Il cliente ha diritto di recedere in ogni momento da un contratto a tempo indeterminato senza penalità e senza spese».

nel caso in cui sia previsto un termine per il rapporto sia nel caso in cui questo sia a tempo indeterminato.[180]

Per quanto riguarda invece il recesso dell'intermediario, il comma 2 prevede che: «Il prestatore di servizi di pagamento può recedere da un contratto quadro a tempo indeterminato se ciò è previsto dal contratto e con un preavviso di almeno due mesi, secondo le modalità stabilite dalla Banca d'Italia», tali modalità sono «la forma scritta, su supporto cartaceo o su altro supporto durevole concordato con il cliente».

La disposizione si conclude al comma 3 stabilendo che «in caso di recesso dal contratto dell'utilizzatore o del prestatore di servizi di pagamento, le spese per i servizi fatturate periodicamente sono dovute dall'utilizzatore solo in misura proporzionale per il periodo precedente al recesso; se pagate anticipatamente, esse sono rimborsate in maniera proporzionale.

3. Le dinamiche dell'operazione di pagamento: il d.lgs. 11/2010

Nella disamina della normativa in tema di servizi di pagamento di fondamentale importanza è il già citato d.lgs. n. 11/2010 «*attuazione della direttiva 2007/64/CE, relativa ai servizi di pagamento nel mercato interno, recante modifica delle direttive 97/7/CE, 2002/65/CE, 2006/48/CE, e che abroga la*

[180] In tal senso si v. E. CECCHINATO, *I servizi di pagamento*, *op. cit.*, p.395; si v. anche M. DE POLI, sub *art. 126*-septies,.in Capriglione.(dir..da), *Commentario al Testo Unico delle Leggi in Materia Bancaria e Creditizia*, t. III, cit., pp. 2279 ss; critico sulla differenza di disciplina tra rapporti a tempo determinato e a tempo indeterminato A. MIRONE, *La rilevanza del tempo nella disciplina dei rapporti bancari*, *op. cit.*, pp. 422 e ss.

direttiva 97/5/CE» riguardante le dinamiche delle operazioni di pagamento.

Il primo articolo riguarda alcune questioni definitorie, come la definizione di "consumatore"[181], "servizio di informazione sui conti"[182], "servizio di pagamento"[183] e altre.

La definizione cruciale[184] del decreto è sicuramente quella dei "servizi di pagamento", la quale rinvia a quella data dal TUB, questo perché contribuisce a delimitare i destinatari della disciplina del Titolo II del d.lgs. n. 11 del 2010.

Per quanto riguarda il suo ambito di applicazione il comma 1 dell'art. 2 recita che «il presente decreto si applica ai servizi di pagamento prestati in euro o nella valuta ufficiale di uno Stato membro non appartenente all'area dell'euro o di uno Stato appartenente allo Spazio economico europeo»; al comma 2 dello stesso articolo invece vengono elencate tutte le esclusioni come ad esempio: a) le operazioni di pagamento effettuate esclusivamente in contante direttamente dal pagatore al beneficiario, senza alcuna intermediazione; b) operazioni di pagamento dal pagatore al beneficiario effettuate tramite un agente commerciale autorizzato a negoziare o concludere la

---

[181] Inteso come «la persona fisica di cui all'articolo 3, comma 1, lettera a), del decreto legislativo 6 settembre 2005, n. 206, e successive modificazioni».

[182] Inteso come «un servizio online che fornisce informazioni relativamente a uno o più conti di pagamento detenuti dall'utente di servizi di pagamento presso un altro prestatore di servizi di pagamento o presso più prestatori di servizi di pagamento».

[183] La cui elencazione è già stata presa in considerazione nel precedente capitolo e a cui si rimanda.

[184] Così P.M. REEDTZ in *commentario al Decreto legislativo n.11/2010*, Giappichelli, p. 8.

vendita o l'acquisto di beni o servizi per conto del pagatore o del beneficiario, *etc.*[185]

[185] «c) trasporto materiale, a titolo professionale, di banconote e monete, ivi compresa la raccolta, il trattamento e la consegna; d) operazioni di pagamento consistenti nella raccolta e nella consegna di contante, a titolo non professionale, nel quadro di un'attività senza scopo di lucro o a fini di beneficenza; e) servizi in cui il beneficiario fornisce contante al pagatore nel contesto di un'operazione di pagamento, a seguito di una richiesta esplicita del pagatore di servizi di pagamento immediatamente precedente l'esecuzione dell'operazione di pagamento attraverso un pagamento destinato all'acquisto di beni o servizi; f) operazioni di cambio di valuta contante contro contante nell'ambito delle quali i fondi non sono detenuti su un conto di pagamento; g) operazioni di pagamento basate su uno dei seguenti tipi di documenti cartacei, con i quali viene ordinato al prestatore di servizi di pagamento di mettere dei fondi a disposizione del beneficiario: assegni, titoli cambiari, voucher, traveller's cheque, vaglia postali; h) operazioni di pagamento realizzate all'interno di un sistema di pagamento o di un sistema di regolamento dei titoli tra agenti di regolamento, controparti centrali, stanze di compensazione e/o banche centrali e altri partecipanti al sistema e prestatori di servizi di pagamento, fatto salvo l'articolo 30; i) operazioni di pagamento collegate all'amministrazione degli strumenti finanziari, compresi i dividendi, le entrate o altre distribuzioni, o ai rimborsi o proventi di cessioni, effettuate dalle persone di cui alla lettera h), ovvero da imprese di investimento, enti creditizi, organismi di investimento collettivo o società di gestione patrimoniale che prestano servizi di investimento ed ogni altra entità autorizzata ad avere la custodia di strumenti finanziari; l) servizi forniti dai prestatori di servizi tecnici, che supportano la prestazione dei servizi di pagamento, senza mai entrare in possesso dei fondi da trasferire, compresi l'elaborazione e la registrazione di dati, i servizi fiduciari e di protezione dei dati personali, l'autenticazione dei dati e delle entità, la fornitura di reti informatiche e di comunicazione, la fornitura e la manutenzione di terminali e dispositivi utilizzati per i servizi di pagamento; m) servizi basati su strumenti che possono essere utilizzati per acquistare beni o servizi solo nella sede utilizzata dall'emittente o in base ad un accordo commerciale con l'emittente, all'interno di una rete limitata di prestatori di servizi o per una gamma limitata di beni o servizi; n) operazioni di pagamento eseguite tramite qualsiasi dispositivo di telecomunicazione, digitale o informatico, quando i beni o servizi acquistati sono consegnati al dispositivo di

L'obiettivo primario di tale decreto è quello di disciplinare i diritti e gli obblighi delle parti nell'operazione di pagamento, dal momento della loro autorizzazione a quello della loro esecuzione, avendo un occhio di riguardo per i numerosi progressi tecnologici di questi ultimi anni. Si può dire che complessivamente il decreto realizza un buon bilanciamento tra l'esigenza di assicurare un efficiente funzionamento del mercato dei pagamenti e quella di tutelare la clientela dagli intermediari. [186]

3.1 Autorizzazione del pagamento

Il Capo II del Titolo II del decreto in esame si occupa dell'autorizzazione delle operazioni di pagamento di cui si riporta la definizione di cui al primo comma lett. c): «l'attività, posta in essere dal pagatore o dal beneficiario, di versare, trasferire o prelevare fondi,

telecomunicazione, digitale o informatico, o devono essere utilizzati tramite tale dispositivo, a condizione che l'operatore di telecomunicazione, digitale o informatico, non agisca esclusivamente quale intermediario tra l'utilizzatore di servizi di pagamento e il fornitore dei beni e servizi; o) operazioni di pagamento realizzate tra prestatori di servizi di pagamento, relativi agenti o succursali per proprio conto; p) operazioni di pagamento tra un'impresa madre e la relativa filiazione, o tra filiazioni della stessa impresa madre, senza alcuna intermediazione da parte di un prestatore di servizi di pagamento diverso da una delle imprese appartenenti al medesimo gruppo; q) servizi, forniti da prestatori, di prelievo di contante tramite sportelli automatici per conto di uno o più emittenti della carta, che non sono parti del contratto quadro con il cliente che preleva denaro da un conto di pagamento, a condizione che detti prestatori non gestiscano altri servizi di pagamento elencati nell'articolo 1».

[186] Così nel suo riepilogo E. CECCHINATO, *I servizi di pagamento*, *op. cit.*, p. 412.

indipendentemente da eventuali obblighi sottostanti tra pagatore e beneficiario».

L'articolo che tratta l'autorizzazione è l'art. 5 intitolato «consenso e revoca del consenso». Al comma 1 afferma che «Il consenso del pagatore è un elemento necessario per la corretta esecuzione di un'operazione di pagamento. In assenza del consenso, un'operazione di pagamento non può considerarsi autorizzata», ciò significa che qualsiasi pagamento deve avere la previa autorizzazione del pagatore per il c.d. *principle of consent*[187].

La disposizione appena richiamata potrebbe sembrare un po' ridondante e poco precisa, parlando prima di "consenso" e poi di "autorizzazione".[188]

Per quanto riguarda le modalità con cui deve essere prestato il consenso, al comma 2 si legge che «Il consenso ad eseguire un'operazione di pagamento o una serie di operazioni di pagamento è prestato nella forma e secondo la procedura concordata nel contratto quadro o nel contratto relativo a singole operazioni di pagamento», precisando al comma successivo riguardo ai tempi, che «l'autorizzazione può essere data prima o, ove concordato tra il pagatore e il proprio prestatore di servizi di pagamento, dopo l'esecuzione di un'operazione di pagamento».

Sempre con rigurdo allo stesso articolo, al comma 4, si fa riferimento alla revoca del pagamento «Il consenso può essere revocato in

---

[187] Secondo questo principio il consenso deve essere esplicito, il che si verifica quando qualcuno acconsente esplicitamente all'operazione di pagamento. Si veda E. CECCHINATO, *I servizi di pagamento*, *op. cit.*, p. 402.

[188] Così in maniera critica sempre E. CECCHINATO, *I servizi di pagamento*, *op. cit.*, p. 403.

qualsiasi momento, nella forma e secondo la procedura concordata nel contratto quadro o nel contratto relativo a singole operazioni di pagamento, purché prima che l'ordine di pagamento diventi irrevocabile ai sensi dell'articolo 17[189]. Le operazioni di pagamento eseguite dopo la revoca del consenso ad eseguire più operazioni di pagamento non possono essere considerate autorizzate».[190]

La revoca altro non è che la comunicazione alla propria banca di voler ritirare l'ordine di addebito già ordinato alla banca esecutrice.[191]

L'art. 17[192] affronta il tema della irrevocabilità dopo che il pagatore abbia trasmesso l'ordine al beneficiario o dopo che egli abbia dato il consenso ad eseguirlo. Questo articolo si riferisce alle operazioni effettuate tramite carte di pagamento, non agli

---

[189] Comma 2 art. 17 «Fatto salvo quanto previsto all'articolo 5, comma 4, se l'operazione di pagamento è disposta su iniziativa del beneficiario o per il suo tramite, il pagatore non può revocare l'ordine di pagamento dopo averlo trasmesso al beneficiario o avergli dato il consenso ad eseguire l'operazione di pagamento.»

[190] V. PROFETA, *I third party provider: profili soggettivi e oggettivi*, in *Le nuove frontiere dei servizi bancari e di pagamento fra PSD 2, criptovalute e rivoluzione digitale*, a cura di F. MAIMERI e M. MANCINI, in *Quaderni di ricerca giuridica della consulenza legale di Banca d'Italia*, n. 87, 2019, pp. 49 e ss.

[191] Cfr. Circolare Abi, *Serie tecnica n. 14 – 31 marzo 2010*, Bancaria ed., 6, *sub* art. 5, in cui si sottolinea che il consenso viene espresso, nell'addebito diretto, dal pagatore attraverso la sottoscrizione e la consegna del mandato alla propria banca; poco più sotto la Circolare richiama il fatto che, ove l'addebito abbia ad oggetto il consenso ad eseguire più operazioni di pagamento, le operazioni di pagamento successive non possono essere autorizzate (art. 4 d. lgs. 11/2010).

[192] Per approfondimenti si v. M.C. LUPACCHINO, *Commento all'art. 17,* in *Aa.Vv., La nuova disciplina dei servizi di pagamento. Commentario al d.lgs. 27 gennaio 2010, n. 11*, Giappichelli, 2011, pp. 192 ss.

addebiti diretti per i quali invece si deve guardare al comma 3[193], il quale sostiene che il pagatore può revocare l'ordine non oltre la fine della giornata operativa precedente il giorno concordato per l'addebito dei fondi. Una volta scaduti i tempi utili per aversi la revoca, l'ordine di pagamento può essere revocato solo se concordato tra l'utilizzatore ed il proprio prestatore di servizi e sussistendo il consenso del beneficiario.[194]

Le operazioni di pagamento eseguite dopo la revoca del consenso non possono essere considerate autorizzate.

Va evidenziato che la progressiva digitalizzazione dei servizi di pagamento e l'incremento dei rischi di frode hanno spinto il legislatore a rivedere i criteri con cui una operazione si considera autorizzata, e quali sono gli "step" che devono essere compiuti per autorizzarla. Si fa qui riferimento alla autenticazione forte del cliente di cui si è già discusso, la quale è uno standard tecnico previsto dal regolamento delegato (UE) 2018/389 della Commissione imposto agli intermediari.

Va tenuto in considerazione che il consenso per compiere operazioni di pagamento può essere prestato anche mediate un terzo intermediario, ossia il prestatore di servizi di disposizione di ordini di

[193] Comma 3 art 17: «Nel caso di addebito diretto e fatti salvi i diritti di rimborso, il pagatore può revocare l'ordine di pagamento non oltre la fine della giornata operativa precedente il giorno concordato per l'addebito dei fondi. Il prestatore di servizi di pagamento del pagatore dà tempestiva comunicazione della revoca al prestatore di servizi di pagamento del beneficiario, ove le modalità e i tempi di effettuazione della revoca lo consentano».

[194] Si veda G. B. BARILLÀ, *Dal rid al nuovo addebito diretto SEPA*, in *Analisi Giuridica dell'Economia*, n. 1/2015, pp. 85 ss.

pagamento, i cd. *PISP* di cui si parlava sopra al paragrafo 1.1 del capitolo [195].

La disposizione di un ordine di pagamento impartito da un *PISP* da solo l'avvio ad un'operazione che verrà eseguita da e verso prestatori diversi. Il servizio di fornitura di informazioni relative ai dati contenuti nei conti di pagamento ha un carattere del tutto accessorio rispetto all'operazione di pagamento, alla quale non inerisce se non al fine di dare all'utente conoscenza più immediata dell'esistenza e della quantità di fondi disponibili.[196]

Si noti che nel caso di prestatori terzi – *TPP* – il consenso avviene in maniera informatica (anche se invero è da precisare che ormai, al di là che sia coinvolto o meno un *TPP*, il consenso è sempre informatizzato), considerando la natura informatica dell'attività da essi svolta e le modalità con cui essi interagiscono con gli utenti.[197]

In quanto il requisito del consenso è fondamentale per l'operazione, all'intermediario è richiesto di rifiutare l'accesso al conto di pagamento al *PISP* in diverse ipotesi: quando riscontra l'accesso fraudolento o non autorizzato al conto di pagamento dell'utente, compresi i casi di ordini di pagamento fraudolenti o non autorizzati, o quando riceve dall'utente la revoca del

---

[195] Si veda per ulteriori approfondimenti V. PROFETA, *I third party provider: profili soggettivi e oggettivi*, in *Le nuove frontiere dei servizi bancari e di pagamento fra PSD 2, criptovalute e rivoluzione digitale*, *cit.*

[196] Al riguardo V. DE STASIO, *Operazione di pagamento non autorizzata e restituzioni*, Giuffrè, Milano, 2016, pp. 141-151

[197] BANCA D'ITALIA, *I pagamenti nel commercio elettronico: una mappa per orientarsi*, reperibile al sito www.bancaditalia.it

consenso alla prestazione del servizio di disposizione[198], ma in tal caso dovrà informare immediatamente di ciò anche i terzi *provider* coinvolti (art. 6-bis, comma 3, d.lgs 11/2010).[199]

Il citato art. 6-bis si intitola «Limiti all'accesso ai conti di pagamento da parte dei prestatori di servizi di pagamento» e assimila alle ipotesi di accesso non autorizzato al conto, le ipotesi di ordini di pagamento fraudolenti o non autorizzati e l'individuazione di questi ultimi comporta una attenta valutazione delle ipotesi in cui il consenso all'operazione di pagamento correttamente prestato sia stato successivamente legittimamente revocato dall'utente.

A tal riguardo merita menzione anche l'art. 5-ter «disposizioni per l'accesso ai conti di pagamento in caso di servizi di disposizione di ordine di pagamento», il quale detta importanti previsioni legislative con riguardo al prestatore di servizi di disposizione di ordine di pagamento.

Il primo comma è inerente al conto di pagamento che sia accessibile *on line*, e si legge che «il pagatore ha il diritto di avvalersi di un prestatore di servizi di disposizione di ordine di pagamento per il servizio di pagamento di cui all'articolo, 1, comma 2, lettera h-septies.1), n. 7, del decreto legislativo 1° settembre 1993, n. 385».

Al secondo comma si leggono poi una serie di indicazioni che riguardano il prestatore di servizi di disposizione di ordine di pagamento: «a) non detiene in alcun momento i fondi del pagatore in relazione alla prestazione del servizio di disposizione di ordine di pagamento; b)

---

[198] In tal senso il combinato dei commi 2 e 4 dell'art. 5 d.lgs. 11/2010

[199] Si veda in questo senso G. BERTI DE MARINIS, *La disciplina dei pagamenti non autorizzati nel nuovo sistema delineato dal recepimento della direttiva PSD2,* in *Diritto della Banca e del mercato finanziario*, 2018, pp. 645 e ss.

provvede affinché le credenziali di sicurezza personalizzate dal pagatore non siano accessibili ad altri fuorché al pagatore stesso e all'emittente delle credenziali di sicurezza personalizzate e che esse siano trasmesse attraverso canali sicuri ed efficienti (…)». Si tratta di modalità di comunicazione sicure alle quali sono obbligati tanto i prestatori di servizi di pagamento di radicamento del conto quanto i prestatori di servizi di disposizione di ordine di pagamento e di informazione sui conti.[200]

3.2 La corretta esecuzione del pagamento e la centralità dell'IBAN [201]

Il sistema di tutele così delineato dal legislatore ed accolto dalla giurisprudenza sembra ben capace di proteggere il cliente

---

[200] Per ulteriori approfondimenti si rimanda alla lettura integrale dell'art. 5-ter e 5-quater del d.lgs. 11/2010 in vigora dal 13/01/2018. Si v. anche V. PROFETA, *I third party provider: profili soggettivi e oggettivi*, *op. cit.* Per approfondimenti E. CERVONE, *Strumenti di pagamento innovativi, interoperabilità e neutralità tecnologica: quali regole e quale governance per un mercato sicuro, efficiente ed innovativo*, in Riv. trim. diritto dell'economia, 2016, p. 41; G. GIMIGLIANO e G. NAVA, *L'inquadramento giuridico dei Mobile payment: profili ricostruttivi e distonie regolamentari*, in Smart cities e diritto dell'innovazione a cura di G. OLIVIERI e V. FALCE, Milano, 2016, p.190.

[201] Acronimo di "*International Bank Account Number*" I codici IBAN italiani sono formati da 27 caratteri e sono composti da: 1) due caratteri della sigla nazionale ("IT"); 2) due numeri di controllo, calcolati sulla base degli altri caratteri dell'IBAN; 3) codice CIN (Control Internal Number), un carattere che serve a verificare la corretta trascrizione dei successivi 22 caratteri; 4) codice ABI (cinque caratteri assegnati dall'Associazione Bancaria Italiana per identificare la banca); 5) codice CAB (Codice di avviamento bancario),formato da cinque caratteri per individuare l'agenzia o la filiale dell'istituto di credito identificato dal codice ABI; 6) 12 caratteri per il numero di conto corrente (preceduto dagli zero nel caso in cui il numero del conto fosse inferiore ai 12 caratteri).

rispetto ad eventuali tentativi fraudolenti. Purtroppo, però, al giorno d'oggi diversi di questi tentativi sono attuati con una tecnica ancora più «subdola»[202] mostrando una "falla" nel sistema normativo.

In particolare, la situazione che si prospetta è la seguente: un criminale si inserisce nella corrispondenza a mezzo *mail* tra due soggetti legati da rapporti commerciali e, carpendo le credenziali dell'*account mail* del beneficiario del pagamento o attraverso un *account* con un nominativo simili a quello di quest'ultimo, indica al pagatore un diverso indirizzo al quale destinare i pagamenti. Quindi a questo punto il pagatore, raggirato, dispone il pagamento a favore dell'indirizzo IBAN indicatogli dal criminale.

Questo accade anche perché per la corretta esecuzione di un ordine di pagamento, viene attribuito un ruolo centrale all'identificativo unico IBAN; infatti l'art. 24 («identificativi unici inesatti») del decreto, al comma 1, stabilisce che «se un ordine di pagamento è eseguito conformemente all'identificativo unico, esso si ritiene eseguito correttamente per quanto concerne il beneficiario e/o il conto indicato dall'identificativo unico».

Al secondo comma si precisa che «se l'identificativo unico[203] fornito dall'utente è inesatto, il prestatore di servizi di pagamento non è responsabile, ai sensi dell'articolo 25, «della mancata o inesatta esecuzione dell'operazione di pagamento» tuttavia il prestatore di servizi di pagamento del pagatore è invitato a compiere «sforzi ragionevoli per recuperare i

---

[202] Così E. CECCHINATO, *I servizi di pagamento*, *op. cit.*, p. 409.

[203] Per approfondimenti in tema di disciplina del codice identificativo unico si veda M. C. LUPACCHINO, *sub art. 24*, in *La nuova disciplina dei servizi di pagamento*, a cura di MANCINI, RISPOLI FARINA, SANTORO, SCIARRONE ALIBRANDI e O. TROIANO, Giappichelli, 2011, 242 ss.

fondi oggetto dell'operazione di pagamento» anche collaborando con il prestatore di servizi di pagamento del beneficiario «comunicando al prestatore di servizi di pagamento del pagatore ogni informazione utile» ed eventualmente addebitando al cliente le spese sostenute ove concordato nel contratto-quadro.[204] Nel caso in cui non sia possibile il recupero dei fondi, il prestatore di servizi di pagamento del pagatore, su «richiesta scritta del pagatore è tenuto a fornirgli ogni informazione disponibile che sia utile ai fini di un'azione di tutela».

Nell'ordine di pagamento si indicano anche altri dati, come, ad es., il nominativo del beneficiario: quindi, viene spontaneo chiedersi se l'intermediario sia tenuto a verificare che l'IBAN indicato dal pagatore sia riferibile al nominativo del beneficiario; il comma 3 risponde a tale interrogativo specificando che «il prestatore di servizi di pagamento è responsabile solo dell'esecuzione dell'operazione di pagamento in conformità con l'identificativo unico fornito dall'utente anche qualora quest'ultimo abbia fornito al suo prestatore di servizi di pagamento informazioni ulteriori rispetto all'identificativo unico» e sia la giurisprudenza nazionale che quella comunitaria è particolarmente rigorosa nell'applicare questa regola.[205]

---

[204] Sul punto G. MARINO, *IBAN "sbagliato" e responsabilità delle banche nell'esecuzione dell'operazione di bonifico*, La nuova giurisprudenza civile commentata, n. 10, 2016, p.1266.

[205] Così E. CECCHINATO, *I servizi di pagamento*, *op. cit.* pp. 409 e ss.; riportando alcune pronunce sul punto per quanto riguarda la giurisprudenza a livello nazione quali App. Milano, sez. I, 16/07/2020, n. 1855, in *Giur. Comm.*, 2021, II, p. 1107 ss., con nota di Marasà; si v. Corte UE, sez. X, 21/03/2019, causa C-245/18, *Tecnoservice Int.*, in *Banca, borsa, tit. cred*, 2019, II, p. 653 ss. per quanto riguarda la giurisprudenza a livello comunitario.

Tale comma 3, nonostante in prima lettura possa risultare iniquo, ben si concilia con l'esigenza della celerità degli scambi, che verrebbe sicuramente compromessa qualora si imponesse agli intermediari di accertare la corrispondenza tra IBAN e nominativo del beneficiario del pagamento. Nella visione, prima del legislatore europeo, e poi di quello nazionale, si coglie come l'IBAN sia un elemento standard, una sorta di «alfabeto comune a tutti gli operatori del sistema dei pagamenti» [206]. Questo al fine di assolvere a una generale funzione di uniformazione e snellimento della circolazione monetaria di tipo intermediato, assicurando l'esatta esecuzione delle operazioni sui conti di pagamento.[207]

Nonostante la Commissione Europea stia lavorando al fine di prevenire le frodi, valutando l'obbligo di verificare la corrispondenza tra nome del beneficiario e identificativo unico (IBAN), l'unico rimedio a disposizione del cliente che abbia disposto un pagamento con IBAN errato è di avvalersi del supporto dell'intermediario, il quale però non è sempre efficace come abbiamo già vista sopra.[208]

Le cose però potrebbero cambiare: una attenzione particolare, infatti, è stata rivolta al rafforzamento dei presidi di sicurezza che sono attualmente previsti in normativa. Uno di questi è proprio il c.d. *IBAN/name check services*. Recentemente è stato pubblicato un regolamento comunitario (Regolamento 2024/886/UE) in materia di bonifici istantanei

---

[206] Così G. MARINO, *IBAN "sbagliato" e responsabilità delle banche nell'esecuzione dell'operazione di bonifico*, *op.cit.*, p. 1266

[207] Per quanto riguarda l'esercizio dell'attività bancaria e la responsabilità che ne segue T. VITALE, *Funzione bancaria e responsabilità contrattuale della banca*, in *Funzione bancaria rischio e responsabilità della banca*, a cura di S. MACCARONE e A. NIGRO, Giuffrè, 1981, 6; G.L. PELLIZZI, *La responsabilità della banca, in Banca*, *borsa, tit. cred.*, 1985, I, 157 ss.; P. GAGGERO, *voce «Responsabilità della Banca»*, nel *Digesto* IV ed., Disc. priv., sez. civ., agg., Utet, 1998, 724 ss.

[208] E. CECCHINATO, *I servizi di pagamento*, *op. cit.*, pp. 409 e ss.

che prevede che i PSP si dotino di un meccanismo di *IBAN/name check* che verifica la corrispondenza tra identificativo unico e nominativo del beneficiario del pagamento. Ebbene la Commissione Europea ha proposto di estendere tale meccanismo anche ai bonifici tradizionali, questo concorrerà a rafforzare gli standard di sicurezza dei pagamenti all'interno dell'UE e la tutela degli utenti, anche se inevitabilmente comporterà maggiori costi in capo agli intermediari.[209]

4. La proposta PSD3[210] che modifica la disciplina sui sevrizi di pagamento

La proposta di *PSD3* rappresenta quindi una evoluzione della normativa europea sui servizi di pagamento. Tra i motivi principali che hanno portato alla proposta di *PSD3* si deve annoverare: l'innovazione tecnologica dovuta alla crescita delle imprese *Fintech*[211] e all'*Open Banking*; l'implementazione della sicurezza e la protezione dei consumatori; la armonizzazione del Mercato Unico; la stimolazione dell'innovazione e della concorrenza.

Come si faceva notare all'inizio dell'elaborato, nel 2022 è stata fatta una valutazione di gradimento della *PSD2*[212]: in

[209] *Verso la revisione della PSD2: il dialogo della Banca d'Italia con gli operatori del mercato dei pagamenti*, reperibile al sito www.bancaditalia.it

[210] Proposta di direttiva 2023/0209/COD

[211] Intese qui come aziende Fintech, imprese che utilizzano la tecnologia per offrire servizi finanziari in modo innovativo e spesso più efficiente rispetto ai tradizionali istituti finanziari.

[212] Direttiva 2015/2366/CE.

generale si nota che «nonostante alcune carenze, l'attuale quadro della *PSD2* ha consentito di compiere progressi nel raggiungimento degli obiettivi prefissati ed è stato allo stesso tempo relativamente efficiente per quanto riguarda i costi, creando valore aggiunto dell'UE»[213].

La valutazione d'impatto presenta un pacchetto di opzioni prescelte volte al conseguimento di obiettivi specifici:

«1. rafforzare la protezione degli utenti e la loro fiducia nei pagamenti;[214]

2. migliorare la competitività dei servizi bancari aperti;[215]

3. migliorare l'applicazione e l'attuazione negli Stati membri;[216]

---

[213] Così le valutazioni ex post/vaglio di adeguatezza della legislazione vigente nella proposta di direttiva 2023/0209/COD, p. 4.

[214] Continua la valutazione d'impatto che precede la *PSD3*: «una migliore applicazione dell'autenticazione forte del cliente, una base giuridica che preveda lo scambio di informazioni in materia di frodi e un obbligo a informare i clienti in merito alle frodi, l'estensione della verifica dell'IBAN a tutti i bonifici e l'inversione condizionata di responsabilità per le frodi che inducono a effettuare pagamenti ritenuti erroneamente come dovuti; l'obbligo per i prestatori di servizi di pagamento di migliorare l'accessibilità dell'autenticazione forte del cliente per gli utenti con disabilità, le persone anziane e per chiunque altro incontri difficoltà nell'uso dell'autenticazione forte del cliente; misure per migliorare la disponibilità di contante; il miglioramento dei diritti dell'utente e delle informazioni fornitegli».

[215] Continua la valutazione d'impatto che precede la *PSD3*: «obbligo per i prestatori di servizi di pagamento di radicamento del conto (ASPSP) di predisporre un'interfaccia dedicata per l'accesso ai dati; "pannelli di gestione delle autorizzazioni" volti a consentire agli utenti di gestire le autorizzazioni di accesso ai servizi bancari aperti concesse; specifiche maggiormente dettagliate dei requisiti minimi per le interfacce di dati per i servizi bancari aperti».

[216] Continua la valutazione d'impatto che precede la *PSD3*: «sostituzione di gran parte delle disposizioni della PSD2 con un regolamento direttamente applicabile; rafforzamento delle disposizioni riguardanti le sanzioni; precisazioni riguardo ad aspetti che presentano ambiguità; integrazione dei regimi di autorizzazione per gli IP e gli IMEL».

4. migliorare l'accesso (diretto o indiretto) dei prestatori di servizi di pagamento non bancari ai sistemi di pagamento e ai conti bancari».[217]

La *PSD3* fa parte del "Payment Package[218]" del 28 giugno 2023, che comprende anche il *PSR*[219] (Payment Service Regulation o Regolamento sui Servizi di Pagamento) e il *FIDA*[220] (Financial Data Acces o quadro per l'accesso ai dati finanziari).

Fondamentalmente il regolamento *PSR* è stato introdotto perché la *PSD3* rimane una direttiva incentrata sull'operatività dei fornitori di servizi di pagamento e continuerà a dover essere attuata nella legislazione locale. Il resto di quello che prima faceva parte della *PSD2*, viene regolato tramite il *PSR*, il quale ricopre perlopiù la responsabilità dei prestatori di servizi di pagamento, diventando automaticamente legge per tutti gli Stati membri dell'UE senza bisogno di essere recepito. In particolare, la *PSD3* continuerà a regolare le autorizzazioni ad operare per gli istituti di pagamento e i requisiti di tutela, si occuperà della fornitura del denaro contante e il prelievo di contanti offerti da ATM, dei servizi di moneta elettronica e dei requisiti in materia di tutela. Il *PSR* invece chiarisce ed

---

[217] Continua la valutazione d'impatto che precede la *PSD3*: «rafforzamento dei diritti degli IP/degli IMEL per quanto riguarda un conto bancario; consentire la partecipazione diretta degli IP e degli IMEL a tutti i sistemi di pagamento, inclusi quelli designati dagli Stati membri a norma della SFD, con ulteriori precisazioni sulle procedure di ammissione e di valutazione dei rischi».

[218] Il pacchetto include una serie di proposte legislative e strategiche volte a promuovere la concorrenza nel settore dei pagamenti, migliorando la *user experience* nel settore dei pagamenti, nonché garantire la protezione dei dati e la sicurezza delle transazioni.

[219] Proposta di regolamento 2023/0210/COD.

[220] Non è di diretto interesse di questo elaborato, basti evidenziare che questo Regolamento stabilisce diritti e obblighi chiari per gestire la condivisione dei dati dei clienti nel settore finanziario al di là dei conti di pagamento.

introduce alcune definizioni e tratta dei temi riguardanti interfacce e dashboard, SCA, gestione dei dati, sicurezza e frodi.

Insieme *PSD3* e *PSR* hanno come obiettivo di: mitigare e combattere le frodi nei pagamenti, migliorare i diritti dei consumatori, appianare ulteriormente le differenze tra prestatori di servizi bancari e non, implementare il funzionamento dell'open banking, implementare il prelievo di contanti nei negozi e presso gli ATM, armonizzare ulteriormente il mercato dei pagamenti dell'UE e rafforzare l'applicazione delle leggi europee. [221]

È importante ricordare che *PSD3* e *PSR* sono ancora in fase di prima lettura da parte del Parlamento europeo, con la conseguenza che la normativa che viene di seguito descritta potrebbe mutare prima della sua definitiva approvazione.

4.1 La Strong Customer Authentication

La *SCA – Strong Customer Authentication*[222] è ora stata proposta di essere regolata dal *PSR*, ciò significa che, nel momento in cui sarà in vigore

[221] Sul punto I. COMUNALE e C. PELLEGRINI, *Payments Package: PSD3 e PSR*, reperibile al sito www.deloitte.com.

[222] Si evidenzia che la definizione di autenticazione forte del cliente non è mutata rispetto alla precedente contenuta nella *PSD2*, infatti all'articolo 3, punto 35) del PSR si afferma che è una «autenticazione basata sull'uso di due o più elementi, classificati nelle categorie della conoscenza (qualcosa che solo l'utente conosce), del possesso (qualcosa che solo l'utente possiede) e dell'inerenza (qualcosa che caratterizza l'utente, che sono indipendenti, in quanto la violazione di uno non compromette l'affidabilità degli altri, e che è concepita in modo tale da tutelare la riservatezza dei dati di autenticazione», con la specifica all'art. 85 comma 12 che «i due o più elementi di cui all'articolo 3, punto 35), su cui è basata l'autenticazione forte del cliente non devono necessariamente appartenere a categorie diverse, purché la loro indipendenza sia pienamente preservata».

tale regolamento, la *SCA* è uno di quegli aspetti che non necessiterà di essere recepito ma sarà direttamente applicabile e uniforme in tutti gli Stati membri dell'UE.

L'obbiettivo primario della riforma di questo aspetto è la prevenzione delle frodi e la consapevolezza ed educazione del consumatore al fine di prevenire le frodi. Di questo tema tratta il Capo 7 del *PSR* intitolato "Rischi operativi e di sicurezza e autenticazione".

Innanzitutto, si legge all'art. 82 «Segnalazione delle frodi» che «I prestatori di servizi di pagamento forniscono almeno annualmente alle autorità competenti dati statistici sulle frodi connesse ai diversi mezzi di pagamento. Tali autorità competenti forniscono questi dati in forma aggregata all'ABE e alla BCE».[223] Tale procedimento di segnalazione frodi e raccolta dati è finalizzato ad assicurare che tutte le informazioni sulle frodi nei pagamenti siano raccolte, segnalate e analizzate in modo coerente a livello europeo, così da poter monitorare e contrastare meglio le frodi.

Vengono previste maggiori responsabilità per i prestatori di servizi di pagamento (PSP), rispetto ai tentativi di frode. Infatti, all'art. 84 "Rischi e tendenze in materia di frodi nei pagamenti" si legge che «I prestatori di servizi di pagamento avvertono i loro clienti con tutti i mezzi e i supporti opportuni qualora emergano nuove forme di frode nei pagamenti, tenendo conto delle esigenze dei gruppi di clienti più vulnerabili. I prestatori di servizi di pagamento forniscono ai loro clienti indicazioni chiare su come individuare i tentativi fraudolenti e li avvertono in merito alle

[223] Per la lettura integrale dell'articolo si rimanda all'art. 82 della proposta di regolamento 2023/0210/COD.

misure e alle precauzioni necessarie da adottare per evitare di cadere vittime di azioni fraudolente rivolte nei loro confronti. I prestatori di servizi di pagamento indicano ai loro clienti dove possono segnalare le azioni fraudolente e ottenere rapidamente informazioni relative alle frodi», e, al comma 2, si prevede che i PSP organizzino «almeno una volta l'anno» dei programmi di formazioni per i dipendenti sui «rischi e tendenze in materia di frodi nei pagamenti, ciò al fine di assicurare che i dipendenti siano formati in maniera adeguata a svolgere i loro compiti».[224]

L'art. 85 invece si occupa specificamente dell'autenticazione forte del cliente. Al primo comma sono individuati gli ambiti di applicazione della *SCA*: rispetto alla precedente normativa viene introdotta l'autenticazione forte anche quando il pagatore «b) accede alle informazioni sui conti di pagamento»[225]. Al comma 2 si mantiene la previsione di esenzione per quanto riguarda le operazioni periodiche specificando che «Le operazioni di pagamento non disposte dal pagatore ma solo dal beneficiario non sono soggette all'autenticazione forte del cliente nella misura in cui tali operazioni sono disposte senza alcuna interazione o coinvolgimento del pagatore». Questo può accadere in situazioni come i pagamenti ricorrenti, dove il beneficiario del pagamento avvia il pagamento automatico, senza che il pagatore debba intervenire ogni volta.

[224] Per la lettura integrale si rimanda all'art. 84 della proposta di regolamento 2023/0210/COD.

[225] Art. 85 comma 1: «Il prestatore di servizi di pagamento applica l'autenticazione forte del cliente quando il pagatore: a) accede al suo conto di pagamento online; b) accede alle informazioni sui conti di pagamento; c) impartisce un ordine di pagamento per un'operazione di pagamento elettronico; d) effettua qualsiasi azione, tramite canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi».

Nei commi seguenti vengono individuati altri casi specifici[226] di esenzione dall'autenticazione forte o di applicazione della stessa.

Per tutti i casi non specificamente menzionati, il comma 11 afferma che «Eventuali esenzioni dall'applicazione dell'autenticazione forte del cliente che l'ABE deve elaborare a norma dell'articolo 89[227] sono basate su uno o più dei criteri seguenti: a) il livello di rischio connesso al servizio prestato; b) l'importo, la frequenza dell'operazione, o entrambi; c) il canale di pagamento utilizzato per l'esecuzione dell'operazione».

Nel complesso quindi si denota una maggiore precisazione da parte del legislatore europeo per quanto riguarda l'autenticazione forte del cliente rispetto alla *PSD2*, prevedendo norme più rigorose per le procedure di autenticazione e controllo delle transazioni, al fine di contribuire a ridurre il rischio di transazioni fraudolente e migliorare la sicurezza delle operazioni finanziarie online. [228]

---

[226] Ad esempio con riguardo al paragrafo 7: «Le operazioni pagamento per le quali il pagatore impartisce ordini di pagamento con modalità diverse dall'uso di piattaforme o dispositivi elettronici, quali ordini di pagamento su supporto cartaceo, ordini per corrispondenza o meccanismi telefonici, non sono soggette all'autenticazione forte del cliente, indipendentemente dal fatto che l'operazione sia eseguita elettronicamente, a condizione che il prestatore di servizi di pagamento del pagatore provveda ai requisiti e ai controlli di sicurezza in modo da consentire una forma di autenticazione dell'operazione di pagamento diversa dall'autenticazione forte del cliente».

[227] È una delega a produrre norme tecniche di regolamentazione (RTS).

[228] *La nuova direttiva PSD3: innovazione, sicurezza e inclusività nei pagamenti online*, reperibile al sito www.opengateitalia.com

Oltre che ad una implementazione delle misure di sicurezza da parte degli utenti, anche l'educazione finanziaria degli utenti è centrale al fine di ridurre l'impatto delle frodi.

Gli utenti devono essere consapevoli circa i rischi legati ai servizi di pagamento. La clientela va educata con particolare riferimento ai servizi digitali, al loro corretto utilizzo, alle implicazioni in termini di responsabilità, ai comportamenti da tenere anche con riguardo ai prestatori di servizi di pagamento nel fornire le informazioni che sono necessarie per l'identificazione e la gestione di eventi fraudolenti.[229]

Banca d'Italia è coinvolta in varie iniziative volte a informare il pubblico sul tema delle frodi nei pagamenti e a come prevenirle, e anche gli istituti di credito cercano tramite i loro canali ufficiali e in base alle loro risorse di rendere edotti i propri utenti di eventuali frodi in corso o di cosa può o non può richiedere l'intermediario via mail o sms.

4.2 Trasparenza delle operazioni di pagamento

Come si legge nei risultati delle valutazioni ex post, delle consultazioni dei potatori di interesse e delle valutazioni d'impatto «la *PSD2* è stata particolarmente efficace per quanto riguarda l'obiettivo di aumentare l'efficienza, la trasparenza e la scelta degli strumenti di pagamento per gli utenti di servizi di pagamento», ma si sono comunque

[229] *Verso la revisione della PSD2: il dialogo della Banca d'Italia con gli operatori del mercato dei pagamenti*, reperibile al sito www.bancaditalia.it

introdotti nel *PSR* dei requisiti in più per aumentare la trasparenza delle condizioni e requisiti informativi per i servizi di pagamento.

Al considerando 41 del *PSR* si legge che «per aumentare il livello di trasparenza, i prestatori di servizi di pagamento dovrebbero fornire al consumatore, senza oneri aggiuntivi, informazioni di base sulle operazioni di pagamento eseguite. In caso di un'operazione di pagamento singola, il prestatore di servizi di pagamento non dovrebbe addebitare separatamente le spese di informazione. Analogamente, i prestatori di servizi di pagamento dovrebbero fornire, a titolo gratuito e su base mensile, informazioni successive sulle operazioni di pagamento nell'ambito un contratto quadro (…)».[230]

La trasparenza è centrale per il *PSR*[231], all'articolo 1 infatti si legge che «Il presente regolamento stabilisce obblighi uniformi per la prestazione di servizi di pagamento e di servizi di moneta elettronica per quanto riguarda: a)la trasparenza delle condizioni e i requisiti informativi per i servizi di pagamento e i servizi di moneta elettronica; b) i rispettivi diritti e obblighi degli utenti di servizi di pagamento e di moneta elettronica e dei prestatori di servizi di pagamento e di moneta elettronica in relazione alla prestazione di servizi di pagamento e di servizi di moneta elettronica».

Ad occuparsene in maniera molto dettagliata è il Titolo III della proposta di regolamento in commento "Trasparenza

[230] «Tuttavia, considerate l'importanza della trasparenza nello stabilire i costi e le differenti esigenze del cliente, le parti contraenti dovrebbero poter concordare l'addebito di spese per informazioni aggiuntive o più frequenti».

[231] Proposta di regolamento 2023/0210/COD.

delle condizioni e requisiti informativi per i servizi di pagamento", il cui ambito di applicazione è generale, e si applica infatti «alle operazioni pagamento singole, ai contratti quadro e alle operazioni di pagamento contemplate da tali contratti» (art. 4 paragrafo 1).

La valuta dell'operazione deve concordarsi preventivamente tra le parti (art. 5 paragrafo 1).

Il beneficiario è tenuto «qualora imponga una spesa o proponga una riduzione per l'utilizzo di un determinato strumento di pagamento» ad informare il pagatore prima di disporre l'operazione di pagamento (art. 6 paragrafo 1). Questo vale anche per il prestatore di servizi di pagamento o un terzo coinvolto nell'operazione, questi devono informare in proposito l'utente dei servizi di pagamento prima di disporre l'operazione di pagamento (paragrafo 2). Il pagatore è esentato dal pagare le spese di cui ai due commi appena descritti a meno che non gli fosse stato reso noto prima di disporre l'operazione di pagamento (paragrafo 3).

A differenza della precedente direttiva, si noti come i prestatori di servizi di pagamento siano caricati di più responsabilità, infatti si legge che «il prestatore di servizi di pagamento è soggetto all'onere di dimostrare che si è attenuto ai requisiti informativi di cui al presente titolo» (art. 9).

Il capo due del titolo III si occupa poi più specificamente delle operazioni di pagamento singole che sono tutte quelle operazioni che «non rientrano in un contratto quadro[232]».

Il prestatore di servizi ha l'obbligo di fornire determinate informazioni prima, al momento della stipula e nel corso dell'eseuzione dell'operazione di pagamento.

[232] Così l'art. 11 della proposta di regolamento 2023/0210/COD.

Per quanto riguarda le «informazioni generali preliminari» (art. 12) il prestatore di servizi di pagamento «rende disponibili all'utente di servizi di pagamento, in modo facilmente accessibile, le informazioni e le condizioni di cui all'articolo 13, per quanto riguarda i propri servizi», eventualmente su richiesta possono anche essere fornite su supporto cartaceo o altro durevole. Inoltre, le informazioni e le condizioni devono essere redatte «in termini di facile comprensione e in forma chiara e leggibile, in una lingua ufficiale dello Stato membro nel quale viene prestato il servizio di pagamento o in qualsiasi altra lingua convenuta dalle parti».

Per quanto attiene alle operazioni di pagamento contenute in un contratto quadro (Capo tre del Titolo III) all'art. 19 si legge che «prima che l'utente di servizi di pagamento sia vincolato da un contratto quadro o da un'offerta, il prestatore di servizi di pagamento gli fornisce su supporto cartaceo o altro supporto durevole le informazioni e le condizioni di cui all'art. 20». Quindi, la differenza con le operazioni di pagamento singole sta nel fatto che le informazioni e le condizioni devono essere sempre fornite (non solamente su richiesta dell'utente) in un supporto cartaceo o simile. Si mantiene fermo ciò che è già stato detto sulle singole operazioni di pagamento per quanto riguarda la forma delle infromazioni e condizioni.

Si segnalano in questa sede solamente le modifiche sostanziali che si sono proposte di apportare. Innanzitutto, per quanto riguarda la deroga ai requisiti informativi per gli strumenti di pagamento per importi ridotti e la moneta elettronica per le

operazioni di pagamento nazionali, viene soppressa la possibilità per gli Stati membri di adeguare gli importi ai limiti di spesa.

L'obbligo di informare l'utente di servizi di pagamento in merito alle procedure di risoluzione alternativa delle controversie nei contratti quadro è esteso anche alle operazioni di pagamento singole (era infatti già previsto con riguardo alle operazioni di pagamento contenute in un contratto quadro).[233]

Viene inserito un chiarimento per garantire che i prestatori di servizi di pagamento inseriscano negli estratti del conto di pagamento le informazioni necessarie per identificare con chiarezza il beneficiario, compreso un riferimento alla sua denominazione sociale.

Vengono inseriti ulteriori requisiti informativi per i prelivi da ATM nazionali.[234]

Per quanto riguarda i bonifici e le rimesse di denaro dall'UE verso un paese terzo, è introdotto l'obbligo per i prestatori di servizi di pagamento di indicare all'utente di servizi di pagamento il tempo stimato entro cui i fondi devono essere ricevuti dal prestatore di servizi di pagamento del beneficiario situato al di fuori dell'UE[235]. Inoltre, le spese di conversione valutaria stimate di tali operazioni internazionali devono essere espresse allo stesso modo di quelle per i bonifici all'interno dell'UE, quindi come maggiorazione percenutale rispetto agli ultimi tassi di cambio di riferimento disponibili per l'euro emessi dalla BCE.[236]

---

[233] lett. g) par. 1, art. 13 del *PSR*.

[234] lett. c) ii), art. 20 del *PSR*.

[235] lett. c), par. 1, art. 13 del *PSR*; lett. b) vi), art. 20 del *PSR*.

[236] lett. f), par. 1, art. 13 del *PSR*; lett. c) v), art. 20 del *PSR*.

4.3 La rivoluzione della responsabilità per IBAN inesatto

Per quanto concerne l'autorizzazione delle operazioni di pagamento si legge al considerando 93 l'introduzione della previsione per il prestatore di servizi di pagamento, «ove tecnicamente possibile e senza che sia necessario un intervento manuale, di verificare la coerenza dell'identificativo unico e, qualora si rilevi l'incoerenza dell'identificativo unico[237], rifiutare l'ordine di pagamento ed informarne il pagatore».

Una disposizione analoga è già prevista con riguardo ai bonifici istantanei dal regolamento 2024/886/UE, il quale prevede un servizio immediato di verifica della corrispondenza tra l'IBAN e il nome del beneficiario, da svolgere subito dopo che il pagatore abbia fornito le pertinenti informazioni e prima che gli sia offerta la possibilità di autorizzare il bonifico.[238] In caso di mancata corrispondenza, infatti, il prestatore di servizi di pagamento ne dà notifica al pagatore informandolo dei rischi dell'operazione con la possibilità di autorizzarla comunque. Nel caso di inosservanza di tali obblighi da parte del prestatore di servizi di pagamento e che quindi venga a determinarsi un'esecuzione inesatta del pagamento, il PSP è tenuto a

[237] Con "identificativo unico" si intende: la combinazione di lettere numeri o simboli che il prestatori di servizi di pagamento indica all'utente di servizi di pagamento e che quest'ultimo deve fornire per identificare con chiarezza un altro utente del servizio di pagamento o il conto di pagamento dell'altro utente del servizio di pagamento per un'operazione di pagamento» così il punto 39 dell'art. 3 della proposta di regolamento 2023/0210/COD.

[238] Art. 5-*quater* par. 8 del reg. 2024/886/UE

rimborsare immediatamente l'importo del bonifico, salvo a sua volta essere risarcito dal prestatore di servizi di pagamento del beneficiario che, venendo meno agli obblighi di verifica, abbia cagionato la mancata conformità e il conseguente danno.[239]

Allo stesso modo questo è stato proposto di essere applicato a tutti i tipi di bonifici al fine di realizzare un quadro coerente. La disposizione della proposta di regolamento *PSR* si applica ai bonifici che non sono bonifici istantanei in tutte le valute dell'Unione e ai bonifici istantanei in valute diverse dall'euro.

Stando alla disposizione la notifica della discrepanza tra IBAN e nome del beneficiario deve essere effettuata prima che il pagatore finalizzi l'ordine di pagamento e prima che il prestatore di servizi di pagamento eseguil bonifico, a quel punto l'utente rimane libero di decidere se presentare l'ordine di pagamento.[240]

Come si legge all'art. 57 il prestatore di servizi di pagamento del pagatore è ritenuto responsabile dell'intero importo del bonifico nel caso in cui non abbia notificato al pagatore una discrepanza rilevata tra l'identificativo unico e il nome del beneficiario fornito dal pagatore. In questo caso, «entro 10 giornate operative successive a quella in cui prende atto di un'operazione di bonifico eseguita nelle circostante di cui al paragrafo 1 o riceve una notifica in merito», il prestatore di servizi di pagamento ha due possibili modi di comportarsi: a) rimborsa al pagatore l'intero importo del bonifico autorizzato; b) fornisce una motivazione del rifiuto del rimborso e indica gli organismi ai quali il pagatore può deferire

[239] Sul tema L. MIOTTO, *I pagamenti elettronici*, in *Diritto del Fintech*, M. Cian e C. Sandei (a cura di), CEDAM, II ed. 2024, p. 280.

[240] Si rimanda all'art. 50 del *PSR*.

la questione a norma degli articoli 90, 91, 93, 94 e 95[241] se non accetta i motivi addotti.

Solo nel caso di ragionevoli motivi per sospettare una frode da parte del pagatore, il prestatore di servizi di pagamento può rifiutarsi di rimborsare il pagatore. In questo caso il prestatore di servizi di pagamento deve motivare il rifiuto del rimborso e indicare gli organismi ai quali il pagatore può deferire la questione.[242]

Infine, viene introdotto l'obbligo per i prestatori di servizi di comunicazione elettronica di cooperare con i prestatori di servizi di pagamento al fine di prevenire tali frodi.[243]

4.4 Servizi di fornitura del denaro contante

Un'altra novità introdotta dal *Payment Package*, più precisamente nella *PSD3* ha come fine quello di aumentare ulteriormente l'accesso al contante. Ai negozi al dettaglio (per esempio i supermercati di determinate aree rurali o remote dove le infrastrutture bancarie tradizionali possono essere limitate) dovrebbe essere consentito di offrire un servizio di fornitura di contante anche in assenza di un acquisto da parte del cliente, senza dover ottenere un'autorizzazione come prestatore di servizi di pagamento, una registrazione o essere un agente di un istituto di pagamento. Questi servizi dovrebbero essere offerti dai negozi fisici su base volontaria e dipendono dalla disponibilità di

[241] Tali articoli fanno parte del capo 8 intitolato "Procedure di esecuzione, autorità competenti e sanzioni".

[242] Si rimanda al par. 3 e 4 dell'art. 59 del *PSR*.

[243] Si rimanda al par. 5 dell'art. 59 del *PSR*.

contante da parte del dettagliante, imponendo comunque un massimale di 50 EUR per operazione in modo da non creare concorrenza sleale con i gestori di ATM.[244]

L'art. 37 tratta di una esenzione dell'applicazione della direttiva, e quindi di operare come istituti di pagamento, nel caso in cui «le persone fisiche o giuridiche che forniscono contante nei punti vendita indipendentemente dal fatto che sia effettuato o meno un acquisto, purché siano soddisfatte le condizioni seguenti: 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».

L'altro articolo centrale per la questione è l'art. 38 rubricato "Servizi che permettono prelievi in contante, offerti da gestori di ATM[245] che non prestano servizi di pagamento di radicamento del conto", il quale tratta della registrazione delle persone fisiche o giuridiche che prestano i servizi di prelievo di contante e che non forniscono servizi di pagamento di radicamento del conto né altri servizi di pagamento. Queste non sono soggette ad autorizzazione ma si registrano presso l'autorità competente dello Stato membro di origine prima di avviare l'attività.

4.5 La moneta elettronica

Come ultimo aspetto meritevole di attenzione [246] non si può mancare dal menzionare la moneta elettronica. Infatti, la proposta di direttiva 2023/0209/COD (*PSD3*) aggiorna e chiarisce le disposizioni

[244] Così il considerando 62 della proposta di direttiva 2023/0209/COD.

[245] Automated Teller Machine.

[246] Opinione di chi scrive.

relative agli Istituti di pagamento e integra gli ex IMEL come una sottocategoria degli Istituti di pagamento, di conseguenza la seconda direttiva sulla moneta elettronica[247] verrà abrogata dalla data di applicazione della direttiva *PSD3*.

Come evidenziato dal considerando 5, la moneta elettronica è disciplinata dalla direttiva 2009/110/CE, mentre l'uso della moneta elettronica per finanziare operazioni di pagamento è disciplinato in gran parte dalla *PSD2*. Nel corso degli anni le autorità competenti incaricate dell'autorizzazione e della vigilanza degli istituti di pagamento e degli istituti di moneta elettronica hanno incontrato difficoltà di ordine pratico nel delineare in modo chiaro i due regimi e nel distinguere i prodotti e i servizi di moneta elettronica dai servizi di pagamento e di moneta elettronica offerti da istituti di pagamento. Si è ritenuto quindi opportuno allineare ulteriormente il regime di autorizzazione e di vigilanza applicabile agli istituti di moneta elettronica con il regime applicabile agli istituti di pagamento.

L'esigenza della comprensione della moneta elettronica in un'unica direttiva sui servizi di pagamento è dovuta prevalentemente a esigenze di carattere sistematiche, non rappresentando concretamente una novità in termini di tutela del cliente.

La piena armonizzazione è evidenziata dall'art. 1 della direttiva *PSD3*[248] "Oggetto e ambito di applicazione" il quale stabilisce al comma 3 che «Salvo diversa disposizione,

[247] Direttiva 2009/110/CE.

[248] Proposta di direttiva 2023/0209/COD.

ogniqualvolta nella presente direttiva è fatto riferimento ai servizi di pagamento, questi sono intesi come servizi di pagamento e servizi di moneta elettronica», con l'ulteriore precisazione al comma 4 che «salvo diversa disposizione, ogniqualvolta nella presente direttiva è fatto riferimento ai prestatori di servizi di pagamento, questi sono intesi come prestatori di servizi di pagamento e prestatori di servizi di moneta elettronica».

Nel complesso si denotano norme più stringenti per gli emittenti di moneta elettronica introducendo requisiti più rigidi per le istituzioni emettono moneta elettronica; l'introduzione dell'autenticazione forte del cliente anche per quanto riguarda transazioni che coinvolgono moneta elettronica con la conseguente introduzione di misure più avanzate per la prevenzione delle frodi; una maggiore protezione dei consumatori tramite rimborsi e risarcimenti in caso di transazioni non autorizzate o errate effettuate con moneta elettronica e una maggiore trasparenza nelle tariffe e nelle condizioni con l'obbligo per gli emittenti di moneta elettronica di fornire ai clienti informazioni chiare e trasparenti sulle tariffe applicate, i tempi di esecuzione delle transazioni e i termini e condizioni del servizio.

La direttiva mira a garantire che gli emittenti di moneta elettronica e i fornitori di servizi di pagamento tradizionali operino su una base di parità, riducendo le barriere normative e promuovendo una concorrenza leale nel mercato.

CAPITOLO III

-

PROFILI DI CONTENZIOSO IN MATERIA DI SERVIZI DI PAGAMENTO

1. Introduzione

Analizzando la normativa sui servizi di pagamento emergono due principali profili di responsabilità in capo all'intermediario[249]: sia per quanto riguarda «operazioni di pagamento non autorizzate»[250]; sia per «mancata, inesatta o tardiva esecuzione dell'operazione di pagamento».[251]

Ciò che distingue le due ipotesi è la presenza o meno dell'autorizzazione da parte dell'ordinate. Infatti, nel primo caso il consenso del pagatore manca completamente ma l'operazione viene comunque eseguita[252]. Il problema risiede nella fase di inizio dell'operazione, poiché manca una legittima autorizzazione all'avvio e all'esecuzione dell'operazione di pagamento che dovrebbe provenire da una volontà consapevole e non viziata del cliente. Nel secondo caso,

[249] Intermediario, PSP o prestatore di servizi di pagamento sono utilizzati quali sinonimi nel presente capitolo.

[250] Art. 11 del d.lgs. 11/2010.

[251] Art. 25 del d.lgs. 11/2010.

[252] Ciò accade ad esempio nel momento in cui si ha una richiesta fraudolenta da parte di terzi non autorizzati che utilizzano le credenziali dell'utente per accedere agli strumenti di pagamento, come siti o app di internet banking, si è parlato approfonditamente dei tipi di frode nel capitolo I a cui si rimanda.

invece, l'operazione è stata autorizzata dall'utente, ma nel momento dell'esecuzione si sono verificati dei problemi, la cui responsabilità è generalmente da imputarsi al prestatore di servizi di pagamento del pagatore, che ha impedito l'esecuzione o ha causato una tardiva o inesatta esecuzione.

In entrambe le ipotesi, basta una contestazione tempestiva da parte dell'utente per far sorgere due diversi obblighi a carico dell'intermediario: nel caso di un'operazione «non autorizzata» sorge l'obbligo di rimborso immediato; mentre nel caso di «mancata, inesatta o tardiva esecuzione» sorge l'obbligo di ripristinare la situazione precedente all'esecuzione dell'operazione o alla sua richiesta, in caso di mancata esecuzione. [253]

È importante evidenziare anche che il prestatore di servizi di pagamento potrebbe sospendere l'esecuzione di un'operazione, ad esempio, in caso di sospetto riciclaggio/finanziamenti al terrorismo, anche senza una esplicita revoca del consenso da parte dell'utente, in questo modo potrebbe prevenire danni e responsabilità prima della frode.

[253] Si veda V. DE STASIO, *Ordine di pagamento non autorizzato e restituzione della moneta*, Giuffrè, Milano 2016, p. 135. Si veda anche I.A. CAGGIANO, *Pagamenti non autoriz- zati tra responsabilità e restituzioni. Una rilettura del d. legisl. 11/2010 e lo scenario delle nuove tecnologie*, in *Riv. dir. civ.*, 2017, p. 459 ss.

2. Le operazioni di pagamento non autorizzate

Il fine della disciplina sui servizi di pagamento è di regolamentare i comportamenti che devono tenere l'utente e il prestatore di servizi di pagamento, al fine della corretta esecuzione del procedimento di trasferimento dei fondi in conformità con un ordine di pagamento che sia sorretto dal consenso del pagatore.[254]

È un dato pacifico che l'allocazione del rischio di pagamenti non autorizzati sia cruciale ai fini dell'effettività della disciplina e della diffusione dei servizi di pagamento.[255] Le scelte quindi del legislatore devono essere capaci di garantire un'allocazione del rischio in grado di prevenire e reprimere gli esiti inefficienti derivanti da comportamenti non rispettosi, dalla predisposizione di sistemi di sicurezza adeguati e, per quanto riguarda l'utente, dalla diligenza nella custodia dello strumento di pagamento e delle relative credenziali.[256]

---

[254] Cosi V. DE STASIO, *Riparto di responsabilità e restituzioni nei pagamenti non autorizzati*, in *Innovazione e regole nei pagamenti digitali: il bilanciamento degli interessi nella PSD2, op. cit.;* si veda anche V. DE STASIO*, Ordine di pagamento non autorizzato e restituzione della moneta*, Giuffrè, Milano 2016, p. 135; sul ruolo del consenso del pagatore v. anche O. Troiano e V.V. Cuocci, *Commento all'art. 5*, in *La nuova disciplina dei servizi di pagamento*, a cura di M. Mancini, M. Rispoli Farina, V. Santoro, A. Sciarrone Alibrandi e O. Troiano, *cit.*, p. 84 ss.

[255] Cfr. 95° considerando, Dir. 2366/2015: «*La sicurezza dei pagamenti elettronici è fondamentale per garantire la protezione degli utenti e lo sviluppo di un contesto affidabile per il commercio elettronico*».

[256] M. C. PAGLIETTI, *Questioni in materia di prova nei casi di pagamenti non autorizzati*, in *Innovazioni e regole nei pagamenti digitali: bilanciamento degli interessi nella PSD2, a cura di* M. C. Paglietti e M. I. Vangelisti, Università degli Studi Roma Tre Dipartimento di Giurisprudenza, Roma Tre-Press, 2020, p. 43.

Come si diceva poco sopra, una operazione di pagamento per essere correttamente avviata deve avere l'autorizzazione dell'utente[257]. E questo consenso[258] deve essere manifestato secondo le modalità previste dal comma 2[259] dell'art. 5 del D.Lgs. n. 11/2010 e nelle forme stabilite dal comma 3[260]. Ricordando che tale consenso può essere prestato anche tramite un terzo intermediario, ossia il prestatore di servizi di disposizione di ordini di pagamento (indicato con l'acronimo PISP).[261] Il rapporto che si viene a creare tra intermediario e pagatore si basa su un accordo in base al quale il prestatore è autorizzato a spendere il nome dell'utente[262], prestando il consenso all'operazione di pagamento che verrà

[257] Si riporta per completezza di esposizione l'art. 5 comma 1 del d.lgs. 11/2010: «Il consenso del pagatore è un elemento necessario per la corretta esecuzione di un'operazione di pagamento. In assenza del consenso, un'operazione di pagamento non può considerarsi autorizzata».

[258] Di cui si è già ampiamente trattato nel capitolo precedente e a cui si rimanda.

[259] Si riporta per completezza di esposizione l'art. 5 comma 2 del d.lgs. 11/2010: «Il consenso ad eseguire un'operazione di pagamento o una serie di operazioni di pagamento è prestato nella forma e secondo la procedura concordata nel contratto quadro o nel contratto relativo a singole operazioni di pagamento».

[260]Si riposta per completezza di esposizione l'art. 5 comma 3 del d.lgs. 11/2010: «Il consenso può essere dato prima o, ove concordato tra il pagatore e il proprio prestatore di servizi di pagamento, dopo l'esecuzione di un'operazione di pagamento».

[261] A tal proposito si veda si veda V. PROFETA, *I third party provider: profili soggettivi e oggettivi*, in *Le nuove frontiere dei servizi bancari e di pagamento fra PSD 2, criptovalute e rivoluzione digitale*, a cura di F. Maimeri e M. Mancini, in *Quaderni di ricerca giuridica della consulenza legale di Banca d'Italia*, n.87, 2019, p. 49 e ss.; A. MESSORE, *La nuova disciplina dei servizi di pagamento digitali prestati dai Third Party Providers*, in *Le Nuove Leggi Civili Commentate*, n. 2, 1 marzo 2020, p. 523 e ss.

[262] Sulla spendita del nome si veda con riferimento a A. MESSORE, *La nuova disciplina dei servizi di pagamento digitali prestati dai Third Party Providrs,* in *Le nuove leggi civili commentate*, n. 2, 1 Marzo 2020, p. 523 e ss.

successivamente eseguita dall'istituto di radicamento del conto. A quest'ultimo inoltre non sarà richiesto di dover verificare la sussistenza di una relazione contrattuale tra utente e prestatore di servizi di disposizione di ordini di pagamento, dato che si potrà presumere per effetto dell'autenticazione e dell'utilizzo delle credenziali di accesso al conto che quest'ultimo agisca sulla base del consenso esplicito del cliente.[263]

Innanzitutto, dietro all'espressione «operazione di pagamento» si cela una pluralità di «schemi di pagamento» riconducibili a categorie come: il bonifico[264], l'addebito diretto[265], la carta di credito[266], la carta di debito[267] e ciascuno di questi ha un differente procedimento mediante il quale si trasmettono sia «i fondi» dal conto del pagatore a quello del beneficiario sia l'informazione dell'ordine di pagamento che dà inizio al procedimento.[268]

---

[263] In tal senso si v. V. PROFETA, *I third party provider: profili soggettivi e oggettivi*, *op.cit*, p. 72.

[264] Per approfondimenti si veda A. SCIARRONE ALIBRANDI, *L'interposizione della banca nell'adempimento dell'obbligazione pecuniaria*, Giuffrè, Milano 1997; sul SEPA *Credit transfer*, ora V. De Stasio, *Sul momento e il luogo nel quale il beneficiario di un bonifico bancario acquista la disponibilità della somma oggetto dell'ordine di pagamento dell'ordinante*, in *Banca, borsa, tit. cred.*, 2017, II, p. 304 ss., testo e nt. 7, e 311 ss.

[265] Sul punto G.B. BARILLÀ, *L'addebito diretto*, Giuffrè, Milano 2014.

[266]Per approfondimenti F. CIRAOLO, *Le carte di debito nell'ordinamento italiano*, Milano, 2008; ma anche M. ONZA, *Estinzione dell'obbligazione pecuniaria e finanziamento dei consumi: il pagamento con la "carta"*, Giuffrè, Milano 2013.

[267] Al riguardo si v. U. MALVAGNA, *Clausola di «riaddebito» e servizi di pagamento*, Giuffrè, Milano 2018.

[268] Così V. DE STASIO, *Riparto di responsabilità e restituzioni nei pagamenti non autorizzati*, in *Innovazione e regole nei pagamenti digitali: il bilanciamento degli interessi nella*

Fatta questa premessa, si può affermare generalmente che, nelle operazioni di pagamento, si viene a creare una situazione patologica nel momento in cui manchi il consenso del pagatore. A questo punto la situazione che si viene a creare è quella di una operazione di pagamento «non autorizzata» da parte del pagatore. Infatti, stando all'art. 5, comma 1, ultima parte, «in assenza del consenso una operazione di pagaemento non può considerarsi autorizzata».

La normativa, oltre a prevedere obblighi specifici a carico delle parti e un regime probatorio invertito in caso di un difetto di autorizzazione dell'operazione di pagamento, prevede anche ipotesi specifiche per i casi in cui il difetto di autorizzazione sia ricollegabile all'utilizzo «abusivo» di uno strumento di pagamento, il quale unitamente ad altri codici di accesso, funga da mezzo per l'attribuzione della paternità dell'ordine.[269]

La situazione in cui uno strumento di pagamento (che consente di effettuare operazioni su un conto di pagamento) venga utilizzato da un soggetto non autorizzato dal pagatore, ovvero in senso contrario alla sua volontà, si ha nel momento il cui ci sia un furto o la sottrazione o indebito utilizzo di strumenti di pagamento, finalizzato ad effettuare sia pagamenti online che prelievo di contate.

Riguardo allo strumento di pagamento utilizzato da un soggetto non autorizzato dal pagatore, è intervenuta la sentenza

---

PSD2, M.C Paglietti e M.I. Vangelisti (a cura di), Università degli Studi Roma Tre Dipartimento di Giurisprudenza, Roma Tre-Press, 2020, pp. 25 e ss.

[269] In tal senso I. A. CAGGIANO, *Pagamenti non autorizzati tra responsabilità e restituzioni. Una rilettura del d. legisl. 11/2010 e lo scenario delle nuove tecnologie*, *op. cit.*

n. 20639 della Corte di Cassazione del 2019, nella quale risultava coinvolta una s.r.l. (titolare di un conto corrente con annesso servizio di banca multicanale per aziende) che nel luglio 2007, da accertamenti contabili, rilevava ammanchi per oltre 240.000 euro derivanti da numerosi bonifici che erano stati effettuati tramite il canale di *home banking* da un collaboratore autonomo, regolarmente abilitato ad operare sul conto della società e per questo dotato di codici di identificazione. Nel caso di specie venivano disposti 19 bonifici, in un tempo limitato, verso un beneficiario con discrepanza tra nome e coordinate bancarie e incongruenza di causale (veniva asserito il pagamento di fatture ma il destinatario era una persona fisica e non giuridica o titolare di partita iva).

La società in questo caso citava in giudizio la banca per inadempimento dell'obbligo di effettuare i dovuti controlli sulle operazioni disposte mediante *internet banking*, ma l'istituto di credito resisteva eccependo che i bonifici venivano effettuati da soggetto legittimato il quale poteva accedere alla banca multicanale e quindi si professava libera da qualsiasi onere di accertamento in ordine alla legittimazione dei soggetti esecutori delle operazioni.

La questione, essendo datata 2007 e quindi prima dell'entrata in vigore della *PSD* e del conseguente d.lgs. 11/2010, è stata risolta ritenendo esclusa la colpa grave e la mancata diligenza della banca, la quale non era tenuta al controllo di merito sulla congruità delle operazioni commerciali sottese alle disposizioni di bonifico disposte dal rappresentante del correntista. Inoltre, il sistema operativo in uso all'epoca, non avrebbe

consentito tecnicamente il rilievo automatico di eventuali discrasie fra il nominativo del beneficiario e il titolare effettivo del conto del bonifico.[270]

Alla luce del d.lgs. 11/2010, occorre notare come sarebbe stata risolta a posteriori la questione e, se e quali tipi di responsabilità sarebbero sorte in capo al prestatore di servizi di pagamento. Innanzitutto, si tratta di un caso di operazioni di pagamento a distanza disposte dal pagatore, tra le quali rientra il bonifico *online* impartito in nome del correntista da un suo delegato mediante uso dell'*home banking*. In questo contesto ci si chiede se ci si trovi nella fattispecie di una «operazione non autorizzata» o nel caso di «mancata, inesatta o tardiva esecuzione delle operazioni di pagamento»[271].

Ebbene in questo caso il consenso del pagatore non è mancante, perché è espresso per il tramite del proprio rappresentante, ma è viziato per conflitto di interessi di quest'ultimo in quanto beneficiario dei pagamenti (artt. 1394-

[270] Venivano mosse anche altre questioni: veniva contestata la correttezza del principio affermato dal giudice delle leggi secondo cui la normativa antiriciclaggio non è in grado di spiegare alcuna interferenza sul piano civilistico e i rimedi esperibili dal correntista nei confronti dell'istituto di credito per operazioni di bonifico bancario in base ai principi generali del codice civile, con riguardo all'abuso del potere di rappresentanza da parte del delegato. Queste questioni non sono di interesse per il seguente elaborato ma si rimanda per approfondimenti a E. FUSCO, *Utilizzo improprio di un home banking da parte del rappresentante del correntista e perimetro della (ir)responsabilità di credito, tra legge antiriciclaggio, codice civile e disciplina sui servizi di pagamento*, in *Banca Borsa e tit. cred.,* fasc. 4, 2021, pp.499.

[271] In questo caso non sono intervenuti fatti imputabili al PSP che ne hanno impedito il compimento o hanno determinato una esecuzione tardiva o inesatta.

1395 c.c.)[272]. In altri termini, nell'ordine di bonifico disposto dal rappresentante in conflitto di interessi, il consenso del delegato deve considerarsi efficace e vincolate fino a quando il correntista non ne abbia ottenuto la caducazione *ex post* mediante l'azione di annullamento. Quindi alla luce di ciò sembra che il rimedio di cui all'art. 11 d.lgs. 11/2010 per «operazione non autorizzata» non avrebbe trovato applicazione nemmeno se i fatti di causa si fossero svolti dopo l'entrata in vigore di tale decreto in commento. Diverso sarebbe stato il caso di difetto o eccesso di rappresentanza che quindi comportava la inefficacia dell'atto da parte del falso rappresentato e di conseguenza avrebbe comportato a considerarla come una «operazione non autorizzata» con conseguente rimborso immediato *ex* art. 11.[273]

Secondo la disciplina sui servizi di pagamento, nel caso di bonifico *online* disposto dal rappresentante del correntista, il prestatore di servizi di pagamento è tenuto a verificare il rispetto della delega (e relativi limiti), nonché il corretto uso delle credenziali di accesso da parte del soggetto autorizzato ad operare sul conto.[274]

---

[272] Secondo i principi generali, l'atto del rappresentante in conflitto di interessi, sebbene viziato, resta pienamente produttivo di effetti fino alla pronuncia di annullamento da parte del tribunale, che accerta la ricorrenza delle condizioni fissate dall'art. 1394 c.c.).

[273] E. FUSCO, *Utilizzo improprio di un home banking da parte del rappresentante del correntista e perimetro della (ir)responsabilità di credito, tra legge antiriciclaggio, codice civile e disciplina sui servizi di pagamento*, *op. cit.*, pp.499.

[274] Numerosa è la giurisprudenza in tema di pagamenti non autorizzati e più in particolare sul riparto di responsabilità tra utente e prestatore di servizi di pagamento. Alcune pronunce saranno infatti richiamate nei paragrafi successivi.

Un dibattito giurisprudenziale che anima la disciplina dei «pagamenti non autorizzati» è quello del rapporto e dei confini tra restituzione e risarcimento[275], questo perché la moneta costituisce sia oggetto del servizio sia misura di un eventuale risarcimento. Tendenzialmente la linea di distinzione tra i due rimedi si individua proprio in considerazione del procedimento di pagamento e del momento in cui può verificarsi l'anomalia del procedimento stesso.

Infatti, se il vizio attiene alla autorizzazione, la logica delegatoria individua nella carenza di consenso del pagatore all'ordine di pagamento il vizio, e quindi si ritiene consona una ripetizione nei confronti del beneficiario in capo al prestatore di servizi di pagamento di radicamento del conto che abbia dato avvio al trasferimento dei fondi del cliente. Se invece l'anomalia attiene all'esecuzione del trasferimento dei fondi, la natura del rimedio va ricercata nell'area del risarcimento del danno.[276]

Concretamente la differenza sta nel fatto che, nella restituzione l'oggetto del trasferimento è già individuato e, di conseguenza, l'azione restitutoria costituisce la tutela più efficace per il cliente che si vede ripristinare la disponibilità della moneta sul proprio conto. Per quanto attiene al risarcimento questo

---

[275] Si veda per approfondimenti P. SIRENA, *La gestione di affari altrui*, Torino 1999, p. 24 ss. e p. 25, nt. 103. Si veda, inoltre, P. BARCELLONA, *Note critiche in tema di rapporti fra negozio e giusta causa dell'attribuzione*, in *R. trim. d. proc. civ.*,1955, p. 11. Si veda anche per approfondimenti V. DE STASIO, *Ordine di pagamento non autorizzato e restituzione della moneta*, Milano, 2016, pp. 169 e ss.

[276] Così V. DE STASIO, *Riparto di responsabilità e restituzioni nei pagamenti non autorizzati*, *op. cit.*, pp. 29.

include danni o perdite che possono andare oltre all'ammontare dell'operazione non autorizzata.[277]

In ogni caso, data la potenziale difficoltà nel quantificare danno emergente e lucro cessate si evidenzia come gli intermediari sono soliti a risolvere la questione sul nascere in quanto vengono previste a livello contrattuale la quantificazione del danno negli interessi legali o convenzionale per il periodo in cui l'importo non addebitabile è stato sottratto alla disponibilità dell'utente.[278]

Con riguardo al regime di responsabilità delle operazioni non autorizzate la proposta *PSD3* e la proposta *PSR* si è curata di chiarire alcuni concetti che la *PSD2* richiamava nel dettare il regime di responsabilità ma senza darne una compiuta definizione. Si fa riferimento, ad esempio, alle espressioni quali «colpa grave», «frodi» e «truffe» che hanno ricevuto una definizione armonizzata. Tali concetti, infatti, risultano diversificati in base ai diversi ordinamenti nazionali e quindi non è sempre facile cercare di armonizzarli a livello comunitario, ma d'altra parte potrebbe essere utile avere un chiarimento al fine di risolvere eventuali dubbi interpretativi e le disomogeneità applicative.

Viene rafforzato inoltre il ruolo di guida e indirizzamento per i prestatori di servizi di pagamento in capo all'EBA, la quale, con i suoi

---

[277] Si veda per approfondimenti V. DE STASIO, *Ordine di pagamento non autorizzato e restituzione della moneta*, *op.. cit.*

[278] Così E. CECCHINATO, *I servizi di pagamento*, *op. cit.*, pp. 405. Sul punto O. TROIANO, CUOCCI, *sub art 11*, in Mancini-Rispoli Farina-Santoro-Sciarrone Alibrandi-Troiano O. (a cura di), *La nuova disciplina dei servizi di pagamento*, Giappichelli, 2011, pp. 140.

orientamenti e raccomandazioni, dovrebbe indirizzare l'operato dei prestatori di servizi di pagamento.[279]

2.1 Il rimborso del pagamento non autorizzato

Per quanto riguarda le modalità di rimborso del pagamento «non autorizzato» si deve guardare all'art. 11 d.lgs. 11/2010. L'art. 11 del decreto prevede che in caso di operazioni di pagamento non autorizzate il pagatore abbia diritto al rimborso entro la fine della giornata operativa successiva a quella in cui il prestatore di servizi di pagamento prende atto dell'operazione eseguita in assenza di autorizzazione. Nello specifico si legge che «il prestatore di servizi di pagamento rimborsa al pagatore l'importo dell'operazione medesima immediatamente e in ogni caso al più tardi entro la fine della giornata operativa successiva a quella in cui prende atto dell'operazione o riceve una comunicazione in merito. Ove per l'esecuzione dell'operazione sia stato addebitato un conto di pagamento, il prestatore di servizi di pagamento riporta il conto nello stato in cui si sarebbe trovato se l'operazione di pagamento non avesse avuto luogo, assicurando che la data valuta dell'accredito non sia successiva a quella dell'addebito dell'importo».

Si noti che nel breve termine imposto dall'art. 11 d.lgs. 11/2010, ossia una giornata operativa, il prestatore di servizi di pagamento non deve (né può[280]) verificare se l'autorizzazione

[279] *Verso la revisione della PSD2: il dialogo della Banca d'Italia con gli operatori del mercato dei pagamenti*, reperibile al sito www.bancaditalia.it

[280] Non può perché non è una valutazione semplice da compiersi.

dell'utente è del tutto priva di vizi o se sia frutto di una frode perpetrata da un terzo e che abbia visto come vittima lo stesso utente.

Tale accertamento oltre che essere precluso dalla stringente tempistica, non è neppure richiesto dalla norma in commento, la quale chiede solamente di accertare se sussista o meno una autorizzazione dell'utente, rilasciata nella forma e secondo la procedura concordata nel contratto quadro *PSD2*[281].

I successivi commi 2 e 3 precisano che l'intermediario può sospendere il rimborso in caso di motivato sospetto di frode, dandone comunicazione «immediata»[282] a Banca d'Italia anche in un momento successivo in cui l'operazione di pagamento era stata autorizzata. In questo caso il prestatore di servizi di pagamento ha il diritto di chiedere direttamente all'utente e ottenere da quest'ultimo la restituzione dell'importo rimborsato.[283]

Al comma 2-bis si precisa, per quanto riguarda l'operazione di pagamento disposta mediante un prestatore di servizi di disposizione di ordine di pagamento, che in questo specifico caso «il prestatore di servizi di pagamento di radicamento del conto rimborsa al pagatore immediatamente, e in ogni caso, entro la fine della giornata operativa successiva, l'importo dell'operazione non autorizzata, riportando il conto di pagamento addebitato nello stato in cui si sarebbe trovato se l'operazione di pagamento non avesse avuto luogo».

---

[281] Direttiva 2366/2015/CE.

[282] Cosi la *littera legis* al comma 2 dell'art. 11 d.lgs. 11/2010.

[283] Sul punto TROIANO. O-CUOCCI, *sub art. 11*, in *La nuova disciplina dei servizi di pagamento*, a cura di MANCINI, RISPOLI FARINA, SANTORO, SCIARRONE ALIBRANDI e O. TROIANO, Giappichelli, 2011, pp.140 e ss.

In merito all'art. 11 del d.lgs. 11/2010 è meritevole di attenzione la comunicazione emanata da Banca d'Italia datata 30 ottobre 2023 e avente ad oggetto «Obbligo di segnalazione di cui all'art. 11 d.lgs. 11/2010 Template per le comunicazioni alla Banca d'Italia».

In tale sede viene ribadito che il prestatore di servizi di pagamento è tenuto «a effettuare in favore del pagatore un rimborso integrale, immediato e non svantaggioso» rimanendo ferma la possibilità per il prestatore di servizi di pagamento di «non rimborsare qualora l'operazione non autorizzata derivi da un comportamento fraudolento che si caratterizzi per elementi specifici che denotano l'intenzione dell'utente di raggirare il il prestatore di servizi di pagamento e che lo stesso non possa consistere nella mera inosservanza dolosa o colposa degli obblighi di comunicazione e di custodia gravanti sull'utente medesimo».

Il prestatore di servizi di pagamento ha anche la possibilità di rimborsare subito la somma e dimostrare in un momento anche successivo che l'operazione era stata autorizzata e di ri-addebitare il conto dell'utente.[284]

Viene chiarito anche, da Banca d'Italia, che il comportamento fraudolento si caratterizza per elementi specifici che denotano l'intenzione dell'utente di raggirare il prestatore di servizi di pagamento e che tale comportamento intenzionale dell'utente non può consistere nella mera inosservanza dolosa o

[284] Così R. FRAU, *Home banking, phishing e responsabilità civile della banca*, nota a Cass. Civ., sez. VI, 12/04/2018, n. 9158, in *Resp. Civ. prev.*, 2019, p. 622 ss.

colposa degli obblighi di comunicazione e custodia gravanti su di esso in forza dell'art. 7 d.lgs. 11/2010.

L'utente che contesta la mancata autorizzazione di un'operazione di pagamento eseguita non sarà onerato di dimostrare quale tra i prestatori coinvolti sia in concreto responsabile dell'esecuzione di tale pagamento. Viene infatti semplificata la posizione dell'utente che ha diritto di rivalsa nei confronti del PISP che ha eventualmente preso parte all'operazione di pagamento. Il PISP, dal canto suo, per ottenere la restituzione delle somme rimborsate deve dimostrare di aver adempiuto correttamente agli obblighi di autenticazione, corretta registrazione e inesistenza di guasti tecnici o altri inconvenienti operativi.[285]

Per quanto riguarda il risarcimento di danni ulteriori subiti può essere previsto «in conformità della disciplina applicabile al contratto stipulato tra l'utente e il prestatore di servizi di pagamento compreso, se del caso, il prestatore di servizi di disposizione di ordine di pagamento». Data la potenziale difficoltà nel quantificare danno emergente e lucro cessante, come si è detto sopra, si ricorda nuovamente in questa sede che gli intermediari sono soliti prevenire l'insorgere della questione risolvendola a livello contrattuale, stabilendo il danno negli interessi legali

[285] Così V. PROFETA, *I third party provider: profili soggettivi e oggettivi*, *op. cit.*, p. 73 e ss.; G. BERTI DE MARINIS, *La disciplina dei pagamenti non autorizzati cit.*, p. 651; I.A. CAGGIANO, *Pagamenti non autorizzati tra responsabilità e restituzioni. Una rilettura del d.lgs. 11/2010 e lo scenario delle nuove tecnologie*, *op. cit.*; G. MARINO, *Carte di pagamento con funzione contactless, uso non autorizzato e responsabilità dei prestatori di servizi di pagamento*, *op. cit.*

o convenzionali per il periodo in cui l'importo non addebitabile è stato sottratto alla disponibilità dell'utente.[286]

Per quanto riguarda gli aggiornamenti previsti dalla *PSD3* e dal *PSR* in materia di rimborso rimangono ferme le previsioni appena descritte.[287]

2.2 La rettifica ex art. 9 d.lgs. 11/2010

A livello di disciplina nazionale al fine di comprendere ciò che avviene a seguito di un pagamento non autorizzato, si deve guardare all'art. 9 del decreto legislativo in commento, rubricato «notifica e rettifica di operazioni non autorizzate o non correttamente eseguite», il quale impone al cliente che sia venuto a conoscenza di un'operazione di pagamento non autorizzata di darne notizia all'intermediario «senza indugio» e «secondo i termini e le modalità previste nel contratto quadro o nel contratto relativo a singole operazioni di pagamento» solo in questo modo il cliente avrà diritto alla rettifica dell'operazione.[288]

---

[286] Sul punto E. CECCHINATO, *I servizi di pagamento*, *op. cit.*; si veda per ulteriori approfondimenti TROIANO O. – CUOCCI, *Sub. Art. 11*, in *La nuova disciplina dei servizi di pagamento*, a cura di MANCINI, RISPOLI FARINA, SANTORO, SCIARRONE ALIBRANDI e O. TROIANO, Giappichelli, 2011, p.140 s.; I.A. CAGGIANO, *Pagamenti non autorizzati tra responsabilità e restituzioni. Una rilettura del d.lgs.. 11/2010 e lo scenario delle nuove tecnologie*, *op. cit.*

[287] Si veda l'art. 62 della proposta di regolamento 2023/0210/COD.

[288] In questo senso si veda E. CECCHINATO, *I servizi di pagamento*, *op. cit.*, p.9; per approfondimenti cfr. pure Circolare Abi, Serie tecnica n. 14 – 31 marzo 2010, Bancaria ed., 6, sub art. 5, in cui si sottolinea che il consenso viene espresso, nell'addebito diretto, dal pagatore attraverso la sottoscrizione e la consegna del mandato alla propria banca; poco più sotto la Circolare richiama il fatto che, ove l'addebito abbia ad oggetto il consenso ad eseguire più operazioni di pagamento, le

Bisogna sempre tenere a mente le due situazioni patologiche di partenza, la prima è quella appena vista in cui sia viziata del tutto la volontà di partenza e quindi che l'operazione di pagamento che è stata compiuta non sia stata autorizzata da pagatore e quindi tale operazione non è pertanto a lui riferibile. La seconda, che si vedrà in seguito, è quella in cui un utente ha correttamente fornito informazioni al proprio prestatore di servizi di pagamento (o al proprio prestatore di servizi di disposizione di ordine di pagamento) e quindi egli ha effettivamente inteso voler compiere un'operazione di pagamento (quindi non manca di autorizzazione), ma si rende conto che il proprio prestatore non l'ha eseguita come richiesto da lui. Il comma 3 dell'articolo 9 afferma infatti che «un'operazione di pagamento si intende non eseguita correttamente quando l'esecuzione non è conforme all'ordine o alle istruzioni impartite dall'utente al proprio prestatore di servizi di pagamento». In questo caso il pagatore può avvalersi della rettifica *ex art.* 9 il quale prevede la possibilità di rettifica di un'operazione che non è stata correttamente eseguita o autorizzata.

L'utente, nello specifico, qualora «sia venuto a conoscenza di un'operazione di pagamento non autorizzata o non correttamente eseguita, ivi compresi i casi di cui all'articolo 25[289], ha il diritto di ottenerne la rettifica solo se comunica senza indugio tale circostanza al prestatore di servizi di pagamento secondo i termini e le modalità previste nel contratto quadro o nel contratto relativo a singole operazioni di pagamento» tale

operazioni di pagamento successive non possono essere autorizzate (art. 4 d. lgs. 11/2010).

[289] Per ora basti affermare che si tratta di responsabilità dei prestatori di servizi di pagamento per la mancata, inesatta o tardiva esecuzione delle operazioni di pagamento. Di cui si parlerà in maniera più approfondita in questo capitolo.

comunicazione però deve essere eseguita entro 13 mesi[290] dalla data di addebito, nel caso del pagatore, o di accredito nel caso del beneficiario.

In questo modo, soddisfando entrambi i requisiti, si avrà la tutela immediata del titolare del conto.[291]

Da notarsi però che il termine di 13 mesi non opera «se il prestatore di servizi di pagamento ha omesso di fornire o di mettere a disposizione le informazioni relative all'operazione di pagamento secondo quanto previsto dalle disposizioni in materia di trasparenza delle condizioni e di requisiti informativi per i servizi di pagamento di cui al titolo VI del testo unico delle leggi in materia bancaria e creditizia (…)».[292]

Anche qualora fosse coinvolto un prestatore di servizi di disposizione di ordine di pagamento, l'utente ha «il diritto di ottenere la rettifica del prestatore di servizi di pagamento di

[290] Con specifico riferimento a tale termine di 13 mesi si fa riferimento ad un caso in cui le operazioni di pagamento siano state effettuato da un *falsus procurator* (Cass. 20639/2019). Viene stabilito infatti che, in mancanza di tempestiva contestazione nel termine di 13 mesi, si ha il venir meno dell'obbligo di rimborso in capo al PSP. Questo si ha per il combinato disposto degli artt. 9 e 5 comma 3°, d.lgs. 11/2010, da cui si evince che la mancata contestazione può essere valorizzata come "ratifica" del pagatore, il quale autorizza implicitamente l'operato del terzo che abbia ecceduto il potere rappresentativo, determinando *ex post* l'efficacia del pagamento.

[291] E FUSCO, *Utilizzo improprio di un home banking da parte del rappresentante del correntista e perimetro della (ir)responsabilità dell'istituto di credito, tra legge antiriciclaggio, codice civile e disciplina sui servizi di pagamento*, in *Banca Borsa e titoli di credito*, fasc. 4, 2021, pp. 499.

[292] Così il comma 2 dell'articolo 9.

radicamento del conto a norma del primo comma, fatti salvi gli articoli 11, comma 2-bis[293], e 25-bis, comma 1[294]».

Per quanto riguarda l'aggiornamento previsto dalla proposta *PSD3*, la notifica e rettifica di operazione non

[293] Il quale comma 2-bis art. 11 afferma che « Se l'operazione di pagamento è disposta mediante un prestatore di servizi di disposizione di ordine di pagamento, il prestatore di servizi di pagamento di radicamento del conto rimborsa al pagatore immediatamente e, in ogni caso, entro la fine della giornata operativa successiva, l'importo dell'operazione non autorizzata, riportando il conto di pagamento addebitato nello stato in cui si sarebbe trovato se l'operazione di pagamento non avesse avuto luogo. In caso di operazione di pagamento non autorizzata, se il relativo ordine di pagamento è disposto mediante un prestatore di servizi di disposizione di ordine di pagamento, quest'ultimo è tenuto a rimborsare immediatamente e, in ogni caso, entro la fine della giornata operativa successiva, senza che sia necessaria la costituzione in mora, al prestatore di servizi di pagamento di radicamento del conto su richiesta di quest'ultimo, gli importi rimborsati al pagatore. Se il prestatore di servizi di disposizione di ordine di pagamento è responsabile dell'operazione di pagamento non autorizzata, risarcisce immediatamente e, in ogni caso, entro la fine della giornata operativa successiva senza che sia necessaria la costituzione in mora il prestatore di servizi di pagamento di radicamento del conto, su richiesta di quest'ultimo, anche per le perdite subite. In entrambi i casi è fatta salva la facoltà del prestatore di servizi di disposizione di ordine di pagamento di dimostrare, in conformità a quanto disposto dall'articolo 10, comma 1-bis, che, nell'ambito delle sue competenze, l'operazione di pagamento è stata autenticata, correttamente registrata e non ha subito le conseguenze di guasti tecnici o altri inconvenienti relativi al servizio di pagamento da questo prestato, con conseguente diritto in questi casi alla restituzione delle somme da quest'ultimo versate al prestatore di servizi di pagamento di radicamento del conto ai sensi del presente comma.

[294] Il quale comma 1 art 25-bis sostiene che «1. Fatti salvi gli articoli 9, 24, commi 2 e 3, e 28 se l'ordine di pagamento è disposto mediante un prestatore di servizi di disposizione di ordine di pagamento il prestatore di servizi di pagamento di radicamento del conto rimborsa al pagatore l'importo dell'operazione di pagamento non eseguita o non correttamente eseguita e, se del caso, riporta il conto di pagamento addebitato nello stato in cui si sarebbe trovato se l'operazione non correttamente eseguita non avesse avuto luogo».

autorizzate, autorizzata o non correttamente eseguite si trova all'art. 54 del *PSR*. La nuova disciplina muta il termine entro il quale l'utente deve notificare una operazione non autorizzata, autorizzata o non correttamente eseguita, che diventa di 18 mesi dalla data di addebito, ferme mantenendo le altre previsioni dell'articolo.

2.3 Questioni probatorie nei casi di pagamenti non autorizzati

L'art. 10 d.lgs. 11/2010 recita che «Qualora l'utente di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento già eseguita o sostenga che questa non sia stata correttamente eseguita, è onore del prestatore di servizi di pagamento provare che l'operazione di pagamento è stata autenticata, correttamente registrata e contabilizzata e che non ha subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti».

In virtù del principio di vicinanza della prova[295], tale art. 10 pone in capo all'intermediario (*PSP* o *PISP*[296]) l'onere della prova. Tale

[295] Principio che si applica in varie aree del diritto, incluso il diritto dei servizi di pagamento, il quale stabilisce che l'onere della prova debba essere attribuito alla parte che si trova nella posizione migliore per fornire la prova rilevante. Si veda E. CECCHINATO, *op.cit.*, p. 405.

[296] Da precisare che in questo caso la responsabilità del prestatore di servizi di disposizione di ordini di pagamento sarà limitata all'ambito «delle proprie competenze ed agli inconvenienti connessi al servizio di disposizione di ordine di pagamento prestato». Sul punto G. BERTI DE MARINIS, *La disciplina dei pagamenti non autorizzati nel nuovo sistema delineato dal recepimento della direttiva PSD2*, in *Diritto della Banca e del mercato finanziario*, 2018, p. 645.

argomento è delicato, in quanto la ripartizione dell'onere della prova è cruciale ai fini dell'esito della lite.[297]

Innanzitutto, la norma in commento ha carattere imperativo, non è quindi derogabile dall'autonomia privata del consumatore:[298] tale caratteristica è comune nella contrattazione asimmetrica; infatti, la tutela della parte debole del rapporto negoziale si svolge anche attraverso una speciale ripartizione degli oneri probatori.

In presenza di contestazioni da parte dell'utilizzatore titolare di uno strumento di pagamento, la disciplina esclude che il mero utilizzo dello strumento possa costituire prova sufficiente dell'esistenza di un'autorizzazione.[299] Questo è quanto si afferma

---

[297] M. C. PAGLIETTI, *Questioni in materia di prova nei casi di pagamenti non autorizzati*, in *Innovazioni e regole nei pagamenti digitali: bilanciamento degli interessi nella PSD2, op. cit.,* pp. 43.

[298] Considerando 72 direttiva 2366/2015/CE: «I termini e le condizioni contrattuali per la fornitura e l'uso di uno strumento di pagamento, il cui effetto sarebbe quello di aumentare l'onere della prova per il consumatore o ridurre l'onere della prova per l'emittente, andrebbero considerate nulle e prive di effetti».

[299] I.A. CAGGIANO, *Pagamenti non autorizzati tra responsabilità e restituzioni. Una rilettura del d.lgs. 11/2010 e lo scenario delle nuove tecnologie*, *op. cit.*; Ad esempio, p. 7 condizioni generali « Che banca! » ove « L'uso congiunto della carta e del P.I.N. — o, per la carta di credito, l'uso della carta e la sottoscrizione della me- moria di spesa, ove prevista — costituiscono prova dell'avvenuta identificazione del cliente» [...] «Per le operazioni disposte tramite sportelli automatici [...] i terminali elettronici [...] il cliente presta consenso all'esecuzione di un'operazione di pagamento con la digita- zione del P.I.N.» Si veda anche art. 42, comma 5o, Condizioni generali di contratto c/c «You do» e dei servizi associati BPM « Se un Ordine di pagamento è eseguito conforme- mente all'Identificativo unico indicato dal Cliente, esso si ritiene eseguito correttamente per quanto concerne il Beneficiario e/o il conto indicato dall'Identificativo unico »; infine, art. 8 (p. 9), art. 2 (p. 6)) Conto Bancoposta Click « Nel caso in cui sia richiesta per l'utilizzazione della Carta presso i terminali POS e ATM la digitazione del PIN, quest'ultimo costituisce l'esclusivo strumento di identificazione del Correntista », « Il Correntista, si impegna ad utilizzare correttamente gli strumenti identificativi e operativi [...] a non cederli a terzi, né a

al comma 2 dell'art. 10 che precisa: «è onere del prestatore di servizi di pagamento, compreso, se del caso, il prestatore di servizi di disposizione di ordine di pagamento, fornire la prova della frode, del dolo o della colpa grave dell'utente».

Si è poi discusso se l'indirizzo IP[300] dell'utente possa costituire prova della circostanza che l'ordine di pagamento sia stato effettivamente impartito dal computer dell'utente, escludendo di coseguenza la responsabilità del prestatore di servizi di pagamento o integrando la negligenza.La critica mossa a questa ricostruzione però contesta l'affidabilità degli indirizzi IP in quanto questi potrebbero essere oggetto di un furto, il malfattore potrebbe appropriarsi anche dell'indirizzo IP della vittima quindi si desume che questo non abbia idoneità per costituire piena prova della riferibilità dell'ordine di pagamento al computer dell'utente.

In tema di prova di autenticazione dell'utente, si riscontrano numerose decisioni dell'Arbitro Bancario e Finanziario sulla sua rilevanza ai fini della determinazione della responsabilità del prestatore di servizi di pagamento. In tali sedi l'Arbitro Bancario e Finanziario ha affermato dei principi, alcuni dei quali vengono elencati qui di seguito:

---

consentirne l'utilizzo da parte di terzi, assumendosi la responsabilità di ogni conseguenza dannosa che possa derivare dall'abuso o dall'uso illecito di essi». La contrattualistica citata è rinvenibile sui siti Internet degli intermediari. Frequenti le clausole sulle incedibilità: «La carta [...] è strettamente personale e non può essere ceduta a terzi». Le condizioni generali riportate sono disponibili su siti *web* dei relativi istituti.

[300] Definiti dalla Corte di Giustizia come «sequenze numeriche assegnate a computer collegati a Internet al fine di consentire la comunicazione tra i medesimi attraverso tale rete»

1. In caso di totale assenza di prova di autenticazione forte, la responsabilità per le operazioni di pagamento contestate ricade interamente sul prestatore di servizi di pagamento.[301]
2. L'autenticazione forte deve essere provata anche con riguardo a tutte le fasi prodromiche delle operazioni di pagamento disconosciute.[302]
3. Il prestatore di servizi di pagamento deve essere in grado di provare l'invio dei codici OTP tramite sms ovvero l'invio della notifica *push* al dispositivo mobile associato alla carta/conto corrente dell'utente, l'eventuale attivazione del c.d. riconoscimento biometrico, nonché evidenza di quale sia il *device* sul quale è stata installata l'applicazione dei servizi di internet banking.[303]
4. Il prestatore di servizi di pagamento deve essere in grado di provare le evidenze dell'inserimento dei singoli fatti di autenticazione forte, ovvero specificare i motivi per cui non siano stati valorizzati gli specifici "campi" relativi all'autenticazione.[304]

---

[301] *Cfr.* Collegio di Milano, Decisione n. 1963 del 14 febbraio 2024; Collegio di Bologna, Decisione n. 1905 del 14 febbraio 2023; Collegio di Milano, Decisione n. 1634 del 8 febbraio 2024; Collegio di Milano, Decisione n. 1612 del 6 febbraio 2024; Collegio di Milano, Decisione n. 1598 del 6 febbraio 2024; ; Collegio di Milano, Decisione n. 1460 del 1 febbraio 2024; Collegio di Torino, Decisone n. 643 del 15 gennaio 2024; Collegio di Bologna, Decisione del 12 gennaio 2024, n. 577; Collegio di Milano, Decisione n. 158 del 4 gennaio 2024.

[302] *Cfr.* Collegio di Coordinamento, Decisione n. 21285 dell'11 ottobre 2021; Collegio di Milano, Decisione n. 1964 del 14 febbraio 2024; Collegio di Milano, Decisione n. 1606 del 6 febbraio 2024; Collegio di Torino, Decisione n. 1487 del 2 febbraio 2024; Collegio di Bari, Decisione n. 388 del 9 gennaio 2024; Collegio di Palermo, Decisione n. 11980 del 4 dicembre 2023.

[303] *Cfr.* Collegio di Milano, Decisione n. 905 del 20 gennaio 2024; Collegio di Bari, Decisione n. 1556 del 6 febbraio 2024.

[304] Collegio di Bologna, Decisione n. 12476 del 13 dicembre 2023.

In aggiunta alla prova di autenticazione dell'utente, verrà richiesta al prestatore dei servizi di pagamento, nel caso in cui voglia invocare una responsabilità esclusiva dell'utente, di «fornire la prova della frode, del dolo o della colpa grave dell'utente».[305]

La disposizione relativa all'onere probatorio non era nuova al nostro ordinamento, infatti prima dell'entrata in vigore della *PSD2* l'ordinamento conosceva già la fattispecie delineata dal comma 1 dell'articolo 10 d.lgs. 11/2010 ed era stata oggetto di interpretazioni giurisprudenziali sempre particolarmente rigorose in modo da predisporre la più ampia tutela verso il cliente.[306]

Il prestatore di servizi di pagamento al fine di non rimborsare l'utente dovrà innanzitutto dimostrare che quest'ultimo ha eseguito e autorizzato correttamente l'operazione, realizzando i comportamenti e le procedure richieste dalla normativa e, in generale, soddisfare gli standard richiesti nel settore dei pagamenti.

Si noti che la scelta della ricaduta dell'onere della prova sull'intermediario è totalmente in linea con i principi generali del nostro ordinamento che opera una inversione dell'onere della prova a favore della parte debole coinvolta. Infatti, la tutela della parte debole del rapporto negoziale si svolge anche attraverso una speciale ripartizione degli oneri probatori.[307]

---

[305] Art. 10 comma 2 d.lgs. 11/2010.

[306] Sul punto M. RISPOLI FARINA, *La nuova direttiva PSD2: i principali tratti di novità,* in *L'evoluzione dei sistemi dei servizi di pagamento nell'era del digitale*, (a cura di) B. Russo, CEDAM, 2020, pp. 6 e ss; si veda anche E. CECCHINATO, *I servizi di pagamento*, *op. cit*, pp. 405 e ss.

[307] Solitamente deve essere l'attore (in questo caso l'utente che richiede il rimborso per l'operazione non autorizzata) a doversi sobbarcare l'onere di dimostrare, ai sensi del comma 1 dell'art. 2697 c.c.: «Chi vuol far valere un diritto in giudizio deve provare i fatti che ne costituiscono il fondamento» ma in quanto parte

Tale *modus operandi*, per quanto riguarda l'onere probatorio, è stato consolidato anche dalla giurisprudenza, la quale ha emanato un orientamento in virtù del quale, una volta che il creditore (in questo caso l'utente che ha diritto al rimborso) abbia fornito evidenza della fonte negoziale o legale del diritto fatto valere e del rispetto del termine di scadenza, potrà allegare senza provarlo, il fatto dell'inadempimento, essendo onere dell'intermediario dimostrare di aver correttamente adempiuto o che, eventualmente, la mancata esecuzione della prestazione sia dovuta a causa a lui non imputabile.[308]

Recentemente la Suprema Corte ha precisato che «anche al fine di garantire la fiducia degli utenti nella sicurezza del sistema, è del tutto ragionevole ricondurre nell'area del rischio professionale del prestatore dei servizi di pagamento, prevedibile ed evitabile con appropriate misure destinate a verificare la riconducibilità delle operazioni alla volontà del cliente, la possibilità di una utilizzazione dei codici di accesso al sistema da parte dei terzi, non attribuibile al dolo del titolare o a comportamenti totalmente incauti da non poter essere fronteggiati in anticipo. Ne consegue che (…) la banca, cui è richiesta una diligenza di natura tecnica,

debole del rapporto viene previsto un'inversione dell'onere probatorio a carico della parte più forte, quindi l'intermediario. In tal senso (anche per quanto riguarda i cd. TPP), si veda M. C. PAGLIETTI, *Questioni in materia di prova nei casi di pagamenti non autorizzati*, *Innovazione e regole nei pagamenti digitali. Il bilanciamento degli interessi nella PSD2*, (a cura di) M. C. Paglietti e M. I. Vangelisti, Consumatori e Mercato, n.9, Roma Tre-Press, 2020, p.63.

[308] Così Cass. Civ., sez. II, 21/05/2019, ordinanza n.13685, in *dejure.it*.

da valutarsi con il parametro dell'accorto banchiere[309], è tenuta a fornire la prova della riconducibilità dell'operazione al cliente».[310]

Per quanto riguarda l'aggiornamento della normativa ad opera del *PSR*[311] l'argomento viene tratto all'art. 55 della proposta di regolamento, il quale conferma l'onere in capo all'intermediario la dimostrazione che «l'operazione di pagamento è stata autorizzata, correttamente registrata e non ha subito le conseguenze di guasti tecnici o altri inconvenienti legati al servizio fornito dal prestatore di servizi di pagamento».

2.4 La diligenza richiesta al prestatore di servizi di pagamento

Riguardo agli obblighi previsti in capo al prestatore di servizi di pagamento, l'articolo di riferimento è il n. 8 d.lgs. 11/2010, il quale afferma che il prestatore di servizi di pagamento che emette uno strumento ha l'obbligo di: 1. Assicurare che le credenziali di sicurezza personalizzate[312] non siano accessibili a soggetti diversi dall'utente abilitato a usare lo strumento di pagamento; 2. Astenersi dall'inviare strumenti di pagamento non richiesti, a meno che lo strumento di pagamento già consegnato all'utente debba essere sostituito; 3. Assicurare che siano sempre disponibili gli strumenti adeguati affinché l'utente di servizi di

[309] Figura che verrà in seguito approfondita.

[310] Così Cass. Civ., sez. VI, 12/04/2018, in *Resp. Civ. prev*, 2019, p. 621, con nota di Frau, *Home banking, phishing, e responsabilità divile della banca*, p. 622.

[311] Proposta di direttiva 2023/0209/COD.

[312] Art. 1, comma 1, lett. q-*ter* del D.lgs. n. 11/2010, laddove per "*credenziali di sicurezza personalizzate*" si intendono le "*funzionalità personalizzate fornite a un utente di servizi di pagamento dal prestatore di servizi di pagamento a fini di autenticazione*".

pagamento possa eseguire la comunicazione di smarrimento, furto, appropriazione indebita, uso non autorizzato, nonché la richiesta di riattivazione dello strumento di pagamento o l'emissione di uno nuovo ove l'intermediario non vi abbia già provveduto; 4. Impedire qualsiasi utilizzo dello strumento di pagamento successivo alla comunicazione dell'utente di avvenuto smarrimento, furto, appropriazione indebita, uso non autorizzato.

Tali obblighi sono da assolvere attraverso la predisposizione ed il costante aggiornamento di requisiti organizzativi e procedure interne al fine di garantire una inviolabilità dei sistemi attraverso cui si svolgono le operazioni messe in atto dall'utente.

Tra i sistemi di sicurezza di natura preventiva richiesti ai PSP c'è sicuramente la predisposizione del sistema di autenticazione forte del cliente, di cui si è già ampiamente parlato nel precedente capitolo dell'elaborato e a cui si rimanda.[313]

La predisposizione di determinati sistemi di sicurezza era già prevista, per via giurisprudenziale nel nostro ordinamento, tramite il ricorso alle regole di diritto generale delle obbligazioni e a quelle della responsabilità per attività pericolosa. Poi successivamente anche in virtù della legislazione sub primaria e speciale, dando una compiuta definizione e tipizzazione del corretto comportamento del prestatore di servizi.

[313] Si ricorda che l'autenticazione forte del cliente è applicata, secondo l'art. 10 bis d.lgs 11/2010, quando l'utente: a) accede al conto di pagamento *on line*; b) dispone un'operazione di pagamento elettronico; c) effettua qualsiasi azione tramite canale a distanza che può comportare rischio di frode.

Dalla *law in action*[314] dell'ABF (Arbitro Bancario Finanziario) emerge che entrambi gli approcci, ossia quello di disciplina generale e quello che si rifà alla disciplina sub primaria, garantiscono l'adeguatezza dei presidi di sicurezza informativa allo scopo e agli standard consentiti dallo sviluppo della tecnologia e aggiornato all'evoluzione del fenomeno criminale.

Sul piano sub primario, la prima menzione della necessità di un sistema multi-fattore è stata anticipata dalla Circolare n. 285/2013[315] della Banca d'Italia, la quale ha introdotto una specificazione Sezione (la nuova sezione VII «Principi organizzativi relativi a specifiche attività o profili di rischio» volta a disciplinare gli obblighi imposti alle banche che prestano servizi di pagamento tramite canale internet.

Un elemento cruciale incidente sull'allocazione della responsabilità è la presenza di un servizio di sms-alert, volto ad evitare il compimento di ulteriori prelievi tramite la notifica (che può essere un sms, una e-mail o una notifica push) all'utente. Questo sistema fa in modo che l'utente sia informato delle operazioni compiute presso il suo conto. Tale misura deve essere adottata dall'intermediario in modo generalizzato in virtù dell'obbligo di diligenza professionale; è da escludere però che la sua mancata predisposizione sia fatto generatore di responsabilità

[314] Con tale espressione ci si riferisce alla modalità pratica con cui vengono applicate le normative e i principi legali nel contesto della risoluzione delle controversie bancarie e finanziarie. A questa si contrappone la *law in the books* che non è altro che la legge scritta, ovvero le norme teoriche codificate nei testi giuridici. Per approfondimenti si veda M. DI PIRRO, *L'arbitro Bancario Finanziario: La risoluzione stragiudiziale delle controversie bancarie*, Giuffrè Editore, 2017.

[315] Circolare del 17 maggio 2016 intitolata «*Disposizioni di vigilanza per gli istituti di pagamento e gli istituti di moneta elettronica*».

nell'ipotesi di assenza del nesso causale tra l'occorrenza del danno e l'assenza della messaggistica di alert.

Un altro comportamento che è indice di diligenza da parte dell'intermediario è il blocco automatico della carta a seguito di operazioni anomale per frequenza e tipologia. All'ASPSP[316] si richiede, in questo caso, non il monitoraggio di ogni singola operazione, ma la predisposizione di sistemi automatici di blocco di operazioni che sono caratterizzate da un rapido succedersi e non in linea con la normale operatività del titolare del conto.

Meritevole in materia è la sentenza della Suprema Corte che si occupa di enunciare il principio secondo cui la responsabilità della banca debba essere valutata con maggiore rigore in forza del proprio status professionale.[317] In questo specifico caso la Corte si è limitata a definire il grado di diligenza esigibile dalla banca, richiamando la figura dell'"accorto banchiere[318]". La Corte invoca l'art. 1176 comma 2[319] c.c. come parametro valutativo utile a misurare ex post se la banca abbia effettivamente agito secondo quel grado di diligenza esigibile dal proprio status, mentre il parametro dell'"accorto banchiere" viene in rilievo solo in un secondo

[316] Acronimo di *Account Servicing Payment Service Provider*, sono gli enti che detengono e gestiscono conti di pagamento per i propri clienti, come le banche, gli istituti di credito o altri fornitori di servizi di pagamento.

[317] Cassazione Civile n. 16573/2018: «*La responsabilità della banca per operazioni effettuate a mezzo di strumenti elettronici, con particolare riguardo alla verifica della loro riconducibilità alla volontà del cliente mediante il controllo dell'utilizzazione illecita dei relativi codici da parte di terzi ha natura contrattuale e, quindi, va esclusa solo se ricorre la situazione di colpa grave dell'utente*».

[318] Si richiamano tra le altre al riguardo Cass. 9158/2018; Cass. 2950/2017.

[319]«Nell'adempimento delle obbligazioni inerenti all'esercizio di un'attività professionale, la diligenza deve valutarsi con riguardo alla natura dell'attività esercitata».

momento, e funge quale clausola generale ed elastica alla quale possono essere assegnati molteplici contenuti.

La Corte, nello specifico, fa riferimento all'espressione "accorto banchiere" tutte le volte in cui intende fare appello al complesso di strumenti e conoscenze tecniche che consentono al professionista di ponderare preventivamente i rischi tipici della sua attività, in modo da essere in grado di eseguire correttamente la prestazione a lui richiesta e di adottare presidi idonei a identificare e bloccare i danni che ne potrebbero derivare.[320]

La giurisprudenza è abbastanza allineata in questo senso: si può richiamare anche la recente sentenza n. 23683 del 4 settembre 2024 in cui viene ribadito nuovamente[321] che la diligenza posta a carico del professionista, per quanto concerne i servizi posti in essere in favore del cliente, ha natura tecnica e deve valutarsi tenendo conto dei rischi tipici della sfera professionale di riferimento assumendo come parametro quello dell'accorto banchiere. Dunque, la diligenza della banca va riferita ad operazioni che devono essere ricondotte nella sua sfera di controllo tecnico, sulla base anche di una valutazione di prevedibilità ed evitabilità.

Il parametro della diligenza è poi integrato dalla giurisprudenza con le disposizioni di legge che disciplinano l'esercizio dell'attività bancaria in generale: si esigono in capo al prestatore del servizio il rispetto di obblighi di informazione e

[320] Per approfondimento sull'evoluzione della responsabilità dell'"accorto banchiere" si veda *amplius* A. SCARPA, G. FORTUNATO, *Banche e Responsabilità civile*, Milano, Giuffrè, 2008. Ma anche R. CARATOZZOLO, *La responsabilità delle banche per la violazione degli obblighi contrattuali*, Milano, Giuffrè, 2007.

[321] Tale pronuncia richiama la precedente n. 3780/2024.

sensibilizzazione, nonché l'adozione di rimedi preventivi al fine di proteggere l'interesse del cliente.[322]

Per quanto riguarda le novità apportate dalla nuova proposta di direttiva *PSD3* e di regolamento *PSR* viene ribadito che il PSP del pagatore dovrebbe agire con la dovuta diligenza e verificare la coerenza dell'identificativo unico e rifiutare l'ordine di pagamento ed informarne il pagatore.[323]

All'art. 54 del *PSR* «Notifica e rettifica di operazioni non autorizzate, autorizzate o non correttamente eseguite» si legge che «Il prestatore di servizi di pagamento rettifica le operazioni di pagamento non autorizzate, non correttamente eseguite o le operazioni di pagamento autorizzate solo se l'utente di servizi di pagamento informa il prestatore di servizi di pagamento conformemente agli articoli 57 e 59 senza indebito ritardo dopo essere venuto a conoscenza di un'operazione di questo tipo che dà luogo a una rivendicazione, ivi compresi i casi di cui all'articolo 75, e non oltre 18 mesi dalla data di addebito».

La responsabilità del PSP per le operazioni di pagamento non autorizzate viene disciplinata dall'art. 56, il quale afferma che «Fatto salvo l'articolo 54, nel caso di un'operazione di pagamento non autorizzata il prestatore di servizi di pagamento del pagatore rimborsa al pagatore l'importo dell'operazione di pagamento non autorizzata, immediatamente e in ogni caso al più tardi entro la fine della giornata operativa successiva a quella in cui prende atto dell'operazione non autorizzata o riceve una notifica in merito, a meno che il prestatore di servizi di pagamento del

[322] Si veda S. CIRIELLI, *Utilizzo non autorizzato dello strumento di pagamento e responsabilità della banca*, in *Giurisprudenza Commerciale*, fasc.2, 2022, p. 443.

[323] Considerando 93 della proposta di regolamento 2023/0210.

pagatore abbia ragionevoli motivi per sospettare una frode e comunichi tali motivi per iscritto alla pertinente autorità nazionale competente».

Nel caso di motivati sospetti di frode, il PSP deve, entro 14 giornate operative successive a quella in cui prende atto dell'operazione o riceve una notifica in merito, rimborsare al pagatore l'importo dell'operazione di pagamento non autorizzata se è stato accertato che non è stata compiuta nessuna frode, o in alternativa fornire all'autorità nazionale pertinente e al pagatore una motivazione del rifiuto del rimborso e indicare gli organismi ai quali il pagatore può deferire la questione.

2.5 La diligenza dell'utente e la colpa grave del pagatore

È noto che il rischio di operazioni fraudolente dipende tanto dal comportamento delle parti, quanto dal livello di sicurezza del servizio adottato dall'operatore[324].Infatti si può dire che la collaborazione attiva dell'utente risulta decisiva al fine di prevenire, limitare e arrestare i casi di utilizzo indebito degli strumenti di pagamento. Per quanto attiene alla responsabilità dell'utente, l'art. 12 d.lgs. 11/2010 prevede un duplice e alternativo regime di responsabilità dell'utente, limitata e illimitata.

Premettendo che la disciplina dei servizi di pagamento non è di immediata comprensione per l'utenza media e che al

[324] M. C. PAGLIETTI, *Questioni in materia di prova nei casi di pagamenti non autorizzati*, in *Innovazioni e regole nei pagamenti digitali: bilanciamento degli interessi nella PSD2, op. cit.,* p. 45.

contempo gli utenti devono essere preservati da eventuali rischi[325], all'utenza media non si richiede altro che la «comprensione del funzionamento e dei connessi rischi di strumenti che, sebbene tecnologicamente complessi, si propongano viceversa sul mercato come di utilizzo intuitivo, al quale si collega peraltro un generale affidamento che è necessario per lo sviluppo del settore»[326]. In questo senso agli utenti, al fine di evitare di incorrere in responsabilità per colpa grave[327], non sarebbe richiesto altro se non di gestire le credenziali di accesso ed i dispositivi messi a disposizione dalla banca secondo la «normale diligenza».

Il primo comma dell'art. 12 prevede che «Salvo il caso in cui abbia agito in modo fraudolento (l'unico caso in cui l'utente sarà ritenuto responsabile per il proprio comportamento) l'utente non sopporta alcuna perdita derivante dall'utilizzo di uno strumento di pagamento smarrito, sottratto o utilizzato indebitamente intervenuto dopo la comunicazione eseguita (…)»

L'utente non è nemmeno «responsabile delle perdite derivanti dall'utilizzo dello strumento di pagamento smarrito, sottratto o utilizzato indebitamente quando il prestatore di servizi di pagamento non ha adempiuto all'obbligo (…)»

---

[325] Vedi considerando 7 della direttiva 2366/2015.

[326] In tal senso si veda L. MIOTTO e M. SPERANZIN, *I pagamenti elettronici*, in *Diritto del Fintech*, M. Cian e C. Sandei (a cura di), CEDAM, 2020 p. 189.

[327] Per colpa grave da intendersi, secondo il 72° considerando della Direttiva 2366/2015/CE, un «comportamento che implica un grado significativo di mancanza di diligenza; ad esempio, lasciare le credenziali usate per autorizzare un'operazione di pagamento vicino allo strumento di pagamento, in un formato aperto e facilmente individuabile da terzi».

In ogni caso, a meno che l'utente «non abbia agito in modo fraudolento o non abbia adempiuto a uno o più obblighi cui all'articolo 7, con dolo o colpa grave, il pagatore può sopportare, per un importo comunque non superiore a euro 50, la perdita relativa a operazioni di pagamento non autorizzate derivanti dall'utilizzo indebito dello strumento di pagamento conseguente al suo furto, smarrimento o appropriazione indebita».

Nel caso invece in cui l'utente abbia agito in modo fraudolento, con dolo o colpa grave, venendo meno ai propri obblighi di custodia delle credenziali e dello strumento di pagamento, dice il comma 4 che «l'utente sopporta tutte le perdite derivanti da operazioni di pagamento non autorizzate e non si applica il limite di 50 euro di cui al comma 3».

Come si diceva poco sopra, il principio che orienta la valutazione del comportamento dell'utente è quello secondo cui la divulgazione dei dati identificativi riservati che abilitano all'utilizzo del proprio conto vale a configurare una condotta gravemente colposa. È per questo motivo che si considera il fenomeno *phishing* come noto ai più[328] tanto da ritenere che la consapevolezza del rischio di attacchi informativi e della circostanza che gli istituti di credito non richiedano informazioni

[328] Nello specifico, il comportamento del titolare del conto assume i caratteri della «colpevole credulità», tanto per aver comunicato «le proprie credenziali di autenticazione al di fuori del circuito operativo dell'intermediario», tanto più colpevole se si considera che la notorietà del fenomeno del *phishing*: Coll. coord., Dec. n. 1820/13.

personali via mail come fatto notorio.[329] A maggior ragione nel caso in cui il messaggio ingannatorio risulti verosimile.[330]

Un altro indice di grave negligenza del pagatore viene rinvenuto nella non tempestività del blocco richiesto dall'utente una volta presa coscienza del furto o dello smarrimento. Anche se tale circostanza non è sufficiente, da sola, a configurare una responsabilità in capo all'intermediario.[331] L'orientamento dell'ABF in questi casi è sfavorevole all'utente che è colpevole di ingenuità e per questo motivo il suo errore non è scusabile.[332]

Non costituisce, invece, colpa in capo all'utente il verificarsi di fenomeni criminali con un elevato connotato tecnologico ed ingannatorio, in virtù della non richiesta elevata diligenza tecnica di cui poco sopra si diceva. Non costituisce altresì colpa grave l'affidamento dello strumento ad un familiare del titolare.[333]

---

[329] Così M. C. PAGLIETTI, *Questioni in materia di prova nei casi di pagamenti non autorizzati*, in *Innovazioni e regole nei pagamenti digitali: bilanciamento degli interessi nella PSD2, op. cit.,* p. 73

[330] È questo, ad esempio, il caso in cui tramite un messaggio whatsapp, da un numero non conosciuto, ci si finga madre, padre o figlio del diritto interessato del messaggio, chiedendo un accredito in favore di un conto a loro sconosciuto e con una motivazione evidentemente farlocca.

[331] Art. 7 d.lgs. 11/2010 afferma alla lettera b) che l'utente ha l'obbligo di «comunicare senza indugio, secondo le modalità previste nel contratto quadro, al prestatore di servizi di pagamento o al soggetto da questo indicato lo smarrimento, il furto, l'appropriazione indebita o l'uso non autorizzato dello strumento non appena ne viene a conoscenza».

[332] Tra le tante pronunce: ABF Milano n. 18738/2021; ABF Bologna n. 1307/2019.

[333] Non può, infatti, ritenersi che l'affidamento temporaneo ad un familiare possa essere invocato a supporto del riconoscimento di una colpa grave dell'utente «potendosi ritenere non infrequente, né irragionevole, che nell'ambito del nucleo familiare uno stretto congiunto sia delegato a procedere ad un determinato utilizzo della carta nell'interesse comune»: Coll. Roma, Dec. n. 2339/2013.

All'art. 7 d.lgs. 11/2010 (articolo cruciale per classificare la colpa grave dell'utente) è previsto inoltre che l'utente ha l'obbligo di: «utilizzare lo strumento di pagamento in conformità con i termini, esplicitati nel contratto quadro che ne regolano l'emissione e l'uso e che devono essere obiettivi, non discriminatori e proporzionati».

Altre circostanze che integrano colpa grave dell'utente secondo l'Arbitro Bancario e Finanziario con violazione degli obblighi di cui all'art. 7 sono: l'aver svelato le credenziali di sicurezza personalizzate ai terzi frodatori[334]; l'alternanza tra operazioni fraudolente e operazioni genuine, la prossimità degli sportelli ATM presso i quali sono stati effettuati i prelievi disconosciuti rispetto a quelli abitualmente utilizzati dall'utente;[335] la mancata dovuta attenzione agli allert del prestatore di servizi di pagamento ricevuti dall'utente a mezzo e-mail, notifica push e sms, ovvero all'avvenuta richiesta di autorizzazione per l'esecuzione di operazioni fraudolente[336]; *etc.*

---

[334] Cfr. Cass. Civ. 13 marzo 2023, n. 7214; Cass. Civ. 8 novembre 2023, n. 31136; Tribunale di Milano, 8 gennaio 2020, n. 79/2020; Collegio di Bari, Decisione n. 367 del 9 gennaio 2024.

[335] Se le operazioni contestate sono avvenute in un'area circoscritta e prossima al domicilio dell'utente e presso sportelli abitualmente utilizzati dal medesimo, si ritiene che la dinamica dei prelievi non presenti gli elementi tipici comuni agli episodi di clonazione che normalmente avvengono in luoghi diversi e lontani dal domicilio del titolare della carta (Coll. coord., Dec. nn. 897 e 3479 del 2014).

[336] Sul punto, si richiama la Collegio di Bologna, decisione. n. 2593 del 28 febbraio 2024 laddove si legge che "*(…)* Richiamate le norme, il Collegio con riferimento alle operazioni contestate rileva come l'intermediario produca la tracciatura dalla quale le operazioni risultano correttamente autenticate con doppio fattore, anche per quanto concerne l'attivazione alle ore 17:05:15 del 31 gennaio 2023, sull'utenza internet banking del ricorrente, di una nuova licenza ad operare,

Come si può desumere da tale disamina non esistono indici di presunzioni assolute di negligenza dell'utente, ma, ai fini della configurazione di questa, deve svolgersi una valutazione delle circostanze del caso concreto.

È interessante notare, nella prassi, come l'Arbitro Bancario Finanziario, nelle ipotesi di utilizzo non autorizzato sottoposte alla sua attenzione, abbia sempre posto l'accento sui doveri di diligenza e buona fede di entrambe le parti del rapporto in esame. Le pronunce dell'Arbitro muovono sempre dalla prospettiva di valutare con attenzione sia il rispetto degli obblighi di diligente custodia e conservazione degli strumenti di pagamento posti a carico dell'utente, sia la diligenza professionale che ricade sul prestatore di servizi di pagamento. Al di là dei casi in cui il cliente abbia chiaramente fornito a terzi le proprie credenziali, le decisioni dell'Arbitro tendono a far ricadere la responsabilità sulla parte contrattualmente più forte, ossia l'intermediario.[337]

presumibilmente dal terzo truffatore sul proprio dispositivo mobile, per la quale si dovevano necessariamente inserire i dati (Password + OTP) ricevuti dal cliente. Il Collegio precisa, comunque, che la prova prodotta dall'intermediario non è di per sé sufficiente per attribuire le conseguenze patrimoniali della frode al titolare dello strumento di pagamento (cfr. Collegio di Coordinamento, decisione n. 22745/2019) e che è pertanto chiamato a valutare la sussistenza o meno della colpa grave del titolare dello strumento, in base a tutte le circostanze allegate. Alla luce delle circostanze esaminate nel caso in specie e della documentazione prodotta, in particolare la copia delle comunicazioni ricevute dal cliente via mail che lo informavano sia della installazione della nuova utenza, sia delle singole operazioni, il Collegio ritiene integrato tale requisito".

[337] In questo senso S. SICA, B. M. SABATINO, *Disintermediazione finanziaria e tutela del cliente e dell'utilizzatore*, in *Diritto dell'informazione e dell'informatica*, fasc. 1, 2021, pp. 1-19.

Se la giurisprudenza dell'Arbitro Bancario Finanziario rimarrà fedele alle linee maturate sino ad ora, per i nuovi strumenti si prospettano sempre minori possibilità di riconoscere la colpa grave in capo all'utente. Questo perché il rischio che le informazioni sensibili vengano acquisite (anche in relazione alle recenti modalità *contactless* o all'impiego di *smart object*) è sempre più alto, rientrando in una condizione di inconsapevolezza della sottrazione da parte dell'utente che poi risulta incompatibile con uno stato soggettivo di colpa grave.[338]

Con la proposta di revisione della *PSD*[339] e la proposta di regolamento *PSR,* il legislatore europeo propone di disciplinare le operazioni oggetto di frode con furto di identità mediante il nuovo art. 59 del regolamento *PSR* in cui si prevede che: «Se un utente di servizi di pagamento che è un consumatore è stato manipolato da un terzo che ha finto di essere un dipendente del prestatore di servizi di pagamento del consumatore o qualsiasi altro ente pertinente di natura pubblica o privata utilizzando illecitamente il nome o l'indirizzo di posta elettronica o il numero di telefono di tale ente e tale manipolazione ha dato luogo a successive operazioni di pagamento autorizzate fraudolente, il prestatore di servizi di pagamento rimborsa al consumatore l'intero importo dell'operazione di pagamento autorizzata fraudolenta, a condizione che il consumatore abbia tempestivamente segnalato la frode alla polizia e ne abbia informato il prestatore di servizi di pagamento».

---

[338] Di questa opinione sono L. MIOTTO e M. SPERANZIN, *I pagamenti elettronici*, in *Diritto del Fintech*, M. Cian e C. Sandei (a cura di), CEDAM, 2020, p. 187.

[339] Proposta di direttiva 2023/0209/COD

Una volta ricevuta la segnalazione di una operazione autorizzata fraudolenta, unitamente alla denuncia effettuata dalla polizia, il PSP avrà 10 giorni operativi, dalla ricezione di una notifica in merito all'operazione di pagamento autorizzata fraudolenta da parte del consumatore, nonché il rapporto della polizia,[340] per valutare se rimborsare il consumatore o rigettare la richiesta di rimborso se dovesse ritenere sussistenti «ragionevoli motivi per sospettare una frode o una negligenza grave del consumatore» fornendo all'autorità nazionale competente «una motivazione del rifiuto del rimborso e indica al consumatore gli organismi ai quali quest'ultimo può deferire la questione».

L'utente non ha diritto al rimborso dell'operazione, recita il paragrafo 3 qualora «il consumatore ha agito in modo fraudolento o per negligenza grave o se si rifiuta di collaborare all'indagine del prestatore di servizi di pagamento o di fornire informazioni pertinenti in merito alle circostanze del furto di identità». Inoltre, «spetta al prestatore di servizi di pagamento del consumatore dimostrare che il consumatore ha agito in modo fraudolento o per negligenza grave». Quindi anche nella proposta di regolamento *PSR*[341] in caso di colpa grave dell'utente, questo non avrebbe diritto al rimborso per le operazioni autorizzate fraudolente, si riconosce che la colpa grave configura un comportamento che presenta un grado significativo di incuranza.

Sul tema delle frodi nelle operazioni di pagamento è meritevole di attenzione, ad opinione di chi scrive, il parere dell'ABE di aprile 2024[342],

---

[340] Si noti che aumenta il tempo che viene concesso al PSP nella valutazione di una operazione non autorizzata.

[341] Proposta di regolamento 2023/0210/COD.

[342] EBA, *Draft EBA Opinion on new types of payment fraud and possible mitigants,* April 2024 (EBA-Op/2024/01).

il quale ha rilevato più elevati tassi di frode per i bonifici istantanei e per le operazioni di pagamento transfrontaliere. Quindi pur esprimendo apprezzamento per le proposte di direttiva *PSD3* e di regolamento *PSR* l'ABE ritiene utili ulteriori azioni per mitigare il rischio di frodi.

3. L'art. 24 d.lgs. 11/2010: identificativi unici inesatti

Ai fini di una completa trattazione è utile ricordare lo svolgimento corretto dell'operazione di bonifico, che rappresenta una delle modalità di pagamento più utilizzate a livello internazionale.

Le parti coinvolte in questo tipo di operazione sono quattro[343]: il beneficiario[344], l'ordinante, il prestatore di servizi incaricato e il prestatore di servizi del beneficiario.[345] Per la corretta esecuzione la banca che riceve l'ordine di bonifico dovrà

[343] Con la precisazione che nelle transazioni internazionali le parti coinvolte sono di piu al fine di garantire a ciascuna delle parti che l'operazione si svola in maniera corretta e secondo le tempistiche previste. Ad esempio, potrebbe essere coinvolta una banca terza rispetto a quella del beneficiario che si occupi del trasferimento del bonifico qualora le due banche non abbiano rapporti di conto. Per approfondimenti sul punto si veda F. MARRELLA, *I pagamenti ed i contratti di finanziamento*, in *Manuale di diritto del commercio internazionale. Contratti internazionali, imprese globali ed arbitrato,* Wolters Kluwer, 2017, p. 405 e ss.

[344] Per approfondimenti V. DE STASIO, *Sul momento e il luogo nel quale il beneficiario di un bonifico bancario acquista la disponibilità della somma oggetto dell'ordine di pagamento dell'ordinante*, in *Banca Borsa Titoli di Credito*, fasc.3, 2017, p. 305.

vedersi trasmesse una serie di informazioni da parte dell'ordinante stesso al fine di individuare correttamente il beneficiario.[346]

Tra i profili di rischio maggiori di anomalia di una operazione di pagamento vi è l'errore sull'identità di colui che riceve l'accredito finale. Tale errore, incontra una maggiore probabilità di dare luogo ad una anomalia definitiva del procedimento perché l'accredito non richiede un comportamento attivo di collaborazione del beneficiario dell'erroneo accredito, il quale dovrà essere sollecitato solo in un secondo momento.[347]

La condizione che sicuramente deve essere soddisfatta è la conformità dell'identificativo unico. Al comma 1 si legge che: «Se un ordine di pagamento è eseguito conformemente all'identificativo unico, esso si ritiene eseguito correttamente per quanto concerne il beneficiario e/o il conto indicato dall'identificativo unico».

Si deve precisare che con l'espressione «identificativo unico inesatto» utilizzato dal legislatore si deve rilevare sia il caso dell'IBAN inesistente sia il caso dell'IBAN esistente ma errato in quanto

---

[346] Tra le informazioni fondamentali: estremi del beneficiario, quali nome e cognome o denominazione sociale nel caso di persona giuridica, l'indirizzo del suo domicilio, la banca su cui compiere l'accredito, il codice IBAN del beneficiario, il codice BIC SWIFT dell'operazione in corso, l'importo da trasferire e la relativa valuta e la "clausola", cioè il motivo del trasferimento dell'importo. Anche se ai fini dell'esecuzione del bonifico ciò che è fondamentale per il prestatore di servizi di pagamento è l'IBAN, le altre informazioni sono ai fini dell'antiriciclaggio.

[347] Si veda V. DE STASIO, *Riparto di responsabilità e restituzioni nei pagamenti non autorizzati*, *op. cit.,* pp. 37; ma anche I.A. Caggiano, *Pagamenti non autorizzati tra responsabilità e restituzioni. Una rilettura del d.lgs. 11/2010 e lo scenario delle nuove tecnologie*, cit., p. 474 ss.;

corrispondente a un beneficiario diverso dal legittimo destinatario a cui il pagatore voleva destinare il pagamento.

Se siamo nella prima ipotesi, dell'IBAN inesistente, si deve ritenere che ai sensi del comma 2 dell'art. 24 «il prestatore di servizi di pagamento non è responsabile, ai sensi dell'art. 25, della mancata o inesatta esecuzione dell'operazione di pagamento».[348]

Nella seconda ipotesi invece, l'operazione è eseguita regolarmente, ma risulta essere viziata dal fatto che il pagamento è accreditato da un soggetto diverso da quello effettivamente voluto dal pagatore in quanto legittimo creditore della somma trasferita. In questo caso, a differenza che nel primo, la banca ha a disposizione anche altre informazioni sul beneficiario del pagamento, come ad esempio la banca di accredito della somma trasferita, avendo quindi tutti gli elementi necessari per individuare l'incongruenza tra identificativo unico e il titolare del conto indicati dell'ordine.[349]

Quest'ultima circostanza è quella che ha fatto scaturire alcuni dubbi interpretativi circa l'individuazione della responsabilità del prestatore di servizi di pagamento.

In particolare, la giurisprudenza si è soffermata sulla corretta interpretazione del comma 3 che recita: «il prestatore di servizi di pagamento è responsabile solo dell'esecuzione dell'operazione di pagamento in conformità con l'identificativo unico fornito dall'utilizzatore anche qualora quest'ultimo abbia

---

[348] Il comma 2 è stato oggetto di modifica da parte del d.lgs. n. 218/2017 che ha introdotto il principio di collaborazione tra gli intermediari partecipanti al procedimento di pagamento.

[349] Sul punto M. C. LUPACCHINO, *sub. Art. 24*, in *La nuova disciplina dei servizi di pagamento*, *op. cit.*, p. 242.

fornito al suo prestatore di servizi di pagamento informazioni ulteriori rispetto all'identificativo unico». Il dubbio interpretativo riguarda la possibilità di applicare il dettato solo all'intermediario del pagatore o anche a quello del beneficiario.

Il primo orientamento in materia[350] sostiene che: in quanto il terzo comma non specifica a quale intermediario deve riferirsi la disposizione, l'esonero da responsabilità, che è in esso contenuto, sarebbe riferibile solamente al prestatore di servizi di pagamento del pagatore.

Questa limitazione muove dal fatto che mentre l'intermediario di partenza dell'operazione non conosce né potrebbe conoscere la titolarità del conto di accredito dell'operazione, così non è per il prestatore di servizi del beneficiario che dovrebbe conoscere l'intestazione del conto di accredito e quindi avrebbe tutti gli elementi per rilevare l'incongruità delle informazioni relative al pagamento, e di conseguenza dovrebbe essere lui ad agire al fine che l'operazione non venga eseguita erroneamente.

Questo orientamento è frutto di una precedente normativa, addirittura antecedente alla introduzione della disciplina specifica sui servizi di pagamento, riguardo il rapporto giuridico che viene ad instaurarsi tra la banca e il cliente, equiparato al mandato. Sulla scia di questa interpretazione quindi le prime applicazioni dell'art. 24 ritenevano

[350] Seguito soprattutto da alcune decisioni del Collegio di Roma. Ad esempio, decisione 8 aprile 2016, n. 3278 secondo la quale l'art. 24 «sembra destinata a regolare i rapporti tra l'ordinante e la sua banca, sollevando quest'ultima da ogni responsabilità qualora essa esegua l'ordine in conformità all'identificativo unico fornito dal pagatore, ma nulla dice in ordine al grado di diligenza che la banca del beneficiario deve osservare nell'accreditare la somma ricevuta dalla banca dell'ordinante».; decisione 25 marzo 2016, n. 2841; decisione 19 gennaio 2016, n. 405; *etc* reperibili sul sito ufficiale dell'Arbitro Bancario Finanziario, www.arbitrobancariofinanziario.it

l'intermediario del beneficiario del bonifico astrattamente responsabile della difformità tra il conto di destinazione del pagamento e l'IBAN indicato nell'ordine, rientrando il suo comportamento di controllo nell'area dei principi di buona fede e diligenza professionale, mentre era da ritenersi esente da responsabilità solamente l'intermediario del pagatore. [351]

Tale configurazione però esponeva l'intermediario del beneficiario del pagamento ad essere ritenuto inadempiente qualora non avesse adottato un sistema in grado di rilevare l'errore dell'utente

Un orientamento più recente[352] ritiene che la limitazione di responsabilità valga tanto per il prestatore di servizi del pagatore che per quello del beneficiario, ciò al fine di semplificare il procedimento di pagamento e rendere effettivo l'obiettivo della legislazione europea di rendere i pagamenti efficienti e veloci.

Infatti si noti che prima della creazione della SEPA, il sistema utilizzato dalla banche era strutturato in modo tale da riuscire a rilevare gli eventuali errori fatti dal cliente, questo però andava a discapito della velocità dell'operazione che subiva un rallentamento significativo perché il sistema a quel punto quando individuava l'errore bloccava il procedimento di pagamento ed era necessario l'intervento manuale dell'operatore dell'intermediario

---

[351] Così F. MARASA, *Riflessioni su Iban errato e responsabilità degli intermediari*, in *Banca, borsa, tit. cred.,* fasc. 6, 2019, p. 655.

[352] Collegio di Roma, 21 febbraio 2019, n. 5543; Collegio di Bologna, 20 marzo 2018, n. 6341; Collegio di Roma, 5 febbraio 2018, n. 3069; Collegio di Milano, 30 novembre 2017, n. 15857; Collegio di Bari, 8 novembre 2017, n. 14205; Collegio di Milano, 11 giugno 2014, n. 3692; Collegio di Milano, 31 marzo 2016, n. 1935, tutte reperibili sul sito ufficiale dell'ABF, www.arbitrobancariofinanziairio.it.

che verificava l'errore e solo dopo aver contattato il cliente dava seguito al procedimento. La SEPA invece ha introdotto un sistema in cui l'IBAN è l'unico identificativo da utilizzare per eseguire l'operazione e quindi ha eliminato di conseguenza il controllo di congruità tra questo e le altre informazioni fornite dal pagatore che ordina il pagamento.[353]

Seguendo l'ultima interpretazione, l'identificativo unico fa sorgere una presunzione di correttezza della stessa che è uguale per entrambi gli intermediari che partecipano al procedimento. Nessuno dei due sarebbe infatti tenuto ad eseguire un controllo circa la congruità delle informazioni relative al pagamento fornite dall'utente.

Per chiudere il dibattito è intervenuto il Collegio di Coordinamento dell'ABF, la cui posizione è stata successivamente confermata dalla Corte di Giustizia con la sentenza C-245/18, 21 marzo 2019[354] affermando che il disposto dell'art. 74 della direttiva 2007/64/CE è applicabile anche all'intermediario del beneficiario in quanto l'identificativo unico svolge la funzione di indirizzare i pagamenti consentendone l'esecuzione interamente automatizzata, rimuovendo l'obbligo del intermediario, tanto di quello del pagatore che di quello del beneficiario, di un controllo *ex ante* che potrebbe inficiare l'efficienza del sistema di pagamento.

---

[353] Sempre F. MARASA, *Riflessioni su Iban errato e responsabilità degli intermediari*, *op. cit.*, p. 664.

[354] La pronuncia della Corte di Giustizia era stata richiesta tramite un rinvio pregiudiziale operato dal tribunale di Udine il 3 aprile 2018, atteneva alla corretta interpretazione degli articoli 74 e 75 della direttiva 2007/64/CE relativa ai servizi di pagamento nel mercato interno nell'ambito di una controversia intercorrente tra la società Tecnoservice Int. S.r.l. in fallimento e Poste Italiane S.p.a. in merito al pagamento di un bonifico ad un beneficiario erroneo, a causa di un identificativo unico inesatto fornito dal pagatore.

Il motivo di tale orientamento deve essere rinvenuto nei principi che hanno ispirato le due normative (in questo caso la *PSD* e il d.lgs. 11/2010), i quali al fine di creare un mercato dei pagamenti efficienti e concorrenziale, hanno elaborato regole speciali di condotta che permettono all'intermediario di semplificare e velocizzare il procedimento di pagamento, creando «uno standard di comportamento per tutti gli intermediari coinvolti nella realizzazione di un bonifico, volto a promuovere l'esecuzione dell'operazione esclusivamente sulla base dell'identificativo unico fornito dall'ordinante senza bisogno e senza obbligo di effettuare alcun riscontro con le ulteriori informazioni contenute nell'ordine».[355]

Questo orientamento è stato confermato anche dalla *PSD2*[356] e dal d.lgs. n. 218/2017, le quali hanno ribadito come la

[355] Decisione dell'ABF n. 162 del 2017.

[356] Si fa qui riferimento al considerando 88 della PSD2 (direttiva 2366/2015) in cui si sottolinea che «è opportuno che il prestatore di servizi di pagamento abbia la possibilità di specificare senza ambiguità le informazioni richieste per eseguire correttamente un ordine di pagamento. D'altro canto, tuttavia, per evitare la frammentazione e non mettere in pericolo la creazione di sistemi di pagamento integrati nell'Unione, è opportuno che non sia consentito agli stati membri di imporre l'uso di un particolare identificativo per le operazioni di pagamento. Tuttavia, ciò non dovrebbe impedire agli Stati membri di richiedere al prestatore di servizi di pagamento del pagatore di agire con la dovuta diligenza e di verificare ove tecnicamente possibile e senza che sia necessario un intervento manuale, la coerenza dell'identificativo unico e, qualora si rilevi l'incoerenza dell'identificativo unico, di rifiutare l'ordine di pagamento e di informare il pagatore. È opportuno che la responsabilità del prestatore di servizi di pagamento sia limitata all'esecuzione corretta dell'operazione di pagamento conformemente all'ordine di pagamento dell'utente di servizi di pagamento. Qualora i fondi di un'operazione di pagamento arrivino al destinatario sbagliato, a causa dell'identificativo unico inesatto

responsabilità dell'intermediario ai sensi dell'art. 25 deve essere accertata solo sulla base dell'IBAN che consente l'esecuzione interamente automatizzata dell'operazione.

Quindi, secondo il collegio, nonostante la eliminazione di tale controllo di congruità, possa determinare una minor tutela del singolo utente, ciò risponde comunque a un interesse generale perseguito dalla normativa sui servizi di pagamento, che ha introdotto regole di condotta speciali per gli intermediari in grado di garantire pagamenti rapidi ed efficienti. Nel realizzare ciò il legislatore ha tenuto conto di un attento bilanciamento degli interessi e degli obblighi delle parti.[357]

Anche la Corte di Cassazione è recentemente intervenuta con ordinanza n. 21205 del 2024 su questo tema, affermando che, data la *PSD2* e il d.lgs. 11/2010 che la recepisce, non sussite alcune responsabilità in capo alla banca e tutti i prestatori di servizi di pagamento coinvolti sono autorizzati «ad eseguire l'operazione in conformità dell'IBAN fornito dall'utilizzatore senza tenere conto di eventuali ulteriori informazioni contenute nell'ordine, quale il nome del beneficiario». La Corte spiega inoltre la ratio di tale scelta operata dal legislatore: «il conto di destinazione del bonifico s'individua tramite il solo IBAN al fine di consentire il trattamento completamente automatizzato dell'ordine di bonifico secondo gli standard elaborati dal consorzio interbancario SWIFT».

---

fornito dal pagatore, i prestatori di servizi dovrebbero cooperare compiendo ragionevoli sforzi per recuperare i fondi, comunicando le informazioni pertinenti».

[357] In tal senso F. MARASA, *Riflessioni su Iban errato e responsabilità degli intermediari*, *op. cit.*, pp. 666

In ogni caso nessuna norma vieta all'intermediario di effettuare controlli ulteriori in grado di riuscire a identificare l'errore delle informazioni del pagamento[358]; tuttavia, se decide di eseguirlo egli è soggetto alle norme generali in tema di esecuzione del contratto che gli impongono di agire tutelando l'interesse del cliente.

In questo caso, infatti, se l'intermediario pur consapevole dell'errore, portasse a termine l'operazione, potrebbe essere ritenuto responsabile nei confronti dell'utente per essere venuto meno ai propri doveri di diligenza e buona fede e quindi oltre a doversi adoperare per recuperare la somma, sarebbe anche esposto al rischio di dover risarcire l'utente per gli eventuali danni subiti.

Per quanto riguarda la disciplina dell'identificativo unico inesatto e l'aggiornamento della *PSD2*, all'art. 74 del *PSR* non ci sono state significative novità se non la precisazione al paragrafo 4 che nel caso sia concordato nel contratto quadro, il prestatore di servizi di pagamento potrà addebitare spese all'utente di servizi di pagamento per il recupero in maniera ragionevole e proporzionata ai costi sostenuti.

Inoltre, è stata introdotta al paragrafo 6 la disposizione secondo la quale «Se l'identificativo unico fornito dal prestatore di servizi di disposizione di ordine di pagamento è inesatto, i

[358] Si veda in tal senso G. MARINO, *IBAN "sbagliato" e responsabilità delle banche nell'esecuzione dell'operazione di bonifico*, in *Nuova giurisprudenza civile commentata*, fasc. 10, 2016.

prestatori di servizi di pagamento sono responsabili a norma dell'articolo 76».

L'articolo 76 si occupa della «responsabilità in caso di prestazione di servizi di disposizione di ordine di pagamento per la mancata esecuzione o l'esecuzione inesatta o tardiva delle operazioni di pagamento». È opportuno a norma di tale articolo che il prestatore di servizi di pagamento del pagatore (o il prestatore di servizi di pagamento di radicamento del conto, o, del caso, il prestatore di servizi di disposizione di ordine di pagamento) si assuma la responsabilità della corretta esecuzione del pagamento, anche per quanto riguarda l'intero importo dell'operazione di pagamento e il tempo di esecuzione. In conseguenza di tale responsabilità, nel caso in cui l'intero importo non sia accreditato al prestatore di servizi di pagamento del beneficiario o sia accreditato in ritardo, il prestatore di servizi di pagamento del pagatore dovrebbe rettificare l'operazione di pagamento o rimborsare senza indugio il corrispondente importo dell'operazione al pagatore. Inoltre il pagatore o il beneficiario non debbono farsi carico dei costi relativi a un pagamento non corretto.

Questo vale sia in caso di mancata esecuzione, che nel caso di esecuzione inesatta (anche a causa di identificativo unico inesatto fornito dal prestatore di servizi di pagamento) o tardiva.[359]

4. Art. 25 d.lgs. 11/2010: la responsabilità per mancata, inesatta o tardiva esecuzione

La seconda situazione patologica cui si faceva riferimento in apertura di questo capitolo riguardava il momento in cui si ha il mancato

[359] In tal senso il considerando 95 del *PSR*.

rispetto degli estremi dell'operazione di pagamento, il prestatore di servizi di pagamento del pagatore diviene inadempiente e ciò schiude l'applicazione dell'art. 25[360] d.lgs. 11/2010.

In questo caso a differenza del primo, il consenso è stato correttamente prestato da parte del pagatore ma è intervenuto successivamente un motivo per cui il prestatore di pagamento ha mancato di compiere l'operazione di pagamento, o questa è stata compiuta tardivamente o in modo inesatto.

La disciplina contenuta in tale articolo del decreto si concentra sul modo in cui un'operazione di pagamento viene eseguita e sul caso in cui essa non venga affatto eseguita, prescindendo dagli elementi che hanno dato luogo all'inesattezza o al difetto di esecuzione quali la volontà del pagatore, errori dell'utilizzatore, eventi accidentali o inevitabili.[361]

La *littera legis* recita «Fatti salvi gli articoli 9, 24, commi 2 e 3, e 28, quando l'operazione di pagamento è disposta dal pagatore, il prestatore di servizi di pagamento del pagatore è responsabile nei confronti di quest'ultimo della corretta esecuzione dell'ordine di pagamento ricevuto, a meno che non sia in grado di provare al pagatore ed eventualmente al prestatore di servizi di pagamento del beneficiario che quest'ultimo ha ricevuto l'importo dell'operazione conformemente all'articolo 20, comma

[360] In tal senso, si vedano A. SCIARRONE ALIBRANDI, E. DELLAROSA, sub art.25, in *La nuova disciplina dei servizi di pagamento*, a cura di M. Mancini, Torino, Giappichelli, 2011, p.247 e ss.

[361] Così il provvedimento di Banca d'Italia, del 5 luglio 2011 «Attuazione del Titolo II del Decreto legislativo n. 11 del 27 gennaio 2010 relativo ai servizi di pagamento (Diritti e obblighi delle parti)».

1. In tale caso, il prestatore di servizi di pagamento del beneficiario è responsabile nei confronti del beneficiario della corretta esecuzione dell'operazione di pagamento».

Tale articolo è una tutela per l'utente da eventuali errori tecnici e operativi che possono verificarsi nel processo di pagamento.

Qualora venga riscontrata in capo al PSP del pagatore la responsabilità per la mancata o inesatta operazione di pagamento, gli sarà chiesto un ripristino della situazione a come era prima del verificarsi di detto evento.

Dovrà essere accreditato il conto del pagatore dell'importo del bonifico «senza indugio» avendo l'accorgimento che «la data della valuta dell'accredito sul conto di pagamento del pagatore non deve essere successiva a quella di addebito dell'importo».[362] Questo vale anche nel momento in cui il responsabile sia il prestatore di servizi di pagamento del beneficiario.[363]

Al comma 7 si delinea il dovere dei prestatori di servizi di pagamento di «adoperarsi senza indugio e senza spese, su richiesta dei rispettivi utenti, a rintracciare l'operazione di pagamanto, e li informano del risultato».

---

[362] Così l'art. 25, comma 2 d.lgs. 11/2010.

[363] Art. 25 comma 4 d.lgs. 11/2010: «Qualora il prestatore di servizi di pagamento del beneficiario sia responsabile (…) mette senza indugio l'importo dell'operazione di pagamento a disposizione del beneficiario o accredita immediatamente l'importo corrispondente sul conto di pagamento del beneficiario medesimo. La data di valuta dell'accredito sul conto di pagamento di quest'ultimo non deve essere successiva a quella che sarebbe stata attribuita al beneficiario in caso di esecuzione corretta dell'operazione di pagamento».

Inoltre, al comma 8 si precisa che «i prestatori di servizi di pagamento sono inoltre responsabili nei confronti dei rispettivi utenti di tutte le spese ed interessi loro imputati a seguito della mancata, inesatta o tardiva esecuzione dell'operazione di pagamento».

Quindi sono i PSP (del pagatore e del beneficiario) ad avere l'onere di attivarsi per rimediare alla mancata, inesatta o tardiva operazione di pagamento, sopportando anche eventuali spese dovute a tale operazione.

All'art. 25-bis si delinea la responsabilità nel caso in cui l'operazione sia stata prestata mediante un prestatore di servizi di disposizione di ordine di pagamento, facendo ricadere sul prestatore di servizi di radicamento del conto il dovere di rimborsare l'importo dell'operazione.

All'art. 26 «Risarcimento dei danni ulteriori» si stabilisce che «qualsiasi risarcimento ulteriore rispetto a quelli previsti dalla presente sezione può essere determinato in conformità alla disciplina applicabile al contratto concluso tra l'utente e il prestatore di servizi di pagamento».

Nel caso in cui siano coinvolti degli intermediari ulteriori (in particolare si fa riferimento ai *TPP*[364]) si dovrà applicare l'art. 27 «diritto di regresso» il quale stabilisce che «qualora la responsabilità di un prestatore di servizi di pagamento ai sensi dell'articolo 25 sia attribuibile ad un altro prestatore di servizi di pagamento coinvolto o ad un qualsiasi altro soggetto interposto

[364] In tal senso si v. A. MESSORE, *La nuova disciplina dei servizi di pagamento digitali prestati dai Third Party Providers*, in *Le Nuove Leggi Civili Commentate*, n. 2, 1 marzo 2020, pp. 511 e ss.

nell'esecuzione dell'operazione, quest'ultimo risarcisce il primo prestatore di servizi di pagamento in caso di perdite o di importi versati ai sensi del medesimo articolo 25». Possono anche essere previsti risarcimenti ulteriori in base agli accordi tra i prestatori di servizi di pagamento coinvolti (comma 2 art. 27).

Da ultimo, all'art. 28 viene affermato che la responsabilità del prestatore di servizi di pagamento viene esclusa qualora si riscontrino delle situazioni di caso fortuito o forza maggiore e nei casi in cui il prestatore di servizi di pagamento abbia agito in conformità con i vincoli derivanti da altri obblighi di legge.

Per quanto attiene alle novità introdotte dal *PSR* la disciplina della «responsabilità dei prestatori di servizi di pagamento per la mancata esecuzione o l'esecuzione inesatta o tardiva delle operazioni di pagamento» viene confermata all'art.75.

CONCLUSIONI

Il presente lavoro ha voluto cercare di illustrare la normativa europea che riguarda i servizi di pagamento e la sua introduzione all'interno dell'ordinamento italiano.

Si è visto come dapprima la *PSD* ha cercato di istituire un mercato unico e armonizzato dei servizi di pagamento. Successivamente con la *PSD2* si sono attuate importanti e significative modifiche al fine di adeguare la normativa ai cambiamenti tecnologici che stanno travolgendo il settore dei servizi di pagamento, e da ultimo come l'innovazione tecnologica sia tale per cui ci sia sempre bisogno di un costante aggiornamento della normativa, come testimoniato dal'ultima proposta di modifica *PSD3* e *PSR*.

Si è vista l'incapacità del legislatore europeo di riuscire a dare una definizione generalizzata di servizi di pagamento, complice da un lato la sua prudenza nel ricomprendere o meno un servizio di pagamento all'interno della disciplina e dall'altro l'imprevedibile innovazione tecnologica dei servizi di pagamento, preferendo aggiornare eventualmente l'elenco.

La *PSD2* ha apportato significative novità come il sistema di autenticazione forte, l'*open banking* e l'introduzione di nuovi operatori nell'ambito dei servizi di pagamento quali i Third Party Providers nelle loro diverse sfumature.

Si è esplorata poi la normativa interna, dapprima le modifiche che hanno riguardato il Testo Unico Bancario in tema di trasparenza delle operazioni di pagamento, con una analisi più specifica con riguardo al capo II-bis del testo, per poi volgere uno sguardo agli obblighi di informativa contenuti nel provvedimento di Banca d'Italia del 29/07/2009.

Successivamente si sono esposte le dinamiche dell'operazione di pagamento contenute nel l d.lgs. 11/2010 che ha recepito la direttiva 2007/64/CE (*PSD*), le successive modifiche intervenute con la *PSD2* (recepite con d.lgs. 218/2017) e le proposte di modifica che potrebbero intervenire in vista dell'approvazione definitiva di *PSD3* e *PSR*.

Si è visto come l'autorizzazione da parte dell'utente sia un aspetto centrale, indagando anche gli aspetti problematici come il riparto di responsabilità tra utente e prestatore di servizi di pagamento in operazioni non autorizzate, ambito in cui giurisprudenza della Cassazione e Arbitro Bancario Finanziario hanno un ruolo di forte indirizzamento, notando un chiaro interesse verso la tutela dell'utente. Si è esaminato anche il caso in cui l'utente disponga un pagamento fornendo un IBAN errato e cosa accade in caso di inesatta, mancata o tardiva esecuzione del pagamento.

A parere di chi scrive, in generale sui servizi di pagamento, è fondamentale anche l'educazione dell'utente dei servizi di pagamento ad una corretta *self-protection*, al fine di non cadere in frodi quali il *phishing* o le più subdole tecniche di sottrazione di credenziali di accesso all'istituto di pagamento. Infatti, la protezione dell'utente deriva da un duplice fattore: il suo comportamento e la capacità del prestatore di servizi di pagamento di attuare misure di protezione adeguate.

Assieme ai vantaggi emersi con la costante innovazione tecnologica, non si possono non notare anche le sfide davanti cui è messo in primis il legislatore europeo, e poi di conseguenza quello nazionale, che deve cercare di garantire un equilibrio tra innovazione e sicurezza dell'utente.

Il futuro dei servizi di pagamento appare in continua evoluzione, attualmente non è prevedibile fino a che punto arriveranno le nuove tecnologie e come queste possano ulteriormente trasformare il panorama

normativo del settore bancario e finanziario. É in ogni caso necessario, a parere di chi scrive, un approccio europeo al fine di aversi un settore armonizzato, e uno stretto coordinamento tra le autorità. Lo sviluppo e l'integrazione delle modalità innovative con cui vengono prestati i servizi di pagamento, infatti, richiedono regole comuni al fine di realizzare un concreto *level playing field*.

ABBREVIAZIONI

ABE: Autorità Bancaria Europea

ASPSP: Account servicing payment service provider

ATM: Automated teller machine

BCE: Banca Centrale Europea

CISP: Card Issuer Service Providers

DLT: Distributed ledger technology

EBA: European Banking Authority

EMD: Electronic Money Directive

ESA: European Supervisory Authorities

GDPR: General Data Protection Regulation

IBAN: International bank account number

NFC: Near Field Communication

NFT: non fungible token

PAD: Payment Account Directive

PISP: Payment Initiation Service Provider

PSD: Paymente Services Directive

PSP: prestatore di servizi di pagamento

PSR: Payment Services Regulation

SCA: Strong Costumer Authentication

SEPA: "*Single Euro Payments Area"*

NORMATIVA DI RIFERIMENTO

1. *Direttive e regolamenti europei*

Payment Services Directive 1 (PSD1) Direttiva 2007/64/CE

Payment Services Directive 2 (PSD2) Direttiva 2015/2366/CE

Payment Services Directive 3 (PSD3) Proposta di direttiva 2023/0209/COD

Payment Services Regulation (PSR) Proposta di regolamento 2023/0210/COD

Payment Account Directive (PAD) Direttva 2014/92/UE

Electronic Money Directive (EMD) Direttiva 2009/110/CE

Regolamento europeo sulle cripto-attività (MICA) 2023/1114

Regolamento Generale Sulla Protezione dei Dati (GDPR) 2016/679

Regolamento delegato (UE) 2018/389 della Commissione del 27 novembre 2017

2. *Diritto nazionale*

Testo Unico Bancario (TUB) d.lgs. 1° settembre 1993 n. 385

D.lgs. 11/2010, Attuazione della direttiva 2007/64/CE

GIURISPRUDENZA

Cassazione Civile n. 16573/2018

Cassazione Civile n. 9158/2018

Cassazione Civile n.13685/2019

Cassazione Civile n. 7214/2023

Cassazione Civile n. 31136/2023

Cassazione Civile n. 3780/2024

Cassazione Civile n. 23683/2024

Corte di Giustizia 21/03/2019, sentenza C-245/18

Pronunce da parte dell' Arbitro Bancario Finanziario:

Collegio di Coordinamento, Decisione n. 1820/2013

Collegio di Coordinamento, Decisione n. 22745/2019

Collegio di Coordinamento, Decisione n. 21285/2021

Collegio di Bari, Decisione n. 388/2024

Collegio di Bologna, Decisione n. 6341/2018

Collegio di Bologna, Decisione n. 1307/2019

Collegio di Bologna, Decisione n. 1905/2023

Collegio di Bologna, Decisione n. 577/2024

Collegio di Bologna, Decisione n. 2593/2024

Collegio di Milano, Decisione n. 18738/2021

Collegio di Milano, Decisione n. 1963/2024

Collegio di Milano, Decisione n. 1634/2024

Collegio di Milano, Decisione n. 1612/2024

Collegio di Milano, Decisione n. 1598/2024

Collegio di Milano, Decisione n. 1460/2024

Collegio di Milano, Decisione n. 158/2024

Collegio di Milano, Decisione n. 1964/2024

Collegio di Milano, Decisione n. 1606/2024

Collegio di Palermo, Decisione n. 11980/2023

Collegio di Torino, Decisone n. 643/2024

Collegio di Torino, Decisione n. 1487/2024

Collegio di Roma, Decisione n. 2339/2013

Collegio di Roma, Decisione n. 2841/2016

Collegio di Roma, Decisione n. 5543/2019

PROVVEDIMENTI DELLE AUTORITÀ

Atti del Governo, *Servizi di pagamento nel mercato interno,* 20 gennaio 2020

Banca d'Italia, *Disposizioni di vigilanza per gli istituti di pagamento e gli istituti di moneta elettronica*

Circolare del Ministero dello Sviluppo Economico del 21/02/2007 recante "Chiarimenti in merito all'applicazione dell'art. 10 della legge 4 agosto 2006, n. 248

Circolare Abi, *Serie tecnica n. 14 – 31 marzo 2010*, Bancaria ed., 6, *sub* art. 5

Circolare del 17 maggio 2016 intitolata «*Disposizioni di vigilanza per gli istituti di pagamento e gli istituti di moneta elettronica*»

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, Bruxelles, 24.9.2020

Provvedimento di Banca d'Italia del 29/07/2009

Provvedimento di Banca d'Italia, del 5 luglio 2011 «Attuazione del Titolo II del Decreto legislativo n. 11 del 27 gennaio 2010 relativo ai servizi di pagamento (Diritti e obblighi delle parti)»

BIBLIOGRAFIA

G. ARDIZZI, A. GAMBINI, A. NOBILI, E. PIMPINI, G. ROCCO, *L'impatto della pandemia sull'uso degli strumenti di pagamento in Italia* in *Mercati, Infrastrutture, sistemi di pagamento*, 8/2021

A. ARGENTATI, *Le banche nel nuovo scenario competitivo. Fintech, il paradigma Open banking e la minaccia delle big tech companies*, n. 3/2018

I. AVEGNO, *Regolamentazione delle cripto-attività: lo scenario comunitario*, *Riv. Amministrazione & Finanza*, n. 1/2024

S. BALSAMO TAGNANI, *Il mercato europeo dei servizi di pagamento si rinnova con la PSD2*, in *Contr. Impr. Eur.*, 2018

BANCA D'ITALIA, *Verso la revisione della PSD2: il dialogo della Banca d'Italia con gli operatori del mercato dei pagamenti*

P. BARCELLONA, *Note critiche in tema di rapporti fra negozio e giusta causa dell'attribuzione*, Giuffreè, 1964

A. BARENGHI, *Note sulla Trasparenza Bancaria. Venticinque anni dopo,* in *Banca, Borsa, Tit. Cred.*, n. 2/2018

G.B. BARILLÀ, *L'addebito diretto*, Giuffrè, Milano 2014

G. B. BARILLÀ, *Dal rid al nuovo addebito diretto SEPA*, in *Analisi Giuridica* dell'Economia, n. 1/2015

G. BERTI DE MARINIS, *La disciplina dei pagamenti non autorizzati nel nuovo sistema delineato dal recepimento della direttiva PSD2,* in *Diritto della Banca e del mercato finanziario*, 2018

E. BOUGLEX, F. DECLICH, G. BARRERA, *GDPR tra protezione dei dati personali e privacy. Intervista a Giulia Barrera*, consultabile su www.doi.org/10.4000/aam.4089

A. CALONI, *Deposito di cripto attività presso una piattaforma exchange: disciplina e attività riservate*, in *G. comm*., 2020

F. CASCINELLI e L.BETTINELLI, *Verso la PSD3 e il nuovo Regolamento sui Servizi di Pagamento,* consultabile al sito: www.dirittobancario.it

I.A. CAGGIANO, *Pagamenti non autorizzati tra responsabilità e restituzioni. Una rilettura del d. legisl. 11/2010 e lo scenario delle nuove tecnologie*, in *Riv. dir. civ*., 2017

E. CAPOBIANCO *I contratti bancari*, in *Trattato*, M. RESCIGNO-E. GABRIELLI (a cura di), Torino, 2016

R. CARATOZZOLO, *La responsabilità delle banche per la violazione degli obblighi contrattuali*, Milano, Giuffrè, 2007

A. CAROBENE, M. MASTRANGELO, *La tutela dei dati personali in un mondo digitale. Il regolamento europeo sulla privacy*, ,in *Riv. Aggiornamenti Sociali*, Giugno-Luglio 2019.

P. CARRIERE, *Decreto Fintech e MICAR: il quadro normativo sulle cripto-attività*, dal sito www.dirittobancario.it

P. CARRIERE, *Il fenomento delle cripto-attività in una prospettiva societaria*, in Banca Imprese e Società, n. 3/2020.

M. CATENACCI, C. FORNASARO, *PSD2: i prestatori di servizi di informazione sui conti (AISPS)*, aprile 2018, 3-4, disponibile su www.dirittobancario.it

E. CECCHINATO, *I servizi di pagamento* in *Il diritto bancario oggi: aspetti sostanziali processuali*, F. Aratari e Guido Romano (a cura di), Wolters Kluwer, 2023

E. CERVONE, *Strumenti di pagamento innovativi, interoperabilità e neutralità tecnologica: quali regole e quale governance per un mercato sicuro, efficiente ed innovativo*, in Riv. trim. diritto dell'economia, 2016

E. CERVONE, *Servizi di pagamento e innovazione tecnologica. Ruolo dell'Autorità bancaria europea alla luce della giurisprudenza della Corte di Giustizia*, in *Analisi Giuridica dell'Economia, Studi e discussioni sul diritto dell'impresa*, n. 2/2018

N. CIOCCA, *Servizi di custodia, negoziazione e regolamento di cripto-attività*, in *Oss. dir. civ. comm.*, 2022

F. CIRAOLO, *Le carte di debito nell'ordinamento italiano*, Milano, 2008

F. CIRAOLO, *I servizi di pagamento nell'era Fintech*, in *Fintech. Introduzione ai profili giuridici in un mercato unico tecnologico dei servizi finanziari*, Paracampo (a cura di), Torino, 2019

F. CIRAOLO, *Open Banking, Open Problems.* Riv. Dir. Banc., n. 4/2020

S. CIRIELLI, *Utilizzo non autorizzato dello strumento di pagamento e responsabilità della banca*, in *Giurisprudenza Commerciale*, n. 2/2022

I. COMUNALE e C. PELLEGRINI, *Payments Package: PSD3 e PSR*, in Deloitte, 2023.

I. D'AMBROSIO, *La tutela del consumatore nei pagamenti elettronici e la nuova direttiva europea PSD2*, n. 6/2019

M. DEOTTO, *Per le cripto-attività una disciplina criptica e anche un po' critica*, in *il fisco*, n. 45/2023

M. DE POLI, *Contrattazione bancaria e «dorsale informativa»*, in *Riv. dir. comm*., 2016

M. DE POLI, *Fundamentals of Banking Law*, CEDAM, II ed., 2020

M. DE POLI, sub *art. 126*-septies, in F. Capriglione (a cura di), *Commentario al Testo Unico delle Leggi in Materia Bancaria e Creditizia*, n. 4/2018, CEDAM

V. DE STASIO, *Sul momento e il luogo nel quale il beneficiario di un bonifico bancario acquista la disponibilità della somma oggetto dell'ordine di pagamento dell'ordinante*, in *Banca Borsa Titoli di Credito*, n. 3/2017

V. DE STASIO, *Operazione di pagamento non autorizzata e restituzioni*, Giuffrè, Milano, 2016

V. DE STASIO, *Riparto di responsabilità e restituzioni nei pagamenti non autorizzati*, in *Innovazione e regole nei pagamenti digitali: il bilanciamento degli interessi nella PSD2,* a cura di M. C. Paglietti e M. I. Vangelisti, Università degli Studi Roma Tre Dipartimento di Giurisprudenza, Roma Tre-Press, 2020

M. DI PIRRO, *L'arbitro Bancario Finanziario: La risoluzione stragiudiziale delle controversie bancarie*, Giuffrè Editore, 2017

M. DONNELLY, *Payments in the digital market: Evaluating the contribution of Payment Services Directive II*, Law School University College in Cork, Ireland

A. ENRIA, Commissione VI della Camera dei deputati sul "*Recepimento della direttiva sui servizi di pagamento*" in data 1° dicembre 2009

European Open Banking Forecast, 2022-2027 | Forrester, 2022

European Central Bank, *Card payments in Europe – current landscape and future prospects: A Eurosys- tem perspective*, 2019; e dello European Cards Stakeholders Group, *Feasibility Study on the development of open specifications for*

a card and mobile contactless payment application, 2017, entrambi disponibili all'indirizzo https://www.ecb.europa.eu

F. FERRETTI, *L'open finance. Quali prospettive regolatorie per una strategia UE in materia di protezione dei consumatori nella finanza digitale?*, in *Banca Impresa Società*, n. 2/2023

R. FRAU, *Home banking, phishing e responsabilità civile della banca*, nota a Cass. Civ., sez. VI, 12/04/2018, n. 9158, in *Resp. Civ. prev*., 2019

E. FUSCO, *Utilizzo improprio di un home banking da parte del rappresentante del correntista e perimetro della (ir)responsabilità di credito, tra legge antiriciclaggio, codice civile e disciplina sui servizi di pagamento*, in *Banca Borsa e tit. cred.,* n. 4/2021

P. GAGGERO, *voce «Responsabilità della Banca»*, nel *Digesto* IV ed., Disc. priv., sez. civ., agg., Utet, 1998

M. GAMBINI, *Ius variandi bancario e finanziario,* in Banca, Borsa e tit. cred., n. 4/2012

G. GIMIGLIANO e G. NAVA, *L'inquadramento giuridico dei Mobile payment: profili ricostruttivi e distonie regolamentari*, in *Smart cities e diritto dell'innovazione* a cura di G. OLIVIERI e V. FALCE, Milano, 2016

D. GIROMPINI, *PSD2 e Open Banking. Nuovi modelli di business e ruolo delle banche,* in *Bancaria*, n. 1/2018

LEMME-PELUSO, *Criptomoneta e distacco dalla moneta legale: il caso bitcoin*, in *Riv. Dir. Banc.*, n. 4/2016

M.C. LUPACCHINO, *Commento all'art. 17,* in *Aa.Vv., La nuova disciplina dei servizi di pagamento. Commentario al d.lgs. 27 gennaio 2010, n. 11*, Giappichelli, 2011

M. C. LUPACCHINO, *sub art. 24*, in *La nuova disciplina dei servizi di pagamento*, a cura di MANCINI, RISPOLI FARINA, SANTORO, SCIARRONE ALIBRANDI e O. TROIANO, Giappichelli, 2011

U. MALVAGNA, *Clausola di «riaddebito» e servizi di pagamento*, Giuffrè, Milano 2018

R. MENZELLA, *Il ruolo dei big data e il mobile payment,* in *Le nuove frontiere dei servizi bancari e di pagamento fra PSD", Criptovalute e Rivoluzione Digitale,* a cura di F. MAIMERI e M. MANCINI, *Quaderni di Ricerca Giuridica della Consulenza Legale di Banca d'Italia*, n. 87/2019.

F. MARASA, *Riflessioni su Iban errato e responsabilità degli intermediari*, in *Banca, borsa, tit. cred.,* n. 6/2019

G. MARCHIANÓ, *Brevi riflessioni sulla proposta di creare l'euro digitale*, in *Amm. E Cont.*, 2021

G. MARINO, *IBAN "sbagliato" e responsabilità delle banche nell'esecuzione dell'operazione di bonifico*, in *La nuova giurisprudenza civile commentata*, n. 10/2016

G. MARINO, *Carte di pagamento con funzione contactless, uso non autorizzato e responsabilità dei prestatori di servizi di pagamento*, in *Osservatorio del diritto civile e commerciale,* n. 1/2021

F. MARRELLA, *I pagamenti ed i contratti di finanziamento*, in *Manuale di diritto del commercio internazionale. Contratti internazionali, imprese globali ed arbitrato,* Wolters Kluwer, 2017

A. MESSORE, *La nuova disciplina dei servizi di pagamento digitali prestati dai Third Party Providers,* in *Le nuove leggi civili commentate*, n. 2/2020

L. MIOTTO e M. SPERANZIN, *I pagamenti elettronici*, in *Diritto del Fintech*, M. Cian e C. Sandei (a cura di), CEDAM, 2020

L. MIOTTO, *I pagamenti elettronici*, in *Diritto del Fintech*, M. Cian e C. Sandei (a cura di), CEDAM, II ed. 2024

A. MIRONE, *La rilevanza del tempo nella disciplina dei rapporti bancari*, in *Banca, Borsa e tit. cred*., n. 4/2016

A. MIRONE, *Profili evolutivi della trasparenza bancaria*, in *Osservatorio del diritto civile e commerciale*, n. 1/2018

S. MONETI, *«Mobile payments»: gli sviluppi del mercato e l'inquadramento normativo*, in *Analisi Giuridica dell'Economia*, n. 1/2015

MUCCIARONE, *La trasparenza bancaria*, in *Trattato dei contratti*, V. ROPPO (a cura di), Milano, 2014

M. ONZA, *La trasparenza dei servizi di pagamento in Italia*, in *Banca, Borsa e tit. cred.*, n. 5/2013

M. Onza, *Estinzione dell'obbligazione pecuniaria e finanziamento dei consumi: il pagamento con la "carta"*, Giuffrè, Milano 2013

M. ONZA, *Gli strumenti di pagamento nel contesto dei pagamenti on line*, in *Dir. banc. fin.*, 2017

F. PANETTA, *L'innovazione digitale nell'industria finanziaria italiana*, Milano, 26 Settembre 2017, reperibile su www.bancaditalia.it

F. PANETTA, *Plasmare il futuro digitale dell'Europa: il percorso verso un euro digitale*, Bruxelles, 2023

A. PANTALEO, *I Prestatori di servizi su cripto-attività*, in S. CAPACCIOLI - M.T. GIORDANO (a cura di), Crypto-asset: Regolamento MiCA e DLT Pilot Regime. Analisi ragionata su token, stablecoin, CASP, Milano 2023

M.-T. PARACAMPO*, I prestatori di servizi per le cripto-attività. Tra mifidizzazione della MICA e tokenizzazione della Mifid*, Torino 2023

F. P. PATTI, *L'offerta al pubblico di cripto.attività nel titolo II del regolamento MICA*, in *Riv. Di diritto civile*, 1/2024

PSD3 e PSR: le norme sui servizi di pagamento approvate dal Parlamento Europeo, reperibile al sito www.dirittobancario.it

J PEGADO LIZ, Parere del Comitato economico e sociale europeo sul tema Autoregolamentazione e co-regolamentazione nel quadro legislativo dell'UE, INT/754

G.L. PELLIZZI, *La responsabilità della banca, in Banca*, *borsa, tit. cred.*, 1985, I

B. PIACENTINI, *La trasparenza nei servizi di pagamento: il provvedimento di Banca d'Italia 20 Giugno 2012 in Banca, borsa, tit. cred.*, n. 1/2014

M. PIERRO*, Contributo all'individuazione della nozione di crypto-asset e suoi riflessi nell'ordinamento tributario nazionale,* in *Rass. trib.*, n. 3/2022

M. PIERRO, *L'origine europea della nozione di cripto-attività e la scelta del legislatore nazionale*, in *Corriere Tributario*, n. 4/2024

T. N. POLI, *MiCA, Pilot Regime e Decreto Fintech: la regolazione del fenomeno crypto e le difficoltà di inquadramento nel sistema finanziario*, in *Dir. Bancario*, Dicembre 2023

M. C. PAGLIETTI, *Questioni in materia di prova nei casi di pagamenti non autorizzati*, in *Innovazioni e regole nei pagamenti digitali: bilanciamento degli interessi*

nella PSD2, a cura di M. C. Paglietti e M. I. Vangelisti, Università degli Studi Roma Tre Dipartimento di Giurisprudenza, Roma Tre-Press, 2020

F. PORTA, *Obiettivi e strumenti della PSD2,* in *Le nuove frontiere dei servizi bancari e di pagamento fra PSD", Criptovalute e Rivoluzione Digitale* a cura di F. MAIMERI e M. MANCINI, *Quaderni di Ricerca Giuridica della Consulenza Legale di Banca d'Italia*, n. 87/2019

V. PROFETA, *I third party provider: profili soggettivi e oggettivi*, in *Le nuove frontiere dei servizi bancari e di pagamento fra PSD 2, criptovalute e rivoluzione digitale*, a cura di F. MAIMERI e M. MANCINI, in *Quaderni di ricerca giuridica della consulenza legale di Banca d'Italia*, n. 87/2019

V. RABBITI e SCIARRONE ALIBRANDI, *I servizi di pagamento tra PSD2 e GDPR: Open Banking e conseguenze per la clientela*, in *Liber Amicorum Giudo Alpa*, a cura di Capriglione, Padova, Cedam, 2019

P.M. REEDTZ in *commentario al Decreto legislativo n.11/2010*, Giappichelli

M. RISPOLI FARINA, *Informazione e Servizi di Pagamento*, in *Analisi Giuridica dell'Economia*, Studi e discussioni sul diritto dell'impresa, 1/2015

M. RISPOLI FARINA, *La nuova direttiva PSD2: i principali tratti di novità,* in *L'evoluzione dei sistemi dei servizi di pagamento nell'era del digitale*, (a cura di) B. Russo, CEDAM, 2020

D. RUGGIU, *Secondary use", così la Ue ribalta il Gdpr e apre all'accesso indiscriminato ai nostri dati*, Agenda Digitale EU, articolo disponibile su www.research.unipd.it

B. RUSSO*, L'evoluzione dei sistemi e dei servizi di pagamento nell'era del digitale*, CEDAM, 2020

V. SANTORO, *I servizi di pagamento*, in *Rivista di studi giuridici IANUS*, n. 6/2012

M. SCHIEPPATI, *Banche, «pensare come Google»?*, in *Bancaria*, n. 3/2017

A. SCIARRONE ALIBRANDI, *L'interposizione della banca nell'adempimento dell'obbligazione pecuniaria*, Giuffrè, Milano 1997

A. SCIARRONE ALIBRANDI, *Impostazione sistematica della Direttiva PSD2*, reperibile al sito www.romatrepress.uniroma3.it

A. SCIARRONE ALIBRANDI, E. DELLAROSA, sub art.25, in *La nuova disciplina dei servizi di pagamento*, a cura di M. Mancini, Torino, Giappichelli, 2011

S. SICA, B. M. SABATINO, *Disintermediazione finanziaria e tutela del cliente e dell'utilizzatore*, in *Diritto dell'informazione e dell'informatica*, n. 1/2021

P. SIRENA, *La gestione di affari altrui*, Torino 1999

O. TROIANO E V.V. CUOCCI, *Commento all'art. 5*, in Mancini-Rispoli Farina-Santoro-Sciarrone Alibrandi-Troiano O. (a cura di), *La nuova disciplina dei servizi di pagamento*, Giappichelli, 2011

O. TROIANO, CUOCCI, *sub art 11*, in Mancini-Rispoli Farina-Santoro-Sciarrone Alibrandi-Troiano O. (a cura di), *La nuova disciplina dei servizi di pagamento*, Giappichelli, 2011

S. VANINI, *L'attuazione in Italia della seconda direttiva sui servizi di pagamento nel mercato interno: le innovazioni introdotte dal d.lgs. 15 dicembre 2017, n. 218*, in *Rivista Le nuove leggi*, 4/2018, Wolters Kluwer.

C. VENANZONI , *I servizi bancari online*, in *Il diritto bancario oggi: aspetti sostanziali e processuali*, F. Aratari e Guido Romano (a cura di), Wolters Kluwer, 2023

S. VEZZOSO, *Fintech, access to data, and the role of competition policy*, consultabile all'indirizzo https://ssrn.com/abstract=3106594

T. VITALE, *Funzione bancaria e responsabilità contrattuale della banca*, in *Funzione bancaria rischio e responsabilità della banca*, a cura di S. MACCARONE e A. NIGRO, Giuffrè, 1981

A. ZANUSSI in *Internet of Things e privacy. Sicurezza e autodeterminazione informativa.* , P. MORO e C. SARRA (a cura di), *Tecnodiritto: temi e problemi di informatica e robotica giuridica*, FrancoAngeli, 2017

RINGRAZIAMENTI

Alla mia mamma, che non mi ha mai fatta sentire inadeguata, che non mi ha mai fatta sentire in ritardo e che dopo otto anni di università non ha ancora capito bene come funziona. Mi sono sempre sentita guardata con ammirazione e mi ha sempre dato la spinta ad andare avanti. Mi hai vista gioire e rattristarmi, ma sicuramente una cosa che non vedrai più sono i miei libroni in giro.

Al mio papà, che ha sempre avuto una parola di conforto quando non riuscivo e un "bravissima bellissima del papà" quando finalmente passavo un altro scoglio. Che non mi ha mai messo pressione sul mio percorso e mi ha lasciato prendere le scelte che ritenevo più opportune.

A Giada e Silvia miei due pilastri della vita universitaria e che piano piano lo sono diventate anche fuori. Grazie di avermi fatto conoscere il piacere di bere the caldo, tisane calde e tisane fredde (di cui non conoscevo neanche l'esistenza), che in realtà erano solamente una scusa per fare due chiacchiere durante le sessioni di studio. Grazie per avermi sempre accolta nelle vostre case a "studiare" in qualsiasi stagione dell'anno. Grazie per tutto il vostro supporto sia dopo un esame andato bene che dopo un esame andato male. Grazie per avermi spinta sempre a provare, probabilmente senza di voi non sarei arrivata dove sono ora. Sono profondamente grata di avervi avute al mio fianco.

Ai miei compagni di uni Ale, Nicole, Gianmaria e Fanta per tutte le risate di questi anni, spero che le nostre strade trovino sempre il modo di incrociarsi nonostante le vie diverse che prenderemo.

A Lia, mia amica di sempre e spero per sempre, che silenziosamente mi è sempre stata vicina. In te vedo un punto fermo anche quando tutto intorno sta cambiando.

Alle mie sorelle Anna e Chiara, che anche se siamo diverse e qualche volta incompatibili potranno sempre contare su di me come io spero di poter contare su di loro.

Al mio fratellino Andrea (o Andreino) che entrava in camera almeno 5/6 volte a pomeriggio, nonostante lo esortassi a non disturbarmi mi ha sempre riempita di gioia vederlo aprire la mia porta. Gli dedico questo traguardo per fargli capire che niente è impossibile se lo si vuole davvero.

Ai miei nonni che mi hanno cresciuta e supportata in tutti i momenti della mia vita fino ad ora, che ad ogni esame passato hanno gioito con me, e mi hanno dato conforto quando non andavano bene. (P.S. Nonna mi dispiace dirlo ma non mi sono laureata grazie a Gesù, ma lo ringrazio lo stesso per il suo aiuto).

Al secondo Andrea della mia vita, che è arrivato in uno dei momenti più impegnativi del mio percorso universitario, che con pazienza (tanta) mi è sempre stato vicino, mi ha ascoltata ripetere e mi ha sempre spinta a non arrendermi e a rialzarmi dopo che le cose non andavano come avevo previsto, che non mi ha mai fatta sentire sbagliata, facendomi capire che non c'è un tempo per fare le cose ma che ognuno ha il suo. Che questo sia il primo di tanti importanti traguardi che taglieremo insieme.

A tutti i miei amici che ci sono stati in questi anni (come Margherita, Ilenia e Diletta) e che, anche inconsapevolmente, mi hanno sempre dato il coraggio e la forza di dare di più, grazie per i momenti di spensieratezza.