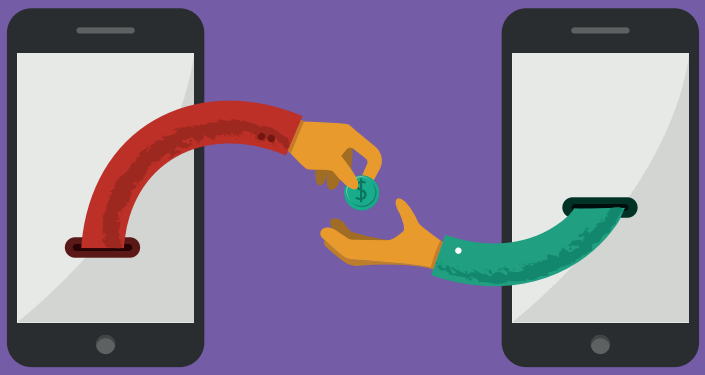
INNOVAZIONE E REGOLE NEI PAGAMENTI DIGITALI

IL BILANCIAMENTO DEGLI INTERESSI NELLA PSD2



A cura di
Maria Cecilia Paglietti
Maria Iride Vangelisti

Consumatori e Mercato 9

Nella stessa Collana

1. V. Zeno-Zencovich (a cura di), *Cosmetici. Diritto, regolazione, bio-etica*, 2014

2. M. Colangelo, V. Zeno-Zencovich, *Introduction to European Union transport law*, I ed. 2015; II ed. 2016; III ed. 2019.

3. G. Resta, V. Zeno-Zencovich (a cura di), *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, 2015

4. V. Zeno-Zencovich, *Sex and the contract* (II ed.), 2015

5. G. Resta, V. Zeno-Zencovich (a cura di), *La protezione transnazionale dei dati personali. Dai "safe harbour principles" al "privacy shield"*, 2016

6. A. Zoppini (a cura di), *Tra regolazione e giurisdizione*, 2017

7. C. Giustolisi (a cura di), *La direttiva consumer rights. Impianto sistematico della direttiva di armonizzazione massima*, 2017

8. R. Torino (a cura di), *Introduction to European Union internal market law*, 2017

Università degli Studi Roma Tre
Dipartimento di Giurisprudenza

INNOVAZIONE E REGOLE NEI PAGAMENTI DIGITALI

IL BILANCIAMENTO DEGLI INTERESSI NELLA PSD2

A cura di
Maria Cecilia Paglietti
Maria Iride Vangelisti

Consumatori e Mercato 9

RomaTrE-Press
2020

Elenco e qualifiche degli autori:

Daniele De Paoli, *Dirigente Dipartimento realtà economiche e produttive, Autorità Garante per la protezione dei dati*
Vincenzo De Stasio, *Professore ordinario di Diritto commerciale, Università degli studi di Bergamo*
Domenico Gammaldi, *Titolare del Servizio Supervisione sui mercati e sul sistema dei pagamenti, Banca d'Italia*
Vito Meli, *Responsabile Direzione Credito, Poste e Turismo, Autorità Garante della concorrenza e del mercato*
Simone Mezzacapo, *Professore associato di Diritto dell'economia, Università degli studi di Perugia*
Maria Cecilia Paglietti, *Ricercatrice di Diritto comparato, Università degli studi Roma Tre*
Maddalena Rabitti, *Professore ordinario di Diritto dell'economia, Università degli studi Roma Tre*
Antonella Sciarrone Alibrandi, *Professore ordinario di Diritto dell'economia, Università Cattolica del Sacro Cuore, Milano*
Bruna Szego, *Titolare del Servizio Regolamentazione e Analisi Macroprudenziale, Banca d'Italia*
Vincenzo Zeno-Zencovich, *Professore ordinario di Diritto comparato, Università degli studi Roma Tre*

Coordinamento editoriale:
Gruppo di Lavoro *Roma TrE-Press*

Elaborazione grafica della copertina: MOSQUITO. mosquitoroma.it

Impaginazione e cura editoriale: Colitti-Roma colitti.it

Edizioni: *Roma TrE-Press* ©
Roma, marzo 2020
ISBN: 978-88-32136-98-2

http://romatrepress.uniroma3.it

L'attività della *Roma TrE-Press* è svolta nell'ambito della
Fondazione Roma Tre-Education, piazza della Repubblica 10, 00185 Roma

Presentazione della collana "Consumatori e Mercato"

La Collana "Consumatori e mercato", pubblicata in open access dalla Roma TrE-Press, intende essere una piattaforma editoriale multilingue, avente ad oggetto studi attinenti alla tutela dei consumatori e alla regolazione del mercato. L'intento è di stimolare un proficuo scambio scientifico attraverso una diretta partecipazione di studiosi appartenenti a diverse discipline, tradizioni e generazioni.

Il dialogo multidisciplinare e multiculturale diviene infatti una componente indefettibile nell'àmbito di una materia caratterizzata da un assetto disciplinare ormai maturo tanto nelle prassi applicative del mercato quanto nel diritto vivente. L'attenzione viene in particolare rivolta al contesto del diritto europeo, matrice delle scelte legislative e regolamentari degli ordinamenti interni, e allo svolgimento dell'analisi su piani differenti (per estrazione scientifica e punti di osservazione) che diano conto della complessità ordinamentale attuale.

****

The "Consumer and market" series published, in open access, by Roma TrE-Press, aims at being a multilingual editorial project, which shall focus on consumer protection and market regulation studies. The series' core mission is the promotion of a fruitful scientific exchange amongst scholars from diverse legal systems, traditions and generations. This multidisciplinary and multicultural exchange has in fact become fundamental for a mature legal framework, from both the market practice and the law in action standpoints. A particular focus will be given on European law, where one can find the roots of the legislation and regulation in the domestic legal systems, and on the analysis of different levels, in line with the current complexity of this legal sector.

Indice

Introduzione

La Direttiva 2015/2366 sui servizi di pagamento, riformulando la normativa previgente, si propone di promuovere un mercato interno integrato dei pagamenti elettronici. La sua introduzione in Italia segna il dischiudersi all'interprete di nuove prospettive, sullo sfondo della duplice istanza del rafforzamento delle regole di sicurezza e della garanzia del *level playing field*.

La Direttiva ha il difficile compito di accompagnare lo sviluppo dei pagamenti elettronici con un quadro normativo fatto di regole certe ma adattabili ai diversi casi concreti, in grado di assicurare efficienza, sicurezza e uniformità dei servizi offerti. A questo fine, il legislatore comunitario si appoggia ad un organismo tecnico, l'Autorità Bancaria Europea, incaricata di stilare l'insieme delle norme tecniche di supporto all'applicazione della Direttiva.

La Banca d'Italia e l'Università di Roma Tre, in un'iniziativa congiunta, hanno inteso promuovere un momento di riflessione e confronto sulla materia, estremamente complessa sia per il tecnicismo degli argomenti legati all'esecuzione dei pagamenti e alla loro regolazione, sia per l'interdisciplinarietà di alcuni temi che investono le competenze di diverse Autorità. Le relazioni e le discussioni successive hanno trattato temi diversi e fra loro complementari. Tra questi, la tutela della concorrenza, la protezione dei consumatori, il *trade-off* fra sicurezza ed efficienza dei pagamenti. Particolare attenzione è stata dedicata al problema della sovrapposizione tra *corpus* di norme talora congeneri, che pone delicati problemi di raccordo quali, ad esempio, il riparto delle responsabilità tra prestatori di servizi di pagamenti e le intersezioni con la disciplina sulla privacy.

L'ampia portata della normativa è stata analizzata muovendo da una riflessione – articolata e congiunta – che accogliesse i più variegati punti di osservazione, appartenenti all'Accademia, alla Banca centrale nella sua funzione di Vigilanza sugli intermediari e di Sorveglianza sul sistema dei pagamenti e alle altre Autorità di controllo coinvolte dall'applicazione della Direttiva.

Lo sviluppo dei servizi di pagamento richiede che venga assicurata a tutti i soggetti la piena fiducia nei mezzi di trasferimento della moneta.

L'offerta di strumenti tecnologicamente avanzati, rispondenti alle esigenze di cittadini e imprese, deve essere affidabile e a prezzi sostenibili. È pertanto necessario che la connessione fra finanza, tecnica e diritto non risponda alla logica dell'uniformità, ma lasci all'interprete, tramite un complesso lavoro ricostruttivo, il compito di garantire all'assetto istituzionale la coerenza e l'effettività delle norme di cui si compone.

La problematica indagata pone, dunque, due ordini di necessità: un approccio scientifico, che avvii una riflessione di sistema sulle scelte di vertice compiute dal legislatore unionista prima, e domestico, poi, su temi giuridicamente e tecnicamente complessi come, ad esempio, quelli in tema di riparto di responsabilità; un approccio pratico, che suggerisca modelli ricostruttivi idonei a guidare tanto l'operatore del diritto nello *ius dicere* quanto utenti e prestatori di servizi di pagamento nell'individuazione concreta dei propri diritti e doveri.

La conoscenza diffusa del quadro regolamentare – e la sua corretta ricostruzione - sono funzionali anche allo sviluppo del mercato di riferimento: i cittadini e le imprese saranno invogliati a utilizzare gli strumenti elettronici in alternativa al contante tanto più si sentiranno sicuri e protetti anche nel caso di errore o frode. In questo modo sarà possibile realizzare un'ampia diffusione di strumenti di pagamento elettronici, intrinsecamente più efficienti e moderni rispetto al contante, assicurando alle imprese di poter sfruttare le economie di rete proprie del mercato dei pagamenti ed essere in grado di sostenere gli elevati costi dell'innovazione tecnologica, e agli utenti di poter godere dei relativi benefici.

Maria Cecilia Paglietti
Maria Iride Vangelisti
Roma, gennaio 2020

Prefazione

L'entrata in vigore della Direttiva 2366/15 (c.d. PSD2) ha degli effetti sistemici che vanno ben oltre la ormai consolidata e pervasiva regolamentazione dei servizi che riguardano gli strumenti di pagamento ed i soggetti che vi sono coinvolti.

i. Il primo, e quasi ovvio, fattore da considerare è la presa d'atto della ormai irreversibile avanzata di sistemi interamente digitali, con la completa dematerializzazione della moneta. Un processo che è iniziato molti anni orsono – circa un trentennio – e che è facile prevedere avrà ulteriori sviluppi tecnologici e dunque regolamentari. Beninteso si tratta solo di una tappa nella millenaria storia della moneta, e che dunque va vista senza indulgere nella neolatria. Dal metallo alla carta ai bit la strada è lunga, ed ogni passaggio implica oltre a opportunità anche rischi che non possono e non devono essere sottovalutati, ed in effetti non lo sono nella Direttiva.

ii. Il secondo punto è quello del nuovo ambiente popolato dai soggetti imprenditoriali nel sistema dei pagamenti. Una volta esso vedeva al centro l'istituto di emissione, circondato da una pletora di istituti di credito e dai pochissimi emittenti carte di credito. La realtà economica e sociale è profondamente mutata e non poteva essere altrimenti: sarebbe stato poco realistico immaginare che i sistemi di pagamento rimanessero immuni dai processi di digitalizzazione dei rapporti economici che coinvolgono miliardi di individui. Proprio perché in larga misura questi rapporti comportano la corresponsione di un corrispettivo monetario, questo dovrà adattarsi al nuovo ambiente. Si è ampiamente scritto su questa traiettoria ed in particolare se ciò comporti il tramonto della nozione di banca così come si è sviluppata almeno nell'ultimo secolo, e quali siano gli effetti di lunga durata sul modello c.d. renano indissolubilmente legato allo sviluppo del capitalismo nell'Europa occidentale. Il problema – ben chiaro nella Direttiva – consiste nel delineare un quadro regolamentare che garantisca una costante vigilanza prudenziale e al tempo stesso, legittimando soggetti intrinsecamente non bancari, eviti abusi ed ancor più strumentalizzazioni da parte di soggetti criminali.

iii. Tuttavia, quel che cambia non è solo il numero dei soggetti regolamentati, la loro intrinseca de-territorializzazione, la loro varietà, ma soprattutto il loro diverso rapporto con il denaro. Se il mondo finanziario è un ecosistema, siamo di fronte all'ingresso di nuove specie allogene destinate a modificare gli equilibri esistenti. Una delle principali caratteristiche di queste nuove specie è che si tratta di soggetti che possiamo qualificare anche come "data companies", ovverosia imprese che oltre ad intermediare fra debitore e creditore, in tale attività raccolgono milioni di dati che consentono loro di avere, in tempo reale, una radiografia che va ben al di là del singolo e mero pagamento. Mettendo insieme il dove, il quando, il quanto, il perché sotteso al trasferimento finanziario, attraverso tutti questi c.d. metadati i nuovi soggetti acquisiscono una conoscenza del mercato, delle sue tendenze, dei processi di consumo come già di per sé stessa, in termini di segmentazione per classi, ha uno straordinario valore. A ben vedere si tratta di un notevole passo avanti rispetto alla più generale acquisizione ed elaborazione di dati attraverso l'utilizzo da parte dei singoli delle reti di comunicazione. Tradizionalmente da tali dati aggregati si punta ad inferire comportamenti di rilievo economico. Nel mondo dei sistemi a pagamento non si tratta di inferire ma di avere evidenza diretta e dunque poter monitorare i flussi finanziari e prevedere le successive azioni. È la differenza fra inferire le intenzioni di viaggio di un gruppo di persone (mare, montagna, città d'arte) da una serie di ricerche in rete effettuate, e la scelta già avvenuta e che si è in grado di monitorare in tempo reale.

iv. Il valore di questi dati è tale da spiegare agevolmente il rapido affollamento di centinaia di soggetti intenzionati a trarre profitto dal nuovo contesto normativo. Anche qui il mutamento è significativo. Il valore delle operazioni di pagamento attraverso reti e sistemi digitali è in fisiologica crescita. Quel che cambia è il moltiplicarsi di soggetti non bancari. Non è detto che tutti superino la prova del mercato, ma si tratta di un processo irreversibile. Il cambiamento, tuttavia, non è senza aporie. I mercati finanziari sono, intrinsecamente, mercati fondati sulle informazioni e sulla conoscenza. La raccolta di dati è dunque essenziale per il buon funzionamento del mercato, sia per controllare in tempo reale la posizione dei soggetti, sia per valutare rischi e opportunità nelle operazioni di credito. "*Know your client*" non è solo uno slogan, ma un preciso obbligo.

v. Tutto questo però collide frontalmente con la retorica della protezione dei dati personali, incarnata dal Regolamento generale sulla protezione dei dati personali (GDPR – Regolamento 679/16) che vorrebbe sottoporre l'acquisizione, la elaborazione e la circolazione dei dati personali ad un

costante controllo dell'interessato, di cui la pietra di volta è il consenso e la indisponibile facoltà di revoca dello stesso, sempre, comunque e senza oneri economici o motivazionali.

La vicenda dei servizi di pagamento mette in luce la elefantiaca declamatorietà del GDPR. Da un lato, da tempo, la disciplina comunitaria prevede obblighi di comunicazione a carico dei soggetti finanziati (si v. in particolare le Direttive 48/2008 sul credito al consumo; e la Direttiva 17/2014 sui mutui ipotecari). Ma anche doversi di acquisizione di dati a carico degli istituti finanziari. Il principio della meritevolezza del credito, che è uno dei pilastri della stabilità finanziaria e delle politiche sia micro che macro-prudenziali. È ovvio che il "*credit scoring*" non può che fondarsi sulla piena accessibilità ai dati economico-finanziari dei singoli, i quali peraltro sono, e devono essere, condivisi da tutti. Se c'è un debitore a rischio questo non può approfittare delle eventuali asimmetrie informative per ottenere da B quel che gli è stato negato da A.

vi. In questo senso si possono leggere le disposizioni della Direttiva PSD2 sull'accesso dei fornitori dei servizi di pagamento ai dati bancari. E la giurisprudenza della Corte di giustizia che limita la tutela dei dati personali e il diritto all'oblio con riguardo ai dati finanziari in ragione di una "funzione sociale" della trasparenza (Caso C-398/15, *Manni c. Camera Commercio Lecce*). Si tratta peraltro di un percorso parabolico che partendo dal segreto bancario, si trasforma in "*disclosure*" a favore dei soggetti pubblici (in primo luogo delle autorità fiscali), per arrivare alla condivisa accessibilità a tali dati da parte degli operatori del settore. L'ingresso di piccole e grandi *data companies* nei mercati finanziari ha dunque l'effetto di innalzare la complessità dello scenario, mettendo in luce dinamiche in passato sottotraccia ed esaltando accanto al valore del pagamento il valore dei dati relativi ai pagamenti.

vii. È realistico immaginare che questo porti, in un certo numero di casi, ad un conflitto fra norme fra loro scarsamente compatibili (GDPR e politiche di trasparenza e prudenza finanziaria), e che si manifesteranno in primo luogo in conflitti di competenza fra i numerosi soggetti, in genere "indipendenti" preposti al governo del settore e fra i quali il coordinamento appare ancora lontano. Inevitabilmente ciò porterà ad un ulteriore sovraccarico di lavoro per la Corte di Giustizia UE che sempre più finirà per essere il "decisore di ultima istanza".

Vincenzo Zeno-Zencovich

Antonella Sciarrone Alibrandi

Impostazione sistematica della Direttiva PSD2

Sommario: 1. Le ragioni del passaggio da PSD a PSD2: innovazione tecnologica e *open banking* – 2. I principi cardine della PSD2: proporzionalità e trasparenza – 3. (*Segue*) il principio di *technological neutrality*. I problemi aperti dalle API.

1. *Le ragioni del passaggio da PSD a PSD2: innovazione tecnologica e* open banking

I servizi di pagamento, nell'intera dimensione del sistema finanziario, sono il comparto che, prima di ogni altro, è stato interessato dall'innovazione tecnologica: innovazione che, ormai da anni, ha spinto i *player* del settore verso modelli di *business* e soluzioni operative connotati da maggior efficienza, velocità e sicurezza. Ben può dirsi, quindi, che il settore dei servizi di pagamento sia una sorta di antesignano dell'odierno fenomeno del *FinTech*, inteso come "innovazione finanziaria abilitata dalle tecnologie digitali".

Proprio il costituire un fronte avanzato in termini di applicazione della digitalizzazione all'attività d'impresa ha permesso al settore in discorso di avere anche un primato, se così si può dire, dal punto di vista normativo. Le ragioni alla base della *Payment Services Directive* 2 (c.d. PSD2), adottata nel 2015 a soli sette anni di distanza dalla prima Direttiva in materia di servizi di pagamento (c.d. PSD)[1] risalente al 2007, si legano, infatti, principalmente alla emersione in tale settore di servizi (e soggetti) che, facendo leva sul canale digitale e sulla automazione dei processi, hanno generato nuove opportunità ma anche potenziali nuovi rischi per gli utenti e per il sistema nel suo complesso. Da qui la necessità di un secondo, ravvicinato intervento del legislatore europeo, chiamato a confrontarsi – prima che in altri ambiti del settore finanziario – con la frantumazione in atto della tradizionale catena del valore per effetto di nuove forme di attività e nuovi operatori, focalizzati solo su specifici segmenti della filiera, che puntano a sottrarre

[1] Direttiva 2007/64/Ce, attuata nel nostro ordinamento attraverso il D.lgs. n. 11 del 2010.

clientela agli *incumbent* e a disintermediarli.

Per meglio comprendere la portata della PSD2 e poterne apprezzare i tratti di novità rispetto allo scenario normativo di fondo, è bene volgere per un attimo lo sguardo al passato. Nel 2007 il legislatore europeo con la PSD ha per la prima volta delineato regole base comuni per un sistema armonizzato dei servizi di pagamento, contribuendo senz'altro, pur con tutti i limiti emersi in seguito, a creare un *level playing field* tra gli operatori europei nel settore in discorso. Sempre alla PSD si deve, infatti, grazie all'introduzione degli Istituti di Pagamento (IP) accanto ai già previsti Istituti di Moneta Elettronica (IMEL), l'erosione del monopolio bancario rispetto allo svolgimento di questa specifica attività di impresa.

Merita sottolineare subito - perché, come si vedrà in seguito, sotto questo profilo il contesto d'origine della PSD2 è differente e da tale diversità discendono conseguenze di un certo rilievo - che la prima Direttiva sui servizi di pagamento ha preso le mosse da un'iniziativa esterna alle istituzioni dell'Unione. L'impulso alla creazione di un sistema dei pagamenti omogeneo nell'Eurozona proveniva, infatti, direttamente dal sistema bancario, attraverso il Consiglio Europeo dei Pagamenti, cui si deve la predisposizione di un piano programmatico e tecnico per l'attuazione della c.d. SEPA (*Single Euro Payment Area*)[2]. La PSD si era potuta quindi muovere lungo linee (a livello di procedure, strutture tecnologiche e standard operativi) già tracciate e condivise fra gli operatori.

La cornice giuridica dei servizi di pagamento venutasi a formare nel 2007 ha tuttavia mostrato, già dopo pochi anni di applicazione, una sostanziale incapacità a stare al passo con i tempi (in specie sotto il profilo della innovazione tecnologica e dei modelli operativi).

In particolar modo, a provocare la sua "obsolescenza" è stata la diffusione nella prassi operativa di servizi ad alto tasso di innovazione, offerti da nuovi *player*, estranei al sistema finanziario e non regolati dalla PSD, terzi rispetto al rapporto tra cliente e banca/IP di radicamento del conto. senza necessità di radicare presso di essi i conti di pagamento degli utenti.

In forza di questo fenomeno, il conto di pagamento (*bank account*) - categoria chiave della PSD, sia pure non sufficientemente univoca a livello di fattispecie (e purtroppo non chiarita neppure dalla PSD2)[3] – non ha più

[2] Per alcune utili osservazioni in relazione al progetto SEPA v. P. Gaggi, *L'apporto dell'autoregolamentazione alla realizzazione della SEPA*, in *Armonizzazione europea dei servizi di pagamento e attuazione della direttiva 2007/64/CE*, a cura di M. Mancini, M. Rispoli Farina, V. Santoro, A. Sciarrone Alibrandi e O. Troiano, Giappichelli, Torino 2011, p. 243 ss.

[3] L'art. 4, par. 12, della PSD2 ripropone, infatti, come definizione di "conto di pagamento"

costituito, se non in via mediata, il presupposto necessario di ogni servizio di pagamento reso; con la conseguenza che un numero sempre maggiore di servizi comunque inerenti al settore (e di rapporti giuridici ad essi correlati) è rimasto fuori dall'ambito di applicazione della normativa.

Tale nuova fisionomia del mercato ha portato con sé – accanto a potenziali benefici in termini di efficienza e concorrenza - nuovi rischi e problematiche. Basti pensare che i servizi in discorso, per poter essere forniti, presupponevano l'accesso del *provider* all'*account* del cliente (e ai relativi dati) presso la banca/IP di radicamento del conto. E ciò in assenza di qualsivoglia disciplina di regolamento del rapporto tra il terzo soggetto e la banca (in special modo in assenza di alcun obbligo di cooperazione in merito alle informazioni relative al cliente "in comune"). In tale contesto, la più frequente modalità per entrare in possesso delle informazioni necessarie per la prestazione del nuovo servizio era il c.d. *screen scraping*: pratica, oggi vietata dalla PSD2, attraverso cui il *provider* utilizzava le credenziali del cliente, dallo stesso fornitegli, per accedere al conto di pagamento ed acquisire le informazioni utili.

Più in generale, l'operatività delle terze parti ha posto, nel giro di poco tempo, seri interrogativi riguardanti soprattutto la sicurezza in punto di gestione dei dati dei clienti: si pensi al rischio di un uso improprio e illegittimo dei medesimi, come all'incertezza in merito al loro utilizzo una volta acquisiti, nonché allo scarso potere di controllo del cliente in relazione all'intero svolgersi dei nuovi servizi. Proprio a partire da tali problematiche il legislatore europeo ha deciso di intervenire con la PSD2, introducendo nuove regole specificamente volte a disciplinare alcuni di questi nuovi servizi di pagamento e a fornire statuto giuridico anche ai c.d. *Third Party Providers* (TPP).

Dal punto di vista oggettivo, sono tre le attività, già diffuse nella prassi, che sono state individuate e "tipizzate" dalla nuova Direttiva.

La prima è costituita dal servizio di disposizione di ordini di pagamento (*Payment Initiation Service, PIS*) con il quale il terzo soggetto (*Payment*

quella di "conto detenuto a nome di uno o più utilizzatori di servizi di pagamento utilizzato per l'esecuzione di operazioni di pagamento". A fronte di tale definizione, sintetica ma incerta, la PSD è stata recepita in maniera diversificata nei diversi Paesi e lo stesso sta accadendo anche con riguardo alla PSD2. Più in dettaglio, il problema sta nell'individuare quali prodotti e servizi rientrino in tale nozione. Per fare un esempio, per la normativa francese i conti di deposito rientrano nella nozione di *compte de paiement*, mentre in Belgio no (e su questo profilo è intervenuta anche la Corte di Giustizia). Nel nostro Paese, Banca d'Italia ha chiarito che le carte di credito e le prepagate sono funzionalmente assimilabili a conti di pagamento e, di conseguenza, soggette alla medesima disciplina, ma altri Paesi è stata data un'interpretazione diversa.

Initiation Service Provider, PISP) si frappone tra l'utente-pagatore e il soggetto presso cui è radicato il conto, generalmente banca/IP (*Account Servicing Payment Service Provider*, ASPSP), dando impulso al pagamento (v. art. 4, comma primo, n. 15 della Direttiva).

La seconda attiene al servizio di informazione sui conti (*Account Information Service*, AIS), con il quale la terza parte (*Account Information Service Provider,* AISP) fornisce un servizio *online* di consolidamento delle informazioni relative ai conti di pagamento che uno stesso soggetto detiene presso altri prestatori di servizi di radicamento del conto (ASPSP) (v. art. 4, comma primo, n.16 della Direttiva).

La terza infine si sostanzia nel *fund checking*, ossia nell'attività del soggetto terzo (*Card Issuer Credit Provider,* CISP) che si obbliga a dare conferma al cliente in merito alla disponibilità sul proprio conto di determinate somme, per eseguire pagamenti tramite carta (v. art. 65 della Direttiva).

Così individuati i nuovi servizi di pagamento, la Direttiva 2366/2015 definisce le possibilità operative dei nuovi entranti sul mercato, ossia i TPP, e – sia pure senza rendere necessaria la sussistenza di una specifica relazione contrattuale tra TPP e ASPSP[4] - prevede una ripartizione delle responsabilità fra i soggetti coinvolti, disegnando il perimetro di interazione tra vecchi e nuovi operatori sul mercato.

Lo scenario normativo così delineato - in cui i nuovi servizi presuppongono, come si è detto, l'accesso del fornitore terzo ai conti che il proprio utente detiene presso altri prestatori di servizi di radicamento del conto (ASPSP) senza che questi ultimi possano, salvo giustificato motivo, negare tale accesso – è stato battezzato *Open Banking* e da esso derivano conseguenze senz'altro dirompenti per il tradizionale assetto del sistema bancario, Da essa discende, innanzitutto, l'obbligo per gli ASPSP di dotarsi di infrastrutture tecnologiche adeguate a consentire un'efficace e sicura interazione con i TPP a tutela dei dati degli utenti. La necessità di un'interazione efficace apre una serie di questioni legate alla adozione/integrazione delle API, mentre la necessità di un'interazione sicura rende necessario un coordinamento fra la PSD2 e le disciplina generale in materia di trattamento dei dati personali di cui al GDPR. Ma la scelta compiuta dalla PSD2 in favore dell'*open banking* pone anche una questione ulteriore,

[4] Con riferimento al rapporto tra TPP e ASPSP viene anzi più volte espressamente escluso che, al fine di garantire l'erogazione dei nuovi servizi, debbano ricorrere vincoli di natura contrattuale fra i medesimi ma, al contempo, si impongono obblighi di leale collaborazione, nonché obblighi connessi alla corretta e sicura gestione dei dati e delle comunicazioni.

cui si può, in questa sede, fare solo un sintetico cenno. Ci si riferisce al tema del *pricing*, vale a dire alla necessità di definire uno schema di compensi per le banche, a fronte dello *sharing* di informazioni, che renda sostenibile il *business model* e risponda alle esigenze di *revenues*. È questo un tema di cruciale importanza – anche in considerazione del fatto che il *data sharing* previsto da PSD2 è, per così dire, unidirezionale (solo da ASPSP a TTP, ivi compresi i *Tech Giants*, e non viceversa) - e ancora tutto da esplorare, anche alla luce della disciplina di trasparenza che la normativa contiene.

2. *I principi cardine della PSD2: proporzionalità e trasparenza*

Nella PSD2 assumono un ruolo determinante alcuni principi di fondo dell'odierna regolamentazione del sistema finanziario (proporzionalità, trasparenza, neutralità tecnologica), divenuti, però, talmente ricorrenti in disparati contesti disciplinari da rischiare di perdere il significato loro proprio riducendosi quasi a una sorta di "clausola di stile".

Per evitare tale rischio, merita allora svolgere qualche considerazione riguardo a ognuno dei tre principi cardine su cui la PSD2 poggia e che sorreggono la scelta in favore dell'*Open Banking* in essa compiuta.

Obiettivo dichiarato della PSD2 è quello di garantire una maggiore efficienza, concorrenza e trasparenza nell'offerta di servizi di pagamento, rafforzando, al contempo, la fiducia dei consumatori in un mercato dei pagamenti armonizzato. Come si è già sottolineato, la via prescelta è soprattutto quella di ampliare il novero dei servizi di pagamento coperti dalla Direttiva favorendo l'ingresso, in chiave pro-concorrenziale, di nuove categorie di prestatori di servizi di pagamento, i TPP, che si aggiungono a quelli già autorizzati a operare. Il legislatore risponde così alle crescenti richieste della clientela di potersi avvalere di forme di pagamento nuove e più evolute, richieste provenienti soprattutto dalle imprese che operano attraverso piattaforme digitali di servizi e prodotti (*e-commerce*)[5].

[5] Si realizza così un complessivo regime di favore per chi voglia avvalersi dei nuovi servizi di pagamento, che si sostanzia, fra le altre cose, in maggiori opportunità di scelta in tale ambito; in una semplificazione dell'onere della prova a favore del cliente per l'ipotesi di utilizzo fraudolento degli strumenti di pagamento, in limitazioni a spese e commissioni e nel divieto di *credit surcharge* (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, n. 218*, in *Nuove Leggi Civ. Comm.*, 2018, p. 839 ss.; S. Balsamo Tagnani, *Il mercato*

Tale scelta porta con sé la discussa questione del se e come assicurare un *regulatory level playing-field* fra i diversi *provider* di servizi di pagamento (anche in termini di adeguate tutele per gli utenti). A tale questione la nuova Direttiva risponde ricorrendo al principio di proporzionalità che, come è noto, è uno dei principi più dibattuti (soprattutto per quanto concerne modalità ed effettivo grado di realizzazione) nel settore bancario-finanziario europeo.

Il principio è declinato in modo puntuale nella PSD2 in quanto, anche in questo secondo intervento in materia di servizi di pagamento, si è mantenuta (se non, a mio avviso correttamente, accentuata) l'impostazione già presente nella PSD volta a introdurre regole differenziate (disciplina prudenziale, copertura assicurativa obbligatoria, regole organizzative/di *governance*, regole di condotta) e di intensità graduata a seconda della tipologia di attività svolta dai vari prestatori dei servizi. Più precisamente, sulla base dell'assunto per cui "*same business, same risks, same rules*", il criterio primo in forza del quale vengono imposti requisiti più o meno stringenti agli operatori è quello della maggiore o minore rischiosità e complessità del servizio reso.

Un secondo principio presente nella PSD2 e ormai da tempo radicato nella legislazione europea in materia bancaria-finanziaria è quello della trasparenza. Come emerge già dal considerando n. 6, la Direttiva si propone, infatti, di fornire maggiore "chiarezza giuridica" al sistema dei pagamenti. È questo un aspetto già molto presente nella PSD cui si deve, come è noto, l'introduzione di una disciplina speciale di trasparenza concernente i servizi di pagamento fatta di obblighi informativi nei confronti della clientela (trasparenza in senso stretto) accanto a vere e proprie regole di condotta (trasparenza in senso lato).

Nella PSD2 il principio viene riaffermato estendendosi, però, nella logica dell'*open banking*, anche al profilo della circolazione e della corretta gestione dei dati del cliente. È questo un aspetto particolarmente delicato che il legislatore europeo si è trovato a gestire nella PSD2 anche a fronte della, sostanzialmente coeva, strategia regolatoria di cui al Regolamento europeo sul trattamento dei dati personali noto come GDPR (*General Data Protection Regulation* n. 2016/679) con il quale non si è riusciti a trovare un raccordo convincente. Sotto questo profilo anche nella PSD2, come già nella PSD, la trasparenza (in senso lato) viene declinata su più livelli, il primo dei quali consiste, nella prospettiva più immediata e tradizionale,

europeo dei servizi di pagamento si rinnova con la PSD2, in *Contratto e impresa/Europa*, 2018, p. 609 ss.).

nel porre l'utente del servizio nelle condizioni di avere consapevolezza, tramite apposite informative, dell'uso dei propri dati e di consentirvi. Al fine di tutelare i dati del cliente, tuttavia, la PSD2 non si limita ad imporre obblighi informativi ma introduce anche specifiche regole negoziali e misure di sicurezza inerenti alla circolazione dei dati fra i diversi soggetti coinvolti nei processi: misure riconducibili al principio di precauzione in senso lato e solo in apparenza in contraddizione con la spinta all'apertura del mercato a terze parti.

Sotto questo profilo, tuttavia, le soluzioni adottate nella Direttiva lasciano aperti numerosi problemi su cui si è aperto un dibattito a livello internazionale[6].

3. *(*Segue*) il principio di* technological neutrality. *I problemi aperti dalle API*

Un ultimo principio cardine della PSD2, richiamato con sempre maggiore insistenza dal legislatore europeo, più generale anche nell'ambito *FinTech*[7], è quello che va sotto il nome di neutralità tecnologica.

Nel contesto della PSD2, a livello di fonti normative il principio viene declinato a diversi livelli.

Innanzitutto, il 21° considerando della PSD2 richiede ai legislatori nazionali, al preciso scopo di tutelare ed incentivare l'innovazione, che, dal punto di vista della costruzione delle singole normative, non si definiscano con rigidità le modalità tecnologiche con cui i singoli servizi di pagamento devono essere erogati. La definizione dei singoli servizi di pagamento deve mantenersi cioè neutra sotto il profilo tecnologico.

In questo modo, si intende permettere al prestatore del servizio, nel rispetto degli standard di sicurezza imposti nello svolgimento dell'attività, di continuare a sviluppare le proprie strutture, via via trovando modalità tecniche più innovative ed efficienti di attuazione del modello di *business.*

Il principio di neutralità tecnologica trova poi ulteriore declinazione, a

[6] Su alcune questioni sollevate dal rapporto tra PSD2 e GDPR v. M. Rabitti e A. Sciarrone Alibrandi, *I servizi di pagamento tra PSD2 e GDPR: open Banking e conseguenze per la clientela*, in *Liber Amicorum Guido Alpa*, a cura di F. Capriglione, Cedam, Padova 2019, p. 711 ss.

[7] Nel *FinTech Action Plan* del marzo 2018 il principio viene qualificato come "*one of the guiding principles of the Commission's policies*". Per qualche spunto su tale principio nel contesto *FinTech* v. G. Falcone, *Tre idee intorno al c.d. "FinTech"*, in *Riv. dir. banc.*, dirittobancario.it, 2018, p. 37.

livello di fonti secondarie europee, nel Regolamento Delegato UE 2018/389 della Commissione del 27 novembre 2017 che va ad integrare la PSD2 con norme tecniche di regolamentazione (Regulatory Technical Standards) per l'autenticazione forte del cliente e gli *standard* aperti di comunicazione comuni e sicuri. Duplice è l'obiettivo di tale Regolamento, fondato sull'art. 98, par. 2, 3, 4 della PSD2. In primo luogo, si impone ai prestatori di servizi di pagamento di predisporre procedure di autenticazione più rigorose e sicure al fine di mettere l'utente nella condizione di controllare l'accesso al proprio conto di pagamento e, di conseguenza, ai propri dati personali[8]. Inoltre, nella logica dell'*open banking* e della comunicazione dei dati dei clienti tra banche/IP e TPP, ai prestatori di servizi di pagamento di radicamento del conto, che gestiscono conti di pagamento *online*, si impone la predisposizione di spazi aperti di comunicazione con i TPP per permettere a questi ultimi di erogare i propri servizi. Più in dettaglio, ai primi viene richiesta la creazione di un'apposita interfaccia digitale (*Application Programming Interface*: API), che costituisca un canale di comunicazione con i soggetti terzi e a loro dedicato, attraverso il quale scambiare le informazioni relative ai diversi servizi di pagamento[9].

Nel contesto degli RTS in discorso, il richiamo al principio di neutralità tecnologica compiuto dai considerando n. 4 e n. 20 è funzionale a richiedere ai legislatori nazionali - in relazione sia alle modalità di autenticazione "forte" del cliente, sia alle interfacce di comunicazione tra ASPSP e TPP – di

[8] Si tratta della c.d. autenticazione "forte", costruita, ai sensi dell'art. 4, par. 2 degli RTS, su un codice di autenticazione personale del cliente ideato, dal gestore del servizio di pagamento, sulla base di "due o più elementi che sono classificati nelle categorie della conoscenza, del possesso e dell'inerenza". Di recente è stato osservato, in una differente prospettiva, che le nuove modalità di autenticazione del cliente sono volte, oltre che a risolvere un problema di sicurezza e controllo dei dati da parte del cliente, anche ad accertare che dietro la conclusione di un contratto *online* vi sia effettivamente la genuina volontà negoziale del soggetto che effettua il pagamento (così 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. 655).

[9] Le *Application Programming Interfaces* sono costituite da un insieme di protocolli che definiscono in che modo possono interagire le componenti dei software. L'obiettivo è quello di giungere a una standardizzazione delle modalità di esecuzione dei pagamenti digitali e di rendere più sicure le transazioni ottenendo così una maggior tutela degli utenti. Per uno studio specifico relativo allo sviluppo e all'applicazione di questa tecnologia nel mondo finanziario si rimanda a O. Borgogno e G. Colangelo, *Data Sharing and Interoperability Trough APIs: Insights from European Regulatory Strategy*, *European Union Law Working Paper*, Stanford – Vienna *Transatlantic Technology Law Forum*, 2018; M. Noctor, *PSD2: the Banking Industry Prepared*, in *Computer Fraud & Security*, 2019, p. 9 e ss.

non imporre ai prestatori dei servizi di pagamento l'adozione di specifiche tecnologie.

Anche in questo ambito, comunque, il principio di neutralità tecnologica è finalizzato alla promozione dell'innovazione e della concorrenzialità del mercato dei pagamenti.

Dopo l'emanazione della PSD2, si sono levate alcune voci, per lo più appartenenti al *milieu* delle terze parti, dubitative circa l'effettiva neutralità tecnologica della scelta di un dispositivo quale è l'API[10]. E ciò in quanto lasciando a ciascun prestatore di servizi di radicamento del conto la libertà di predisporre la propria personale interfaccia, si obbligherebbero i TPP a predisporre tante interfacce quanti sono gli interlocutori o meglio a mettersi nelle condizioni di utilizzare linguaggi tecnologici differenti.

La questione non è semplice anche in ragione della relativa novità del principio di neutralità tecnologica nel panorama giuridico e di alcune incertezze che avvolgono la sua precisa portata. Merita perciò svolgere sul punto qualche considerazione ulteriore e, prima ancora, tenere a mente che, a differenza di quanto si è visto essere accaduto con la PSD e la SEPA, la seconda Direttiva sui servizi di pagamento non è nata in un contesto in cui procedure e standard tecnologici sono stati condivisi fra gli operatori.

Ciò precisato, a mio avviso l'impostazione della PSD2 rispetto alle API può dirsi in sé neutra sotto il profilo tecnologico perché la creazione di un'interfaccia informatica di dialogo tra ASPSP e TPP, nel contesto di rapporti e servizi completamente digitalizzati in cui anche le informazioni assumono forma digitale, costituisce oggi nella sostanza l'unica modalità attraverso cui può attuarsi un'interazione sicura tra i soggetti coinvolti[11]. Si tratta, in altri termini, del riferimento non a una specifica soluzione tecnologica bensì a un nuovo paradigma tecnologico (successivo alla preesistente tecnologia dei c.d. *web-services*), che, come ogni paradigma tecnologico, non può restare estraneo a un certo modello di *business* (e dunque nemmeno alla sua regolazione) andando, in un certo senso, a connotarlo[12].

[10] V. I. Oliinyk e W. Echikson, in *Research Report Ceps*, n. 6 del 2018.

[11] È ipotizzabile che, in futuro, una valida alternativa alle API possa essere costituita dall'utilizzo della tecnologia *Blockchain*. Perché ciò avvenga, però, è necessario un profondo cambio di paradigma da parte delle banche che dovrebbero sostituire i data base individuali con un registro di informazioni condivise trasferibili via *Blockchain*. In assenza di tale registro, infatti, anche la *Blockchain*, in quanto piattaforma digitale, utilizza le API come modalità tecnica di supporto per l'interazione fra diversi soggetti e non può dunque essere considerata strumento radicalmente alternativo ad esse.

[12] Correttamente, invece, il principio di neutralità tecnologica non consente al regolatore

Se questo è vero, problematica (se non addirittura criticabile) potrebbe, invece, sembrare la scelta di imporre la costruzione delle API con spazio di dialogo tra ASPSP e TPP (le API), senza definire in quale "lingua" debbano avvenire le comunicazioni. In altri termini, il limite della soluzione individuata dalla PSD2 potrebbe consistere nel fatto che gli *standard* di comunicazione non sono comuni tra tutti i prestatori di servizi di radicamento del conto, ben potendo ciascuno di essi adottarne uno proprio e personalizzato, e non garantiscono quindi una facile interoperabilità.

La notazione coglie senz'altro nel segno ma vi è da chiedersi se davvero sarebbe stata preferibile una scelta differente da parte del legislatore europeo, nel senso di imporre, sul terreno normativo, l'adozione di standard comuni. Proprio l'esperienza di attuazione della PSD2 mostra, infatti, che, al fine di garantire l'interoperabilità, sono percorribili quantomeno due strade. La prima vede l'intervento del regolatore (in questo caso a livello nazionale, come è accaduto nel Regno Unito[13]) che determina regole tecniche di comunicazione comuni ai soggetti prestatori dei servizi di pagamento, siano essi ASPSP o TTP. La seconda, invece, ruota attorno a soluzioni di sistema provenienti dal mercato (come è accaduto in Italia[14]). In entrambi i casi, peraltro, ad essere rilevante è l'utilizzo, da parte dell'interfaccia, di standard di comunicazione sviluppati da organismi di normazione internazionali e nazionali[15].

La variante tecnologica non si pone più, infatti, come meramente strumentale allo svolgimento di attività "tradizionali": essa al contrario, è in grado di riconfigurare le dinamiche di mercato, le relazioni fra i suoi attori e, di conseguenza, non può non avere impatto anche sul piano delle regole.

La neutralità tecnologica rischia, perciò, in concreto di diventare solo una formula vuota, laddove venga disancorata dalla sostanza dei rapporti

di riferirsi a specifiche soluzioni tecnologiche (che possono essere *open source* o proprietarie del *software* di base o una soluzione mista nel caso in cui sia proprietaria l'architettura che tiene insieme segmenti *open source*).

13 Ci si riferisce al modello di interfacce digitali attuato nel Regno Unito, ove è stato predisposto un modello di interazione tra ASPSP e TTP realmente *open* e *common*, tramite l'ideazione, sotto il controllo dell'autorità di settore, di un'unica API comune alle nove più importanti banche britanniche. Per un'analisi approfondita del caso anglosassone si rinvia all'interessante lavoro di M. Zachariadis e P. Ozcan, *The API Economy and Digital Trasformation in Financial Services: the Case of Open Banking*, in *Swift Institute Working Paper*, n. 2016-001.

14 Nel nostro paese, il consorzio Cbi, in collaborazione con Nexi e con l'appoggio dell'Abi, ha progettato un modello unico di piattaforma digitale cui hanno aderito otto tra i maggiori gruppi bancari nazionali e Poste Pay.

15 Come puntualizzato, del resto, già dal legislatore europeo nel 21° considerando della PSD2.

tra utenti di servizi finanziari e relativi prestatori così come concretizzata dall'uso delle tecnologie abilitanti.

Abstract
La nuova Direttiva sui servizi di pagamento (PSD2) ambisce a sostenere lo sviluppo dell'innovazione tecnologica e della competizione fra operatori nel settore dei pagamenti al dettaglio. Gli RTS sulla *strong customer authentication* e sulle API innalzeranno la sicurezza dei pagamenti e la protezione dei dati, con l'obiettivo di trovare un bilanciamento fra gli interessi dei differenti provider.

Parole chiave: Servizi di pagamento; autenticazione forte; neutralità tecnologica.

Abstract
The revised Payment Services Directive (PSD2) will support technological innovation and competition in retail payments. The RTS on strong customer authentication and API will enhance the security of payment transactions and the protection of consumer data, with the aim to strike a balance between the interests of the different players.

Keywords: Payment services; strong customer authentication; technological neutrality

Vincenzo De Stasio

Riparto di responsabilità e restituzioni nei pagamenti non autorizzati

Sommario: 1. I fondi come oggetto del trasferimento regolato dalla PSD2: dalla logica bilaterale del pagamento come consegna di banconote e monete a quella dell'esecuzione del procedimento per il tramite di uno strumento (e di uno schema – e di un sistema) di pagamento che coinvolge uno o più PSP – 2. Logiche restitutorie e logiche risarcitorie: la confusione sorge dall'identità tra l'oggetto del trasferimento e l'oggetto del risarcimento – 3. Possibilità di mantenere una distinzione tra restituzioni e risarcimenti facendo leva sul concetto di disponibilità dei fondi sul conto di pagamento, funzionalmente equivalente al possesso del denaro mediante affidamento chiuso del borsellino a persona di fiducia. La sicurezza dei fondi e l'art. 73 PSD2: irrevocabilità dell'ordine nella PSD2 e definitività dell'ordine immesso in un sistema di pagamento. L'eccezione dei servizi più complessi, secondo una recente proposta di lettura – 4. La corretta esecuzione del procedimento come paradigma interpretativo della PSD2: obblighi posti a carico del prestatore di servizi e a carico del pagatore – 5. La necessaria collaborazione del PSP e la verifica dell'identità dell'ordinante e dell'identità del beneficiario: le regole dell'autenticazione e la regola dell'esecuzione secondo prevalenza dell'IBAN sul nome del beneficiario – 6. I nuovi servizi della PSD2 e il rapporto tra i nuovi operatori e il PSP di radicamento del conto: logiche restitutorie e risarcitorie e rischio di overcompensation nell'attuazione italiana della Direttiva, probabilmente non coerente con le indicazioni del legislatore europeo (art. 73.2. PSD2).

1. *I fondi come oggetto del trasferimento regolato dalla PSD2: dalla logica bilaterale del pagamento come consegna di banconote e monete a quella dell'esecuzione del procedimento per il tramite di uno strumento (e di uno schema – e di un sistema) di pagamento che coinvolge uno o più PSP*

La disciplina unionale dei servizi di pagamento è simultaneamente presa d'atto e accompagnamento di una delle più intrusive modifiche delle quotidiane abitudini che la rivoluzione telematica ha portato con sé.

Abituati da millenni alla gestione dei micropagamenti – e talora anche di pagamenti più consistenti – mediante la dazione di banconote e monete metalliche, gli uomini del XXI secolo si vanno progressivamente

convertendo dall'atto bilaterale del pagamento, che comporta la consegna (cioè la trasmissione del possesso) di un oggetto materiale[1], all'utilizzo di un procedimento più sofisticato per adempiere le obbligazioni pecuniarie, mediante l'avvio e l'esecuzione di un'operazione di pagamento.

Le analogie con il pagamento a mezzo di contanti – che pure sono necessarie, al fine di collocare nella sua corretta visione funzionale il nuovo procedimento, almeno per quanto concerne il trasferimento dei fondi, che realizza una diminuzione di potere di spesa del pagatore e un simmetrico incremento in capo al beneficiario, né più né meno che se venisse consegnato denaro contante – non devono fare trascurare la dimensione aggiuntiva della trasmissione di un ordine, cioè di una serie di informazioni che sono essenziali per consentire tanto l'avvio quanto la corretta esecuzione dell'operazione di pagamento[2].

Dietro quest'ultima espressione si cela una pluralità di "schemi di pagamento"[3], riconducibili alle categorie del bonifico[4], dell'addebito diretto[5], della carta di debito[6] e della carta di credito[7], ciascuno dei quali

[1] A. Di Majo, *Il diritto comunitario dei pagamenti pecuniari*, in *Annuario del contratto 2010*, diretto da A. D'Angelo e V. Roppo, Giappichelli, Torino 2011, p. 6; D. Linardatos, *Das Haftungssystem im bargedlosen Zahlungsverkehr nach Umsetzung der Zahlungsdiensterichtlinie*, Nomos, Baden-Baden 2013, p. 24.

[2] V. De Stasio, *Ordine di pagamento non autorizzato e restituzione della moneta*, Giuffrè, Milano 2016, p. 135.

[3] Si tratta di un'impostazione figlia della "SEPA-Vision", cioè della creazione di un'area unica dei pagamenti in euro, che valorizza la creazione di regole tecnico-operative bancarie omogenee, a opera del *European Payment Council*, organismo di autoregolamentazione nato nel 2002 dall'iniziativa del settore bancario europeo come organo decisionale e di coordinamento (A. Santoro, *Commento all'art. 1, comma 1, lettera z)*, in *La nuova disciplina dei servizi di pagamento*, a cura di M. Mancini, M. Rispoli Farina, V. Santoro, A. Sciarrone Alibrandi e O. Troiano, Giappichelli, Torino 2011, p. 32 ss.; Staudinger/Omlor Vorbem zu §§ 675c-676 c, *Rn.* 13, 2012; E. Rigler, SEPA, in *Bankrechts-Kommentar* (2. Auflage), a cura di K. Langenbucher, D.H. Bliesener e G. Spindler, Grin, München 2016, p. 610 ss.; J.M. López Jiménez, *Comentarios a la Ley de Servicios de Pago*, Editorial Boch, Barcelona 2011, p. 146 ss.). Sulla nozione di "schema di pagamento", v. in particolare art. 2, n. 7), del Regolamento (UE) n. 260/2012.

[4] 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.

[5] G.B. Barillà, *L'addebito diretto*, Giuffrè, Milano 2014.

[6] F. Ciraolo, *Le carte di debito nell'ordinamento italiano*, Milano, 2008; M. Onza, *Estinzione dell'obbligazione pecuniaria e finanziamento dei consumi: il pagamento con la "carta"*, Giuffrè, Milano 2013.

[7] U. Malvagna, *Clausola di «riaddebito» e servizi di pagamento*, Giuffrè, Milano 2018.

regola un differente procedimento mediante il quale si trasmette non più una sola entità, "i fondi" che dal conto del pagatore devono pervenire a quello del beneficiario, bensì anche, necessariamente, un'informazione, costituita dall' "ordine di pagamento", che dà inizio al procedimento e che nella sua configurazione minima efficace deve contenere un importo, con la valuta che costituisce l'unità di conto numerata dall'importo, e consentire di individuare due conti di pagamento: quello del pagatore, da cui si devono prelevare i fondi nell'importo e nella valuta contenuti nell'ordine, e quello del beneficiario, dove i fondi devono essere accreditati.

Lo svolgimento dell'operazione di pagamento, come definita nelle direttive europee sui servizi di pagamento e nell'art. 1, lett. *c*), d.lgs. 11/2010, richiede l'esecuzione del trasferimento dei fondi da parte di uno o più imprenditori bancari o finanziari, che assumono il ruolo di prestatori del servizio di pagamento e che si pongono in una nuova relazione coi fondi del cliente e con le informazioni che il cliente trasmette.

Questa duplicità di dimensioni dell'operazione di pagamento deve essere costantemente tenuta presente: se il pagamento in contanti presso un distributore automatico comporta il totale anonimato del pagatore, di contro l'utilizzo di un servizio di pagamento comporta la trasmissione di dati che consentano di individuare e registrare gli estremi essenziali dell'operazione e gli utenti del servizio[8]. Con la inevitabile creazione di un enorme *database*, localizzato in primo luogo presso il prestatore di radicamento del conto, cioè la banca o l'istituto di pagamento presso il quale l'utente mantiene depositati i propri fondi.

Questo patrimonio di dati, se analizzato con i moderni strumenti dell'intelligenza artificiale, consente a chi ne disponga di produrre ulteriore informazione, proprio in un ambito nel quale le persone, nei precedenti millenni, hanno cercato di mantenere discreto riserbo. Informazione altamente affidabile, perché non espressiva di mere opinioni o desideri, bensì basata sull'inequivocabile dato economico del contestuale trasferimento dei fondi.

Se la prima Direttiva sui servizi di pagamento (2007/64/CE) ha accompagnato l'uniformazione dell'attività imprenditoriale di trasferimento dei fondi mediante servizi di pagamento, grazie all'armonizzazione massima[9] delle regole relative ai rapporti tra clienti e prestatori del servizio, avendo principalmente di mira il problema della corretta esecuzione del trasferimento

[8] D. Janssen, *Die Zahlungsdiensterichtlinie (PSD I) und ihre aufsichtrechtliche Umsetzung im Vereinigten Königreich und Deutschland*, Duncker & Humblot, Berlin 2017, p. 201 ss.
[9] Sui limiti posti dall'interpretazione nazionale all'armonizzazione: H.-S. Budde, *Das Vertragsrecht der Zahlungsdienste*, Duncker & Humblot, Berlin 2017, e la recensione di V. De Stasio, in *Eur. Rev. Contr. L.*, 2017, p. 332, e in *Banca, borsa, tit. cred.*, 2018, I, p. 131 ss.

dei fondi in base alla corrispondenza con un ordine di pagamento autorizzato dal pagatore[10], la seconda Direttiva (2015/2366/UE) focalizza l'attenzione sugli aspetti informativi relativi alla trasmissione dei dati dell'operazione di pagamento, aprendo il mercato ai nuovi prestatori di servizi di pagamento, non bancari perché definiti proprio in base al mancato "radicamento del conto", che accedono – in base a un principio di stretta finalità - al "database" del cliente e si inseriscono nel procedimento di trasmissione delle informazioni che rendono possibile l'avvio dell'operazione di pagamento.

E' stato rilevato[11] che l'obbligo di cooperazione posto a carico dei "prestatori di radicamento" determina una ulteriore anomalia del diritto dei pagamenti rispetto al diritto privato comune, posto che l'obbligo di collaborazione della banca (o IP) presso cui è radicato il conto, con i nuovi prestatori di servizi di informazioni sui conti o di servizi di disposizione di ordine, non è fondato su un preesistente rapporto contrattuale con i suddetti operatori, ma direttamente nella legge. Ne consegue, per i giuristi tedeschi molto attenti alla coerenza dogmatica del diritto nazionale, un'ulteriore crisi del paradigma interpretativo dei servizi di pagamento, sempre più vicino a una configurazione di "Netzvertrag" inteso come strumento idoneo al superamento dei limiti della *privity of contract*.

Sempre che la logica del contratto sia davvero ancora idonea a cogliere il fatto regolato: sembrandomi invece, da tempo, più appropriata la sussunzione del pagamento in una logica procedimentale e di impresa[12], nella quale il contratto è "contratto quadro" avente la funzione di regolazione normativa dei procedimenti di pagamento – e cioè dei trasferimenti di fondi – che possono essere avviati dal prestatore di radicamento del conto, che è a sua volta l'unico soggetto presso il quale si trova la moneta scritturale, cioè i fondi nell'esclusiva disponibilità del cliente.

[10] Sulla distinzione del procedimento di pagamento in fasi: B. Sorg, *Die zivilrechtliche Haftung im bargeldlosen Zahlungsverkehr*, Duncker & Humblot, Berlin 2015, p. 337 e *passim*.
[11] J. Köndgen, *Jenseits des Relativitätsprinzip: Haftungsstrukturen im neuen Zahlungsdiensterecht*, in *ZBB*, 2018, p. 141 ss.
[12] V. De Stasio, *Ordine di pagamento non autorizzato e restituzione della moneta*, cit., p. 237 s. e *passim*; Id., *Operazione di pagamento non autorizzata e restituzioni*, EDUCatt, Milano 2013; Id., *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*, cit., p. 311; M. Onza, *Gli strumenti di pagamento nel contesto dei pagamenti* on line, in *Dir. banc. merc. fin.*, 2017, p. 683 ss.

2. *Logiche restitutorie e logiche risarcitorie: la confusione sorge dall'identità tra l'oggetto del trasferimento e l'oggetto del risarcimento*

Il diritto dei pagamenti è area nella quale la confusione tra restituzione e risarcimento può più facilmente instaurarsi[13], dato che la moneta costituisce sia oggetto del servizio sia misura di un eventuale risarcimento. La posizione attiva di chi ha diritto a un risarcimento postula la necessità della liquidazione di un danno, cioè l'individuazione del momento rilevante per la liquidazione e l'accoglimento di una teoria che faccia riferimento o all'interesse positivo o a quello negativo[14], oltre all'accertamento del nesso causale e all'individuazione dell'obbligato e degli obbligati solidali; infine dei rapporti interni tra questi ultimi[15]. La determinazione del *quantum* di un risarcimento richiede un'attività di valutazione del danno risarcibile, che rende improbabile un automatismo. La tutela restitutoria – riportare il conto di pagamento nelle condizioni in cui si sarebbe trovato se non fosse stato addebitato delle somme trasferite con l'operazione di pagamento non autorizzata – appare praticamente e concettualmente più efficace, per il cliente, rispetto alla titolarità di un credito risarcitorio[16].

Una prima linea di distinzione tra i due rimedi dipende proprio dalla considerazione del procedimento di pagamento e dalla distinzione delle fasi in cui può verificarsi l'anomalia del procedimento stesso: se è la fase di autorizzazione a essere viziata, ecco che è la logica delegatoria a individuare nella carenza di consenso del pagatore all'ordine di pagamento il vizio di base dell'agire come delegato in capo al prestatore di radicamento del conto. La carenza dello *iussum* comporta la non conteggiabilità del pagamento nel rapporto tra cliente e PSP di radicamento del conto, e la titolarità dell'azione

[13] G. Mucciarone, *La prima sentenza della Cassazione sulle conseguenze civilistiche dell'uso della carta di credito ad opera di portatore non titolare* (nota a Cass., 17 luglio 2006, n. 16102), in *Banca, borsa, tit. cred.*, 2008, II, p. 7 ss.; V. De Stasio, *Ordine di pagamento non autorizzato e restituzione della moneta*, cit., p. 16 s.; 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, p. 459 ss.

[14] Sulla teoria del danno applicabile, v. di recente A. Zoppini, *La consulenza tecnica nel giudizio arbitrale: alla ricerca di standard condivisi nel risarcimento del danno contrattuale*, in *La consulenza tecnica nel giudizio arbitrale. Il danno da inadempimento contrattuale*, Atti del Convegno (Istituto Unidroit, 17 aprile 2015), a cura di S. Azzali, G. Rojas Elgueta e A. Zoppini, Giuffrè, Milano 2016, p. 14 ss.

[15] Sull'argomento v. ora i saggi raccolti in *Le "nuove" obbligazioni solidali. Principi europei, orientamenti giurisprudenziali, interventi legislativi*, a cura di U. Breccia e F.D. Busnelli, Cedam, Padova 2016.

[16] V. ora anche R. Bocchini, *La tutela assoluta dei servizi*, Iovene, Napoli 2018.

di ripetizione nei confronti del beneficiario in capo al PSP di radicamento del conto (privo di autorizzazione al pagamento) che abbia dato avvio al trasferimento dei fondi del cliente.

Nel caso in cui l'anomalia attenga all'esecuzione del trasferimento dei fondi, senza che sia negata l'imputazione al pagatore dell'ordine di trasferimento dei fondi non correttamente eseguito, la natura del rimedio va concettualmente ricercata nell'area del risarcimento del danno.

Si possono così individuare due fasi principali dell'operazione di pagamento: la iniziazione (tutte le fasi procedimentali che antecedono l'inizio del trasferimento dei fondi da parte del PSP di radicamento del conto del pagatore) e la successiva esecuzione. Le anomalie della prima fase si lasciano trattare nello schema della delegazione di pagamento e danno spazio a rimedi restitutori. Le anomalie della seconda fase (l'esecuzione) si verificano in un procedimento che vede come normale o frequente la presenza di schemi (tecniche di trasferimento dei fondi) nei quali la cooperazione e il coordinamento di diversi soggetti è essenziale, nella realizzazione del risultato finale del trasferimento dei fondi al beneficiario. Le deviazioni dallo schema procedimentale in questa seconda fase danno luogo a rimedi la cui natura è risarcitoria di un danno provocato da un inadempimento o da un fatto illecito. La determinazione dell'esistenza di un inadempimento o di un illecito dipende dal concreto schema (o schemi) di pagamento utilizzati dal (o dai) PSP del pagatore e del beneficiario, ed è soggetta alle regole speciali della disciplina di settore, che integrano quelle generali del codice civile.

3. *Possibilità di mantenere una distinzione tra restituzioni e risarcimenti facendo leva sul concetto di disponibilità dei fondi sul conto di pagamento, funzionalmente equivalente al possesso del denaro mediante affidamento chiuso del borsellino a persona di fiducia. La sicurezza dei fondi e l'art. 73 PSD2: irrevocabilità dell'ordine nella PSD2 e definitività dell'ordine immesso in un sistema di pagamento. L'eccezione dei servizi più complessi, secondo una recente proposta di lettura*

Nella restituzione l'oggetto della prestazione da rendere è già individuato e pertanto la disponibilità di un'azione restitutoria, o di un automatico rimedio di rimborso, costituisce la più efficace tutela, in assoluto, per il cliente, che si veda così ripristinare la disponibilità della moneta scritturale sul proprio conto. La possibilità di mantenere una distinzione concettuale

tra restituzioni e risarcimenti fa leva sul concetto di disponibilità dei fondi sul conto di pagamento, funzionalmente equivalente al possesso del denaro mediante affidamento chiuso del borsellino a persona di fiducia.

L'uso del denaro contante è in una fase di accentuata recessione, scoraggiato sia dai limiti antiriciclaggio, sia dagli obblighi di pagamento con mezzi tracciabili. Stipendi e salari, pagamenti nei quali è coinvolta la p.a., devono tutti avvenire con mezzi di pagamento diversi dal contante[17].

[17] G. Guerrieri, *I rischi connessi alla circolazione della moneta elettronica*, in *Nuove leggi civ. comm.*, 2014, p. 1044, nt. 1, espone un elenco di recenti disposizioni normative volte a prevedere che specifiche tipologie di pagamenti non avvengano in contanti, bensì con altri strumenti di pagamento variamente denominati («pagamenti con modalità informatiche», per quanto concerne i pagamenti alle p.A. e le società interamente partecipate o a prevalente capitale pubblico: art. 5 cod. amm. digitale, ripetutamente novellato; «carte di debito», per i pagamenti dei clienti a imprese e professionisti: art. 15, comma 4, d.l. n. 197/2012, conv. dalla legge n. 221/12, a norma del quale «a decorrere dal 30 giugno 2014 i soggetti che effettuano l'attività di vendita di prodotti e di prestazione di servizi, anche professionali, sono tenuti ad accettare anche pagamenti effettuati attraverso carte di debito»; «strumenti di pagamento elettronico», per servizi di parcheggio, *bike sharing*, accesso ad aree a traffico limitato e sistemi di mobilità e trasporto; etc.). V. anche l'art. 1, lett. *q*), legge 7 agosto 2015, n. 124, con il quale il Governo è stato delegato ad adottare, entro dodici mesi dalla data di entrata in vigore della legge, «uno o più decreti legislativi volti a modificare e integrare, anche disponendone la delegificazione, il codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82», nel rispetto, fra l'altro, del seguente principio e criterio direttivo: «… prevedere che i pagamenti digitali ed elettronici effettuati con qualsiasi modalità di pagamento, ivi incluso l'utilizzo per i micropagamenti del credito telefonico, costituiscano il mezzo principale per i pagamenti dovuti nei confronti della pubblica amministrazione e degli esercenti servizi di pubblica utilità». L'Art. 5 cod. amm. digitale (con rubrica: *Effettuazione di pagamenti con modalità informatiche*) attualmente prevede che «1. I soggetti di cui all'articolo 2, comma 2 [: *a) le pubbliche amministrazioni di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, nel rispetto del riparto di competenza di cui all'articolo 117 della Costituzione, ivi comprese le autorità di sistema portuale, nonché alle autorità amministrative indipendenti di garanzia, vigilanza e regolazione; b) i gestori di servizi pubblici, ivi comprese le società quotate, in relazione ai servizi di pubblico interesse; c) le società a controllo pubblico, come definite nel decreto legislativo 19 agosto 2016, n. 175, escluse le società quotate di cui all'articolo 2, comma 1, lettera p), del medesimo decreto che non rientrino nella categoria di cui alla lettera b)*], sono obbligati ad accettare, tramite la piattaforma di cui al comma 2, i pagamenti spettanti a qualsiasi titolo attraverso sistemi di pagamento elettronico, ivi inclusi, per i micro-pagamenti, quelli basati sull'uso del credito telefonico. Tramite la piattaforma elettronica di cui al comma 2, resta ferma la possibilità di accettare anche altre forme di pagamento elettronico, senza discriminazione in relazione allo schema di pagamento abilitato per ciascuna tipologia di strumento di pagamento elettronico come definita ai sensi dell'articolo 2, punti 33), 34) e 35) del regolamento UE 2015/751 del Parlamento europeo e del Consiglio del 29 aprile 2015 relativo alle commissioni interbancarie sulle operazioni di pagamento basate su carta. - 2. Al fine di dare attuazione al comma 1, l'Agenzia per l'Italia Digitale mette a disposizione, attraverso il Sistema pubblico di connettività, una piattaforma

A imprese e professionisti è imposto di munirsi di sistemi POS, che consentano di ricevere il pagamento a mezzo di carte[18]. Difficile oggi negare alla moneta scritturale la qualifica di moneta legale, nel senso dell'art. 1277 c.c. L'equiparazione della moneta scritturale al contante, impossibile sul piano fisico-strutturale, viene realizzata sul piano funzionale[19]. Gli strumenti e i paradigmi giuridici adoperati devono confrontarsi con l'antropologia e

tecnologica per l'interconnessione e l'interoperabilità tra le pubbliche amministrazioni e i prestatori di servizi di pagamento abilitati, al fine di assicurare, attraverso gli strumenti di cui all'articolo 64, l'autenticazione dei soggetti interessati all'operazione in tutta la gestione del processo di pagamento. - 2-*bis*. Ai sensi dell'articolo 71, e sentita la Banca d'Italia, sono determinate le modalità di attuazione del comma 1, inclusi gli obblighi di pubblicazione di dati e le informazioni strumentali all'utilizzo degli strumenti di pagamento di cui al medesimo comma. - 2-*ter*. I soggetti di cui all'articolo 2, comma 2, consentono di effettuare pagamenti elettronici tramite la piattaforma di cui al comma 2 anche per il pagamento spontaneo di tributi di cui all'articolo 2-*bis* del decreto-legge 22 ottobre 2016, n. 193, convertito, con modificazioni dalla legge 1° dicembre 2016, n. 225. - 2-*quater*. I prestatori di servizi di pagamento abilitati eseguono pagamenti a favore delle pubbliche amministrazioni attraverso l'utilizzo della piattaforma di cui al comma 2. Resta fermo il sistema dei versamenti unitari di cui all'articolo 17 e seguenti del decreto legislativo 9 luglio 1997, n. 241, Capo III, fino all'adozione di un decreto del Presidente del Consiglio dei ministri o del Ministro delegato, su proposta del Ministro dell'economia e delle finanze, di concerto con il Ministro del lavoro e delle politiche sociali, sentite l'Agenzia delle entrate e l'AgID, che fissa, anche in maniera progressiva, le modalità tecniche per l'effettuazione dei pagamenti tributari e contributivi tramite la piattaforma di cui al comma 2. - 2-*quinquies*. Tramite la piattaforma di cui al comma 2, le informazioni sui pagamenti sono messe a disposizione anche del Ministero dell'economia e delle finanze - Dipartimento Ragioneria generale dello Stato. […] - 4. L'Agenzia per l'Italia digitale, sentita la Banca d'Italia, definisce linee guida per la specifica dei codici identificativi del pagamento di cui al comma 1 e le modalità attraverso le quali il prestatore dei servizi di pagamento mette a disposizione dell'ente le informazioni relative al pagamento medesimo. - 5. Le attività previste dal presente articolo si svolgono con le risorse umane, finanziarie e strumentali disponibili a legislazione vigente». Il D.Lgs. 13 dicembre 2017, n. 217 ha disposto (con l'art. 65, comma 2) che «L'obbligo per i prestatori di servizi di pagamento abilitati di utilizzare esclusivamente la piattaforma di cui all'articolo 5, comma 2, del decreto legislativo n. 82 del 2005 per i pagamenti verso le pubbliche amministrazioni decorre dal 1° gennaio 2019».

[18] V. De Stasio, *Verso un concetto europeo di moneta legale: valute virtuali, monete complementari e regole di adempimento*, in *Banca, borsa, tit. cred.*, 2018, I, p. 750 s.

[19] G.F. Campobasso, *Bancogiro e moneta scritturale*, Cacucci, Bari 1979; B. Inzitari, *Moneta*, in *Digesto* (4. Edizione), *Disc. priv.*, *Sez. civ.*, vol. VIII, UTET, Torino 1991, p. 395 ss.; L. Farenga, *La moneta bancaria*, Giappichelli, Torino 1997; G. Lemme, *Moneta scritturale e moneta elettronica*, Giappichelli, Torino 2003; I. A. Caggiano, *Circolazione del denaro e strumenti di tutela* (2. Edizione), ESI, Napoli 2012, p. 140 ss.; v. ora anche V. De Stasio e S. Boatto, *The Euro as Legal Tender from an Italian Perspective*, di prossima pubblicazione negli atti del Convegno (Frankfurt am Main, 21 settembre 2018), a cura di S. Omlor e R. Freitag.

l'umana necessità di realizzare sulla propria riserva di valore, costituita dalla moneta, un controllo altrettanto efficace di quello fisico. Se si può rinunciare a tuffarsi nel denaro contante, passatempo di un noto personaggio dei fumetti[20], non si può fare a meno di circondare il proprio deposito monetario di strumenti di difesa affidabili. L'introduzione del *bail-in* dei depositi ha lasciato il dubbio che una risoluzione bancaria possa fare sparire la moneta scritturale al pari di un incendio quella fisica, così riducendo di molto la fiducia nella sicurezza dei conti di pagamento[21]. Tuttavia la Direttiva sui servizi di pagamento ha invero circondato di particolare efficacia la difesa del conto di pagamento da prelievi per effetto di ordini di pagamento non autorizzati. Il rimedio di base è nell'art. 73 della PSD2, attuato in Italia mediante l'art. 11 d.lgs. 11/2010, che prevede un immediato ripristino del conto dell'utente, al momento del disconoscimento dell'operazione di pagamento non autorizzata, salvo il motivato sospetto di frode[22].

La norma costituisce un aggravamento della posizione del PSP di radicamento del conto, posto che, una volta trasferiti i fondi al beneficiario, o una volta che l'ordine di trasferimento dei fondi stessi dell'utente pagatore presso il PSP di radicamento sia stato immesso per l'esecuzione in un sistema di pagamento regolato dalla Direttiva 98/26/CE, l'operazione è irrevocabile[23]. Il PSP di radicamento del conto, per essere rimborsato dei fondi che abbia trasferito in esecuzione di un'operazione non autorizzata, deve riceverli in restituzione dal soggetto cui i fondi siano pervenuti. Il rischio di non ottenere il rimborso grava, cioè, in linea generale sul PSP di radicamento del conto che – in quanto delegato non autorizzato – è investito della legittimazione al recupero dei fondi trasmessi, mediante un'azione che è, nella sostanza, di ripetizione dell'indebito. Nel rapporto con l'utente addebitato, l'obbligo di immediato rimborso (*i.e.*: la non conteggiabilità del pagamento effettuato) è il contraltare della titolarità in capo al PSP (di radicamento del conto) dell'azione di ripetizione, che appunto non spetta al pagatore non autorizzante[24].

[20] Cfr. il titolo del fascicolo monografico n. 1/2015 di *An. giur. econom.*: «La moneta ai tempi di Internet. Dove si tufferà zio Paperone?», a cura di U. Morera, G. Olivieri e A. Sciarrone Alibrandi.

[21] M. Cera, *Il depositante bancario tra processo economico e mercati*, in *An. giur. econom.*, 2016, p. 271 ss.; N. Ciocca, *Depositi e obbligazioni bancari: disciplina privatistica e strumenti contrattuali di tutela*, ibidem, p. 434 ss., V. De Stasio, *Gestione di portafogli e* bail-in, in *Riv. dir. civ.*, 2017, p. 365 ss.

[22] V. De Stasio, *Ordine di pagamento non autorizzato e restituzione della moneta*, cit., p. 169 ss.

[23] V. De Stasio, *Ordine di pagamento non autorizzato e restituzione della moneta*, cit., p. 178 ss., 181 ss. e 196 ss.

[24] V. De Stasio, *Ordine di pagamento non autorizzato e restituzione della moneta*, cit., p.

Un apprezzamento differente è forse possibile per i servizi più complessi, come quello di carta di credito, nel quale il prestatore del servizio, quanto meno negli schemi trilaterali, ha un previo rapporto contrattuale non solo con il pagatore, ma anche con il beneficiario. Una recente proposta interpretativa[25] sposta interamente il rischio di mancata autorizzazione sul gestore del circuito della carta di credito, incrementando la tutela dell'esercente associato di fronte al rischio di utilizzo della carta di credito da parte del non titolare. La responsabilità per l'esercizio di un'attività di impresa, in questa prospettiva, comporterebbe l'imputazione di ogni rischio al gestore della carta, con una limitazione all'operatività delle clausole di *charge-back* che si estenderebbe anche ai vizi dell'iniziazione del pagamento[26].

4. *La corretta esecuzione del procedimento come paradigma interpretativo della PSD2: obblighi posti a carico del prestatore di servizi e a carico del pagatore*

Lo scopo della disciplina dei servizi di pagamento è di regolare, nei reciproci rapporti, i comportamenti dovuti dall'utente e dal PSP, al fine della corretta esecuzione del procedimento di trasferimento dei fondi ("l'operazione di pagamento"), in conformità con un ordine di pagamento sorretto dal consenso del pagatore[27].

Fino ad ora più semplice è sembrata la questione delle regole di esecuzione dell'operazione di pagamento, contenute nel capo III del d.lgs. 11/2010, con una ben precisa formalizzazione della ricezione dell'ordine di pagamento, dei casi di rifiuto[28], del momento dell'irrevocabilità[29], dei tempi di esecuzione. Più complessa la questione delle regole di responsabilità per l'inadempimento[30].

208 s.; altri riferimenti alle "teorie delegatorie" in U. Malvagna, *Clausola di «riaddebito» e servizi di pagamento*, cit., p. 56 ss.; G.B. Barillà, *L'addebito diretto*, cit., p. 57 ss.

[25] U. Malvagna, *Clausola di «riaddebito» e servizi di pagamento*, cit., p. 69 ss., 87 ss. e 116 ss.

[26] U. Malvagna, *Clausola di «riaddebito» e servizi di pagamento*, cit., p. 189 ss.

[27] V. De Stasio, *Ordine di pagamento non autorizzato e restituzione della moneta*, cit., p. 105 ss.; 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.

[28] M.C. Lupacchino, *Commento all'art. 16*, 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. 184 ss.

[29] 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*, cit., pp. 303 e 307.

[30] A. Sciarrone Alibrandi e E. Dellarosa, *Commento all'art. 25*, in *La nuova disciplina*

Ferma l'autonomia di impresa dei prestatori di servizi di pagamento nel regolare la catena del trasferimento dei fondi, mediante l'adozione dell'uno o dell'altro schema, comunque entro l'ambito delle scelte inizialmente espresse dall'utente mediante l'adozione del contratto quadro, la struttura degli obblighi dell'una e dell'altra parte si incentra, nella sistematica unionale, intorno agli obblighi dell'utente e del prestatore rispetto al nuovo concetto di "strumento di pagamento", munito di "credenziali di sicurezza", e cioè sulla fase iniziale di autorizzazione dell'operazione di pagamento.

Lo strumento di pagamento è definito in termini funzionali rispetto alla sua idoneità a consentire all'utente di impartire un ordine di pagamento, che fa sorgere l'obbligo del PSP di dare corso all'operazione di pagamento. Il suo utilizzo costituisce il momento di avvio del procedimento, che trova la sua base consensuale nella circostanza che lo strumento di pagamento, tanto se sia un "dispositivo personalizzato" quanto se si limiti "a un insieme di procedure", è concordato tra l'utente e il prestatore di servizi di pagamento[31]. Un'operazione di pagamento a distanza, mancando la possibilità di riconoscimento fisico dell'ordinante, richiede appunto il mezzo dello strumento di pagamento per potere essere iniziata. La gravità del rischio consistente nell'impossessamento dello strumento di pagamento da parte di terzi richiede un bilanciamento degli obblighi di custodia tra utente e prestatore, di cui la legge delinea i capisaldi negli artt. 7 e 8 del d.lgs. 11/2010[32]. Costruiti solo in parte in termini di *rules*, e per aspetti essenziali alla stregua di *standard* rimessi alla concretizzazione interpretativa, sono questi articoli al centro dell'attenzione dell'ABF, che ha svolto in questi anni un importante lavoro di applicazione degli *standard* richiesti alle circostanze concrete[33]. Di certo gli esiti interpretativi sono condizionati

dei servizi di pagamento, a cura di M. Mancini, M. Rispoli Farina, V. Santoro, A. Sciarrone Alibrandi e O. Troiano, *cit.*, p. 245 ss.

[31] M.R. Guimarães, *Los medios de pago en el derecho europeo y en los instrumentos europeos de armonización del derecho privado*, in *Banca, borsa, tit. cred.*, 2017, I, p. 566.

[32] A. Pironti, *Commento all'art. 7*, 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. 113 ss.; O. Troiano e A. Pironti, *Commento all'art. 8*, ibidem, p. 118 ss.; M.R. Guimarães, *Los medios de pago en el derecho europeo y en los instrumentos europeos de armonización del derecho privado*, cit., p. 569 ss.

[33] Cfr., ad es., il componimento di orientamenti differenziati nei diversi collegi, menzionato nelle seguenti decisioni: ABF, Collegio di coordinamento, decisione n. 897 del 14 febbraio 2014; ABF, Collegio di coordinamento, decisione n. 991 del 21 febbraio 2014; ABF, Collegio di coordinamento, decisione n. 3947 del 24 giugno 2014. Per un'analisi degli orientamenti dell'ABF: I.A. Caggiano, *Pagamenti non autorizzati tra responsabilità e restituzioni. Una rilettura del d. legisl. 11/2010 e lo scenario delle nuove tecnologie*, cit., p. 474 ss.; F. Ciraolo, *Pagamento fraudolento con carta di credito e ripartizione delle responsabilità.*

dallo stato della tecnica e delle conoscenze informatiche, ben più che in altri settori. Se la "ragionevolezza delle misure idonee a proteggere le credenziali di sicurezza personalizzate" può essere concretizzata con riferimento alle abitudini di vita quotidiane, da tutti apprezzabili, viceversa la verifica che "le credenziali di sicurezza personalizzate non siano accessibili a soggetti diversi dall'utente abilitato a usare lo strumento di pagamento" richiederebbe verifiche in concreto, estranee ai poteri istruttori dell'ABF, che deve limitarsi a cogliere l'evoluzione delle conoscenze specialistiche e della tecnica in materia. Deve comunque apprezzarsi l'attività su questi temi dell'ABF, che fa progressivamente evolvere la conoscenza delle regole del procedimento.

È da ricordare che l'ABF ha sostanzialmente anticipato la nuova Direttiva nell'imporre uno standard di autenticazione forte (basato cioè sull'uso di due o più elementi tra loro indipendenti)[34] come requisito di prova che un'operazione a distanza è stata correttamente autenticata. Ciò ha determinato un incremento degli standard di sicurezza applicati agli strumenti di pagamenti dai PSP in Italia, secondo un approccio ancora in corso di evoluzione[35] in base alle norme tecniche di regolamentazione della Commissione europea, che segue un principio di proporzionalità: possibilità di deroghe all'autenticazione per gli strumenti di pagamento di basso valore (art. 4 d.lgs. 11/2010), che applicano una modalità di inizializzazione *contactless*; autenticazione forte per i pagamenti con accesso al conto di pagamento *online*, e in tutti i pagamenti a distanza a rischio di frode o altri abusi [art. 10-*bis*, par. 1, lett. *a*) e *c*), d.lgs. 11/2010]; autenticazione forte "con elementi che colleghino in maniera dinamica l'operazione a uno specifico importo e a un beneficiario specifico", per i pagamenti elettronici [cfr. art. 5 Reg. del. (UE) 2018/339].

L'approccio adottato è appunto di regolazione tecnica della fase iniziale del procedimento secondo requisiti di sicurezza delle credenziali e dello strumento di pagamento che vengono aggravati in proporzione al rischio di frode, massimo nella sfera dei pagamenti elettronici.

Dagli orientamenti attuali alla revisione della PSD, in *Dir. banc. merc. fin.*, 2017, p. 150 ss.; v. ora anche ABF, Collegio di coordinamento, decisione n. 8553 del 28 marzo 2019.

[34] ABF, Collegio di coordinamento, decisione n. 3498 del 26 ottobre 2012.

[35] I.A. Caggiano, *Pagamenti non autorizzati tra responsabilità e restituzioni. Una rilettura del d. legisl. 11/2010 e lo scenario delle nuove tecnologie*, cit., p. 501 ss.

5. *La necessaria collaborazione del PSP e la verifica dell'identità dell'ordinante e dell'identità del beneficiario: le regole dell'autenticazione e la regola dell'esecuzione secondo prevalenza dell'IBAN sul nome del beneficiario*

Tra i profili di rischio maggiori di anomalia di un'operazione di pagamento vi è non solo l'errore sull'identità di colui che dà il consenso all'operazione di pagamento (cioè sull'identità dell'ordinante, pur con tutte le precisazioni e i distinguo che invece avvolgono di incertezza l'inquadramento dogmatico dell'ordine di pagamento nell'addebito diretto e nei pagamenti su carta il cui importo è determinato dal beneficiario, previsti dall'art. 12-*bis* d.lgs. 11/2010), ma anche l'errore sull'identità di colui che riceve l'accredito finale.

Se un pesante e ingombrante pacco, o una lettera in busta chiusa, giunge all'indirizzo sbagliato, vi sono buone probabilità che il destinatario ne rifiuti la consegna e dia così un'indicazione che è idonea a rendere avvertito il prestatore del servizio di trasporto della non corretta esecuzione. La necessaria cooperazione del beneficiario della consegna consente di ridurre gli errori del vettore nell'individuazione del destinatario.

L'errore nell'individuazione del conto del beneficiario, invece, incontra una maggiore probabilità di dare luogo a una anomalia definitiva del procedimento, perché l'accredito non richiede un comportamento attivo di collaborazione del beneficiario, ma la reazione all'erroneo accredito dipende da una verifica – che dovrebbe essere sollecitata successivamente all'accredito – e da un comportamento volontario conforme a correttezza da parte del beneficiario stesso.

La prassi bancaria anteriore alle Direttive sui servizi di pagamento conosceva dunque tempi lunghi di accredito dei bonifici, giustificati con la necessità di compiere opportune verifiche, da parte della banca del beneficiario, in tutti quei casi in cui risultassero difformità tra l'intestazione del conto di arrivo e il nome contenuto nell'ordine di pagamento.

Una rivoluzione copernicana è stata attuata mediante l'adozione della regola, di origine anglosassone, di prevalenza dell'identificativo unico del conto, indicato sull'ordine di pagamento, rispetto all'intestazione eventualmente difforme del conto, in caso di menzione del nome del beneficiario. Questa "spersonalizzazione" dell'operazione di pagamento, che collega un IBAN di partenza a un IBAN di arrivo, è il sacrificio richiesto dall'automazione bancaria. La regola iniziale della PSD era disumana: l'esecuzione corretta è quella secondo l'IBAN, se vi sono degli errori nel numero, non è un problema del PSP. La nuova versione introduce obblighi

di collaborazione sia del PSP del pagatore sia del PSP del beneficiario[36], che sostanzialmente fanno leva sulla circostanza che rendere avvertiti dell'errore il beneficiario può consentire il recupero della somma, poiché non tutte le persone sono scorrette e anzi la maggioranza si conforma spontaneamente a obblighi collaborativi.

L'autorità nazionale di sorveglianza sul sistema dei pagamenti ha molto insistito sulla necessità di compiere verifiche sulla corrispondenza tra IBAN e beneficiario, pur se non previsti dalla normativa unionale[37]. Il punto più delicato è dato proprio dalla *privity of contract*, e dall'assenza di obblighi contrattuali tra il PSP del beneficiario e il pagatore[38], ove questi non abbia alcun rapporto contrattuale con il PSP che può compiere la verifica, ma solo con il PSP di radicamento del conto da cui i fondi sono stati trasmessi.

La risposta positiva al quesito implica una consapevole adesione alla ricostruzione dell'operazione di pagamento in termini procedimentali, con obblighi delle parti, rispetto al procedimento, che non sono interamente riconducibili al contratto.

Anche in seno all'ABF si sono aperti diversi filoni interpretativi in ordine all'esistenza di obblighi di verifica in capo al PSP del beneficiario: la questione, recentemente risolta dal Collegio di Coordinamento dell'ABF in senso positivo[39], non può essere giudicata in termini difformi negli Stati membri e pertanto è stata di recente sottoposta da un Tribunale italiano alla Corte di Giustizia dell'Unione europea[40]; che l'ha risolta nel senso che la limitazione di reponsabilità si applica anche al PSP del beneficiario.[41]

[36] V. De Stasio, *Ordine di pagamento non autorizzato e restituzione della moneta*, cit., p. 195.
[37] E. Depetris, *La responsabilità della banca per pagamento illegittimo di bonifico bancario*, in *Banca, borsa, tit. cred.*, 2015, II, p. 209 ss.; V. De Stasio, *Ordine di pagamento non autorizzato e restituzione della moneta*, cit., p. 191 ss.
[38] D. Einsele, *Die bereicherungsrechtliche Rückabwicklung von Zahlungen wegen falscher Kontoangabe*, in *Festschrift für Dieter Reuter*, Beck, Berlin 2010, p. 53 ss.
[39] ABF, Collegio di coordinamento, decisione n. 162 del 12 gennaio 2017.
[40] Trib. Udine, ord. 3 aprile 2018, consultata in data 12 gennaio 2019 all'URL http://www.fallimentiesocieta.it/sites/default/files/Trib.%20Udine%203.04.2018_0.pdf
[41] CGUE, 21 marzo 20169, C-245/18.

6. *I nuovi servizi della PSD2 e il rapporto tra i nuovi operatori e il PSP di radicamento del conto: logiche restitutorie e risarcitorie e rischio di overcompensation nell'attuazione italiana della Direttiva, probabilmente non coerente con le indicazioni del legislatore europeo (art. 73.2. PSD2)*

Il superamento della *privity of contract* e la logica procedimentale sono passi e strumenti necessari a comprendere e correttamente applicare le novità della PSD2, che - per consentire un ordinato sviluppo del commercio elettronico - ha inquadrato come nuovi servizi di pagamento le attività di alcuni operatori professionali già esistenti sul mercato, volte a soddisfare il bisogno del venditore *online* di avere sicurezza del pagamento elettronico disposto dal cliente, prima di dare corso all'esecuzione della prestazione dovuta in forza del contratto sinallagmatico stipulato *online*.

L'affidamento che un pagamento disposto *online* da un utente sia effettivamente eseguito dal PSP di radicamento del conto può essere conseguito, dal beneficiario del pagamento stesso, se quest'ultimo può ottenere, da un terzo indipendente dal pagatore, la conferma che l'ordine sia stato regolarmente ricevuto dal PSP di radicamento e che quest'ultimo sia obbligato a darvi corso, per l'esistenza di un saldo disponibile sufficiente a coprire l'importo dell'ordine stesso[42]. Il soddisfacimento di tale esigenza, nell'intervallo tra la conclusione del contratto *online* e la sua esecuzione, è stato appunto l'oggetto dell'attività di operatori collocatasi in una vera e propria zona grigia del settore[43], vista l'operatività conseguita mediante la sollecitazione del cliente alla comunicazione delle proprie credenziali attraverso un canale che, per quanto protetto, non è nella sfera di controllo del PSP di radicamento, bensì in quella del nuovo operatore, che svolge il servizio di informazione sui conti e/o quello di disposizione di ordine di pagamento.

Questo ambito poco regolato, che avrebbe potuto dare luogo a reazioni degli operatori bancari tradizionali basate sulla contestazione della violazione dell'obbligo dell'utente di fornire a terzi le credenziali del proprio strumento di pagamento, e al contempo determinare l'assunzione di responsabilità da fatto illecito in capo a soggetti privi di autorizzazione, di presidi organizzativi e di coperture assicurative, è stato l'oggetto dell'originale intervento della PSD2, che ha richiesto l'assunzione della qualifica di PSP a tali operatori, assoggettandoli ad autorizzazione, obblighi di sicurezza e di *compliance*, assicurazione obbligatoria e sorveglianza, in base all'attribuito *status* di nuovi

[42] S. Werner, *Wesentliche Änderungen des Rechts der Zahlungsdienste durch Umsetzung der zweiten EU-Zahlungsdiensterichtlinie in deutsches Recht*, in *WM*, 2018, p. 449 ss.
[43] V. De Stasio, *Ordine di pagamento non autorizzato e restituzione della moneta*, cit., p. 157.

prestatori di servizi di pagamento. Legittimazione e regolazione al contempo hanno introdotto una nuova modalità di procedimento di autorizzazione dell'operazione di pagamento, che non contempla più soltanto un contatto diretto tra utente e PSP di radicamento, nella trasmissione delle credenziali, ma anche la nuova modalità del contatto mediato dai nuovi operatori, che deve svolgersi secondo regole e condizioni di sicurezza anch'esse oggetto di puntuale disciplina negli artt. 5-*ter* (per i servizi di informazione sui conti) e 5-*quater* (per i servizi di disposizione di ordine di pagamento) del novellato d.lgs. 11/2010.

La nuova operatività si inserisce appunto nella fase di autenticazione dell'operazione – per il servizio di disposizione di ordine – e nella acquisizione di informazioni sul saldo dell'utente, per il servizio di informazione sui conti. Lo scopo di apertura del mercato a nuovi operatori, non necessariamente bancari, ha determinato il legislatore unionale a stabilire un obbligo di collaborazione di fonte legale, non basato su contratto (artt. 5-*ter*, par. 1, secondo periodo, e 5-*quater*, par. 1, secondo periodo, d.lgs. 11/2010) a carico dei PSP di radicamento del conto che consentano agli utenti l'operatività *online*. In particolare i PSP di radicamento devono consentire a tali operatori di utilizzare le medesime procedure di autenticazione forte che abbiano fornito all'utente loro cliente, e dare corso alle richieste di informazione e agli ordini di pagamento trasmessi da tali operatori con parità di trattamento rispetto a quelli trasmessi direttamente dall'utente loro cliente [artt. 10-*bis*, par. 5; 5-*ter*, par. 3, lett. *c*); 5-*quater*, par. 3, lett. *b*), d. lgs. 11/2010]. Analogamente una conferma della disponibilità dei fondi al PSP di radicamento del conto può essere richiesta dal PSP che emette strumenti di pagamento basati su carta (purché non si tratti di carta prepagata), ma in questo caso il PSP di radicamento del conto deve ricevere l'esplicito consenso preventivo dell'utente pagatore, suo cliente, alla richiesta (art. 5-*bis*, d.lgs. 11/2010). Tanto non è invece previsto per i due nuovi servizi, che lasciano il PSP di radicamento esposto a richieste e ordini non preannunciati, che pongono nuovi profili di ripartizione delle responsabilità rispetto a eventuali anomalie del procedimento.

L'art. 73 della Direttiva e l'art. 11, par. 2-*bis*, con disposizioni non esattamente sovrapponibili, hanno fornito delle regole sui rimedi, mantenendo sempre come centrale la posizione di obbligato verso il proprio cliente del PSP di radicamento del conto, in una posizione che è sostanzialmente di garanzia. L'analisi del rimedio a carattere restitutorio a disposizione dell'utente contro il PSP di radicamento del conto, per i casi di addebiti non autorizzati avvenuti anche senza coinvolgimenti di

altri PSP, lascia comprendere che la natura del rimedio dell'utente non muta nell'art. 73.2. rispetto alla previsione dell'art. 73.1. Se l'ordine di pagamento non è autorizzato dal cliente, questi ha diritto all'immediata restituzione, indipendentemente dalla provenienza dell'ordine (che resta irrilevante). Viceversa la provenienza dell'ordine da un PSP, che si presenta come incaricato da un utente le cui credenziali di sicurezza siano state invece violate, o che trasmetta un ordine di pagamento modificato nell'importo, nel beneficiario o in qualsiasi altro dato dell'operazione, pone un problema di responsabilità per inadempimento o per fatto illecito del prestatore del servizio di disposizione di ordine.

Non mi sembra fondata la preoccupazione dei giuristi tedeschi che vedono in questa ipotesi un'anomalia sistematica, e cioè un caso di responsabilità senza colpa del PSP di radicamento verso il proprio cliente, contrario ai principi in materia di responsabilità bancaria[44]. Non ritengo fondata la preoccupazione in quanto di per sé, a mio avviso, si tratta di titoli completamente diversi. Proprio la circostanza che il PSP che si limita a trasmettere l'ordine «non detiene in alcun momento i fondi del pagatore in relazione alla prestazione del servizio di disposizione di ordine di pagamento» [art. 5-*ter*, par. 2, lett. *a*), d. lgs. 11/2010] esclude che questi possa essere destinatario di un'azione a carattere restitutorio dei fondi dell'utente, in quanto per definizione non può appropriarsi di ciò che non detiene.

La netta distinzione tra rimedi risarcitori e restitutori traspare dal testo della Direttiva e invece si confonde nel dettato del secondo periodo del par. 2-*bis* dell'art. 11, che stabilisce un obbligo di rimborso "a catena", in favore del PSP di radicamento del conto, in ogni caso di iniziazione del pagamento non autorizzato per suo tramite. Questa disposizione manca nel testo della Direttiva, che invece richiama l'obbligo risarcitorio del terzo periodo del par. 2-*bis* (tanto si ricava in particolare, nel testo italiano della Direttiva, dall'uso della parola "rimborsa" come prestazione a carico del PSP di radicamento nei confronti dell'utente, e invece della parola "risarcisce" per sancire l'obbligo dell'altro PSP verso il primo). Tra secondo e terzo periodo del par. 2-*bis* vi è una sostanziale sovrapposizione di rimedi, che appare non giustificata e non conforme alla Direttiva, che viceversa menziona un rimedio risarcitorio in favore del PSP di radicamento.

Le differenze sono rilevanti sul piano pratico, in quanto la determinazione del *quantum* risarcibile deve tenere conto dell'eventualità di un recupero parziale dei fondi trasferiti e non conteggiabili all'utente nel rapporto di conto

[44] J. Köndgen, *Jenseits des Relativitätsprinzip: Haftungsstrukturen im neuen Zahlungsdiensterecht*, cit., p. 150 s.

di pagamento, che rende il rimborso da parte del PSP misura eccessiva (di *overcompensation*) rispetto allo scopo. Tenuto conto dell'obbligo di polizza assicurativa posto a carico dei PSP che svolgano i nuovi servizi, si tratta di una norma la cui infelice formulazione potrebbe essere all'origine di eventuali contenziosi. A mio avviso, la duplicazione dei rimedi (restitutorio e risarcitorio) nell'attuazione italiana dell'art. 73.2 della Direttiva merita di essere sottoposta alla Corte di Giustizia, con un eventuale rinvio pregiudiziale.

Abstract

L'operazione di pagamento nella Direttiva PSD2 deve essere inquadrata come un procedimento per il trasferimento di fondi. La circostanza che il denaro sia misura e oggetto sia delle obbligazioni risarcitorie sia di quelle restitutorie può portare a confusioni. L'analisi dei ruoli dei prestatori di servizi di pagamento e degli utenti porta a criticare l'attuazione italiana dell'art. 73.2 della Direttiva PSD2, per il rischio di *overcompensation* a carico dei nuovi operatori (TPP - *Third Party Providers*).

Parole chiave: Operazione di pagamento – PSD2

Maria Cecilia Paglietti

Questioni in materia di prova nei casi di pagamenti non autorizzati

Sommario: 1. La regolazione dei servizi di pagamento come sintesi della modernità – 2. Questioni di metodo: interdisciplinarietà e tecnica legislativa – 3. Questioni di merito: l'allocazione del rischio – 4. 1. L'obbligo di autenticazione forte di matrice giurisprudenziale – 4. 2. L'obbligo di autenticazione forte contenuto nella Direttiva – 5. Vincoli di solidarietà tra IP – 6. La ripartizione degli oneri probatori – 7. Fatti generatori di responsabilità dell'intermediario e mezzi di prova – 8. La colpa grave del pagatore.

1. *La regolazione dei servi di pagamento come sintesi della modernità*

L'argomento degli aspetti probatori dei pagamenti non autorizzati è delicato, soprattutto perché, come noto tanto alla dottrina sostanzialista quanto a quella processualistica (quello della prova è uno dei cosiddetti istituti bifronti, come definiti nella Relazione al codice civile[1]), la ripartizione dell'onere della prova è cruciale sull'esito della lite[2].

Per affrontare il tema compiutamente, mi pare opportuno svolgere alcune premesse in ordine all'impianto sistematico della nuova disciplina in materia di servizi di pagamento, alle scelte *policy* ad esso sottese, all'allocazione della responsabilità, e, in ultimo, alle possibili fattispecie concrete.

L'A. è componente supplente del Collegio di Roma dell'Arbitro Bancario Finanziario. Le opinioni espresse nel lavoro hanno carattere personale e non sono in alcun modo riferibili a tale istituzione.

[1] Così definiti in quanto «ponte di passaggio tra il processo e il diritto soggettivo»: Relazione al codice di procedura civile del ministro Guardasigilli Grandi, presentata al Re, Roma, 1940, n. 6, p. 16.

[2] M. R. Damaška, *Evidence Law Adrift*, Yale University Press, New Haven 1997 (del volume esiste anche una versione italiana, dal titolo *Il diritto delle prove alla deriva*, a cura di M. Taruffo. - Trad. di F. Cuomo Ulloa, V. Riva, Il Mulino, Bologna 1991); M. Mekki, *Regard substantiel sur le "risque de preuve" – Essai sur la notion de charge probatoire*, in *La preuve: regards croisés*, a cura di M. Mekki, L. Cadiet e C. Grimaldi, *La preuve, regards croisés*, Thèmes et commentaires, Dalloz, Paris 2015, p. 7.

La necessità di una nuova disciplina e, dunque, della riformulazione della previgente Direttiva (2007/64/CE)[3] si fonda su due grandi architravi concettuali: sicurezza dei sistemi informatici e fiducia degli utenti[4]. I due temi trovano la loro sintesi nella ricerca di un contemperamento tra le istanze della regolazione (maggiore sicurezza dei pagamenti e protezione del soggetto debole del rapporto negoziale) e la promozione della concorrenza (un mercato dei pagamenti efficiente e integrato[5]; miglioramento del *level playing field* per i *providers*; ampliamento del mercato, tramite l'introduzione di nuovi operatori e nuove tecniche[6]: *mobile payments, wallet providers, third party providers, instant payments*), letti nella filigrana della massiccia diffusione di nuovi mezzi pagamento, tecnicamente complessi, implicanti maggiori rischi di sicurezza[7] e relative lacune regolamentari, che a loro volta si svolgono lungo il crinale delle due grandi traiettorie di sviluppo del Fintech: dematerializzazione e disintermediazione[8].

È notorio che il rischio di operazioni fraudolente dipenda tanto dal comportamento delle parti, quanto dal livello di sicurezza del servizio adottato

[3] Direttiva 2007/64/CE del Parlamento europeo e del Consiglio, del 13 novembre 2007, relativa ai servizi di pagamento nel mercato interno, su cui cfr. AA.VV., *Il nuovo quadro normativo comunitario dei servizi di pagamento. Prime riflessioni*, a cura di M. Mancini e M. Perassi, Banca d'Italia, in *Quaderni di Ricerca Giuridica della Consulenza Legale*, n. 63, Roma 2008; AA.VV., *La nuova disciplina dei servizi di pagamento*, a cura di M. Mancini, M. Rispoli Farina, A. Santoro, A. Sciarrone Alibrandi e O. Troiano, Giappichelli, Torino 2011, p. 9; D. Mavromati, *The Law of Payment Services in the EU, The EC Directive on Payment Services in the Internal Market,* Kluwer Law International, Alphen aan den Rijn 2007.

[4] Che costituiscono i due grandi temi alla base del progetto di riforma del sistema dei pagamenti: cfr. in argomento Banca d'Italia, *Libro bianco sul sistema dei pagamenti in Italia*, Roma 1987.

[5] Inteso quale presupposto di crescita economica della Unione europea e di realizzazione del massimo vantaggio del mercato interno: v. 5° Considerando, Dir. 2366/2015.

[6] Libro Verde della Commissione Europea dell'11 gennaio 2012 "Verso un mercato europeo integrato dei pagamenti tramite carte, internet e telefono mobile", COM (2011) 941 def.; B. Geva, *The Payment Order of Antiquity and the Middle Ages*, Hart Publishing, Oxford 2011.

[7] 7° Considerando, Dir. 2015/2366.

[8] N. Martial-Braz, *L'apport du numérique au droit bancaire: l'émergence des FinTechs*, in *Revue de Droit bancaire et financier*, 2017, dossier 2; sul tema dell'impatto dell'innovazione digitale sull'industria bancaria cfr. G. Barba Navaretti, G. Calzolari, A. F. Pozzolo, *Banche e fintech. amici o nemici?,* in *Fintech*, a cura di F. Finnamò e G. Falcone, ESI, Napoli 2019, p. 25. In Francia, la normativa di recepimento della Dir. 2015/2566 si sovrappone alla *Loi pour une République numérique* (Loi n° 2016-1321 del 7 ottobre 2016), che, per un verso, ha generalizzato il pagamento tramite sms e, per altro, senza attendere la trasposizione della Direttiva (e andando contro l'avviso del *Conseil d'État*: P. Storrer, *Quand un teste mors sujet entend transposer à contretemps une directive DSP2*, in *Revue Banque*, dossier n° 799) ha creato un'eccezione allo statuto del prestatore di servizio di pagamento per gli operatori di telecomunicazioni.

dall'operatore. Questa osservazione, apparentemente scontata, consente tuttavia di evidenziare l'aspetto dirimente che la tecnologia riveste in materia[9].

Sul piano giuridico, il filo conduttore che anima la Direttiva e le riflessioni in materia è la consapevolezza della necessaria gestione di conflitti tra parti diseguali e, quindi, la ricerca di un *balanced equilibrium* (tanto nel momento della progettazione delle norme, quanto in quello della loro applicazione) tra le istanze di sicurezza (dei sistemi, degli utenti) e quelle dell'innovazione[10].

Il tema delle operazioni non autorizzate (nelle ipotesi di smarrimento, furto o appropriazione indebita), che, cioè, si sono svolte senza il consenso del titolare della carta di pagamento (sia essa di debito che di credito)[11], è, dunque, quello dell'imputabilità.

La tematica può essere scomposta in tre segmenti: i) allocazione del rischio (regime di responsabilità e individuazione del soggetto che deve sopportare le conseguenze dell'evento fraudolento); ii) ripartizione degli oneri probatori; iii) individuazione e portata dei mezzi di prova.

2. *Questioni di metodo: interdisciplinarietà e tecnica legislativa.*

La nuova disciplina pone problemi di metodo e di merito.

Con riguardo all'aspetto metodologico, costituisce un dato di pacifico accoglimento che nel *Fintech* l'oggetto della normazione sia fluido e mutevole; e che l'approccio regolatorio, basato sull'interdisciplinarietà, debba essere caratterizzato da pluralismo e dal necessario dialogo tra saperi

[9] Così già O. Troiano, *I servizi elettronici di pagamento. Addebiti in conto non autorizzati: un'analisi comparata*, Giuffrè, Milano 1996, p. 66. Sull'influenza dell'evoluzione tecnologica sul diritto bancario in generale e sul diritto dei pagamenti in particolare, cfr. già: *Innovation technologique et droit bancaire: Cour de cassation*, Rapport annuel 2005, in *Doc. fr.*, 2006, p. 87; P. Leclercq, *Les titres dématérialisés de paiement et de crédit : Le droit privé français à la fin du XXe siècle*, in *Études offertes à Pierre Catala*, Litec, Paris 2001, p. 785.

[10] Sugli indirizzi dell'UE in materia fintech, S. Chishti, J. Barberis, *The FinTech Book: The Financial Technology Handbook for Investors, Entrepreneurs and Visionaries Chichester,* John Wiley & Sons., West Sussex 2016; M.T. Paracampo, *Robo-advisor, consulenza finanziaria e profli regolamentari: quale soluzione per un fenomeno in fieri?*, in *Riv. trim. dir. ec.*, Supp. al n. 4, 2016, p. 256; P. Pailler, *Le consommateur de services financiers au coeur des préoccupations du législateur européen*, in *Revue de Droit bancaire et financier*, 2014, p. 8.

[11] Cfr. F. Ciraolo, *Le carte di debito nell'ordinamento italiano. Il servizio bancomat*, Giuffrè, Milano 2008; O. Troiano, *Contratto di pagamento*, in *Enc. dir.*, Annali, V, Giuffrè, Milano 2012, p. 392 ss.

specialisti (che però parlano linguaggi diversi)[12].

Il momento legislativo, quello interpretativo e quello dell'*enforcement* devono incorporare il dato scientifico, basarsi su di esso, a pena di risultare irragionevoli[13]. L'adeguata compenetrazione tra il dato scientifico e il precetto normativo implica che alla base della giuridificazione ci sia una precomprensione del fenomeno tecnico, e che la legge (o la decisione) rappresentino il medio logico attraverso i quali adeguare il diritto alla scienza.

Il tema è quello dell'interscambio tra tecnologia e diritto (a livello sia legislativo sia giurisprudenziale), che obbliga il giurista ad instaurare un dialogo forzoso non più con le aree culturali maggiormente affini (sociologia, economia) ma con le cosiddette "scienze dure".

Se la forma tradizionale di dialogo familiare ai giuristi (soprattutto a chi, come me, è di estrazione comparatista) è quello tra i formanti, che si svolge dunque *all'interno* del medesimo sapere, ora all'interprete si dischiudono nuovi interlocutori, *esterni* e con specificità culturali differenti: questo tipo di dialogo –necessario- che può più facilmente essere raggiunto all'interno del procedimento legislativo, deve permanere anche nei momenti successivi, quelli dell'applicazione del diritto. È solo il perdurare di questo dialogo che può evitare interpretazioni obsolete o irragionevoli e avallarne di rispettose dell'"evento informatico" -così come si è effettivamente svolto- e conferenti all'evoluzione tecnologica (per giungere a quello che Guido Calabresi chiama significativamente il «miglioramento condiviso del diritto»[14]).

Non si tratta, in questa materia, di contrapporre l'economia al diritto, i bisogni del mercato ai valori della giurisdizione, ma cercare di contemperarli e farli convivere senza attriti.

Vorrei riportare un esempio, anticipando un tema che svilupperò nel prosieguo della relazione: il protocollo 3DSecure viene considerato, in alcune decisioni della *Cour di cassation*, come un elemento che, aumentando la sicurezza del sistema informatico, costituisce indice di una condotta diligente dell'intermediario[15]; per contro, la giurisprudenza

[12] N. Irti, *Norme e luoghi. Problemi di geo-diritto*, Laterza, Roma-Bari 2006; nello specifico dell'influenza dell'evoluzione tecnologica sul diritto bancario e, in particolare, sugli strumenti di pagamento: É. Wéry, *Paiements et monnaie électroniques. Droits européen, français et belge,* Larcier , Brusselles 2007.

[13] Su questi temi v J. Habermas, *Fatti e norme*, *Contributi a una teoria discorsiva del diritto e della democrazia,* curato e tradotto da L. Ceppa, Laterza, Roma-Bari 2013*;* S. Penasa, *La legge della scienza: nuovi paradigmi di disciplina dell'attività medico-scientifica. Uno studio comparato in materia di procreazione medicalmente assistita*, Esi, Napoli 2015.

[14] *Il mestiere di giudice. Pensieri di un accademico americano*, Il Mulino, Bologna 2013, p. 85.

[15] Sentenza 31 maggio 2016, in *Dalloz*, 2016, p. 2305, con note di D. R. Martin, H. Synvet; *Sem. Jur., éd. Entr. Aff*., 2016 p. 1450, con nota di J. Lasserre Capdeville.

italiana (segnatamente, l'Arbitro Bancario e Finanziario) considera il sistema 3DSecure non necessariamente sicuro, il che conduce, unitamente alla presenza di altre circostanze contingenti, all'accoglimento delle istanze attoree. Il tema ha necessitato di un specifico intervento chiarificatore da parte dell'EBA. A me pare che questo sia un caso paradigmatico di quanto la differente valutazione di un "fatto informatico" abbia ricadute sul piano giuridico, esitando in decisioni di segno opposto.

Il tema regolatorio si presenta sin dalla scelta della tecnica legislativa: se la disciplina è troppo specifica, rischia di essere "controtempo" [16] e divenire presto, alternativamente, lacunosa od absoleta[17]. In entrambi i casi il rischio è che si apra uno spazio eccessivo tra la norma ed il contesto applicativo. Per contro, se eccessivamente ampia (norme in bianco), rischia di enfatizzare a dismisura il ruolo degli interpreti[18].

Ed in questo ultimo caso, il nodo cruciale della teoria dell'interpretazione intesa come correttivo al silenzio del legislatore è che gli interpreti divengano "legislatori di seconda istanza"[19], riformulando leggi che i postulati positivistici laddove troppo stretti non consentano, o laddove troppo larghi non prevedano. Tuttavia, questa situazione apre, *ça va sans dire*, alle difformità, considerato che l'attività interpretativa ha, notoriamente, una matrice autobiografica, poiché, come ci ricordano i filosofi, risente delle convinzioni e delle posizioni intellettuali di chi la svolge [20].

Appare, dunque, necessaria, da parte di chi fa le leggi, la predisposizione di un programma legislativo aperto, idoneo a coniugare i requisiti di generalità ed astrattezza con la specificità del caso concreto[21]: l'intento del legislatore dovrebbe essere quello di realizzare un sistema regolatorio equamente basato su clausole generali e fattispecie dal perimetro definito.

Questo appare tanto più vero nel nostro ordinamento, nel quale, come in tutti gli ordinamenti a diritto codificato, non vige il principio dello *stare decisis*, e dunque il precedente giurisprudenziale non assume un valore vincolante, consentendo ai giudici successivi di discostarsi da quanto in

[16] Dal titolo del libro di S. Rossi, *Controtempo. L'Italia nella crisi globale*, Laterza, Roma-Bari 2009, spec. 173 ss.
[17] G. Timsit, *Les noms de la loi*, PUF, Paris 1991, p. 117.
[18] W. Twining, D. Miers, *How to Do Things with Rules: A Primer of Interpretation*, 5th ed., CUP, Cambridge 2010; sull'indeterminatezza del diritto: *Critical Legal Thought: An American-German Debate*, 1989, a cura di C. Joerges e D. M. Trubeck, Baden-Baden, Nomos 1989.
[19] S. Cassese, *Introduzione allo studio della normazione*, in *Riv. trim. dir. pubbl.*, 1992, p. 311.
[20] C. Atias, *Epistemologie juridique*, Dalloz, Paris 1985, p. 94 ss.
[21] J. Habermas, *Fatti e norme*, cit., spec. p. 521 ss.

precedenza statuito[22].

Il tema della "progettazione di norme"[23] appare quindi contiguo e funzionalmente collegato a quello del creazionismo giurisprudenziale.

La prevedibilità delle decisioni assume, poi, una connotazione del tutto specifica nel quadro della vigilanza bancaria, poiché è nella garanzia di un significativo tasso di uniformità che può giungere a compimento il principio della *regulation by litigation*, attraverso la quale conseguire il fine ultimo dell'effettività della tutela del cliente[24].

Non solo perché la ricerca comparatistica evidenzia, negli ordinamenti di *civil law*, uno scollamento fra la teoria positivista e la realtà operazionale -si pensi alle pronunce della Corte costituzionale e all'esistenza di intere aree del diritto coperte esclusivamente dal diritto giurisprudenziale: da noi il danno biologico-, ma perché al ritardo (fisiologico, in materie ad alto tasso di obsolescenza normativa, stante la fluidità del settore regolato) del formante legale non può che sopperire quello giurisprudenziale.

La connessione fra finanza, tecnica, e diritto non risponde alla logica dell'uniformità, e spetta all'interprete, tramite un complesso lavorìo ricostruttivo, il compito di garantire al complesso assetto istituzionale la coerenza e l'effettività delle norme di cui si compone[25].

[22] Cfr., da ultimo, AA.VV., *Il vincolo giudiziale del passato. I precedenti*, a cura di A. Carleo, Il Mulino, Bologna 2018, *passim*.

[23] R. Pagano, *Introduzione alla legistica. L'arte di preparare le leggi*, Giuffrè, Milano 1999; AA.VV., *Normative europee sulla tecnica legislativa*, a cura di R. Pagano, Camera dei Deputati, 1988. Per un'ampia bibliografia sulla legistica o tecnica legislativa si rimanda a L. Pegoraro, *Linguaggio e certezza della legge nella giurisprudenza della Corte Costituzionale*, Giuffrè, Milano 1988 e soprattutto al volume collettaneo *Corso di studi superiori legislativi 1988-1989*, a cura di M. D'Antonio (e segnatamente al contributo di G. Amato, *Principi di tecnica della Legislazione*) Cedam, Padova 1990, p. 48.

[24] D. Wittman, *Prior Regulation v. Post Liability, the Choice Between Input and Output Monitoring*, 6 *Journal Legal Studies*, 1977, p. 193 ss.; S. Breyer, *Breaking the Vicious Circle: Toward Effective Risk Regulation*, Harv. Univ. Press, Cambridge 1993; H. Jonas, *Le principe du responsabilitè. Une ethique pour la civilisation technologique*, trad. a cura di J. Greisch, Le Cerf, Parigi 2001; AA.VV., *Regulation Through Litigation*, a cura di W. K. Viscusi, Brookings Institution Press, Washington 2002; AA.VV., *Better regulation*, a cura di S. Weatherill, Hart Publishing, Oxford 2007; AA.VV., *Regulation by litigation*, a cura di A. P. Morriss, Yale University Press, New Haven 2009. In un'ottica del tutto specifica, quella della *agencies as litigation rulemakers* (particolarmente conferente alla materia qui trattata) cfr. U. Mittal, *Litigation rulemaking*, 127 *Yale Law Journal*, 4, 2018, 1010.

[25] N. MacCormick, *La congruenza nella giustificazione giuridica*, in AA.VV., *L'analisi del ragionamento giuridico. Materiali ad uso degli studenti*, I, a cura di P. Comanducci e R. Guastini, Giappichelli, Torino 1987, p. 243 ss., spec. 247 ss.; A. Celotto, F. Donati, *Interpretazione conforme a diritto comunitario ed efficienza economica*, in *Interpretazione conforme e tecniche argomentative*, atti del convegno svoltosi a Milano, il 6-7 giugno 2008,

3. *Questioni di merito: l'allocazione del rischio*

È un dato di pacifico accoglimento, e presente al legislatore unionista sin dalla prima formulazione della normativa in materia, che l'allocazione del rischio di pagamenti non autorizzati sia cruciale ai fini dell'effettività della disciplina e, soprattutto, della diffusione dei sistemi di pagamento -promossa in sede comunitaria[26]- la quale dipende dalla fiducia che gli utilizzatori ripongono sull'assetto dei rischi che essi garantiscono rispetto al pagamento in contanti[27].

Le scelte di vertice devono, dunque, essere capaci di garantire un'allocazione del rischio in grado di *prevenire* e *reprimere* gli esiti inefficienti derivanti da comportamenti non rispettosi, sul versante dell'impresa, della predisposizione di sistemi di sicurezza *adeguati* e, sul versante dell'utente, della diligenza nella custodia dello strumento di pagamento e delle relative credenziali.

Il tema del criterio d'imputazione della responsabilità, declinato secondo la retorica dell'individuazione del soggetto su cui più efficientemente far ricadere il danno (colui sul quale, cioè, coesianamente, far gravare il costo degli incidenti), è il cuore delle disposizioni e delle scelte politiche in materia[28], che, nei vari ordinamenti, propongono un'allocazione articolata delle perdite subìte, risentendo della maggiore propensione ad optare per la soluzione della responsabilità oggettiva limitata laddove l'attività bancaria venga ascritta alle attività pericolose[29]. Volendo individuare alcuni

raccolti da M. D'Amico e B. Randazzo, Giappichelli, Torino 2009, p. 478 ss.

[26] Cfr., per tutti, R. De Bonis, M.I. Vangelisti, *Dai buoi di Omero ai Bitcoin*, Il Mulino, Bologna 2019.

[27] 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»; cfr. già il classico studio di J. A. Cousins, W. A. Imparato, B. D. Kelley, *Toward a Less-Check Society*, 47 *Notre Dame Law Rev.*, p. 853 1972; nello specifico della materia che interessa, v. B. Geva, *Bank Collections and Payment Transaction—A Comparative legal Analysis*, Oxford University Press, Oxford 2001; É. Wéry, *Paiements et monnaie électroniques. Droits européen, français et belge*, Larcier, Bruxelles 2007; le ipotesi di furto o smarrimento delle carte di pagamento sono ascrivibili, inoltre, ai costi transattivi della transazione principale: R. D. Cooter, E. L. Rubin, *A Theory of Loss Allocation for Consumer Payments*, 66 *Texas L. Rev.*, 1987, p. 63; cfr. altresì R. Steennot, *Allocation of Liability in Case of Fraudulent Use of an Electronic Payment Instrument: the New Directive on Payment Services in the Internal Market*, 24 *Computer L. Security Rev.*,6, 2008, p. 555.

[28] Cfr. B. Geva, *Payment Transactions Under the EU Payment Services Directive: A U.S. Comparative Perspective*, 27 *Penn State International L. Rev.*, 2009, p. 713.

[29] I. Becker, A. Hutchings, R. Abu-Salma, R.J. Anderson, N. Bohm, S. J. Murdoch, A. Sasse, G. Stringhini, *International Comparison of Bank Fraud Reimbursement: Customer*

punti fermi raggiunti dal dibattito europeo in materia, posta la nota tripartizione del tema nei tre criteri del *loss spreading, loss reduction,* e *loss imposition*[30], in primo luogo appare tratto comune a tutti gli ordinamenti la maggiore propensione alla dimensione causale quale unico fondamento della responsabilità, pur residuando alcune ipotesi eccezionalmente ancorate al principio della responsabilità per colpa. Escluse le soluzioni radicali, ovvero, alternativamente, far sopportare il rischio di utilizzi fraudolenti interamente sul prestatore (modello allocativo che ha il pregio di socializzare il rischio, ma incentiva condotte negligenti dei titolari) o interamente sull'utente (schema che, per un verso, contribuisce a ridurre i danni, inducendolo a tenere uno standard di condotta ottimale ed incentivandolo una custodia vigile dello strumento e delle credenziali, ma per altro verso lo obbliga a sopportare anche i casi di furto o di smarrimento[31]), l'impianto sistematico predisposto dalla Direttiva prevede, dunque, un caricamento del rischio (non solo, come si vedrà, degli utilizzi fraudolenti, ma anche del rischio tecnologico e di quello della prova[32]), quasi esclusivamente sul prestatore[33].

Nello specifico, la nuova formulazione dell'art. 12, D.lgs. 11/2010, prevede un duplice e alternativo regime di responsabilità dell'utente, limitata e illimitata. La prima si configura in relazione ad operazioni poste in essere prima della tempestiva comunicazione di cui all'art. 7, nei limiti della franchigia, ora ridotta a euro 50 (art. 12, comma 3).

L'utente risponde invece a titolo di responsabilità illimitata qualora abbia agito in modo fraudolento, con dolo o colpa grave, venendo meno ai propri

Perceptions and Contractual Terms, 3 *Journal of Cybersecurity*, 2018, p. 109.

[30] Il riferimento è al noto lavoro di R. D. Cooter, E. L. Rubin, *op. cit.*, p. 70 ss.; cfr. anche *The Development Of Liability In Relation To Technological Change*, a cura di M. Martín-casals, Cambridge University Press, Cambridge 2014 (2° ed.), spec. p. 3 ss.

[31] O. Troiano, *op. cit.*, p. 81; cfr. in Francia, le riflessioni di M. Cabrillac, B. Teyssié, *Cartes de paiement ou de crédit. Usurpation*, in *RTD com.*, 1994, p. 538, spec p. 539; F. Ekollo, *La charge des débits d'une carte bancaire volée au domicile de son titulaire avec le code confidentiel, le titulaire ayant formé opposition auprès du Groupement carte bleue et à l'établissement de crédit dès l'ouverture de ce dernier,* in *Dalloz*, 1995, p. 167.

[32] M. Mekki, *Le risque de la preuve: aspects de droit substantiel*», in *La preuve, regards croisés*, a cura di M. Mekki, L.Cadiet e C. Grimald, Dalloz, Paris 2015, p. 7.

[33] Alcuni configurano una presunzione di comportamento incolpevole in capo all'utente: D. Legeais, *Appréciation du manquement par négligence grave d'une victime d'un acte de phishing*, in *Sem. Jur., éd. Entr. Aff.*, 2017, p. 1685. Per un'analitica descrizione della disciplina previgente, cfr. R. Bonhomme, *Instruments de crédit et de paiement*, LGDJ, Paris 2015, 11° ed.; 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.*, 2016, p. 10459 ss; D. Maffeis, *Ordini di pagamento e di investimento online nella giurisprudenza di merito e nella fonte persuasiva dinamica dell'ABF*, in *Riv. dir. civ.*, 2013, p. 11273.

obblighi di custodia delle credenziali e dello strumento di pagamento (art. 7, comma 1, lettera a), e comma 3); ovvero se non abbia dato tempestiva comunicazione dello smarrimento, furto, appropriazione indebita dello stesso (art. 7, comma 1, lettera b).

Nelle ipotesi, però, di mancata adozione del prescritto sistema di autenticazione multi-fattore, la responsabilità dell'utente, esclusa anche nel caso la sua condotta sia caratterizzata da dolo o colpa grave, è configurabile solo in caso di frode dello stesso (la cui prova è a carico del prestatore: art. 12, comma 2-bis). In questa ipotesi la "comminatoria" di responsabilità si ricollega ad un chiaro intento afflittivo più che restitutorio.

In tema di allocazione delle responsabilità, va inoltre tenuta in debita considerazione la prospettiva della probabile evoluzione dei fatti fraudolenti nuovi, ossia fatti generatori di responsabilità riconducibili alle ipotesi di danno da ignoto tecnologico (il danno, cioè, verificatosi a causa di una causa sconosciuta, quali possono essere considerati gli «inconvenienti» menzionati dall'art. 10, comma 1-bis), dei quali viene gravata l'impresa[34].

Il legislatore ha, dunque, optato per un sistema -non monolitico ma graduato[35]- di responsabilità oggettiva limitata -prevista, alternativamente, con una duplicità di funzioni, tanto indennitaria, quanto sanzionatoria[36]- alla quale ha affiancato la previsione di un'inversione dell'onere della prova a

[34] B. Geva, *The Harmonization of Payment Services Law in Europe and Uniform and Federal Funds Transfer Legislation in the USA: Which Is a Better Model for Reform?",* in *European Banking and Financial Law Journal*, 2009, pp. 699-733; e, sul punto, già P. Trimarchi, *Rischio e responsabilità oggettiva*, Giuffré, Milano 1961; R. Costi, *Ignoto tecnologico e rischio d'impresa*, in *Il rischio da ignoto tecnologico*, Giuffrè, Milano 2002, 49; C. Hodges, *Development risk: Unanswered Questions*, 61 *Modern L. Rev.*, 1998, p. 560; nella materia d'interesse: D. Maffeis, *op. ult. loc. cit.*

[35] Il concetto di graduazione è ricorrente negli studi *consumers' behavioural*: Howells, *The Potential and the Limits of Consumer Empowerment by Information*, 32 *Journal Law Soc.*, 2005, p. 349 ss.

[36] Nelle operazioni di pagamento con un terzo non legittimato a ricevere il denaro le ipotesi di sovrapposizione tra rimedi restitutori (volti a riportare «*il conto nello stato in cui si sarebbe trovato se l'operazione di pagamento non avesse avuto luogo*» -art. 11, comma 1, D.lgs. 11/2010) e risarcitori (da inadempimento, ravvisabile nell'omissione di un sforzo esigibile) non sono infrequenti, sia per la coincidenza tra l'oggetto del servizio e la misure dell'eventuale risarcimento, sia per la confusione tra i due rimedi in cui è incorsa la normativa (art. 11, comma 2 bis, D.lgs. cit.). Ancorché le soluzioni divergano in dottrina, una base ricostruttiva comune è quella di ravvisare, la compresenza di una pluralità di fattispecie rimediali (sia restitutorie che risarcitorie) nell'àmbito delle operazioni di pagamento, delle quali viene enfatizzata la dimensione procedimentale (V. De Stasio, *Riparto e responsabilità e restituzioni ne pagamenti non autorizzati*, in questo volume; I. A. Caggiano, *Pagamenti non autorizzati tra responsabilità e restituzioni. Una rilettura del d. legisl. 11/2010 e lo scenario delle nuove tecnologie*, cit., p. 10459).

carico del prestatore di servizi di pagamento, denotando una scelta di vertice di forte sensibilità alle esigenze del contraente debole e d'intransigenza per comportamenti sperequativi e pratiche anomale.

Va, tuttavia, sin da subito segnalato che, nonostante le scelte politiche ispirate a unitarietà e sintesi, i commentatori sono concordi nell'individuare il nodo maggiormente problematico dell'intera disciplina nell'applicazione diversificata del concetto di colpa grave (*faute lourde*), stante l'inevitabile localismo dell'*enforcement*[37]: la Direttiva lo definisce quale «comportamento che implica un grado significativo di mancanza di diligenza»[38]; in Italia è ravvisabile in una condotta connotata da straordinaria e inescusabile imprudenza, negligenza o imperizia, la quale presuppone che sia stata violata non solo la diligenza ordinaria del buon padre di famiglia di cui all'art. 1176 c. 1 c.c., ma anche «quel grado minimo ed elementare di diligenza generalmente osservato da tutti»[39]; in Francia viene definito come «*un comportement qui s'écarte largement du comportement qu'aurait eu dans les mêmes circonstances le bon père de famille*»[40].

4.1 *L'obbligo di autenticazione forte di matrice giurisprudenziale*

In materia di rimedi adottabili contro pagamenti non genuini si segnala una duplice linea di tendenza, tanto quella il cui baricentro riposa sulla tutela preventiva e volta ad evitare il danno (la *Strong Customer Authentication*, tipizzata dall'art. 4, comma 30, Dir. 2015/2366[41]), quanto quella successiva e volta a contenerlo (*ex post* rispetto al primo pagamento contestato: Sms o e-mail Alert; sistemi di monitoraggio antifrode).

[37] *Study on the Impact of Directive 2007/64/Ec on Payment Services in the Internal Market and on the Application of Regulation (Ec) No 924/2009 On Cross-Border Payments in the Community*, pp. 81-2 e 151.
[38] 72° considerando, Dir. 2366/2015.
[39] Cass., 19 novembre 2001 n. 14456, in *I Contratti*, 2002, p. 804.
[40] G. Cornu, *Vocabulaire juridique*, PUF, Paris 2007, 7ª éd., p. 387. Sul tema specifico cfr. S. Torck, *L'exécution et la contestation des opérations de paiement*, in *Sem. Jur., éd. Gén.*, 2010, p. 1033 ; N. Kilgus, *L'évolution des procédures de contestation des paiements*, in *Revue de Droit bancaire et financiere*, 2018, Dossier 11; A. Boujeka, *La charge du risque d'utilisation illicite d'une carte bancaire*, in *Dalloz*, 2008, p. 454.
[41] Testualmente «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»: così art. 1, comma 1, lett q-bis, d.lgs. 11/10.

Con riguardo ai sistemi di sicurezza di natura preventiva, uno degli slogan associati alla PSD2 è che essa realizza la transizione da un sistema di autenticazione monofattore a quello doppio/multi fattore[42], richiedendo la predisposizione, da parte dell'intermediario, di un sistema che combina più paradigmi di autenticazione, venendo all'utente richiesto qualcosa che solo egli conosce, qualcosa che solo egli possiede e/o qualcosa che solo egli è[43].

Nel nostro sistema, tuttavia, l'obbligo di predisposizione di sistemi siffatti era già previsto, dapprima per via giurisprudenziale (tramite il ricorso alle regole del diritto generale delle obbligazioni e a quelle della responsabilità per attività pericolosa), e successivamente in virtù della legislazione subprimaria e speciale, dando avvio un generale processo di definizione e tipizzazione giurisprudenziale del corretto comportamento del prestatore di servizi[44].

Dalla *law in action* dell'ABF, che è la giurisprudenza più copiosa sul punto (e qui emerge vistosamente la rilevanza del creazionismo giurisprudenziale e la circostanza che la materia dei servizi di pagamento rappresenti un laboratorio particolarmente prolifico in cui verificare i rapporti tra "giurisdizione" e legislazione), emerge che entrambi gli approcci (tanto quello che muove dalla disciplina generale, quanto quello che si rifà alla disciplina subprimaria) assumono quale punto focale dell'analisi l'esigenza di garantire *l'adeguatezza* dei presidi di sicurezza informatica allo scopo e agli standard consentiti dallo sviluppo della tecnologia e aggiornato all'evoluzione del fenomeno criminale[45]. È questo (l'adeguatezza) lo stilema di giudizio assunto dalla giurisprudenza pratica, la quale giunge all'enunciazione di un obbligo di autenticazione forte, muovendo dal presupposto che la diligenza dell'accorto banchiere implichi, sul piano del diritto generale dei contratti, l'obbligo di adozione di un modello organizzativo adeguato alla tipologia di operazioni posta in essere: appurato che banca debba sottostare al canone dell'art. 1176, comma 2, c.c. (noto essendo che l'attività bancaria è attività

[42] A partire dal 14 settembre 2019: cfr. art. 38, comma 2, 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.

[43] Artt. 1, comma 1, lett. q-bis; 10 bis, comma 1, d.lgs. 11/10 aggiornato.

[44] La previsione è, invece, di assoluta novità per il sistema francese: per un primo commento cfr. P. Storrer, *Derrière la DSP 2: le règlement Authentification forte et Communication sécurisée*, in *Revue Banque*, 2018, p. 86; J. Lasserre Capdeville, J. Bernardin, *Une évolution notable des services de paiement: l'exigence d'authentification forte*, in *Banque et Droit*, 2019, p. 13.

[45] Coll. coord., Dec. n. 3498/2012.

riservata[46] e ascritta alla categoria delle attività pericolose, art. 2050 c.c.), lo sforzo tecnico protettivo richiesto doveva essere idoneo a prevenire possibili eventi pregiudizievoli[47]. Si è statuita, dunque, in relazione ad una controversia relativa a fatti accaduti nel 2009, l'inidoneità della sola *password* statica a tutelare il cliente stante l'esistenza, già all'epoca, di «mezzi più efficienti per fronteggiare il fenomeno della pirateria informatica ... ragione sufficiente per indurre a concludere che un sistema di protezione ad un solo fattore … non può essere considerato misura sufficiente a proteggere adeguatamente il cliente»[48].

Quantunque il dato letterale taccia sul punto, il silenzio della normativa non può ragionevolmente precludere di ritenere che «la mancata adozione delle misure idonee di sicurezza dei codici debba integrare anch'essa un comportamento doloso o gravemente colposo»[49].

La ricostruzione poggia le proprie basi dogmatiche sul principio del rischio d'impresa, sul presupposto, cioè, che sia «razionale far gravare i rischi statisticamente prevedibili legati ad attività oggettivamente "pericolose", che interessano un'ampia moltitudine di consumatori o utenti, sull'impresa, in quanto quest'ultima è in grado, attraverso la determinazione dei prezzi di vendita dei beni o di fornitura del servizio, di ribaltare sulla massa dei consumatori e degli utenti il costo dell'assicurazione di detti rischi»[50].

Sul piano subprimario, la prima menzione della necessità di un sistema multi-fattore è stata anticipata dal 16° aggiornamento della Circolare n. 285/2013 della Banca d'Italia[51], la quale, nel recepire gli "*Orientamenti finali sulla sicurezza dei pagamenti via Internet*" emanati da EBA il 19 dicembre 2014[52], ha introdotto una specifica Sezione volta a disciplinare gli obblighi imposti alle banche che prestano servizi di pagamento tramite canale internet.

[46] Coll. Milano, Dec. n. 1241/2010.
[47] Coll. coord., Dec. n. 3498/12. Ancora in questi termini si esprime la Corte di cassazione, da ultimo nella sentenza 9158 del 12 aprile 2018 su www.dirittobancario.it.
[48] Coll. Milano, Dec. n. 1506/2010.
[49] Coll. coord., Dec. nn. 6166 e 6168, del 2013.
[50] ABF, Dec. n. 1111/2010.
[51] Circolare n. 285/2013 del 17 maggio 2016 "*Disposizioni di vigilanza per gli istituti di pagamento e gli istituti di moneta elettronica*" introduce la nuova Sezione VII "*Principi organizzativi relativi a specifiche attività o profili di rischio*".
[52] ABE/GL/2014/12_Rev1, del 19 dicembre 2014; ma il tema era già stato anticipato nelle *Recommendations For The Security Of Internet Payments*, del dicembre 2013.

4.2. *L'obbligo di autenticazione forte contenuto nella Direttiva*

Il tema della sicurezza, uno dei pilastri tanto della prima quanto della seconda versione della normativa che occupa, viene svolto sulla base dell'assunto che, in materia, è impossibile raggiungere la totale invulnerabilità di un sistema per un periodo prolungato; posto dunque che un margine di rischio è ineliminabile, accorgimenti vengono imposti allo scopo di «mitigare» il rischio, non eliminarlo[53].

Col passaggio dalla PSD1 alla PSD2 si ritiene comunemente normata la transizione dalle regole di autenticazione monofattore a quelle multifattore.

Se è vero, come ricordato, che l'obbligatoria predisposizione di un sistema multifattore non ha carattere di novità nel nostro sistema, il regolatore europeo è intervenuto, sia in sede di legislazione primaria, sia nei *Regulatory technical standards*[54], ad imporre requisiti di sicurezza aggiuntivi e rigorosi, richiedendosi che le misure di sicurezza che presidiano all'autenticazione del pagamento non siano solo plurime (multifattore), ma anche indipendenti e collegate ai parametri della transazione.

Direttiva e decreto di recepimento (rispettivamente, artt. 4, comma 1, n. 30; e 1, comma 1, lett. q-bis) impongono il requisito dell'indipendenza delle misure di sicurezza tra loro, tipizzando dunque la relazione che deve improntarne il rapporto, tale, cioè, che la violazione di una non comprometta l'affidabilità delle altre.

L'assunto è che la piena operatività del sistema di autenticazione multifattore si fondi sull'indipendenza tra le singole misure di sicurezza. L'esistenza di una relazione funzionale tra di esse consentirebbe di eludere il doppio controllo delle credenziali, e rendere, nei fatti, il sistema di autenticazione (non più forte ma) debole.

La necessaria presenza di suddetto requisito era tuttavia già prevista nel nostro ordinamento. La giurisprudenza dell'ABF ha, a più riprese, riconosciuto la portata dirimente allo stesso, ravvisando in capo all'intermediario gli estremi della condotta negligente, non rispettosa della diligenza ad esso richiesta nell'esecuzione delle proprie obbligazioni, nella predisposizione misure di sicurezza tra loro in rapporto di reciproca dipendenza, consentendo che la violazione delle credenziali relative alla

[53] EBA, *Final Report Guidelines on the security measures for operational and security risks of payment services under Directive (EU) 2015/2366 (PSD2)*, 12 dicembre 2017.

[54] 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.

conoscenza comprometta anche le credenziali relative al possesso, in luogo, per converso, della necessaria segregazione logica tra il canale dispositivo della transazione e il canale dispositivo verso il pagatore[55].

Sul piano tecnico, la novità più profonda della PSD2 è, tuttavia, quella relativa all'imposizione di un sistema di autenticazione forte in cui l'elemento dinamico sia collegato ai parametri della transazione (all'importo e al beneficiario specificati dal pagatore al momento di disporre l'operazione)[56].

Di particolare interesse, anche in tema di riparto probatorio, è la sanzione per la mancata predisposizione del sistema di autenticazione forte nel senso normativamente richiesto, che viene prevista -come già ricordato- nell'imputazione a titolo di responsabilità oggettiva per il prestatore, salva la prova della frode dell'utente (art. 12, comma 2-bis, D.lgs. 11/2010). Il legislatore, nel ricorrere al modello di responsabilità oggettiva più severo, appare utilizzare la "comminatoria" di responsabilità quale sanzione, riconoscendole una funzione compensativa dell'ingresso dei nuovi soggetti (terze parti). La previsione dell'unica esimente della frode (che, *a contrario*, esclude la rilevanza alle ipotesi di dolo e colpa grave dell'utente) dota la sanzione di un elevato grado di afflittività, considerato che il prestatore sarà responsabile anche nelle ipotesi di dolo o colpa grave della condotta dell'utente.

Il *proportionality check* circa l'adeguatezza della sanzione appare tuttavia soddisfatto, considerato che l'importanza della norma di diritto sostanziale

[55] Coll. Roma, Dec. n. 14925/2017. L'ABF ha osservato che dalla sequenza dell'attacco informatico -articolato in quattro fasi: 1) l'utilizzo del canale telematico (ricezione da parte degli autori del *phishing* delle credenziali inviate dalla ricorrente); 2) l'uso di codici dispositivi (accesso al portale titolari e modifica del numero di utenza cui inviare il codice alfanumerico); 3) l'effettuazione degli acquisti *online*; 4) la ricezione della *password* dinamica sull'utenza sostituita e conferma della genuinità dell'operazione- era emerso come nel servizio bancario oggetto di contestazione l'efficacia del meccanismo di autenticazione fosse inscindibilmente legata all'utenza telefonica, e che, dunque, la modifica del numero avrebbe dovuto generare una notifica (anche attraverso il medesimo canale telefonico), tale da allertare il titolare nel caso in cui la modifica non sia stata da lui effettuata (nello stesso senso cfr. anche Coll. Roma, Dec. n. 15027/2017; Coll. Bologna, Dec. n. 6987/2017.

[56] L'art. 5, comma 1, lett a, Regolamento Delegato (Ue) 2018/389, cit.: richiede che «a) l'elemento dinamico sia collegato ai parametri della transazione il pagatore è informato dell'importo dell'operazione di pagamento e del beneficiario; b) il codice di autenticazione generato è specifico per l'importo dell'operazione di pagamento e il beneficiario concordato dal pagatore al momento di disporre l'operazione; c) il codice di autenticazione accettato dal prestatore di servizi di pagamento corrisponde all'importo specifico originario dell'operazione di pagamento e all'identità del beneficiario approvato dal pagatore; d) qualsiasi modifica dell'importo o del beneficiario comporta l'invalidamento del codice di autenticazione generato»; cfr. anche art. 97, par. 2, Dir. 2366/2015.

che si assume violata[57], con particolare riferimento alla *ratio* e agli interessi tutelati, appare giustificare il grado di afflittività della previsione, funzionale alla sua effettività e dissuasività[58].

Tornando alle caratteristiche del sistema di sicurezza, oggetto della valutazione è, dunque, principalmente l'adeguatezza dello stesso a prevenire l'uso fraudolento degli strumenti di pagamento ed elevare al massimo livello attualmente possibile il grado di protezione del cliente[59]. L'Arbitro bancario e finanziario ha, al riguardo, una posizione che a me pare molto ragionevole (intendendo *ragionevole* nel senso visto in apertura, ossia di aderenza alla realtà concreta) giacché ritiene che la pur elevata capacità protettiva dell'autenticazione a due fattori (la quale garantisce una probabilità molto bassa che entrambi i canali siano compromessi), non valga di per sé a far automaticamente presumere un negligente comportamento del cliente, dovendosi considerare, oltre al meccanismo offerto, anche l'intero sistema di controlli predisposto dall'intermediario[60]. Questa impostazione ricostruttiva presuppone il dato, aderente alla realtà, che per quanto la forzatura di un sistema a due fattori sia improbabile, non è possibile predicare la totale invulnerabilità per alcun sistema (considerata la continua evoluzione dei metodi di aggressione informatica).

L'impiego dell'OTP non può, dunque, dare origine ad un automatismo deduttivo in virtù del quale ad esso corrisponda una presunzione assoluta di negligenza dell'utente, ma può condurre ad una valutazione più rigorosa della condotta dello stesso.

Il tema è sviluppato nei medesimi termini in Francia, dove la *Cour de cassation* ha escluso la configurabilità di una presunzione di colpa grave dell'utente solo in ragione della presenza di un sistema di autenticazione forte (quantunque non considerando obbligatoria la sua predisposizione)[61].

Il sillogismo, proposto in sede difensiva dagli intermediari, che la predisposizione di un sistema multi-fattore implichi necessariamente un'autorizzazione o la colpa grave del pagatore viene dunque escluso negli

[57] Ricorrendo al principio, elaborato in sede comunitaria, della necessaria proporzionalità tra sanzione e violazione: CGUE, sentenza del 9 novembre 2016, *Home Credit Slovakia a.s. contro Klára Bíróová*, C-42/15, § 63.

[58] CGUE, sentenza del 27 marzo 2014, *LCL Le Crédit Lyonnais SA contro Fesih Kalhan*, C-565/12, § 47.

[59] Ex *multis* Coll. Roma, Dec. n. 6606/16.

[60] Coll. Roma, Dec. n. 2660/2012.

[61] *Cour cass.* 18 gennaio 2017 in *Sem. Jur., éd. Entr.*, 2017, p. 1122, con nota di K. Rodriguez; in *Banque et Droit*, 2017, p. 32, con nota di G. Helleringer e Th. Bonneau; in *Dalloz*, 2017, p. 156 e *idibem*, 2018, p. 259, con osservazioni di A. Aynès; in *RTD com.*, 2017, p. 154, con nota di D. Legeais.

ordinamenti interni, evitando così che il generalizzato innalzamento del livello di sicurezza dei pagamenti possa sortire un paradossale effetto nocivo per gli utenti[62].

Questo è un dato su cui soffermarsi: la valutazione della condotta della banca dovrà essere oggetto di differenti criteri di giudizio, a seconda che abbia adottato o meno un sistema di autenticazione multi-fattore.

Dell'obbligatoria adozione di (almeno) due delle categorie tra quelle della conoscenza, del possesso e dell'inerenza, il Reg (EU) No 1093/2010 e la *Eba opinion*, indicano, a livello esemplificativo[63], che prova della prima possono essere considerati *password*, pin, risposte a domande di sicurezza, frasi di accesso; non, invece, i dettagli della carta o il relativo codice di sicurezza[64]. Prova della seconda, che può avere ad oggetto un bene anche non materiale, quale un'app[65], può essere costituita da un dispositivo (posto che la generazione o la ricezione di un elemento dinamico sul dispositivo costituisce un «*reliable means to confirm possession*»[66]), dalla prova della generazione di una OTP da parte di un software o di un hardware (come token, sms, e-mail), ed, ancora, dalla firma digitale, dalle carte nelle quali sia presente il QR Code; al contrario, il numero di carta ed il codice di sicurezza non sono prova di elementi del possesso[67]. La categoria dell'inerenza, la più innovativa ed in evoluzione delle tre, riferendosi ad elementi intrinseci relativi a caratteristiche biologiche e comportamentali, a loro volta inerenti a proprietà fisiche del corpo e a caratteristiche fisiologiche, comprende la scansione della retina e dell'iride, delle impronte digitali, delle vene, del viso, il riconoscimento vocale, le dinamiche di digitazione (identificando l'utente dal modo in cui digita i tasti al computer), e la verifica di tali elementi determina «*very low probability of an unauthorised party being authenticated as the payer*»[68].

[62] L. C. Henry Marie, L. Guinamant, *L'utilisation frauduleuse de la carte bancaire après hameçonnage: la recherche d'un équilibre*, in *Dalloz*, 2018 p. 2316.
[63] Art. 1, comma 1, lett q-bis, d.lgs. 11/2010.
[64] *Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2* (EBA-Op-2019-06, 21 giugno 2019), p. 6.
[65] *EBA-Op-2019-06*, cit. *supra*, p. 6.
[66] *EBA Opinion on the implementation of the RTS*, pubblicata nel giugno del 2018 (EBA-Op-2018-04), disponibile sul sito https://eba.europa.eu/-/eba-publishes-opinion-on-the-implementation-of-the-rts-on-strong-customer- authentication-and-common-and-secure-communication (ultimo accesso 28 dicembre 2019).
[67] *EBA-Op-2019-06*, cit. *supra*, p. 6.
[68] Art. 8, par. 1, Commission Delegated Regulation (EU) 2018/839 of 27 November 2017 supplementing Directive (EU) 2015/2366 of European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and

5. *Vincoli di solidarietà tra IP*

I menzionati aspetti *Tech* hanno un rilevante punto di caduta anche giuridico, risultando determinanti in caso di controversie sulla ripartizione della responsabilità tra i diversi IP coinvolti in una stessa operazione di pagamento e sull'ammissibilità (e consistenza) di alcuni mezzi di prova.

Il concetto di responsabilità, ed, in particolare, la ripartizione della responsabilità tra i diversi soggetti coinvolti rappresenta una tematica cruciale in quanto strettamente connessa ad una delle maggiori novità introdotte dalla PSD2, ossia l'estensione dell'ambito di applicazione della nuova Direttiva anche ai PISP (*Payment Initiation Service Provider*: servizio con cui si dispone un ordine di pagamento su richiesta dell'utente e rispetto a un conto di pagamento detenuto da altro intermediario[69]) ed AISP (*Account Information Service Provider*: servizio *online* per raccogliere informazioni da conti di pagamento detenuti dall'utente presso altri intermediari[70]).

Nello specifico, come già accennato, la PSD2 non fa dipendere la prestazione di servizi di disposizione di ordini (ovvero di informazione sui conti) dall'esistenza di un rapporto contrattuale tra il PISP/ AISP ed il prestatore di servizi di pagamento di radicamento del conto (ASPSP: *Account Servicing Payment Service Provider*[71]).

L'art. 11, D.lgs. 11/10, stabilisce che, nel caso di operazione di pagamento non autorizzato, incomba sull'ASPSP l'obbligo di rimborso dell'operazione (immediatamente o entro la giornata operativa successiva), a prescindere dall'eventuale coinvolgimento di un PISP. Nel caso, però, l'ordine dell'operazione di pagamento non autorizzata sia disposto mediante Pisp, quest'ultimo è gravato dell'obbligo di rimborso all'ASPSP, che ne faccia richiesta, degli importi già rimborsati al pagatore (comma 2-bis). Entrambi possono sempre dimostrare che l'operazione era stata autenticata e ottenere la restituzione delle somme rimborsate (l'ASPSP dall'utente e il PISP dall'AISP: comma 3).

Il meccanismo restitutorio previsto dal legislatore, volto al fine di regolare il diritto al rimborso dell'utente e ripartire le responsabilità tra i corresponsabili, prevede, dunque, che nel caso in cui sia stata disposta un'operazione di pagamento non autorizzata mediante un PISP, l'ASPSP sia chiamato a rimborsare immediatamente *prima facie* il pagatore dell'importo

common and secure open standards of communication.
[69] Art. 4, par. 1, n. 19, Dir. 2366/2015.
[70] Art. 4, par. 1, n. 18, Dir. 2366/2015.
[71] Art. 4, par. 1, n. 17, Dir. 2366/2015.

corrispondente all'operazione di pagamento non autorizzata, ponendo una delicata questione di ripartizione di responsabilità tra prestatori di servizi di pagamento. È pur vero che la medesima disposizione introduce un diritto di regresso in capo all'ASPSP nei confronti del PISP; qualora, tuttavia, quest'ultimo sia responsabile dell'operazione di pagamento non autorizzata[72], l'eventuale assenza di un rapporto contrattuale potrebbe rendere meno agevole l'applicazione di tale norma.

Il tema si sposta dunque sulla necessità di stabilire se il rapporto richiamato si atteggi nei termini della solidarietà o meno.

Si tratta di valutare se, posta l'astratta configurabilità pratica del concorso di colpa –ossia che in un'operazione contestata, sia l'ASPS che il PISP possano essere responsabili, nel segmento di operazione di loro competenza, di disfunzioni nel sistema di sicurezza- dal tenore della norma e dall'impianto sistematico della Direttiva possa ravvisarsi un vincolo di solidarietà tra i corresponsabili; verificare, cioè, se, posto il principio generale di solidarietà nei rapporti obbligatori con una pluralità di debitori, la fattispecie contemplata dall'art. 10, sia ascrivibile, normativamente, alle ipotesi di cui all'art. 2055, comma 1, c.c. e, in materia qui affine, all'art. 120 *quater*, 7 comma, d. lgs. 1° settembre 1993, n. 385, Testo Unico delle leggi in materia bancaria e creditizia (d'ora in avanti T.U.B.), i quali sono calibrati sulle esigenze di tutela della vittima.

È pacifico che la previsione di un vincolo di solidarietà, ampliando la schiera dei soggetti legittimati ai quali può rivolgersi, sia disposta nell'interesse del debitore; così come incontroverso è il *favor* del diritto europeo per la pluralità dei debitori, in luogo dell'unicità[73].

È altresì pacifico che l'imperativo metodologico europeo (e, quindi, anche interno) richieda la centralità dell'approccio rimediale nei termini dell'effettività della tutela e il superamento culturale della mera ricostruzione dogmatica delle fattispecie normative[74].

La lettura nei termini della solidarietà presenta, da questa angolatura, dei limiti, in primo luogo politici. La necessaria adozione di un angolo prospettico che trascenda la dogmatica concettuale in ragione delle teorie funzionaliste che elevano il piano della tutela a momento centrale della garanzia dei diritti, ha reso il canone dell'effettività il perno concettuale

[72] Sul punto cfr. anche quanto previsto dall'art. 92, par. 1, Dir. 2366/2015.

[73] Cfr., per un'impostazione anche europea, *Le nuove obbligazioni solidali*, a cura di U. Breccia e F. D. Busnelli, in *Quaderni della Rivisita di diritto civile*, Cedam, Padova 2016.

[74] Il richiamo all'effettività è presente anche nella struttura motivazionale dei giudici di legittimità: cfr. per tutte Cass., S.U., sentenza del 12 dicembre 2 14, n. 26242, in *Foro it.*, 2015, I, p. 862.

che deve informare di sé le scelte dell'interprete[75]. Nel caso dell'ABF, e degli *Ombudsmen* in àmbito finanziario, poi, -che sono i decisori maggiormente coinvolti in liti di questo tipo- questo punto di osservazione di arricchisce di un elemento ulteriore. In Italia, alla luce dell'evoluzione della natura dell'attività bancaria, comprensiva, oggi, oltre che dei tradizionali obiettivi della vigilanza prudenziale propriamente detta (racchiusi nella *grundnorm* dell'art. 5 T.U.B.) anche della tutela del cliente (art. 127 T.U.B.)[76], all'ABF viene riconosciuta una duplice funzione: immediata -di risoluzione delle controversie private[77]- e mediata -di regolazione del mercato, producendo le pronunce un effetto conformativo sulla condotta degli intermediari[78]. Il portato, dunque, della funzione regolatoria svolta dall'ABF, è la necessaria considerazione dell'effetto conformativo delle sue pronunce[79]. L'interpretazione e l'applicazione consequenzialista delle norme

[75] L'effettività, divenuta parola chiave delle moderne riflessioni sul diritto, più che un concetto dotato di una propria autonomia e rilevanza normative, costituisce una formula riassuntiva di un indirizzo di politica del diritto (F. Snyder, *New Directions in European Community Law*, Weidenfeld and Nicholson, London 1990, p. 3). Per un inquadramento in ottica moderna e trasversale del principio d'effettività Ad. di Majo, *La tutela dei diritti*, 4° ed., Giuffrè, Milano 2003, pp. 1-2.

[76] Non ancillare rispetto alle finalità dell'art. 5 ma autonoma, equivalente sul piano valoriale, dotata di valenza di interesse pubblico generale, strumentale ai valori obiettivo della vigilanza prudenziale: cfr. I. Visco, *Considerazioni finali del Governatore della Banca d'Italia*, 2010, p. 8.

[77] Art. 127 T.U.B..

[78] Art. 5 T.U.B.; cfr. M. Perassi, *Il ruolo dell'ABF nell'ordinamento bancario: prime riflessioni*, in *Analisi Giuridica dell'Economia*, 2011, pp. 154 ss.; A. Zoppini, *Appunti in tema di rapporti tra tutele civilistiche e disciplina della vigilanza bancaria*, in *Banca, borsa, tit. cred.*, 2012, pp. 26 ss.; P. Sirena, *Il ruolo dell'Arbitro Bancario Finanziario nella regolazione del mercato creditizio*, in *Oss. dir. civ. comm.*, 2017, p. 3 ss. e in *Principi, regole, interpretazione. Contratti e obbligazioni, famiglie e successioni: Scritti in onore di Giovanni Furgiuele*, a cura di G. Conte e S. Landini, Universitas Studiorum, Mantova 2017, p. 511.

[79] Il tema dell'efficacia conformativa dei sistemi ADR - *Alternative Dispute Resolution*- è tipico dei settori regolati (dove gli organismi di risoluzione vengono generalmente incardinati presso i regolatori, dando origine a delle figure ibride, nelle quali coesistono elementi privatistici e pubblicistici: D. Marrani, Y. Farah, *ADR in the Administrative Law: a Perspective from the United Kingdom*, in *Alternative Dispute Resolution in European Administrative Law*, a cura di D. C. Dragos e B. Neamtu, Springer, Berlin-Heidelberg 2014, 259 ss.; in Italia aveva già individuato la tendenza all'espansione dei "moduli misti" L. Torchia, *Il controllo pubblico della finanza privata*, Cedam, Padova 1992, p. 10; A.A. Dolmetta e U. Malvagna, Sul nuovo "*ADR Consob*", in *Banca borsa, tit. cred.*, 2016, p. 251; M. Stella, *Lineamenti degli arbitri bancari e finanziari*, Cedam, Padova 2016, p. 98; M. Remàč, *Coordinating Ombudsmen and the Judiciary: A Comparative View on the Relations Between Ombudsmen and the Judiciary in the Netherlands, England and the European Union*, Intersentia, Cambridge 2014, p. 7; C. Gill, J. Williams, C. Brennan e N. O'Brien, *The Future of Ombudsman Schemes: Drivers for Change*

assume dunque una connotazione del tutto specifica, poiché, collocata nel quadro più complesso della vigilanza bancaria, rappresenta il punto di congiuntura tra l'attività decisoria e la regolazione del mercato svolta dagli organismi di risoluzione[80]. In quest'ottica, l'analisi deve essere svolta con approccio critico che non si appiattisca sulla retorica del contraente debole, nella consapevolezza che gli interventi "a supporto" della parte debole, pur giustificati nella loro impostazione di base, devono tuttavia essere contenuti per evitare comportamenti opportunistici dei consumatori. Le letture enfaticamente pro-consumeriste rischiano, cioè, un paradossale effetto *boomerang*, finendo col danneggiare il soggetto che si intende proteggere.

Nel caso che interessa, considerato che «la prestazione di servizi di disposizione di ordine di pagamento non è subordinata all'esistenza di un rapporto contrattuale»[81], sembra che la regola maggiormente protettiva per l'utente e appagante in termini di effettività economica del sistema, venga integrata dall'azione diretta verso la parte contrattuale più vicina (alla quale viene normativamente attribuita una posizione sostanzialmente di garanzia)[82]: l'adozione di un tale congegno ipersemplificato consolida la fiducia del pagatore (uno degli obiettivi della PSD2, insieme alla sicurezza dei pagamenti e all'integrità del mercato dei sistemi pagamento) e agevola il conseguimento del risarcimento del danno risparmiandogli l'onere di dimostrare l'effettiva distribuzione della responsabilità tra i soggetti coinvolti[83].

and Strategic Responses, Queen Margaret University, Edinburgh 2013, p. 10; S.F. Ali, *Consumer Financial Dispute Resolution in a Comparative Context: Principles, Systems and Practice*, New York, Cambridge University Press 2013, p. 57; I. Benöhr, *Alternative Dispute Resolution for Consumers in the European Union*, in *Consumer ADR in Europe: Civil Justice Systems*, a cura di C. Hodges, I. Benöhr e N.Creutzfeldt-Banda, Hart Publishing Ltd, Oxford 2012, p. 1; I. Ramsay, *Consumer Redress and Access to Justice*, in *International Perspectives on Consumer's Access to Justice*, a cura di C.E. Rickett, T. G. W. Telfer, CUP, Cambridge 2003, p. 167 ss.

80 Esempio più significativo nel nostro ordinamento è la previsione degli artt. 13 e 23 Cod. com. el., il cui combinato disposto correla la soluzione delle controversie agli obiettivi generali del settore e, specificamente, quelli della regolazione.

81 Art. 66, par. 5, Dir. 2015/2366.

82 Così V. De Stasio, *Riparto di responsabilità e restituzioni nei pagamenti non autorizzati*, in questo Volume.

83 Per una critica a quest'impostazione v. A. Gourio, M. Gillouard, *La nouvelle directive sur les services de paiement (DSP 2),* in *Revue de Droit bancaire et financier*, 2016, comm. 91, i quali rilevano che quella introdotta è una la forma di responsabilità del terzo «*pour autrui sans existence d'un lien juridique quelconque entre les personnes concernées apparaît totalement exorbitant du droit commun des États membres et des principes du droit de la responsabilite, animé seulement par l'objectif d'une indemnisation facilitée du payeur*».

6. *La ripartizione degli oneri probatori*

Pacifica la configurabilità di un concorso colposo del pagatore[84], l'onere di provarne la negligenza (o la colpa grave o la frode) incombe, come ricordato, sull'intermediario.

Nell'apprestare la disciplina (e rinnovarla) il legislatore adotta un modello di tutela consolidato nella legislazione diseguale (non solo consumeristica, ma che di essa riproduca gli antagonismi di asimmetria), lavorando con particolare attenzione alla ripartizione degli oneri probatori (art. 10, comma 7, d.lgs. 11/2010)[85].

È pacifico che si sia in presenza di un'inversione dell'onere della prova, non derogabile dall'autonomia privata (la norma è imperativa)[86].

Il tema è un classico della contrattazione diseguale: è un dato acquisito nel dibattito giuridico, infatti, che la tutela del della parte debole del rapporto negoziale si svolga anche attraverso una speciale ripartizione degli oneri probatori, posto che il principio dispositivo (comune a tutti gli ordinamenti, e da noi racchiuso nell'art. 2697 c.c.)[87], è, nella sua formulazione pura, inadeguato alle liti disuguali, rischiando di danneggiare la parte debole.

Comune è, dunque, la tendenza dei sistemi europei a spostare l'assolvimento dell'onere della prova sul professionista, intanto per motivi politici (quale strumento di riequilibrio delle posizioni asimmetriche) e, poi, anche processuali (facilitare l'accertamento dei fatti assegnando l'onere della prova al soggetto che si trova nella posizione migliore per soddisfarlo)[88].

Vorrei però sottolineare che il tema della riferibilità o vicinanza della prova appare, contrariamente ad una convinzione ampiamente diffusa in dottrina, residuale rispetto alle scelte politiche e sistematiche.

Pacifica, dunque, la deroga realizzata per via normativa al principio dell'*actori incumbit probatio*, va verificato, prima, come l'inversione degli oneri probatori si raccordi con la possibilità di fornire la prova liberatoria, riconosciuta in capo all'ASPS, e, poi, quali siano i mezzi di prova idonei ad

[84] Cfr., da ultimo, Coll. Bari, Dec. n. 16875/2018.

[85] Sul problematico rapporto tra l'evoluzione tecnologica e il diritto delle prove: P. Leclercq, *Les titres dématérialisés de paiement et de crédit,* in *Le droit privé français à la fin du XXe siècle. Études offertes à Pierre Catala*, Litec, Paris 2001, p. 785; B. Geva, *Bank Collections and Payment Transaction—A Comparative legal Analysis*, OUP, Oxford 2001; spec. 580.

[86] 72° Considerando, Dir. 2366/2015.

[87] *International Encyclopedia of Comparative Law,* vol. *XI,* «Torts», diretta da A. Tunc, I, Tübingen, The Hague 1983, p. 149-150.

[88] Da Ultimo, N. Hoffshir, *La charge de la preuve en droit civil*, Dalloz, Paris 2014.

esonerare l'ASPS dalla propria responsabilità.

Considerato il problematico ottenimento delle evidenze necessarie per dimostrare la fondatezza della propria posizione, all'intermediario -che non ha accesso ad informazioni relative all'organizzazione dei propri clienti ed alle modalità di custodia dei dispositivi, ulteriori rispetto a quelle dichiarate dai clienti stessi in sede di denuncia e, eventualmente, di giudizio- viene riconosciuta l'ammissibilità del ricorso a prove di natura presuntiva[89]. Tali presunzioni -giudiziali, *ante-judiciaire*[90]- sono state tipizzate, con riferimento alle ipotesi maggiormente diffuse, dalla giurisprudenza, e, nel caso dell' *internet banking*, sono ravvisabili nella decettività del messaggio di abboccamento e nel livello di sofisticazione della frode informatica perpetrata; nel caso di utilizzi fraudolenti, sono individuabili nella dotazione del microchip; nel lasso temporale intercorrente tra il furto e il primo prelievo contestato; nell'alternanza tra operazioni legittime e illegittime; nella tempestività/tardività della richiesta di blocco e della verifica del conto corrente[91].

Nonostante l'apparente chiarezza normativa, il tema della ripartizione dell'onere della prova, crinale lungo il quale si misura l'effettività della tutela, ha dato luogo a decisioni controverse negli ordinamenti interni.

In Francia, ad esempio, la *Cour de cassation*, dopo una sentenza iniziale estremamente criticata, ha dovuto pronunciarsi a più riprese -e talora in modo contraddittorio[92]- elaborando criteri ermeneutici che non privilegiassero unidirezionalmente le interpretazioni in senso preferenziale per il consumatore.

La Corte, infatti, aveva inizialmente statuito -in materia di *internet banking*- che, pur in presenza di un sistema di sicurezza molto elevata (con sistema di autenticazione a due fattori[93]), la prova dell'utilizzo dei dati personali (nella specie: *user id*, *password*, credenziali personali e OTP dinamica inviata sull'utenza telefonica) non fosse sufficiente ad esonerare l'ASPS, affermando la necessità della prova dell'avvenuta divulgazione da parte dell'utente, la quale «*ne peut se déduire du seul fait que l'instrument*

[89] Coll. Napoli, Dec. n. 11189/2016.

[90] A. Danis-Fatôme, *Paiement à distance et preuve de la négligence grave de l'utilisateur d'un service de paiement : une nouvelle probatio diabolica?* in *Revue des contrats*, 2017, p. 274.

[91] Il ritardo nella denuncia è stato, invece, ritenuto irrilevante quando non concorrente a determinare l'entità del danno: cfr. Coll. Roma, Dec. n. 598/2014.

[92] D. Legeais, *Hameçonnage*, in *RTD com.*, 2018, p. 436.

[93] L'intermediario eccepiva la negligenza grave, ai sensi dell'articolo L. 133-19, IV, *Cod. mon. fin.*, sul presupposto che il carattere altamente sicuro del dispositivo implicasse che l'utente avesse «*sinon divulgué ses données personnelles à un tiers, à tout le moins laissé celles-ci à disposition du tiers ayant frauduleusement effectué les débits litigieux*».

de paiement ou les données personnelles qui lui sont liées ont été effectivement utilisés»[94].

L'impostazione difensiva dell'intermediario, che inferiva dall'utilizzo dei dati personali la divulgazione degli stessi a terzi e la conseguente negligenza nella custodia, obbligando l'utente a dare, a sua volta, prova contraria della presunzione, non è stata condivisa dalla Corte, la quale, muovendo dal dato normativo (la lettura congiunta degli artt. L. 133-18, IV, e L. 133-23, *Cod. mon. fin.*), ha dedotto la previsione di un'inversione dell'onere della prova, addossando al prestatore di servizi di pagamento l'onere di dimostrare la negligenza dell'utilizzatore.

Le ragioni del rifiuto della *Cour* di alleggerire il carico probatorio incombente sull'ASPS apparivano di natura politica e giurisprudenziale, inscrivendosi la sentenza essa nel solco delle decisioni precedenti marcatamente *consumer oriented*[95]. Quantunque, infatti, si rinvenissero precedenti di legittimità di segno opposto (che, non ravvisando alcuna inversione dell'onere della prova, applicavano le regole di diritto comune)[96], l'indirizzo maggioritario della giurisprudenza era caratterizzato da un marcato *favor* verso il pagatore (coinciso, sul piano temporale, con l'adozione della legge n° 2001-1062 del 15 novembre 2001 sulla *sécurité quotidienne*)[97], tale da configurare una «*présomption de comportement non*

[94] *Cour cass.*, 18 genn. 2017, in *Dalloz, 2017,* con nota di X. Delpech; in *Sem. Jur., éd. G.*, 2017, p. 117, con nota di K. Rogriguez, *Contestation des opérations de paiement sur Internet: le fardeau de la preuve pour le banquier*; in *Sem. Jur., éd. G.*, 2017, p. 241, con nota di J. Lasserre Capdeville, *Précisions sur la question de la preuve en cas de fraude au paiement sur internet*. Nel caso di specie, l'intermediario lamenta, al contrario, la "negligenza grave", ai sensi dell'articolo L. 133-19, IV, del *Cod. mon. Fin.*, e ricorre in Cassazione sul presupposto che il carattere altamente sicuro del dispositivo implicasse «*nécessairement que [son client] avait, sinon divulgué ses données personnelles à un tiers, à tout le moins laissé celles-ci à disposition du tiers ayant frauduleusement effectué les débits litigieux*».
Che, per la dottrina maggioritaria, è e rimane una questione sostanziale.

[95] Cfr. A. Hontebeyrie, *Perte ou vol d'une carte bancaire: quel régime probatoire? Réflexion sur la nature juridique du dispositif prévu à l'article L. 132-3 du Code monétaire et financier*, in *Dalloz* 2009, p. 1492.

[96] *Cour cass*. 31 maggio 2016, n° 14-29.906, in *Dalloz*, 2016, p. 2305, osservazioni di D. R. Martin e H. Synvet; in *Sem. Jur., éd. Gén.*, 2016, p. 1450.

[97] La prima applicazione della nuova disciplina è solo con la sentenza della *Cour cass.*, 2 ottobre 2007, in *Sem. Jur., éd. G*, 2008, II, p. 10014, con nota di É. Bazin; in *Dalloz*, 2007, p. 2765, con nota di L. Belaval; in *Dalloz*, 2008, p. 454, con nota di A. Boujeka; alla quale seguirono decisioni omogenee: *Cour cass.*, 21 settembre 2010, n° 09-16.534, in *Sem. Jur., éd. Entr. Aff.*, 2010, 2008, co nota di J. Stoufflet; in *Revue de Droit bancaire et fin.*, 2011, comm. 40, con nota di F.-J. Crédot, T. Samin; nonché *Cour cass.*, 28 marzo 2008, in *Sem. Jur., éd. Entr. Aff.*, 1735, con nota di P. Bouteiller; in *Dalloz*, p. 1136, con nota di V. Avena-Robardet; in *RTD com.*, 2008, p. 607, con nota di D. Legeais.

fautif» dell'utente[98], posto che, non solo l'utilizzazione dello strumento veniva considerata insufficiente a provare la colpa del pagatore, ma anche quella dei relativi dati riservati[99].

Tale impostazione ha però suscitato una serie di interrogativi.

Intanto, sul piano procedimentale, le decisioni non indicavano come si sarebbe dovuta provare la negligenza grave, e la prova liberatoria per l'ASPS appariva una prova impossibile[100], configurando una «*quasi-immunité*» dell'utente[101].

Sul piano sistematico, e di conseguenza, tale lettura finiva con lo svuotare di precettività la previsione del rilievo della colpa grave dell'utente; in terzo luogo, sul piano degli esiti politici, tale lettura implicava il rischio di una totale deresponsabilizzazione dell'utente (sui cui effetti v. *retro*, par. 5)[102].

La *Cour* appare quindi aver aderito, nella varietà delle possibili letture, al criterio ermeneutico dell'interpretazione più favorevole per il consumatore, il quale, invece, se non maneggiato con accortezza, rischia di creare un eccesso di frammentazione (eterogenesi dei fini rispetto all'attuale linea di *policy*), facendo incorrere le decisioni in una deriva eccessivamente garantista e producendo il paventato effetto *boomerang* di cui si è già discorso.

Nel tentativo di fornire ricostruzioni, per un verso, maggiormente aderenti alle indicazioni europee, e, per altro verso, di maggior equilibrio tra le istanze contrapposte dell'utilizzatore e dell'ASPS, la *Cour* è tornata a più

[98] D. Legeais, *Appréciation du manquement par négligence grave d'une victime d'un acte de phishing,* in *Sem. Jur., éd. Entr. Aff.*, 2017, p. 1687.

[99] L'impostazione si basava su di una lettura particolarmente rigorosa e filoconsumerista dai dati normativi: la formulazione dell'art. L. 133-19, comma 2, Cod. fin. mon., infatti, non esclude che l'utilizzazione dello strumento e dei relativi dati riservati possa essere sufficiente a provare la colpa del pagatore, ma semplicemente costituisce un invito a tener conto delle circostanze concrete e contingenti e non conferire rilevanza risolutiva all'utilizzo (K. Rodriguez, *Contestation des opérations de paiement sur Internet: le fardeau de la preuve pour le banquier*, in *Sem. Jur., éd. Entr. Aff.*, 2017, p. 1122).

[100] P. Storrer, *Utilisation frauduleuse d'un instrument de paiement: la probatio diabolica?,* in *Revue Banque*, 2017, p. 72; A. Danis-Fatôme, *Paiement à distance et preuve de la négligence grave de l'utilisateur d'un service de paiement: une nouvelle probatio diabolica?,* in *Revue des contrats*, 2017, p. 270.

[101] K. Rodriguez, *Hameçonnage et preuve de la négligence grave du client du banquier*, in *Sem. Jur., éd. Entr. Aff.*, 2018, p. 1272.

[102] S. Piédelièvre, *L'ordonnance du 15 juillet 2009 relative aux conditions régissant la fourniture de services et de paiement,* in *Gaz. Pal.*, 2009, p. 2820; più in generale J. Lasserre Capdeville, *La contestation des opérations de paiement non autorisées*, in *Revue de Droit bancaire et financier*, 2011, dossier 6; S. Torck, *L'exécution et la contestation des opérations de paiement*, cit., p. 1033; M. Roussille, *Contestation et opposition du paiement par carte bancaire*, in *Gaz. Pal.,* 2012, p. 7.

riprese sul punto, tentando di affinare i propri canoni ermeneutici.

Intanto, ha, dapprima, valorizzato l'analisi delle «*circonstances de l'espèce*»[103], introducendo il correttivo della riconoscibilità della natura fraudolenta del messaggio ricevuto dall'utente, e stabilendo che nel caso di non riconoscibilità della c.d. mail civetta, la comunicazione dei dati personali, quantunque intenzionale, è incolpevole[104]. Per converso, il cliente consapevole della natura fraudolenta del messaggio è responsabile, ma l'apprezzamento di tale consapevolezza non deve avvenire in concreto (costringendo l'intermediario anche in questo caso alla prova impossibile dello stato soggettivo dell'utente)[105], ma in astratto, alla stregua del parametro dell'uomo normalmente attento[106]. L'ASPS, dunque, deve dimostrare che l'utente, con un grado di attenzione nella norma, avrebbe dovuto nutrire dei dubbi sulla provenienza della missiva, dubbi che possono essere suscitati da indici quali: errori di ortografia; difformità degli indirizzi; difformità del logo riportato; imprecisioni sul numero di contratto menzionato, inesattezze sull'ammontare reclamato (introducendo la teoria del *faisceau d'indices*)[107].

Una riflessione sull'individuazione di ulteriori indizi dai quali dedurre la negligenza del prestatore dei servizi di pagamento, ha riguardato l'attitudine dell'indirizzo IP (*Internet Protocol*) a costituire prova della circostanza che l'ordine di pagamento sia stato impartito dal computer dell'utente[108] . Una

[103] In linea con quanto previsto anche dal 72° considerando, Dir. 2366/2015.

[104] Cass. com., 25 ottobre 2017, in *Sem. Jur., éd. Entr. Aff.*, 2017, p. 1685, con nota di D. Legeais; in *Revue de Droit bancaire et fin.*, 2017, p. 37, con nota di Th. Samin e S. Torck; in *Dalloz*, 2017, p. 2465, con nota di F. Mélin, *Utilisation frauduleuse des données personnalisées: être victime d'un hameçonnage n'exclut pas la négligence grave*, in *Dr. et proc.*, 2017, p. 262, note É. Bazin.

[105] Come dapprima statuito con la decisione della *Cour de cassation*, 25 ottobre 2017, sopra richiamata.

[106] È alla stregua di questo parametro che la *Cour* valuta gl'indizi contenuti nella mail civetta: Cass., 28 marzo 2018, in *Sem. Jur., éd. Entr. Aff.*, 2008, p. 1735, con nota di P. Bouteiller; e a p. 1496, con nota di M. Roussille; in *Revue de Droit bancaire et fin.*, 2008, con commento di A. Caprioli; in *Sem. Jur., éd. G*, 2008, II, p. 10109, con nota di É. Bazin; in *Dalloz*, 2008, p. 1136, con nota di V. Avena-Robardet; in *RTD com.*, 2008, p. 607, con nota di D. Legeais.

[107] Così come elencati nella decisione della *Cour de cassation* del 6 giugno 2018, che può essere letta in *Comm. Com.*, 2018, p. 43 con il commento di E. Caprioli, *Responsabilité du particulier en cas d'hameçonnage*, e in *Dalloz IP/IT*, 2018, p.643, con osservazioni di J. Lasserre Capdeville, *Confirmation de solutions jurisprudentielles en matière de phishing*; cfr., inoltre, *Cour cass.* 31 maggio 2016, in *Dalloz*, 2016, p. 2305, osservazioni di D. R. Martin e H. Synvet; *Sem. Jur., éd. Entr. Aff.*., 2016, p. 1450.

[108] Sul *tema* cfr. la decisione di Metz, 8 dicembre 2010, n° 08/01529, in *L'essentiel droit bancaire*, 2011, p. 6, con osservazioni di J. Lasserre Capdeville, *Précisions sur la notion d'utilisation frauduleuse d'une carte bancaire*.

critica a questa ricostruzione contesta, tuttavia, l'affidabilità degli indirizzi IP (ovvero «sequenze numeriche assegnate a computer collegati a Internet al fine di consentire la comunicazione tra i medesimi attraverso tale rete», così come definiti dalla Corte di giustizia [109]) facendo leva su considerazioni di carattere tecnico (ecco che ritorna il tema della precomprensione del fatto informatico), potendosi, infatti, ben verificare l'ipotesi che, con un furto di identità, il malfattore si appropri anche dell'indirizzo IP della vittima[110]. L'indirizzo IP, dunque, non ha l'idoneità a costituire piena prova della riferibilità dell'ordine di pagamento al computer dell'utente [111].

7. *Fatti generatori di responsabilità dell'intermediario e mezzi di prova*

Quanto sopra è sufficiente per far emergere la tendenza all'adozione di una prospettiva intesa a valorizzare le circostanze del caso concreto, incluso lo stato soggettivo del pagatore, il quale influisce sulla valutazione dell'organo giudicante[112]. Dal costante scandagliare, da parte della giurisprudenza, il contegno delle parti, può dedursi, sul piano dell'elaborazione generale, la configurazione di un obbligo di diligenza informatica in capo all'utente[113], intesa quale obbligo di consapevolezza «della delicatezza del mezzo telematico e della possibilità che attraverso quel mezzo siano perpetrate frodi, tanto più insidiose quanto meno facilmente riconoscibili»[114], e, simmetricamente, di

[109] CGUE, sentenza del 19 ottobre 2016, *Breyer*, C-582/14.
[110] «*Si des faussaires ont pu se procurer toutes les données qui leur permettent d'usurper l'identité des époux X., il est logique d'imaginer qu'ils ont également eu connaissance de l'adresse IP de l'ordinateur qu'ils utilisaient pour consulter leur compte bancaire*»: Tribunal de commerce de Cannes, 27 luglio 2017, *Dalloz IP/IT*, 2017, p. 661.
[111] J. Lasserre Capdeville, *Problèmes liés à l'adresse IP en matière bancaire*, in *Dalloz IP/IT*, 2017, p. 219.
[112] Il tema, nel caso il pagatore sia un consumatore, s'interseca con quello frammentazione della categoria dei consumatori in base al loro grado di avvedutezza (criterio che ha fatto il suo ingresso anche in àmbito normativo con la Direttiva 2005/29/CE, con l'introduzione della figura del consumatore medio cioè «normalmente informato e ragionevolmente attento ed avveduto»), ovvero *vulnerable, average, smart, responsible*: costruzioni debitrici agli studi americani di analisi economica del diritto, che ricollegandosi a parametri di carattere personale sul presupposto che lo stato di debolezza contrattuale -così come la simmetria e la sperequazione di poteri- possa dipendere anche da circostanze contingenti, prevedono differenti criteri di valutazione delle condotte; cfr. sul tema specifico K. Rodriguez, *ult. op. loc. cit.*
[113] A. Antonucci, *I contratti bancari online,* in *I contratti bancari*, a cura di E. Capobianco, Utet, Torino 2016, p. 422.
[114] Coll. Roma, Dec. n. 33/2010.

un obbligo di predisposizione di un'adeguata organizzazione tecnica idonea a garantire la sicurezza dello svolgimento di incarichi di pagamento in via informatica (la condotta dei prestatori deve essere scrutinata sotto il profilo della conformità ai canoni di correttezza e diligenza del *bonus argentarius* che ne devono informare l'operato). Tale organizzazione deve caratterizzarsi, in particolare, per l'adozione di strumenti in linea con l'evoluzione scientifica e tecnologica del settore[115].

Elemento cruciale (tanto in linea teorica, di ripartizione del rischio, quanto pratica, di frequenza della sua rilevanza) incidente sull'allocazione della responsabilità, è la presenza del servizio di Sms-Alert, presidio di sicurezza *ex post* (attivandosi una volta effettuato un prelievo) volto ad evitare il compimento di ulteriori -rispetto a quello notificato- prelievi. Il sistema prevede che venga notificata all'utente, tramite messaggi di testo sull'utenza cellulare o mail sulla casella di posta elettronica, ogni operazione realizzata, per consentirgli di procedere alla richiesta del blocco della carta nel caso riscontri la presenza di un utilizzo fraudolento. La giurisprudenza, ritenendo tale misura di sicurezza un servizio ormai normalmente esigibile, configura la sua mancata predisposizione come un'ipotesi di responsabilità da inadeguata organizzazione, imputabile all'intermediario (dovendosi escludere che il relativo costo possa essere sopportato dal cliente), il quale dovrebbe adottarla in modo generalizzato in virtù dell'obbligo di diligenza professionale[116]. Ovviamente è da escludere che la mancata predisposizione del presidio sia fatto generatore di responsabilità nell'ipotesi di assenza del nesso causale tra l'occorrenza del danno e l'assenza della messaggistica di Alert. Se l'intermediario, infatti, offre la prova che, alla luce dello svolgimento dei fatti, l'adozione di tale sistema di avvertimento non avrebbe consentito di limitare il pregiudizio sofferto (ad esempio, che la presenza dell'Sms-Alert non avrebbe, verosimilmente, impedito la realizzazione dei prelievi successivi al primo, stante l'arco temporale estremamente ridotto in cui si sono svolte le operazioni contestate[117]), la sua responsabilità sarà esclusa.

Pacifico che la messa a disposizione di strumenti accessori al rafforzamento della sicurezza non valga a tramutare in colpa grave la circostanza che il cliente non se ne sia avvalso[118], è, invece, controverso se l'adozione del sistema di notifica debba avvenire automaticamente o se l'obbligo di diligenza del prestatore sia soddisfatto tramite la mera sollecitazione

[115] Coll. Napoli, dec.n. 985/2011.
[116] Coll. Roma, cfr. Dec. nn. 5543/13 e 2319/2014.
[117] Coll. Roma, Dec. n. 11457/2016; Coll. Napoli, Dec. n. 1372/2016.
[118] Coll. coord., Dec. n. 3498/2012.

all'adozione dello stesso[119]. Sul piano contrattuale, l'alternativa si pone tra un modello di adesione c.d. *opt-out* (basato sul principio dell'autoesclusione: il servizio è attivato per tutti i clienti, ad eccezione di chi comunica di volersene sottrarre) ovvero *opt-in* (l'adesione al servizio avviene solo su base volontaria, previo consenso del cliente).

Se si accoglie l'idea, maggiormente diffusa, che l'imputazione della responsabilità all'ASPSP avvenga su base colposa, la stessa si dovrà escludere nell'ipotesi in cui il cliente, debitamente informato della disponibilità di siffatto strumentario di sicurezza, ometta di avvalersene. Si è, dunque, ritenuto che il meccanismo contrattuale che subordina la ricezione dell'Sms-Alert alla preventiva manifestazione del consenso del cliente (laddove l'offerta, se pure non personalizzata, sia rispettosa dei requisiti di trasparenza e adeguata evidenza) sia sufficiente ad integrare il livello di diligenza protettivo richiesto al fine di prevenire possibili eventi pregiudizievoli[120]. Il prestatore di servizi di pagamento potrà, dunque, essere esente da responsabilità se, producendo il contratto, dimostrerà che esso conteneva un'offerta sufficientemente stimolante all'uso del servizio (non una semplice e indistinta menzione nell'àmbito del contratto) e una descrizione sufficientemente chiara dello stesso, considerato che l'utilità dei presidi di avvertimento viene ormai considerata nota anche al pur non avveduto utente di strumenti di pagamento.

L'inerzia dell'intermediario nell'attivazione d'idonei strumenti di sicurezza può riguardare non solo la mancata predisposizione del servizio di Sms-Alert, ma anche di un sistema di monitoraggio della carta (ai fini del possibile blocco) in relazione ad operazioni anomale per frequenza e tipologia: attesa la pericolosità della clonazione/utilizzo fraudolento delle carte di pagamento, la strategia di contrasto è stata identificata nella velocità d'individuazione delle transazioni suscettibili di configurare un rischio di frode oggettivo, imminente e rilevabile, attraverso l'analisi delle informazioni riguardanti le transazioni "sospette"[121]. A fronte di un rischio

[119] Cass. 24 settembre 2009, n. 20543.

[120] Nello specifico, affinché alla clausola di offerta del servizio di allerta possa essere riconosciuta portata esimente, è necessario che questa presenti una formulazione idonea a consentire una scelta consapevole del consumatore sia in relazione al canone della trasparenza sia in relazione alla sua rappresentazione grafica, dovendo essere indicata con caratteri di adeguata evidenza (così i parametri enunciati dal Collegio di coordinamento, nella citata Dec. n. 3498/2012).

[121] L'art. 8, comma 1, lett. 2, D.M. 30 aprile 2007, n. 112, Regolamento di attuazione della L. 17 agosto 2005, n. 166, recante «Istituzione di un sistema di prevenzione delle frodi sulle carte di pagamento» individua specifici indici di anomalia: "Si configura il rischio di frode di cui all'articolo 3, comma 1 della legge, quando viene raggiunto uno dei seguenti parametri:

di frode così normativamente tipizzato (nonchè in considerazione delle norme in materia di ripartizione del rischio dettate dal D. Lgs. 11/ 2010 e di quelle in materia di concorso colposo del creditore nella causazione dell'evento -art. 1227-, e dell'art 1176 c.c.) si ritiene che l'intermediario diligente sia tenuto ad attivarsi e predisporre il blocco automatico della carta a séguito di operazioni anomale per frequenza e tipologia[122]. All'ASPSP non si richiede il monitoraggio di ogni singola operazione, ma la predisposizione di sistemi automatici di blocco di operazioni caratterizzate da un rapido succedersi, e non in linea con la normale operatività del titolare del conto[123].

Con riguardo all'*internet banking*, posto che il fenomeno maggiormente diffuso è quello del *phishing*[124], l'intermediario deve provvedere a fornire evidenza tanto del grado di accortezza (non) tenuto dall'utente quanto della presenza dei necessari sistemi di sicurezza prescritti.

Il principio che orienta la valutazione della condotta dell'utente è quello per cui la divulgazione dei dati identificativi riservati che abilitano all'utilizzo del proprio conto vale a configurare una condotta gravemente colposa[125], ritenendosi il fenomeno del *phishing* ormai noto al pur non esperto navigatore di Internet[126]. In sostanza, si ritiene che la consapevolezza del rischio di attacchi informatici e della circostanza che gli istituti di credito non richiedano informazioni personali via mail, siano divenuti ormai parte del bagaglio culturale di ogni consociato, assurgendo dunque

(…) lettera a): 1) cinque o più richieste di autorizzazione con carte diverse, rifiutate nelle 24 ore, presso un medesimo punto vendita; 2) tre o più richieste di autorizzazione sulla stessa carta, effettuate nelle 24 ore, presso un medesimo punto vendita (…); lettera b): 1) sette o più richieste di autorizzazione nelle 24 ore per una stessa carta di pagamento; 2) una ovvero più richieste di autorizzazione che nelle 24 ore esauriscano l'importo totale del plafond della carta di pagamento; 3) due o più richieste di autorizzazione provenienti da Stati diversi, effettuate, con la stessa carta, nell'arco di sessanta minuti"; per le decisioni cfr., tra le molte, quelle del Coll. Milano, Dec. n. 20897/2018; Coll. Coord., Dec. n. 3947/2016; Coll. Milano, Dec. n. 2817/2015.

[122] Coll. Coord., Dec. n. 27252/2018; Coll. Milano, Dec. n. 5255/2015.

[123] Coll. Napoli, Dec. n. 1220/2016.

[124] Il *phishing* consiste in "una truffa informatica realizzata inviando un'email con il logo contraffatto di un istituto di credito o una società di commercio elettronico, in cui si invita il destinatario a fornire i dati riservati quali numero di carta di credito, *password* di accesso al servizio di *home banking*, ecc., motivando tale richiesta con ragioni di ordine tecnico." (Cass. pen. 10060/2017).

[125] Coll. Coord., Dec. n. 3498/2012.

[126] 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.

al rango di fatto notorio[127]. Valutata in questa prospettiva la condotta delle parti coinvolte, si comprende la distinzione, elaborata dalla giurisprudenza, tra differenti tipi di truffe informatiche perpetrate -ai quali si accordano distinti metri di valutazione della condotta dell'utente[128]- quale il *phishing* tradizionale (considerato inescusabile, in quanto evitabile da qualunque utente dotato di normale avvedutezza e prudenza[129]) o quello c.d. di seconda generazione (quali, ad esempio, il *real time phishing*[130]), il quale, avvenendo la *captatio* attraverso meccanismi più sofisticati e subdoli, impercettibili anche al più scrupoloso utente, esclude automaticamente la ricorrenza di una colpa grave (e finanche di una colpa lieve) in capo all'utente che pure, inconsapevolmente, abbia cooperato alla realizzazione della frode[131].

Pacifica, in quanto non controversa, sarà la colpa grave dell'utente che ammetta di aver fornito riscontro all'email o all'sms civetta[132], mentre nel caso di negazione dell'abboccamento, la colpa grave (coincidente, sovente, con un grado di avvedutezza inferiore a quella dell'utente medio) andrà provata dall'intermediario, sia tramite la prova del grado di sofisticazione con cui la truffa sarebbe stata perpetrata, sia evidenziando la manifesta decettività del messaggio o l'anomalia ed inusualità della richiesta.

In Francia, invece, il discrimine per distinguere una *naiveté coupable* da una scusabile è individuato nella consapevolezza dell'utente circa la natura fraudolenta della missiva. Valutazione che, a sua volta, deve svolgersi alla luce del parametro della riconoscibilità del carattere fraudolento stesso: la non riconoscibilità (come, ad esempio, la ricezione di una mail recante la perfetta riproduzione del logo dell'intermediario)[133] esclude la negligenza, per cui l'abboccamento, quantunque intenzionale, viene considerato incolpevole. L'apprezzamento del grado di decettività presente nelle *e-mail* (o sms) civetta deve svolgersi *in abstracto*, avendo la *Cour* indicato una serie di elementi che consentono ad un utente "*normalement attentif*" di dubitare

[127] Per una definizione del fatto notorio in chiave contemporanea, cfr. D. Weinberger, *Too Big to Know. Rethinking Knowledge Now That the Facts Aren't the Facts, Experts Are Everywhere, and the Smartest Person in the Room is the Room*, Basic Books, New York 2011 (di cui è disponibile una traduzione italiana a cura di N. Mataldi: *La stanza intelligente. La conoscenza come proprietà della rete*, Codice edizioni, Torino 2012).
[128] Coll. Coord., Dec. n. 3498/2012.
[129] Coll. Coord., Dec. n. 1820/13.
[130] Coll. Milano, Dec. n. 9661/2017.
[131] Coll. Bologna, Dec. n. 14695/2018; Coll. Roma, Dec. n. 1507/2017.
[132] Coll. Bologna, Dec. n. 6323/2018; Coll. Napoli, Dec. n. 9322/2016; *Cour cass.*, 25 ottobre 2017, cit.
[133] *Cour cass.*, 28 marzo 2018, n° 16-20.018, cit.

della sua provenienza[134].

Una recente variante del fenomeno del *phishing* è quella in cui l'acquisizione fraudolenta dei dati rilevanti avviene mediante l'impiego di mezzi di comunicazione apparentemente istituzionali dell'ASPSP. La peculiarità della fattispecie consiste, dunque, nell'ammessa comunicazione, da parte dell'utente, delle *password* dinamiche, giustificata, tuttavia, dal legittimo affidamento che questi eccepisce di aver riposto sulla riconducibilità dell'interlocutore all'intermediario, escludendo di poter incorrere in colpa grave per aver confidato nell'autenticità dell'identità dell'operatore che appariva nella *chat box* con i propri dati anagrafici e il logo dell'intermediario con annessa "spunta blu"[135] (a garanzia dell'autenticità).

In questo caso, a prescindere dal grado di sofisticazione -pur elevato- dell'"ambiente informatico" creato dal frodatore, si è ritenuto che la comunicazione via *chat* delle *password* dinamiche configuri *ex se* una condotta gravemente negligente, essendo ormai noto che gli intermediari non richiedono tramite mail né *chat* dati riservati e *password* dinamiche[136].

Con riguardo alla condotta dell'intermediario, nelle prime decisioni in materia veniva attribuita una (limitata) rilevanza all'eventuale adozione di una politica aziendale volta a prevenire i rischi di frodi informatiche, ammonendo gli utenti a non fornire a terzi i propri dati di identificazione e di accesso ai servizi, ed in particolare rendendo disponibile, con accesso dal proprio sito web istituzionale, una sezione specificamente dedicata al *phishing* con informazioni utili per utilizzare il canale *online* in condizioni di sicurezza[137]. Tale condotta ha progressivamente perso rilevanza sul presupposto che del fenomeno del *phishing* abbia ormai conoscenza anche «il pur non esperto internauta»[138] e che, dunque, «*peu important qu'il soit, ou non, avisé des risques d'hameçonnage*»[139].

---

[134] *Cour cass*., 28 marzo 2018, in *Rev. banque*, 2018, p. 75, con nota di Ph. Storrer; in *Banque et droit*, 2017, p. 32, con nota di Helleringer e Bonneau, in *Contrats, conc., consom.*, 2018, comm. 83, con osservazioni di L. Leveneur.

[135] La frode prende avvio quanto il titolare utilizza la piattaforma *social* ufficiale dell'intermediario (generalmente *chat box* tramite messaggio pubblico visibile a tutti gli utenti) per una richiesta di supporto; dopo la segnalazione viene contattato (di norma sull'utenza telefonica) da un sedicente operatore il quale, a garanzia della propria autenticità, si presenta coi propri dati anagrafici e l'apposizione di una "spunta blu", ossia di un *badge* di verifica all'interno dell'immagine del profilo della piattaforma, richiedendo, ai fini del ripristino delle funzionalità di cui si lamentava il disservizio, i dati sensibili dello strumento di pagamento.

[136] Coll. Milano, Dec. n. 3312/2019; Coll. Bari, Dec. n. 27318/2018.

[137] Difesa ripetutamente sottolineata dalla banche convenute: *Cour cass*., 25 ottobre 2017, cit.

[138] Coll. coord., Dec. n. 3892/2013.

[139] *Cour cassation*, 25 ottobre 2017, cit.

8. *La colpa grave del pagatore*

Escluso che il corretto utilizzo delle credenziali personali possa assumere carattere dirimente nel ravvisare una colpa grave del cliente - stante la contraria previsione normativa dell'art. 10, comma 2, del d.lgs. n. 11/2010 e, in Francia, degli artt. L. 133-16 e L. 133-23 *Cod. mon. fin.*- il tema della colpa grave è quello su cui si sono maggiormente concentrati gli sforzi ricostruttivi della giurisprudenza e della dottrina, le quali hanno tentato una tipizzazione delle ipotesi di colpa grave del pagatore nell'adempimento degli obblighi di custodia, valutandola alla luce di una molteplicità di profili, attinenti sia alle modalità con le quali si è verificata la sottrazione dello strumento di pagamento, sia al comportamento del cliente successivo al furto e/o allo smarrimento.

Con riguardo alle carte di pagamento, la norma che ne detta la disciplina (art. 69, Dir. 2366/2015; art.7, d.lgs. 11/2010, artt. L. 133-16, *Cod. mon. fin.*) viene riformulata sin dalla rubrica (ora intitolata agli "*Obblighi a carico dell'utente dei servizi di pagamento in relazione agli strumenti di pagamento e alle credenziali di sicurezza personalizzate*"), introducendo, dunque, una duplicazione degli obblighi di custodia, tanto dello strumento di pagamento (comma 1)[140], quanto delle credenziali (comma 2) [141].

Anche in questo caso, si tratta di una riformulazione dallo scarso impatto in termini di innovatività, poiché segna il recepimento normativo di un principio (quello che la valutazione dell'adempimento degli obblighi di custodia debba riguardare tanto lo strumento di pagamento quanto le credenziali) pacificamente accolto dalla giurisprudenza.

Posta la reciproca connessione degli obblighi indicati in quanto configurano, unitariamente considerati, il corretto utilizzo degli strumenti di pagamento, le due disposizioni vanno lette congiuntamente, di tal che è sufficiente l'omesso rispetto di uno dei due obblighi legali per la configurazione della responsabilità dell'utente.

Variamente qualificata negli ordinamenti interni è la verifica della permanente disponibilità dello strumento, la cui omissione, in Italia, è stata ascritta alle ipotesi d'incuria nell'utilizzo complessivo dello strumento di pagamento -omissiva di «quel grado minimo di diligenza osservato da

[140] Ossia un «dispositivo personalizzato e/o insieme di procedure concordate tra l'utente e il prestatore di servizi di pagamento e di cui l'utente di servizi di pagamento si avvale per impartire un ordine di pagamento», così come dalla definizione dell'art. 4, par. 1, n. 14, Dir. 2366/2015.

[141] Definite dall'art. 4, par. 1, n. 31, Dir. 2366/2015, come «funzionalità personalizzate fornite a un utente di servizi di pagamento dal prestatore di servizi di pagamento a fini di autenticazione».

tutti»[142], mentre in Francia viene rapportata alle «*habitudes d'utilisation de la carte*»[143], di talchè è stata considerata diligente la condotta dell'utente che abbia tempestivamente proceduto al blocco della carta solo una volta rientrato dalla crociera[144].

Il caso di negligente custodia dello strumento di pagamento, la quale viene valutata in prima battuta con riguardo alla conformità ai termini contrattuali, è tipicamente quello in cui esso venga lasciato incustodito in luoghi pubblici o privati[145].

Nell'ipotesi delle credenziali, invece, il principio generale è che esse debbano essere protette tramite misure ragionevolmente idonee[146]: le

[142] «Il possesso di strumenti per i pagamenti elettronici, intrinsecamente pericolosi perché esposti a rischi di frode e di utilizzi non autorizzati, comporta che gli obblighi di diligente custodia degli stessi comprendano anche un monitoraggio dei conti destinati a recepire le operazioni effettuate a loro mezzo, onde appunto verificarne il corretto impiego. Ora, seppure non può pretendersi che tale monitoraggio venga effettuato in continuo, appare certamente anomala la condotta della ricorrente che per lungo tempo ha omesso ogni riscontro delle operazioni registrate nel conto»: Coll. Napoli, Dec.n. 6472/2014. *Contra* v. però la giurisprudenza di merito per la quale nessuna norma impone verifiche periodiche ravvicinate della disponibilità della carta di credito da parte del suo titolare: Tribunale di Firenze, 19 gennaio 2016 *De Iure*.

[143] Trib. Parigi, 12 dicembre 2002, n° 2002/05702 sentenza citata da J. Lasserre Capdeville, in *Dalloz*, 2013, p. 407, nt 11, cit. alla nt. seguente

[144] *Cour cass.*, 16 ottobre 2012, in *Sem. Jur., éd. Entr. Aff.*, 2012, p. 1680, con nota di S. Piedelièvre; e in *Dalloz*, 2013, p. 407, con nota di J. Lasserre Capdeville; in *Sem. Jur., éd. G*, 2012, p. 1202, con osservazioni di K. Rodriguez.

[145] Luoghi di lavoro, palestre, ospedali: Milano, Dec. n. 377/2014; Coll. Napoli, Dec. n. 6798/2014; Coll. coord., Dec. n. 6168/2013; o automobili posteggiate nella pubblica via (benchè lo strumento di pagamento sia stato nascosto nel vaso portaoggetti): *Cour ass.*, 16 ottobre 2012, cit. nella nota *supra*. Un discorso differente riguarda la custodia in luoghi privati, specialmente in àmbito domestico: il principio che regola la ripartizione delle responsabilità è che «ciascuno è responsabile della propria sfera domestica e non può pretendere di addossare a terzi estranei, nel caso che ci occupa l'intermediario resistente, le conseguenze dannose di comportamenti lesivi posti in essere da chi sia stato ammesso in tale sfera personalissima» (Coll. Milano, Dec. n. 969/2015); parimenti responsabile è colui che, pur vittima di raggiro, consenta a delle persone estranee di introdursi nella propria abitazione senza adottare una maggiore diligenza nella custodia e vigilanza dei propri beni e valori (Coll. Napoli, Dec. n. 2166/2016). In alcune ipotesi di furto presso la propria abitazione, si è, tuttavia, ritenuto che la natura di tale evento, eccezionale e non prevedibile, possa escludere, in assenza di evidenze, da parte dell'intermediario, di adeguata prova della colpa grave dell'utente nella custodia dello strumento di pagamento, la responsabilità dell'utente stesso (Coll. Roma, Dec. n. 590/2014).
Tali distinzioni non sono invece recepite in Francia, dove la circostanza che il furto si avvenuto presso l'abitazione dell'utente è stata considerata irrilevante: *Cour cass.*, 1° marzo 1994, in *RTD com.*, 1995, p. 458, con nota di R. Cabrillac.

[146] Art. 7, comma 2, D.lgs. 11/10.

circostanze relative alla (omessa) custodia delle credenziali vengono considerate avere rilevanza assorbente nella concreta concatenazione degli eventi[147], ferma restando la non configurabilità di un obbligo di memorizzazione, purchè le credenziali non siano immediatamente associabili alla carta[148], posto, al contrario, che l'ipotesi di conservazione congiunta dello strumento e del PIN, configura una totale trascuratezza verso i minimi accorgimenti utilizzati dai consociati al fine di evitare un accadimento dannoso[149]. Il tema viene sviluppato negli stessi termini anche in Francia, dove la conservazione congiunta viene considerata *faute lorde*[150].

La prova -presuntiva- della conservazione del PIN unitamente alla carta viene generalmente rinvenuta sulla base di un criterio temporale, ossia il breve lasso che intercorre tra il momento del furto il primo utilizzo fraudolento[151]. La circostanza che gli utilizzi fraudolenti avvengano con successo nell'àmbito di un ristretto arco temporale viene ritenuta incompatibile con l'eventualità della decrittazione del PIN tramite reiterati tentativi di digitazione, rivelando, al contrario, la necessaria conoscenza dello stesso da parte dei malfattori. In sede di giudizio, l'intermediario ricorre alla produzione dei Log (trascrizione di tracce informatiche) delle operazioni disconosciute che consentono, all'un tempo, di dimostrare la breve sequenza temporale (idonea a fondare la presunzione della sussistenza della colpa grave in capo all'utente) e la corretta e regolare autenticazione delle transazioni (idonea ad

[147] Coll. coord., Dec. n. 991/2014.

[148] La necessaria adozione di tecniche di annotazione opportunamente criptate era già stata evidenziata da X. Favre-Bulle, *Le droit communautaire du paiement électronique*, Schultess éditeur, Zurigo 1992, p. 31. È stato, dunque, considerato scusabile il comportamento di colui il quale conserva il codice nel luogo in cui è tenuta la carta, purché non sia immediatamente associabile alla carta stessa: Coll. Milano, Dec. n. 5540/2014; Coll. coord., Dec. n. 6170/2013.

[149] Per quanto la Direttiva non li recepisca, si rinvengono dei precedenti di soft-law in materia, che raccomandavano espressamente all'utente «di non trascrivere sullo strumento di pagamento l›eventuale numero personale di identificazione o il codice, e di non registrare tali dati su qualsiasi altro documento che egli abitualmente detiene o porta con lo strumento di pagamento, in particolare se tale documento può essere perso o rubato o riprodotto»: cfr. artt. 4.1, lett. c, Racc. 88/590/CEE (Raccomandazione della Commissione del 17 novembre 1988 concernente i sistemi di pagamento, in particolare il rapporto tra il proprietario della carta e l'emittente della carta); 5.1, lett. c, Racc. 97/489/CE (Raccomandazione della Commissione del 30 luglio 1997 relativa alle operazioni mediante strumenti di pagamento elettronici, con particolare riferimento alle relazioni tra gli emittenti ed i titolari di tali strumenti).

[150] V. già *Cour cass.*,10 gennaio, 1995, in *Sem. Jur., éd. Gén.*, 1995, p. 591, la quale avvallava la violazione, da parte del titolare della carta, dell'«*obligation de prudence, et plus particulièrement celle de préserver la confidentialité du numéro de code*»; cfr. anche *Cour cass*., 16 ottobre 2012, cit. *retro*, e *Cour cass.*, 17 maggio 2017, in *Contrats conc. consom.,* 2017, comm. 77, con osservazioni di E. A. Caprioli.

[151] Coll. Torino, Dec. n. 16444/2018; Coll. Palermo, Dec. n. 14353/2017.

assolvere l'onere probatorio relativo alla funzionalità del sistema)[152].

Altri indici di grave negligenza vengono ravvisati nella (in)tempestività del blocco richiesto dell'utente una volta presa coscienza del furto o dello smarrimento (ovvero la verifica, in base alla documentazione versata in atti, che un blocco tempestivo avrebbe consentito di prevenire in toto i prelievi non autorizzati)[153], nonché nella circostanza che la carta sia dotata di microchip (il che rende l'ipotesi di una clonazione così complessa sul piano tecnico e statistico, da considerarla, se non di impossibile evenienza, almeno altamente improbabile): essa, tuttavia, non è sufficiente, da sola, a configurare una responsabilità in capo all'intermediario, se questi offre evidenza della sussistenza, *a latere* dell'adozione della tecnologia a microchip, di ulteriori indici idonei ad escludere l'eventualità dell'utilizzo fraudolento[154].

In considerazione di ulteriori elementi circostanziati sulla dinamica della vicenda, anche l'alternanza tra operazioni fraudolente e operazioni genuine (ossia l'utilizzo dello strumento da parte del legittimo titolare durante il periodo dei prelievi successivamente disconosciuti) viene considerata indice di colpa grave[155], così come la prossimità degli sportelli ATM presso i quali sono stati effettuati i prelievi disconosciuti rispetto a quelli abitualmente utilizzati dall'utente (anche in questo caso la circostanza potrà essere suffragata dai tabulati dei singoli ATM[156]), l'utilizzo di più carte da parte dei terzi non autorizzati[157]; infine, l'affidamento dello strumento ad un

[152] Cfr. Collegio Milano, Dec. n. 605/2015; Coll. Coordinamento, Dec. n. 5304/2013. Per converso, la circostanza che le operazioni disconosciute siano state effettuate in un arco temporale non ravvicinato -ed in giorni fra loro non consecutivi-, è stato considerato indice idoneo ad escludere l'ipotesi di una sottrazione fraudolenta, in quanto incompatibile con l'*id quod plerumque accidit,* in cui l'utilizzo fraudolento delle carte sarebbe caratterizzato da prelievi in rapida successione fino ad esaurimento della disponibilità, nell'intento di trarre il massimo vantaggio dalle operazioni prima che il soggetto derubato si accorga dell'abuso e provveda al blocco della carta (Coll. Roma, Dec. nn. 308 e 4163 del 2015 e 4884/2014).

[153] Coll. Roma, Dec. nn. 2498/2014 e 33/2015; Coll. Coord., Dec. n. 5304/2013.

[154] Coll. Roma, Dec. nn. 1415 e 308 del 2015; Coll. coord., Dec. n. 3947/2014.

[155] Giacché «porta inevitabilmente a concludere che per tutte le operazioni deve necessariamente essere stata utilizzata la medesima carta, ossia quella originale» (Coll. Roma, Dec. n. 4163/2015).

[156] 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).

[157] La contestuale sottrazione di altri strumenti di pagamento, cui è seguito – nello stesso ristretto lasso di tempo – il loro fraudolento utilizzo rende ancor più evidente l'impossibilità

familiare del titolare non costituisce *ex se* colpa grave se temporaneo (cioè circoscritto all'effettuazione di un specifica operazione)[158]. Prova della genuinità dell'operazione viene, invece, considerato il carattere abituale -per ammontare e frequenza- delle operazioni contestate (ad esempio, l'acquisto ogni anno il 31 dicembre del medesimo bene presso il medesimo sito)[159].

In ogni caso, come già rilevato, non esistono indici di presunzioni assolute di negligenza dell'utente, ai fini della configurazione della quale deve svolgersi una valutazione complessiva tutte le circostanze del caso concreto[160].

Nel caso in cui le operazioni disconosciute siano state effettuate in un esteso arco temporale, si ravvisa giudizialmente una presunzione di omesso monitoraggio del proprio conto, indice di grave negligenza. L'ABF, infatti, ritiene che dovrebbe essere ormai noto a tutti gli utilizzatori di strumenti elettronici di pagamento il rischio di incorrere in utilizzi fraudolenti da parte di terzi e ciò dovrebbe indurre ad una vigilanza più frequente, idonea, quanto meno, ad evitare che detti utilizzi risultino ripetuti nel tempo[161].

Con riguardo, infine, al presidio tecnico del 3D Secure, al quale avevo accennato in apertura, il percorso della giurisprudenza francese (la quale l'ha utilizzato quale grimaldello per consentire agli intermediari di fornire la prova della colpa grave dell'utilizzatore, altrimenti considerata impossibile), che ne ha enfatizzato la funzione di elevare la sicurezza di un sistema di autenticazione[162], al quale si contrappone quello della giurisprudenza italiana che, allo stato attuale, lo considera un mero protocollo di trasmissione dei dati (inidoneo a qualificare il sistema di sicurezza di una banca), trovano la loro sintesi nell'intervento chiarificatore dell'EBA che, specificandone la natura di strumento di supporto all'autenticazione forte[163], introduce

per i malviventi di effettuare in tempi così brevi un rilevante numero di tentativi finalizzati all'ottenimento dei PIN di diverse carte (Coll. Roma, Dec. n. 8345/2016).

158 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; per contro, è fonte di responsabilità illimitata dell'utente l'affidamento che abbia i caratteri della stabilità: Coll. Roma, Dec. n. 8383/2014; in materia cfr. G. Liberati Buccianti, *L'affidamento a un familiare della carta di pagamento e l'obbligo di diligente custodia*, in *Nuova giur. civ. comm.*, 2013, I, p. 849 ss.

159 *Cour cass.*, 4 luglio 2018, n° 17-10.158.

160 Così, espressamente, il 72° considerando, Dir. 2366/2015.

161 Coll. Roma, Dec. n. 4444/2016.

162 Cfr. le citate decisioni della *Cour* del 18 gennaio 25 ottobre 2017 e del 28 marzo 2018.

163 Escluso che, allo stato attuale, costituisca un elemento di inerenza (posto che nessuno dei dati scambiati include informazioni relative ad elementi biometrici), ciò non preclude che lo possa divenire in futuro, laddove in grado di trasmettere elementi di inerenza

un'importante distinguo tra la versione 2.0 -e successive- e le versioni precedenti -1.0-, specificando che solo la prima soddisfa i requisiti richiesti dall'autenticazione forte[164].

Conclusivamente, possono rilevarsi alcune traiettorie ricostruttive nella valutazione della condotta dell'utente: intanto la tendenza -comune con la Corte di giustizia e le riflessioni europee in materia di politiche di *decisionmaking* nelle controversie[165]- ad adottare una prospettiva intesa a giustificare e valorizzare soluzioni "contestualizzate", ossia incentrate sulla rilevanza di «*autres éléments extrinsèques*»[166].

Tali elementi sono stati tipizzati dalla giurisprudenza, che, individuando gl'indici sui quali svolgere le proprie valutazioni, ha dunque specificato che il proprio sindacato sul comportamento dell'utente vada effettuato *in abstracto*[167], secondo il modello del "*reasonably circumspected consumer*"[168], criterio che ha fatto il suo ingresso anche in àmbito normativo con la Direttiva 2005/29/CE con l'introduzione della figura del consumatore medio cioè «normalmente informato e ragionevolmente attento ed avveduto»[169]. Il richiamo, tuttavia, alle circostanze contingenti, pone indirettamente l'interrogativo se l'oggetto di valutazione possa essere anche il profilo soggettivo del danneggiato (o asseritamente tale) ed in particolare se e quale rilevanza debba essere riconosciuta alle sue caratteristiche intrinseche. In altri termini, se il sindacato sulla colpa grave del pagatore implichi una distinzione tra vittima accorta e non accorta e, dunque, quale sia la frontiera tra la "colpevole credulità" ("*naivieté exusable*") e la colpa grave ("*negligence coupable*"): la risposta è dirimente, giacché se si accede alla risposta positiva, la circostanza che l'utente sia una persona vulnerabile per ragioni, ad esempio, anagrafiche (caratterizzazione che nel diritto delle nuove tecnologie è tra le più ricorrenti) condurrà a ritenere la sua credulità giustificabile e, dunque, ad escluderne la colpa grave. Viceversa, se si ritengono irrilevanti le caratteristiche soggettive dell'utente nella valutazione della credulità si dovrà escludere rilevanza ad una serie di elementi relativi

(*Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2 -EBA-Op-2019-06*, 21 giugno 2019, punto 21).

[164] *Opinion of the European Banking Authority*, cit. nt. *supra*, punto 23.

[165] Sin dalla sentenza *Océano*, CGCE, 27 giugno 2000, cause riunite C-240/98 a C-244/98.

[166] *Cour cass.*, 21 settembre 2010, cit.

[167] D. Legeais, *Hameçonnage*, cit.

[168] Figura la cui prima menzione in giurisprudenza risale alla sentenza della Corte di Giustizia del 16 luglio 1998, *Gut Springenheide GmbH*, § 31 e 37, C-210/96.

[169] 18° considerando, Direttiva del Parlamento europeo e del Consiglio, dell'11 maggio 2005, relativa alle pratiche commerciali sleali tra imprese e consumatori nel mercato interno.

alla sua qualità di *vulnerable, average, smart,* o *responsible* [170].

Abstract
Nelle controversie in materia di pagamenti non autorizzati, uno degli àmbiti più rilevanti è quello probatorio. È noto, infatti, che la ripartizione dell'onere della prova sia cruciale sull'esito della decisione.
La PSD2, in cui l'imputazione della responsabilità avviene a titolo colpa (ad eccezione di alcune isolate ipotesi in cui l'imputazione avviene a titolo di responsabilità oggettiva per il prestatore di servizi di pagamento), vengono accolte le principali linee di tendenza comuni ai vari ordinamenti interni: lo spostamento dell'assolvimento dell'onere della prova sul professionista -per facilitare l'accertamento dei fatti assegnando l'onere della prova al soggetto che si trova nella posizione migliore per soddisfarlo-; e, al contempo, il rifiuto di una deroga permanente al principio dell'*actori incumbit probatio*.

Parole Chiave: Onere della prova; pagamenti non autorizzati; frode informatica.

Abstract
An issue that concerns the "case-law" on digital payements is that of the burden of proof.
Since the allocation of the burden of proof is key to the outcome of the decision, this represents, as the watershed along which the effective- ness of the protection is measured.
The PSD2 recepies the main tendencies of the domestic legal systems: to shift the burden of proof onto the business, seen as the party that is in the best position tobearit; but, at the same time, a permanent derogation from the principle of the *actori incumbit probatio*, is rejected.

Keywords: Burden of proof; unauthorized payment; phishing.

[170] N. Cayrol, *La Cour de cassation et les faits de société*, in *RTD civ.*, 2018, p. 485.

Maddalena Rabitti

Il riparto di competenze tra autorità amministrative indipendenti nella Direttiva sui sistemi di pagamento

Sommario: 1.Il problema – 2. Il riparto di competenze tra *Authorities* e la giurisprudenza – 3. Banca d'Italia e AGCM: *Credit Surcharge* e pratiche commerciali scorrette. Una buona risposta normativa – 4. Un nuovo problema. Il rapporto tra PSD2 e GDPR – 5. Gli strumenti di tutela: il consenso – 6. (*Segue*). L'*accountability* – 7. Conclusioni: verso una competenza concorrente tra *Authorities.*

1. *Il problema*

La normativa sui servizi di pagamento[1] è un esempio paradigmatico di una disciplina di settore che finisce per essere crocevia di interessi diversi che, in concreto, pongono rilevanti problemi di bilanciamento. L'analisi di impatto del d.lgs. 218/17 mostra la difficoltà che la *compliance* a questa disciplina comporta, tanto più che si aggiungono i provvedimenti di Banca d'Italia che sono necessari per rendere effettiva l'attuazione della PSD2 e anche i *Regulatory Tecnical Standards* EBA entreranno in vigore nel settembre 2019.

Obiettivo dichiarato della PSD2 è quello di garantire una maggiore efficienza, concorrenza e trasparenza nell'offerta di servizi di pagamento rafforzando, al contempo, la fiducia dei consumatori in un mercato dei pagamenti armonizzato[2]. Tra gli ulteriori obiettivi strumentali (anche

[1] Introdotta con la Direttiva PSD2, attuata con d.lgs. 18/2017, che ha modificato il d.lgs. 11/10.

[2] 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 *Nuove Leggi Civ. Comm.*, 2018, p. 839 ss.; S. Balsamo Tagnani, *Il mercato europeo dei servizi di pagamento si rinnova con la PSD2,* in *Contratto e impresa Europa,* 2018, p. 609 ss. Nelle more della pubblicazione di questo articolo, molti altri contributi hanno visto la luce. Per una sintesi dei problemi principali si rinvia a Banca d'Italia, *Le nuove frontiere dei servizi bancari e di pagamento tra PSD2, criptovalute e rivoluzione digitale*, a cura di F. Maimeri e M. Mancini, in *Quad. Giur. 87/2019*. Si rinvia anche a M. Rabitti - A. Sciarrone Alibrandi, *I servizi di*

impliciti) perseguiti, primario è quello di creare un *Common Level Play Field* per i fornitori di servizi di pagamento e adeguate tutele per gli utenti. Su tutto, poi, si pone l'interesse del sistema finanziario europeo a consentire, in chiave pro-concorrenziale, l'ingresso a nuove categorie di prestatori di servizi di pagamento (cosiddetti *Third parties providers:* TPP) che si aggiungono a quelli già autorizzati a operare nel settore dei servizi di pagamento tramite internet.

Sul punto, la PSD2 (e il d.lgs. 218/2017 che la attua) innova fortemente la disciplina sui servizi di pagamento, prevedendo due nuove categorie di operatori non finanziari: coloro che effettuano "servizio di disposizione di ordini di pagamento" (PISP: *Payment Initiation Service Providers*)[3] e coloro che svolgono un "servizio di informazione sui conti" (AISP: *Account Information Service Provider*)[4].

Il legislatore risponde così alle crescenti richieste della clientela di potersi avvalere di forme di pagamento nuove e più evolute, che sono richieste soprattutto dalle imprese che operano attraverso piattaforme digitali di servizi e prodotti (*e-commerce*). Le APIs[5] e il principio di *net neutrality* sono gli strumenti prescelti per favorire l'operatività dell'*Open Banking*.

Si realizza così un complessivo regime di favore per chi voglia avvalersi degli strumenti di pagamento, che si sostanzia: in maggiori opportunità di scelta nei servizi di pagamento; in una semplificazione dell'onere della prova a favore del cliente per l'ipotesi di utilizzo fraudolento degli strumenti di pagamento; in limitazioni a spese e commissioni e nel divieto di *credit surcharge,* solo per elencare alcune tra le misure introdotte.

Tuttavia, l'interprete deve valutare l'impatto della nuova disciplina

pagamento su PSD2 e GDPR: Open banking e conseguenze per la clientela, in *Liber Amicorum Guido Alpa*, a cura di F. Capriglione, Cedam, Padova 2019, p. 711 ss.

[3] Esso ha per oggetto un servizio che dispone l'ordine di pagamento su richiesta dell'utente di servizi di pagamento relativamente a un conto di pagamento detenuto presso un altro prestatore di servizi di pagamento.

[4] Si occupa di fornire un servizio *online* avente ad oggetto informazioni relativamente a uno o più conti di pagamento detenuti dall'utente di servizi di pagamento presso un altro prestatore o presso più prestatori di servizi di pagamento. Si veda art. 2, comma 1, lett. b-*bis)* e lett. b- *ter*) del d.lgs. 218/2017.

[5] *Application Programming Interfaces,* sono costituiti da un insieme di protocolli che definiscono in che modo posso interagire le componenti dei *software*. A livello europeo, il Piano d'Azione della Commissione ha previsto lo sviluppo, da parte di imprese e fornitori di nuove tecnologie, di interfacce di programmazione delle applicazioni (API) standardizzate e conformi a PSD2 e GDPR, alle quali gli altri operatori saranno tenuti ad adattarsi. L'obbiettivo è quello di giungere a una standardizzazione delle modalità di esecuzione dei pagamenti digitali e di rendere più sicure le transazioni, ottenendo così una maggior tutela dei consumatori.

anche da punti di vista diversi: se è vero, ad esempio, che occorre agevolare e semplificare i pagamenti anche *online*, non si può trascurare il rischio che un eccesso di liberismo metta a repentaglio la sicurezza dei dati personali degli utenti, con quel che ne consegue sotto il profilo sia della profilazione della clientela, sia della stabilità del sistema bancario, che potrebbe prossimamente subire un attacco concorrenziale dai giganti del *web* in grado di offrire i più disparati servizi "su misura" del cliente[6].

Questo rischio, tutt'altro che remoto, suscita una serie di perplessità sulla possibilità concreta di attuare la PSD2 senza prima risolvere alcune questioni cruciali per la tutela dei clienti, ma anche per la sopravvivenza del sistema bancario così come è oggi.

Il punto che si intende approfondire in questa sede è quello del riparto di competenze tra Autorità amministrative indipendenti sui due dei profili ora menzionati: il divieto di *credit surcharge* e l'accesso ai dati da parti delle *Third Parties Provider*. La scelta di questo duplice angolo prospettico si giustifica con l'idea di svolgere alcune riflessioni di sistema sul rapporto tra la PSD2, che è disciplina settoriale e verticale e le discipline generali e orizzontali che incrocia, quali il Codice del Consumo e il recente Regolamento GDPR. Come si è recentemente affermato, "agli incroci con i silos verticali non ci sono semafori ma rotonde; si tratta di condividere regole minime di competenze o principi, sufficienti per superare i contrasti tra la tutela dei dati e promozione della concorrenza nel settore bancario (PSD2)"[7].

2. *Il riparto di competenze tra* Authorities *e la giurisprudenza*

Il riparto di competenze tra *Authorities* è un problema ormai classico che, anziché trovare una soluzione nel tempo, ha assunto progressiva complessità e stenta a trovare una risposta di sistema. Le ragioni che possono addursi per spiegare questa difficoltà sono molte.

In primo luogo, è frequente che si assista ad un fenomeno di *overlapping* tra norme che talvolta disciplinano un medesimo fatto in modo diverso.

[6] F. Bassan, *Potere dell'algoritmo e resistenza dei mercati*, Rubbettino, 2019, p. 40 ss. mette in guardia sul rischio che in ambito bancario, assicurativo e finanziario la capacità di gestire dati acquisterà nel prossimo futuro rilievo decisivo, perché sono comparti in cui i bassi investimenti tecnologici, la scarsa condivisione di informazioni e l'assenza di standard tecnologici condivisi e avanzati evidenziano la resilienza minima del sistema attuale in caso di concorrenza aggressiva ad opera di *newcomers* esperti in gestione dati.

[7] Ancora, F. Bassan, *op. cit.,* p. 42.

Capita, cioè, che una disciplina settoriale si intersechi (sovrapponga) con altre discipline – che a volte tutelano lo stesso interesse (ponendosi perciò il problema solo in termini di intensità della tutela) a volte, invece, tutelano interessi diversi – con la conseguenza di dovere stabilire come gestire l'*overlapping* e quali siano le Autorità competenti[8].

L'esempio ad oggi più eclatante, come si dirà, è quello delle pratiche commerciali scorrette, ma non solo. L'ultimo dibattito investe persino la possibilità di immaginare, in prospettiva e allo stato in modo provocatorio, la possibilità di unificare le due autorità dell'AGCOM e della Privacy, perché i principali problemi in tema *privacy* sono legati all'uso dei dati personali su *devices* mobili, app e *web*, ragion per cui la competenza anche dell'AGCOM diventa innegabile e decisiva[9]. Ipotesi alternative, meno radicali, presuppongono comunque una collaborazione più strutturata tra AGCOM e Garante Privacy.

Una seconda ragione che spiega la complessità della questione si può individuare nella matrice europea della maggior parte delle normative che introducono nuove regole del mercato. Accade, cioè, che le norme europee – specialmente i regolamenti e le Direttive *self executing* – entrino direttamente a fare parte dell'ordinamento nazionale comportando un necessario adeguamento del sistema di regole già tendenzialmente completo dello Stato membro che le accoglie. Così, ad esempio, nel tempo si è progressivamente ampliato l'ambito di operatività dell'Autorità garante della concorrenza e del mercato (AGCM), che ha assunto su di sé competenze che

[8] Si pensi alla materia del *market abuse* e, più in generale, al tema del *ne bis in idem*, su cui si sono succeduti interventi della CEDU, della Corte di Giustizia e della Corte Costituzionale e di Cassazione. Per un approfondimento dell'evoluzione giurisprudenziale, si veda Assonime, Ne bis in idem *e potestà sanzionatoria di Banca d'Italia e Consob nella giurisprudenza dell'ultimo quinquennio*, il Caso 1/2019. Sul *coté* sostanziale e sui piani mobili di tutela, cfr. A. Zoppini, *Sul rapporto di specialità tra norme appartenenti ai "codici di settore". Lo* ius variandi *nei codici del consumo e delle comunicazioni elettroniche*, in *Riv. dir. civ.*, 2016, p. 136.

[9] È questa l'opinione di A. Nicita, espressa durante una conferenza dell'Università di Napoli il 23 gennaio 2019 il quale ha dichiarato che: "Sarebbe auspicabile una fusione di Agcom e Garante per la privacy, le cui competenze, sancite a livello europeo, resterebbero intatte e costituirebbero un importante tassello nel percorso per la costruzione di un mercato regolato dell'uso del dato, che va affidata al legislatore. Man mano che il dato diventa il prodotto al centro dei modelli di business della comunicazione digitale, il campo regolatorio dell'Autorità per le garanzie nelle comunicazioni e quello del Garante per la protezione dei dati personali appaiono sempre più sovrapponibili". "Il proliferare di competenze diverse ad *authority* distinte non è certo d'aiuto" ha continuato: "non solo perché possono sempre manifestarsi obiettivi diversi tra le varie autorità indipendenti, ma soprattutto perché questi obiettivi potrebbero essere segmentati o addirittura confliggenti".

originariamente non le erano attribuite in quanto non strettamente legate alla materia della concorrenza.

In altri termini, l'ingresso di una nuova normativa di tutela del mercato può rendere necessario individuare l'autorità amministrativa indipendente competente a vigilare su quel mercato di riferimento, con la necessità per il legislatore di ripensare le attribuzioni delle *Authorities* già esistenti e di rimettere in discussione il criterio funzionale che il legislatore ha seguito al momento dell'istituzione di ciascuna.

Queste ragioni, pur non esaustive, sono sufficienti a rivelare un quadro incerto e mutevole sotto il profilo regolatorio. A fronte dell'inadeguatezza del legislatore, la risposta di sistema ha provato a darla la giurisprudenza che, sempre più, tende a occupare gli spazi lasciati vuoti dalla legge concorrendo alla progressiva "giurisdizionalizzazione" del diritto, con cui si amplia la sfera di discrezionalità del giudice chiamato a partecipare direttamente alla creazione della regola del caso concreto[10]. Anche in questo caso vale, perciò, la pena richiamare la giurisprudenza che si è pronunciata sul tema.

La vicenda è nota e riguarda la competenza sulle pratiche commerciali scorrette in materia di comunicazioni elettroniche: si trattava di stabilire se all'accertamento e sanzione della pratica commerciale scorretta fosse tenuta l'AGCM o l'AGCOM. Rileva, sul piano delle fonti applicabili, l'art. 4, comma 3, della Direttiva 2005/29 CE in materia di pratiche commerciali scorrette secondo cui: "In caso di contrasto, le disposizioni contenute in direttive o in altre disposizioni comunitarie e nelle relative norme nazionali di recepimento che disciplinano aspetti specifici delle pratiche commerciali scorrette prevalgono sulle disposizioni del presente titolo e si applicano a tali aspetti specifici". Questa disposizione è stata sostanzialmente trascritta dall'art. 19, comma 3, del Codice del Consumo. Con Adunanza plenaria del 2012 il Consiglio di Stato ha affermato che il complesso di regole *ex* art. 19,

[10] Si delinea così una nuova fisionomia del ruolo del giudice, specie se di grado superiore, che è interprete del diritto, ma che è anche tenuto a integrare le regole con funzione nomofilattica, con l'obiettivo di dare uniformità e certezza. È questa, ormai, un'esigenza fortemente avvertita che trova la propria origine nel rapporto tra crisi della regolazione e esigenza dell'esecuzione del diritto. Per un approfondimento, si rinvia a quanto già scritto in M. Rabitti, *Il ruolo della Corte di giustizia nel diritto dell'economia*, in *Giudicare l'economia, AGE*, 2/2018, p. 347 ss. e in *La Corte di Giustizia tra scelte di mercato e interessi protetti,* in *I Giudici e l'economia*, a cura di L. Ammannati, P. Corrias, F. Sartori, A. Sciarrone Alibrandi, Torino 2018, p. 459 ss.; M.R. Damaška, *I volti della giustizia e del potere. Analisi comparatistica del processo,* trad. it., Bologna 1991, p. 30 ss., e p. 270 ss.; A.A.S. Zuckermann, *Court Control and Party Compliance. The Quest for Effective Litigation Management*, in *The Reforms of Civil Procedure in Comparative Perspective*, a cura di N. Trocker e V. Varano, Torino 2005, p. 143 ss.; *Il giudice e la legge*, numero monografico di *Questione giustizia*, 2016.

comma 3, "si iscrive nell'ambito del principio di specialità" tra fattispecie normative, ponendo così una limitazione generale all'operatività della disciplina delle pratiche commerciali scorrette e, dunque, alla competenza dell'AGCM, in presenza di una disciplina settoriale esaustiva[11].

Tuttavia, con le sentenze del 9 febbraio 2016, il Consiglio di Stato, in Adunanza plenaria[12], adito sul punto del riparto di competenze, ha mutato indirizzo, concludendo nel senso di riconoscere all'AGCM la competenza a irrogare le sanzioni per "pratica commerciale considerata in ogni caso aggressiva", anche se in materia settoriale di competenza di altra Autorità. Si è, cioè, ritenuto che là dove una condotta, pur comportando la violazione di obblighi informativi dettati da una disciplina settoriale, integri una pratica connotata da profili di aggressività, si applicano le disposizioni del Codice del Consumo e, dunque, è legittimata all'azione l'AGCM, con i poteri di cui all'art. 27 del Codice del Consumo. Il ragionamento condotto dal Consiglio di Stato muove da un'idea diversa del criterio di specialità in relazione all'art. 3, paragrafo 4, della Direttiva 2005/29/CE, che viene definito "per progressione di condotte lesive": ciò significa non fare valere davvero di per sé la specialità per fattispecie normative, quanto piuttosto fare prevalere l'illecito di maggiore gravità, con conseguente applicazione della sanzione più afflittiva. Non è stato questo, tuttavia, l'epilogo della vicenda giurisprudenziale. Lo stesso Consiglio di Stato (Sezione VI) ha ritenuto di non potersi adeguare al principio di specialità per progressione di condotte lesive se non dopo avere sollevato una serie di quesiti di interpretazione pregiudiziale alla Corte di Giustizia sulla compatibilità tra la Direttiva 2005/29/CE e le norme di attuazione del Codice del Consumo[13].

[11] Il Tar Lazio, nelle sentenze nn. 1742/2013 e 1754/2013, in linea con il Consiglio di Stato, ha ribadito l'inapplicabilità della disciplina (generale per materia) sulle pratiche commerciali in presenza di una disciplina specifica (settoriale) idonea a ricomprendere la condotta contestata all'operatore e la cui repressione è affidata a uno specifico soggetto pubblico dotato di poteri ispettivi e sanzionatori. La convivenza tra Autorità indipendenti trasversali, istituite a tutela di specifici interessi pubblici di portata generali, e Autorità di settore, preposte in via esclusiva ad uno specifico settore economico, ha sempre dato luogo a interferenze tra le rispettive attribuzioni. Sul punto si veda S. Cassese, *L'Autorità garante della concorrenza e del mercato nel "sistema" delle autorità indipendenti*, in *Giorn. dir. amm.*, 2011, p. 1.

[12] Chiamato a pronunciarsi di nuovo anche a seguito della procedura di infrazione del 2013 ad opera della Commissione Europea.

[13] Per approfondimenti sulla questione e sull'excursus giurisprudenziale vedi M. Bertani, *Pratiche commerciali scorrette e violazione della regolazione settoriale tra concorso apparente di norme e concorso formale di illeciti*, in *Nuove Leggi Civ. Comm.*, 2018, p. 926 ss.; V. Mosca, *Il riparto di competenze sulla tutela del consumatore all'esame della Corte di Giustizia*, in *Giorn. dir. amm.*, 2017, p. 519 ss.; M.S. Bonomi, *Tutela del consumatore, pratiche commerciali scorrette e riparto di competenze tra autorità indipendenti*, in *Giorn. dir. amm.*, 2016,

Due i profili che qui rilevano: (i) se il principio di specialità debba essere inteso come principio regolatore nei rapporti tra ordinamenti o tra norme o tra *Authorities*; (ii) se la nozione di contrasto presupponga una vera e propria "antinomia" tra le disposizioni o se sia sufficiente che norme settoriali diverse dettino discipline difformi in relazione alla specificità del settore[14].

La Corte di Giustizia si è pronunciata con la sentenza del 13 settembre 2018 chiarendo che, qualora ci sia normativa europea in potenziale conflitto con normativa di matrice non europea, prevale la prima e che la Direttiva sulle pratiche commerciali scorrette si applica solo se non esistono specifiche norme del diritto dell'Unione che disciplinino altrimenti aspetti specifici delle condotte che integrano la pratica scorretta[15]. Da ciò la Corte trae alcune importanti conseguenze: un problema di riparto di competenze tra *Authorities* può porsi solo laddove sussista un "contrasto" tra le disposizioni applicabili, che si ravvisa però solo quando: "il rapporto tra due disposizioni va oltre la mera difformità o la semplice differenza, mostrando una divergenza che non può essere superata mediante una formula inclusiva che permetta la coesistenza di entrambe le realtà, senza che sia necessario snaturarle".

p. 793 ss.

[14] Il Consiglio di Stato all'atto della definizione del merito deferiva alla Corte di Giustizia due gruppi di quesiti. Il primo gruppo riguardava, in estrema sintesi, gli artt. 8 e 9 della Direttiva 2005/29/Ce e l'allegato 1 di detta Direttiva (concernenti le singole ipotesi di pratiche commerciali scorrette); il secondo gruppo aveva, invece, ad oggetto la *ratio* della Direttiva generale 2005/29/Ce, nonché il principio di specialità di cui all'art. 3, comma, 4 della stessa (i rapporti tra discipline). Più in particolare, con le questioni prima e seconda, il giudice del rinvio chiedeva se la nozione di "pratica commerciale aggressiva", di cui agli artt. 8 e 9 della Direttiva 2005/29, o la nozione di "fornitura non richiesta", ai sensi dell'allegato I, punto 29, di tale Direttiva, debba essere interpretata nel senso che ricomprende condotte consistenti nella commercializzazione, da parte di un operatore di telecomunicazioni, di carte SIM sulle quali sono preimpostati e preattivati determinati servizi, quali la navigazione Internet e la segreteria telefonica, senza che il consumatore sia stato previamente ed adeguatamente informato né di tale preimpostazione e preattivazione né dei costi di tali servizi. Le questioni dalla terza alla sesta – quelle che rilevano ai fini del nostro tema – vertevano sostanzialmente sui rapporti tra discipline e sulla possibilità di valutare, ai sensi del richiamato art. 3, paragrafo 4, della Direttiva 2005/29, una condotta integrante una fornitura non richiesta alla luce delle disposizioni della disciplina generale sulle pratiche commerciali sleali, con conseguente incompetenza dell'Autorità di regolazione nazionale ad intervenire in applicazione della Direttiva quadro e della Direttiva servizio universale in materia di servizi di comunicazione elettronica.

[15] Corte di Giustizia, 13 settembre 2018, n. 54: "L'articolo 3, paragrafo 4, della direttiva 2005/29 dispone che, in caso di conflitto tra le disposizioni di tale direttiva e altre norme dell'Unione che disciplinano aspetti specifici delle pratiche commerciali sleali, queste altre norme prevalgono e si applicano a tali aspetti specifici. Tale direttiva trova quindi applicazione, come confermato dal suo considerando 10, soltanto qualora non esistano specifiche norme del diritto dell'Unione che disciplinino aspetti specifici delle pratiche commerciali sleali".

Al di là della soluzione del caso di specie[16], questa sentenza della Corte di Giustizia merita attenzione perché indirizza l'interprete verso una nuova configurazione dei rapporti tra autorità nei seguenti termini: la valutazione relativa alla sussistenza del contrasto riguarda solo il caso in cui uno stesso fatto è regolato da disposizioni diverse, entrambe europee, e si traduce in un conflitto reale. Se, invece, le norme riguardano il medesimo fatto, ma non si traducono in una divergenza insuperabile, magari perché sono preposte alla tutela di interessi diversi, non c'è un problema di conflitto e, dunque, possono in teoria essere applicabili entrambe le discipline e, per l'effetto, si riconosce la possibilità che più di un'Autorità amministrativa indipendente possa essere coinvolta.

Si afferma un principio tendenziale di competenze complementari di più Autorità amministrative indipendenti in chiave funzionale agli interessi protetti, salvo l'ipotesi di conflitto reale, cioè di "contrasto".

3. *Banca d'Italia e AGCM:* Credit Surcharge *e pratiche commerciali scorrette. Una buona risposta normativa*

La PSD2 attuata dal d.lgs. n. 218 del 2017 è, come si diceva, un perfetto banco di prova per testare le soluzioni da ultimo proposte dalla giurisprudenza della Corte di Giustizia in materia di "riparto di competenze tra decisori".

In linea di principio, va chiarito che l'Autorità amministrativa competente a vigilare sull'osservanza della PSD2 è la Banca d'Italia. Questa scelta può, tuttavia, essere messa in discussione almeno in due ipotesi in cui la PSD2 si sovrappone con altre discipline: il divieto di *credit surcharge* e *l'Open Banking*.

L'art. 2, comma 3, del d.lgs. 218/17 (che modifica l'art. 3, comma 4, del d.lgs. 11/10) pone il divieto di *credit surcharge* precludendo al beneficiario del pagamento di applicare commissioni o sovrapprezzi aggiuntivi ai pagatori che scelgano di avvalersi di strumenti di pagamento quali carte di debito e di credito. Questa disposizione deve, però, essere coordinata con

[16] In tal senso, nella sentenza si legge, da un lato, che la Direttiva quadro e la Direttiva servizio universale non prevedono una completa armonizzazione degli aspetti relativi alla protezione dei consumatori, dall'altro, che in base a quanto disposto dall'art. 1, paragrafo 4, della Direttiva servizio universale, l'applicabilità delle disposizioni della disciplina sulle pratiche commerciali sleali non è pregiudicata dalle disposizioni della normativa settoriale. Di qui la conclusione che non sussiste contrasto tra le disposizioni della Direttiva servizio universale e quelle della Direttiva 2005/29/CE in materia di diritto degli utenti finali.

un'analoga previsione del Codice del Consumo, che ascrive il fenomeno del *credit surcharge* tra le pratiche commerciali scorrette che possono essere oggetto di sanzione da parte dell'AGCM. Ai sensi dell'art. 21, comma 4, del Codice del Consumo si considera scorretta la pratica commerciale che richieda un sovrapprezzo di costi per il completamento di una transazione elettronica con un fornitore di beni e servizi. Inoltre, l'art. 62 del Codice del Consumo vieta ai professionisti di imporre ai consumatori spese per l'uso di questi strumenti di pagamento. Si tratta, dunque, di capire quale sia il rapporto di specialità tra queste disposizioni e quale l'Autorità chiamata a sanzionare per l'ipotesi di violazione della regola.

A soccorrere l'interprete, in questo caso, è lo stesso legislatore che, all'art. 3, comma 4-*bis*, individua l'AGCM quale autorità competente a verificare l'osservanza del divieto di *surcharge* e ad applicare le relative sanzioni, con la seguente formulazione: "L'Autorità garante della concorrenza e del mercato è designata quale autorità competente a verificare l'osservanza del divieto di cui al comma 4 e ad applicare le relative sanzioni, avvalendosi a tal fine degli strumenti, anche sanzionatori, previsti dal decreto legislativo 6 settembre 2005, n. 206". Dunque, per disposizione normativa, l'AGCM ha la competenza generale sul *credit surcharge*.

Sul piano delle conseguenze, si osserva, in primo luogo, che con ciò l'AGCM amplia la propria sfera di operatività al di là del rapporto professionista/consumatore, assumendo rilievo più l'attività e il servizio prestato che non la qualità soggettiva del contraente.

L'art. 3, comma 4-*ter*, dispone poi meccanismi di collaborazione tra AGCM e Banca d'Italia per agevolare l'esercizio delle rispettive funzioni. L'importanza della leale cooperazione tra *Authorities* è centrale per il buon funzionamento dell'attività di vigilanza; nel caso di specie, la Banca d'Italia e l'AGCM esercitano funzioni tra loro complementari, in ciò perseguendo interessi convergenti nello sviluppo e mantenimento di adeguati livelli di concorrenza nei mercati e tutela dei consumatori. Tale convergenza di interessi, pur nel rispetto dell'autonomia e dell'indipendenza delle rispettive funzioni, determina l'opportunità di instaurare rapporti di cooperazione per coordinare e rendere più efficace e incisiva l'esecuzione dei rispettivi mandati[17]. Sotto questo profilo, dunque, il decreto di attuazione della PSD2 traccia una strada importante per garantire l'*enforcement* della disciplina, che merita di essere apprezzata tanto più che, in generale, si registra una certa incoerenza tra la tendenza mostrata dalle Autorità europee e nazionali,

[17] In particolare, il principio di leale collaborazione rende necessario condividere informazioni e dati acquisiti nell'esercizio delle rispettive funzioni e competenze, in coerenza con il principio di buon andamento dell'azione amministrativa di cui all'art. 97 della Costituzione.

che cooperano fattivamente tra loro, e la resistenza opposta dalle autorità nazionali competenti per settori.

Il d.lgs. 15 dicembre 2017, n. 218, inserisce anche un nuovo art. 32-*quater* che, al comma 1, fatta salva l'applicazione dell'art. 62 del Codice del Consumo, prevede l'obbligo per le banche di informare gli utenti in merito ai costi dei prelievi di contante tramite sportelli automatici e, al successivo comma 2, demanda all'AGCM l'effettuazione dei controlli circa l'osservanza di tale obbligo da parte delle banche (cfr. art. 2, comma 38).

Viene data infine (art. 34-*quater*) all'AGCM la competenza ad inibire la continuazione e a rimuovere gli effetti delle pratiche commerciali scorrette e delle condotte in violazione della disciplina CRD (Direttiva 2011/83/UE) derivanti dall'inosservanza degli obblighi a carico dei beneficiari posti dal Regolamento (UE) n. 751/2015 - MIF (cfr. art. 3, comma 1), riconoscendole tutti i poteri che le sono attribuiti dall'art. 27 del Codice del Consumo. Si prevede, anche in questo caso, la collaborazione tra le due Autorità.

Da queste indicazioni normative viene fuori un sistema di vigilanza ben articolato in cui, in assenza di indicazioni in seno alla Direttiva, è il legislatore nazionale che ha provveduto a rimediare al silenzio del legislatore europeo. Si può affermare che la vigilanza sulla corretta applicazione delle disposizioni della PSD2 spetta alla Banca d'Italia con le eccezioni richiamate su cui è chiamata a intervenire l'AGCM.

Resta da stabilire se, escluso il contrasto tra norme e risolto il tema del *credit surcharge*, gli ambiti di sovrapposizione si esauriscano in quelli individuati dal legislatore oppure ne sussistano altri.

A ben vedere, la disciplina delle pratiche scorrette si può applicare ad ogni rapporto di consumo in cui il professionista abbia violato gli obblighi di diligenza professionale gravanti su di esso. In tali casi, il rispetto della disciplina settoriale diventa un parametro di riferimento ai fini della definizione del livello di diligenza che deve essere osservato dall'operatore in generale e dell'intermediario nella specie. In questa prospettiva, sembra potersi affermare che il ventaglio di possibili interventi dell'AGCM sia più ampio di quello individuato dal legislatore nel d.lgs. 218/2017, ma che, anche in tal caso, eventuali conflitti tra norme potrebbero essere risolti sulla base dei principi espressi dalla Corte di Giustizia, in una chiave di competenza concorrente funzionale.

In conclusione, con riguardo al rapporto tra Banca d'Italia e AGCM il d.lgs. 218/2017 attua un riparto di competenze tra decisori che mira a salvaguardare al meglio gli interessi dei clienti. Dove non arriva il legislatore,

è il quarto pilastro dell'Unione a soccorrere, cioè la Corte di Giustizia che interviene a supplenza del legislatore europeo, come ormai è consona fare, indicando la via da seguire[18].

4. *Un nuovo problema. Il rapporto tra PSD2 e GDPR*

Problema molto più grave, anche perché trascurato dal legislatore, è quello che investe il riparto di competenze tra Banca d'Italia e Garante Privacy.

A ben vedere, qui l'origine del problema è a monte: manca, infatti, un raccordo espresso tra la disciplina della PSD2 e quella del GDPR[19] e, almeno a prima lettura, vi è persino il rischio di ravvisare tra le due normative un'incompatibilità applicativa potenziale. Se, da un lato, il GDPR tutela il diritto alla protezione dei dati personali come un diritto fondamentale delle persone, ponendo come principio cardine l'autodeterminazione informativa, ossia il diritto del singolo a decidere in prima persona sulla cessione e l'uso dei dati che lo riguardano e tenta quindi di effettuare un bilanciamento tra circolazione e protezione del dato personale a garanzia della dignità delle persone, dall'altro lato, la PSD2 favorisce lo scambio e la condivisione di dati e informazioni tra diversi prestatori di servizi di pagamento rendendo facilmente accessibili dati personali dei clienti.

Uno dei più importanti cambiamenti attuati dalla PSD2 riguarda, infatti, come si è detto, il fatto che le banche devono consentire ai diversi *provider*s l'accesso ai dati dei clienti e ai conti, dando così luce al c.d. "*Open Banking*". La spinta tra innovazione e concorrenza in questa disciplina settoriale si traduce

[18] Si rinvia a quanto da me già rilevato in *La Corte di giustizia e il diritto dell'economia*, cit., p. 352 e cioè che: "Secondo l'insegnamento tradizionale, la Corte esercita il potere giurisdizionale svolgendo, al contempo, quando necessario: (i) un ruolo *normativo* (innova) quando interpreta il diritto applicando, ma anche *integrando*, gli atti legislativi ed esecutivi; (ii) un ruolo *evolutivo*, quando interpreta il diritto dell'UE lasciando, poi, ai giudici nazionali il compito di valutare la compatibilità del diritto interno con il diritto dell'UE; (iii) un ruolo di giudice di *appello* rispetto al tribunale di primo grado. Già da quanto si è fin qui detto, si evince che la Corte di Giustizia ha assunto un ruolo così forte da renderla alla stregua di un *legislatore aggiunto e forse davvero autonomo*. A queste funzioni se ne può aggiungere una ulteriore, che vede la Corte di Giustizia (iv) giudice dell'esecuzione, essendo l'unica che è in grado di dare effettivo contenuto alle disposizioni normative, nell'inerzia o inettitudine degli altri soggetti legittimati a farlo (legislatore, *Authorities)*".

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

soprattutto nell'apertura del mercato dei servizi di pagamento alle c.d. *Third Party Providers* (cosiddette TPP, che si distinguono in "prestatori di servizi di disposizione di ordini di pagamento" e "prestatori di servizi di informazione sui conti") i quali, rispettivamente, possono avere accesso al conto del cliente che è radicato presso il prestatore di servizi (banca) per disporre pagamenti ai terzi beneficiari verificando l'esistenza dei fondi necessari; oppure, per aggregare le informazioni presenti su vari conti *online* e restituire al cliente la visione complessiva della propria situazione finanziaria, senza che il cliente debba contattare i vari prestatori di servizi di pagamento[20].

Con l'ingresso delle terze parti, cioè, il flusso dei dati derivanti da tutte le operazioni di pagamento si sposta dagli operatori bancari tradizionali ai TPP, che si frappongono tra cliente e operatore bancario e acquisiscono, al posto di quest'ultimo, tutte le informazioni relative alla transazione in atto[21]. La novità di PSD2 è di avere combinato il tema delle informazioni legate al conto di pagamento con quello della tecnologia che, attraverso il meccanismo delle APIs[22], consente l'interfaccia fra il mondo della banca e di altri operatori (PISP e AISP)[23].

Sul punto, la PSD2 (e il d.lgs. 218 che la attua) prevede una disciplina articolata e complessa relativa alle regole che devono essere osservate dai prestatori di servizi di pagamento per eseguire le prestazioni richieste quando sono coinvolte le cosiddette Terze parti.

Senza alcuna pretesa di esaustività si richiamano di seguito le principali regole.

L'art. 5 *bis* – concernente le condizioni necessarie per il soddisfacimento della richiesta di disponibilità dei fondi del cliente effettuata dalla Terza Parte al prestatore del servizio di radicamento del conto – prevede che

[20] Si deve trattare di soggetti autorizzati da Banca d'Italia che abbiano stipulato una assicurazione contro i danni (art. 144 *septies,* d.lgs. 19 settembre 1993, n. 385, Testo Unico delle leggi in materia bancaria e creditizia).

[21] Questo tema è di particolare rilevo in Italia dal momento che è l'unico Paese in cui la pratica del multi-affidamento è così diffusa e costituisce un problema serio.

[22] *Application Programming Interfaces* sono un insieme di protocolli che definiscono in che modo posso interagire le componenti dei *software*. A livello europeo, il Piano d'Azione della Commissione ha previsto, entro la metà del 2019, lo sviluppo, da parte di imprese e fornitori di nuove tecnologie, di interfacce di programmazione delle applicazioni (API) standardizzate e conformi a PSD2 e GDPR, alle quali gli altri operatori saranno tenuti ad adattarsi. L'obbiettivo è quello di giungere a una standardizzazione delle modalità di esecuzione dei pagamenti digitali e di rendere più sicure le transazioni ottenendo così una maggior tutela dei consumatori

[23] O. Borgogno – G. Colangelo, *Data Sharing and Interoperability Trough APIs: Insights from European Regulatory Strategy*, European Union Law Working Paper, Stanford – Vienna Transatlantic Technology Law Forum, 2018.

debba trattarsi di conto *online* e che il cliente debba avere prestato il suo consenso al titolare del servizio di radicamento del conto a dare conferma della disponibilità dei fondi al *provider* relativamente a una determinata operazione; mentre il prestatore di servizi di pagamento può chiedere la conferma – che non può consistere nell'estratto del saldo del conto – quando il pagatore ha prestato il consenso esplicito e ha disposto l'operazione di pagamento utilizzando uno strumento di pagamento basato su carta emesso dal prestatore di servizi di pagamento.

L'art. 5 *ter* disciplina, invece, il comportamento che deve essere adottato dal PISP in caso di servizi di disposizione di ordine di pagamento, regolando puntualmente anche l'uso che questi può fare dei dati di cui viene a conoscenza. Si prevede al riguardo che, se il conto di pagamento è accessibile *online*, il PISP non può detenere in alcun momento i fondi del pagatore e deve provvedere affinché le credenziali di sicurezza personalizzate del pagatore medesimo non siano accessibili ad altri fuorché al pagatore e affinché qualunque altra informazione sul pagatore ottenuta nella prestazione del servizio in discorso sia fornita esclusivamente al beneficiario e solo con il consenso esplicito del pagatore medesimo. Inoltre, il PISP, con riferimento specifico al trattamento dei dati di cui viene a conoscenza nel corso dell'operazione: (i) non chiede al pagatore dati diversi da quelli necessari per prestare il servizio di disposizione di ordine di pagamento; (ii) non usa e non conserva dati e non vi accede per fini diversi dalla prestazione del servizio di disposizione di ordine di pagamento; (iii) non conserva dati sensibili relativi ai pagamenti del pagatore. Ancora, per quanto riguarda gli obblighi in capo al prestatore di servizio di radicamento del conto in caso di disposizione di ordine di pagamento, la norma prevede che egli sia tenuto a comunicare con la terza parte in maniera sicura e a fornirle tutte le informazioni disponibili sull'ordine di pagamento.

All'art. 5 *quater* del d.lgs. 218/17 vengono introdotte, poi, alcune regole per l'accesso alle informazioni sui conti di pagamento e all'utilizzo delle stesse nell'ipotesi di servizi di informazioni sui conti (AISP). In questo caso, l'AISP presta il proprio servizio unicamente sulla base del consenso esplicito dell'utente e provvede affinché le credenziali di sicurezza personalizzate dell'utente non siano accessibili ad altri fuorché all'utente stesso. Quanto al trattamento dei dati, l'AISP: (i) accede soltanto alle informazioni sui conti di pagamento designati e sulle operazioni di pagamento effettuate a valere su tali conti, non richiedendo dati sensibili relativi ai pagamenti; (ii) non usa, non conserva dati, non vi accede per fini diversi dalla prestazione del servizio di informazione sui conti, conformemente alle norme sulla protezione dei dati.

L'art. 6 *bis* detta, infine, alcuni limiti all'accesso ai conti di pagamento da parte di PISP e AISP: in particolare, si prevede che il prestatore di radicamento del conto possa rifiutare l'accesso ai TPP solo per giustificate e comprovate ragioni connesse all'accesso fraudolento o non autorizzato al conto di pagamento da parte di tali soggetti. E, in questi casi, il medesimo è tenuto a informare l'utente del rifiuto e dei relativi motivi, nonché a darne immediata comunicazione a Banca d'Italia. Inoltre, il prestatore di radicamento del conto deve rifiutare senza indugio l'accesso se riceve dall'utente la revoca del consenso alla prestazione di tali servizi.

La presenza di tali norme impone all'interprete di svolgere alcune riflessioni di sistema sul rapporto tra PSD2, disciplina settoriale e verticale, e GDPR, disciplina generale e orizzontale. In mancanza di un raccordo espresso fra le due normative sussiste infatti, almeno a prima lettura, il rischio di ravvisare tra esse un'incompatibilità applicativa potenziale. In questa prospettiva, va innanzitutto rammentato che il GDPR tutela il diritto alla protezione dei dati personali come diritto fondamentale – il cui principio cardine è l'autodeterminazione informativa, ossia il diritto del singolo a decidere in prima persona sulla cessione e l'uso dei dati che lo riguardano – e ragiona nell'ottica del bilanciamento tra circolazione e protezione del dato personale a garanzia della dignità degli individui (basandosi sulla nota triade *consent/ownership/portability*)[24]. La PSD2 mira, invece, a favorire lo scambio e la condivisione di dati e informazioni tra diversi prestatori di servizi di pagamento rendendo facilmente accessibili dati personali dei clienti (e in questa prospettiva la parola chiave è *information* su cui si innestano i concetti di *collection/digitisation/repackaging/datafication*).

Una peculiarità non priva di conseguenze, sia teoriche sia pratiche, della disciplina introdotta dalla PSD2 è costituita, come si è detto, dal fatto che non è necessario che sussistano relazioni contrattuali tra i TPP e i prestatori di servizio di radicamento del conto. L'obiettivo di rafforzare la concorrenza nel settore dei servizi di pagamento si traduce cioè nell'imporre alle banche (e agli IP) una "collaborazione forzata" con i TPP, anche in assenza di precedenti relazioni contrattuali[25], obbligandole unicamente a

[24] È chiara in questo senso l'indicazione dell'art. 6, comma 1, lett. *f*), GDPR: il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione di dati personali. Il rispetto del limite posto da questa norma è dato dalla possibilità, in concreto, per l'interessato di essere sempre adeguatamente informato sul modo in cui i dati sono trattati, riconoscendo tra l'altro il diritto di controllare l'accesso ai propri dati.

[25] Se il conto è accessibile *online*, il pagatore ha sempre il diritto di avvalersi del servizio. I

predisporre un'infrastruttura tecnologica idonea a rendere possibile l'accesso alle informazioni e a gestire tutti i possibili rischi che ne conseguono.

La possibile mancanza di antecedenti relazioni contrattuali fra i soggetti coinvolti comporta conseguenze anche sotto il profilo del riparto interno della responsabilità in caso di operazioni di pagamento non autorizzate, ben potendo accadere che i rapporti tra i due prestatori siano regolati unicamente dalla legge.

Questa disciplina per i TPP si affianca all'unica regola che, nel d.lgs. 218/17, si occupa – peraltro con risultati piuttosto deludenti – di coordinare il trattamento dei dati personali da parte dei prestatori dei servizi di pagamento con la disciplina generale sulla *privacy*.

L'art. 29, comma 1, del d.lgs. 11/10 (così come modificato dall'art. 2, comma 34, del d.lgs. 218/17) prevede infatti che "i prestatori di servizi di pagamento" possano trattare dati personali ove ciò sia necessario a prevenire, individuare e indagare casi di frode nei pagamenti. La fornitura di informazioni a persone fisiche in merito al trattamento dei dati personali e ad altro trattamento avviene in conformità al decreto legislativo n. 196 (Codice privacy). In ogni caso, i prestatori di servizi di pagamento, in base a quanto dispone l'art. 29, comma 1 *bis*, "hanno accesso, trattano e conservano i dati personali necessari alla prestazione dei rispettivi servizi di pagamento, solo previo consenso esplicito dell'utente". Si tratta, dunque, di una regola a più ampio spettro che vale per tutti i prestatori di servizi di pagamento e non limitatamente ai conti *online*. Il rapporto tra questa norma e quelle sopra richiamate sembra porsi cioè in una logica di genere a specie.

L'ultimo comma dell'art. 29, in particolare, contiene almeno due regole essenziali che valgono in tutti i casi: la prima è la necessità del consenso contrattuale che il prestatore di servizi di pagamento (sia esso prestatore di servizio di radicamento del conto oppure TPP) e il cliente devono avere manifestato reciprocamente; l'altra è il rispetto, anche a questo riguardo, del "principio di minimizzazione dei dati", in base al quale i prestatori di servizi di pagamento possono utilizzare, accedere, o conservare i dati acquisiti esclusivamente per la prestazione dei servizi tipici da essi offerti. Quest'ultimo principio, enunciato all'art. 5, lett. *c*), del GDPR, è peraltro uno di quelli maggiormente connotanti la disciplina generale del trattamento dei dati personali, tanto più che, come è stato rilevato in dottrina, non vi è dubbio che "meno dati si utilizzano meno rischi si fanno correre all'interessato"[26].

Se questo è, a grandi linee, il regime previsto a tutela del corretto

PISP hanno sempre l'obbligo di "identificarsi" presso gli ASPSP.

[26] F. Pizzetti, *La protezione dei dati personali e la sfida dell'intelligenza artificiale,* in *Intelligenza artificiale, protezione dei dati personali e regolazione*, Giappichelli, Torino 2018, p. 62.

trattamento dei dati personali dalla PSD2, il confronto di tale normativa con il GDPR legittima alcuni interrogativi che hanno grande rilievo pratico. In particolare, occorre chiedersi: (i) quale sia, ai sensi del GDPR, la "base legittima" prevista per legge che consenta ai TPP il trattamento dei dati personali; (ii) quale sia la regola da adottare in presenza di dati "sensibili" cui possa accedere il TPP; (iii) come vadano ripartite le responsabilità tra prestatore di servizi di radicamento del conto e terze parti in caso di utilizzo illecito dei dati, dal momento che la PSD2, come si è detto, prevede che il servizio possa essere prestato all'utente indipendentemente dall'esistenza di un rapporto contrattuale con l'ASPS; (iv) quale criterio consenta di stabilire chi sia, tra prestatore del servizio di radicamento del conto e terze parti, il titolare del trattamento e chi il responsabile dello stesso[27]; (v) quale sia la regola da seguire e il meccanismo di protezione delle cosiddette parti silenti, ossia dei beneficiari dei pagamenti i cui dati "circolano" anch'essi nello svolgimento dell'attività; (vi) chi sia l'Autorità competente a vigilare sul rispetto delle regole imposte da PSD2 e GDPR, quando si effettua il servizio di pagamento in regime di *Open Banking*[28].

5. *Gli strumenti di tutela: il consenso*

Pur non potendosi in questa sede fornire una risposta esaustiva a tutte le questioni appena prospettate – con riguardo alle quali la soluzione non può che provenire dalla cooperazione fra le istituzioni europee maggiormente coinvolte –, si cercherà, nel prosieguo, di dare qualche indicazione utile a partire dalle prime indicazioni che provengono dall'Europa in proposito.

Con lettera del 5 luglio 2018 indirizzata al Parlamento Europeo, lo

[27] La figura del responsabile del trattamento è disciplinata compiutamente nell'art. 28 GDPR, che ne precisa i doveri chiarendo che è un soggetto terzo al quale il titolare ricorre per lo svolgimento di trattamenti che devono comunque essere fatti valere per suo conto e in suo nome. Il rapporto tra i due deve essere regolato da un contratto e il titolare è tenuto ad accertarsi che il responsabile offra garanzie adeguate ad assicurare che i trattamenti siano conformi al Regolamento.

[28] La questione non ha rilievo solo teorico: basti pensare che ai sensi dell'art. 83 GDPR, in caso di violazioni del Regolamento, il Garante per la protezione dei dati personali potrà irrogare una sanzione amministrativa pecuniaria fino a 20 milioni di euro o, per le imprese, fino al 4% del fatturato mondiale annuo dell'esercizio precedente, se superiore; tenendo in debito conto la natura, la gravità, la durata della violazione, il carattere doloso o colposo della stessa, le categorie di dati personali interessate dalla violazione, ecc.

European Data Protection Board (EPDB)[29] – che ha sostituito il WP29 – ha fornito alcune prime indicazioni volte al coordinamento delle due discipline. Si richiamano, perciò, qui di seguito le valutazioni dell'EDPB, nella consapevolezza che questa voce non basta a dare risposte se non è accompagnata dalla voce dell'EBA. In quest'ambito sembra, infatti, opportuno che la cooperazione tra le due *Authorities* trovi espressione in Standard tecnici o Linee Guida condivise.

Innanzitutto, nella lettera del 5 luglio 2018, l'EDPB chiarisce quale sia la corretta base legale per il trattamento dei dati personali effettuato da parte di un prestatore di servizi di disposizione di ordine di pagamento (PISP) che tratta i dati di un soggetto destinatario di un pagamento (la c.d. "parte silente") su ordine del cliente, posto che il consenso non lo ha ricevuto dalla "parte silente" (che non ha alcuna relazione contrattuale con lui), ma dal cliente. Ad avviso dell'EDPB, l'interesse legittimo del titolare e responsabile del trattamento è sufficiente base legale per il trattamento, purché vengano rispettati i principi di minimizzazione, limitazione e trasparenza e quei dati vengano usati solo per tale finalità di trattamento, in linea con quanto previsto dall'art. 6, paragrafo 1, lett. *f*), del GDPR. Il limite è, dunque, dato dalla violazione degli interessi e dei diritti fondamentali dell'interessato.

Un secondo profilo su cui si esprime l'EDPB è quello del significato da attribuire nelle due discipline alla formula "consenso esplicito": si intende, cioè, stabilire se il consenso richiesto dal GDPR possa essere il medesimo imposto dalla PSD2 per l'operatività dei TPP. Si è rilevato che: "natura, funzione e finalità di tali due manifestazioni di «adesione» non sono del tutto omogenei e sovrapponibili nella dinamica dei rispettivi plessi disciplinari, ciò considerato ad esempio anche che, come noto, mentre il GDPR reca un corpus di norme relativo alla protezione delle «persone fisiche» (identificate o identificabili – cosiddetti «interessati») con riguardo al trattamento dei loro «dati personali», nonché alla libera circolazione dei dati stessi, in quest'ambito il focus della PSD 2 è piuttosto sulla protezione dei dati degli «utenti» in genere di servizi di pagamento"[30].

Sostiene l'EDPB che, mentre il consenso indicato dal suddetto art. 94, paragrafo 2, della PSD2 (recepito in Italia all'art. 29 del d.lgs. 218/17) è un consenso di natura contrattuale che lega il prestatore di servizi di pagamento

[29] Lo *European Data Protection Board* è il coordinamento tra i garanti nazionali dell'Unione, cui partecipa anche il Garante europeo per la protezione dei dati e una rappresentanza della Commissione. Il Gruppo formula raccomandazioni, stabilisce *standard* comuni, emette pareri su questioni tecniche per gli Stati membri e per la Commissione europea.

[30] A. Burchi, S. Mezzacapo, P. Musile Tanzi, V. Troiano, *Financial Data Aggregation e Account Information Services*, in *Quaderni, Consob*, Marzo, 2019, p. 33.

e il cliente ed è un consenso limitato al tipo di servizio di pagamento da svolgersi, il consenso richiesto dal GDPR è più generale. Ciò induce a ritenere che il consenso GDPR riguardi il trattamento di qualsiasi altro dato, anche non strettamente necessario per l'esecuzione del contratto, purché si rientri nell'ipotesi dell'art. 6, paragrafo 1, lett. *a*) del GDPR e siano rispettate le condizioni richieste per il consenso dell'interessato dall'art. 7 dello stesso Regolamento.

Il consenso della PSD2 è, pertanto, funzionale alla sola prestazione del servizio di pagamento e ad essa limitato; solo in questo stretto perimetro sostituisce, perciò, il consenso GDPR che rimane, invece, necessario per tutte le ulteriori finalità che il titolare del trattamento è autorizzato a perseguire, purché si rispettino i limiti imposti dal GDPR e le modalità con cui esso deve essere raccolto[31].

Questo aspetto consente anche di dare conto di quale comportamento i TPP debbano adottare quando vengono a conoscenza di "dati sensibili". Al riguardo si rileva che nella PSD2 manca una nozione di "dati sensibili" che, con formulazione lata, sono identificati in quelli "relativi ai pagamenti che possono essere usati per commettere frodi, incluse le credenziali di sicurezza personalizzate". Si prevede, però, come si è detto, che il PISP non possa trattare né conservare dati sensibili del cliente e l'AISP neppure possa richiederli.

Le norme pongono un divieto e, per l'effetto, stabiliscono un limite alla disponibilità negoziale delle parti, non superabile attraverso il consenso. L'obiettivo è la tutela dell'interesse della clientela a non essere vittima di frodi.

[31] In questa prospettiva sembra corretta la lettura offerta da A. Burchi, S. Mezzacapo, P. Musile Tanzi, V. Troiano, *op. cit.,* p. 35, secondo cui verrebbe così a "delinearsi una disciplina differenziata, segnatamente nel senso della previsione di una *protezione extra* o *rafforzata*, per il *trattamento* di "dati personali" nell'ambito della prestazione dei servizi di "*informazione sui conti*", in quanto, ai sensi dell'art. 94, par. 2, della PSD 2, un "*consenso esplicito*" e specifico dei relativi "*utenti*" sembra invece essere sempre necessario, sicché è lasciato all'interprete (e alle Autorità) il compito di stabilire se anche in tale contesto casi trovi applicazione oppure no, e in che misura, l'autonoma e generale condizione di liceità del *trattamento* dei *dati personali* di cui all'art. 6, par. 1, lett. b), del *GDPR*. Partendo dall'assunto che in generale le norme della PSD 2 in materia di protezione dei *dati personali* e quelle del *GDPR* sono da interpretare e applicare in modo il quanto più possibile coordinato e coerente, una possibile lettura del risultante "combinato disposto" potrebbe essere pertanto quella secondo cui la necessità del «*consenso esplicito*» di cui all'art. 94, par. 2, della PSD2 sarebbe invero da intendere nel senso che, da un lato, gli AISPs hanno l'obbligo di mantenere informato l'*utente* dei servizi di "informazione sui conti" circa le *finalità* della raccolta e successivo specifico *trattamento* dei suoi dati personali «*necessari alla prestazione dei rispettivi servizi*», dall'altro, che l'*utente* stesso debba acconsentire esplicitamente a tali *finalità* e *trattamento* e ciò soprattutto ai sensi e per gli specifici effetti delle norme speciali di settore di cui alla PSD 2".

È evidente qui l'assenza di raccordo con il GDPR, in cui la nozione di dato sensibile è centrale, ma assume un significato completamente diverso, facendosi riferimento ai dati relativi a origine razziale o etnica; opinioni politiche; convinzioni religiose o filosofiche; appartenenza sindacale; dati genetici o biomedici; dati relativi alla salute o all'orientamento sessuale della persona.

Un'ulteriore questione trattata dall'EDPB concerne, poi, le API, con riguardo alle quali ci si interroga sul fatto che le medesime siano sufficientemente sicure e idonee a soddisfare il livello di protezione richiesto dal GDPR. Sotto questo profilo, l'EDPB valorizza il ruolo delle Autorità nazionali di vigilanza sulla protezione dei dati personali attribuendo a loro la vigilanza sul fatto che: "il titolare del trattamento e il responsabile del trattamento mettano in atto misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio" (art. 32 GDPR).

Muovendo da queste indicazioni, si possono svolgere un paio di considerazioni ulteriori sotto due profili: (i) il ruolo che assumono AISP e PISP come titolari e/o responsabili del trattamento ai sensi del GDPR[32]; (ii) quali siano le misure che devono essere adottate per prevenire *data breach* e utilizzo illecito dei dati.

La diversa rilevanza del consenso ai fini PSD2 e GDPR porta a ritenere che qualora il TPP chieda l'accesso ai dati possono delinearsi due diversi scenari. Nel caso in cui, non solo intercorra una relazione contrattuale (regolata con consenso espresso, secondo le regole settoriali della PSD2) tra l'interessato e il TPP avente ad oggetto un servizio di disposizione di ordine di pagamento o di informazione sui conti, ma sussista anche un rapporto contrattuale pregresso tra prestatore del servizio di radicamento del conto e TPP, il consenso all'interessato va richiesto da chi effettua il trattamento[33]. Ciò a meno che l'accordo sussistente tra prestatore del servizio di radicamento del conto e TPP stabilisca in via negoziale chi fra i soggetti coinvolti sia il titolare e chi il responsabile del trattamento e preveda un criterio di riparto della responsabilità in caso di frode, utilizzo illecito dei dati e *data breach*, in generale. Nell'accordo potrebbe essere anche stabilito chi è tenuto a comunicare l'incidente all'Autorità competente.

Nel caso invece, verosimilmente più frequente, in cui non preesista

[32] Come ha affermato F. Pizzetti, *op. cit.*, p. 46, il titolare del trattamento è "la pietra angolare e il perno di tutto il sistema di protezione dei dati personali": egli risponde del modo in cui tratta i dati dell'interessato, ha il dovere di informare l'interessato dei trattamenti in corso e di applicare a questi il principio di trasparenza, deve assicurare la tutela dei dati e la protezione dei diritti e delle libertà fondamentali delle persone fisiche.

[33] Purché sia assicurato il rispetto della regola sul consenso GDPR, come configurata dagli artt. 6 e 7 del Regolamento.

alcuna relazione contrattuale tra ASPSP e TPP, la questione è più complessa ed entrambi i soggetti potrebbero essere considerati titolari del trattamento. Certamente, ai fini del GDPR, è titolare dei dati chi effettua l'uso secondario degli stessi: quindi, in questa prospettiva, titolare risulta il TPP, mentre utilizza i dati ai fini degli adempimenti degli obblighi contrattuali.

6. *(*Segue*). L'accountability*

Ma se il consenso è essenziale ai fini del legittimo trattamento dei dati per gli obiettivi della PSD2 e del GDPR esso, tuttavia, non è sufficiente a evitare che possa aversi un uso illecito dei dati o che possa verificarsi un incidente relativo ad essi, eventi rispetto ai quali occorre individuare ulteriori strumenti di tutela a carattere preventivo.

Il passaggio da un adempimento "formale" (quale la raccolta e prova del consenso del cliente) a una "sostanziale" strategia di azione da parte sia degli ASPSP sia dei TPP è, quindi, fondamentale e consiste nell'adozione di presidi organizzativi e procedure adeguate a prevenire i rischi connessi all'attività di prestazione di servizi di pagamento *online* e al trattamento dei dati personali dei clienti.

In questa prospettiva, non va dimenticato che, nel contesto del GDPR, il principio dell'*accountability* riveste un ruolo determinante: ai titolari del trattamento è demandato, infatti, il compito di decidere in autonomia modalità e limiti del trattamento dei dati e a loro viene imposto di organizzarsi con procedure e protocolli idonei all'obiettivo di prevenzione dei rischi che possono derivare dal trattamento dei dati e che vanno sempre commisurati ai diritti e alle libertà personali[34]. Più in dettaglio, l'art. 24

[34] Al tema della protezione e quindi della sicurezza dei dati appartiene il complesso di disposizioni che pongono a carico del titolare l'obbligo di dare avviso prontamente delle violazioni dei dati (artt. 33 e 34); l'obbligo di compiere una preventiva valutazione dei possibili rischi, anche consultando preventivamente l'autorità di controllo (artt. 35 e 36); l'obbligo di designare, in relazione a trattamenti effettuati da soggetti pubblici ovvero aventi ad oggetto particolari categorie di dati, un responsabile della protezione dei dati (art. 37), del quale il Regolamento individua (art. 39) i compiti in maniera dettagliata. A questo novero di obblighi si aggiunge, poi, un ulteriore complesso di regole che, sul piano volontario, prevedono l'adesione a codici di condotta elaborati autonomamente dalle associazioni di categoria (art. 40) ed ancora l'eventuale sottoposizione ad un organismo di vigilanza indipendente, con procedure di certificazione delle misure adottate per la protezione dei dati, affidate ad autonomi organismi di certificazione (artt. 42 e 43) accreditati, al pari

GDPR definisce la responsabilità del titolare del trattamento, chiarendo che questi deve sempre – sia prima di iniziare un trattamento, sia durante il suo svolgimento – "mettere in atto misure tecniche e organizzative adeguate a garantire, e essere in grado di dimostrare, che il trattamento è effettuato conformemente al Regolamento"[35]. Di conseguenza, anche alla luce dell'art. 82 GDPR, il titolare coinvolto nel trattamento risponde in solido per il danno cagionato in violazione del GDPR a meno che non dimostri che l'evento dannoso non gli è imputabile. Particolare rilievo assume, a tal fine, la "Valutazione d'impatto sulla protezione dei dati" (DPIA) disciplinata dall'art. 35, necessaria qualora un certo trattamento necessiti di un'ulteriore valutazione in considerazione di un rischio specifico (specie in caso di uso di nuove tecnologie) e renda opportuna l'adozione di altre puntuali misure di sicurezza e prevenzione dei rischi[36]. Nel caso dell'*Open Banking* con accesso e gestione dei dati da parte dei TPP, questa ulteriore valutazione di rischio può risultare opportuna.

Si valorizza così la discrezionalità dell'intermediario e delle terze parti nel predisporre procedure e cautele specifiche idonee a contrastare il verificarsi del rischio dell'uso illecito dei dati. Spetta, quindi, al titolare del trattamento l'onere di dimostrare la bontà delle proprie scelte organizzative cui si lega un regime di responsabilità rafforzata se le misure adottate non dovessero rivelarsi adeguate sotto il profilo della tutela dei dati imposta dal GDPR.

L'*accountability* è, peraltro, espressione del principio più generale dell'adeguatezza degli assetti organizzativi d'impresa, criterio cardine intorno a cui ruota la regola di responsabilità della gestione dell'impresa sia nella legislazione settoriale bancaria e finanziaria, sia nel Codice civile agli art. 2380 ss.

Allargando lo sguardo in questa direzione, ragionare in termini generali

degli organismi di vigilanza, presso l'Autorità garante. Sul valore dell'*accountability*, v. L. Califano, *Il Regolamento UE 2016/679 e la costruzione di un modello uniforme di diritto europeo alla riservatezza e alla protezione dati personali*, in *Innovazione tecnologica e valore della persona*, a cura di L. Califano e C. Colapietro, Napoli 2018, p. 14 ss.

[35] V. Cuffaro, *Il diritto europeo sul trattamento dei dati personali*, in *Contratto e Impresa Eur.*, 2018, p. 1115, secondo cui: "la prescrizione di obblighi specifici, e specificamente sanzionabili ai sensi dell'art. 83 del Regolamento, viene a spostare il baricentro della disciplina mettendo l'accento sulla necessità di limitare preventivamente il rischio insito nel trattamento dei dati personali. La necessaria adozione di misure preventive, dirette a realizzare il rispetto delle regole di trattamento ed insieme a ridurre il rischio di pregiudizi, determina così una sorta di positivizzazione degli obblighi di protezione".

[36] Il WP29 nelle *Guidelines on data protection impact assessment* afferma che la DPIA è necessariamente successiva ed eventuale rispetto alla valutazione del rischio dell'art. 24 che costituisce secondo F. Pizzetti, *cit.*, p. 63 "l'architrave" di tutto il Regolamento GDPR.

di prevenzione e gestione integrata dei rischi di impresa sembra utile anche per tutelare gli ulteriori interessi riconducibili agli obiettivi propri della PSD2 (favorire la circolazione dei dati e lo *sharing* degli stessi tra i diversi operatori). La gestione integrata dei rischi di impresa[37] è un'esperienza che dimostra, infatti, come ogni nuovo rischio specifico debba essere considerato dal complessivo sistema dei controlli interni e debbano, con riguardo ad esso, essere predisposte procedure atte a prevenire il suo concretizzarsi.

In questa prospettiva, il più efficace strumento per realizzare il coordinamento fra PSD2 e GDPR e per contrastare il rischio di utilizzo illecito dei dati senza tuttavia mortificare la spinta all'apertura e alla concorrenza nel settore dei servizi di pagamento potrebbe rinvenirsi proprio nell'*accountability*, regola trasversale di responsabilizzazione del prestatore di servizi di pagamento, sia esso ASPSP o TPP. In altri termini, lo strumento per tenere insieme le diverse finalità dei due provvedimenti normativi potrebbe essere quello dell'efficiente organizzazione d'impresa in chiave di prevenzione dei rischi; spetta all'impresa, cioè, dimostrare di avere adottato presidi, protocolli e misure organizzative idonee a soddisfare i requisiti richiesti dal Regolamento GDPR senza ostacolare lo sviluppo dell'*Open Banking*.

7. *Conclusioni: verso una competenza concorrente tra* Authorities

L'analisi sin qui condotta induce peraltro a concludere che, per quanto le difficoltà di coordinamento tra le due discipline siano numerose e significative e impongano indirizzi interpretativi unitari e soluzioni tecniche condivise a livello europeo, non si registrano davvero "contrasti tra disposizioni" tali da incidere sulla questione del riparto di competenze tra *Authorities* di vigilanza. E ciò quantomeno se si accoglie l'accezione di "contrasto" come effettiva antinomia fatta propria dalla Corte di Giustizia con la decisione del 13 settembre 2018 che, pur riferendosi a una diversa fattispecie, può rivelarsi un'utile guida alla soluzione del problema. La Corte di Giustizia ha chiarito, infatti, che un problema di riparto di competenze tra *Authorities* può porsi solo laddove sussista un "contrasto" tra le disposizioni

[37] Il concetto di Gestione integrata del rischio di impresa ha l'obiettivo di massimizzare l'efficienza del sistema di controllo interno e ridurre le duplicazioni di attività e il controllo strategico dei rischi. Le componenti del controllo devono essere coordinate e interdipendenti e il sistema nel complesso deve essere integrato nell'assetto organizzativo, amministrativo e contabile della società.

applicabili, da ravvisarsi quando "il rapporto tra due disposizioni va oltre la mera difformità o la semplice differenza, mostrando una divergenza che non può essere superata mediante una formula inclusiva che permetta la coesistenza di entrambe le realtà, senza che sia necessario snaturarle".

Quanto detto, seppure in modo sintetico, è utile per stabilire come operare, in questa materia, il riparto di competenze tra Banca d'Italia e Garante Privacy. In linea con l'indicazione della Corte di Giustizia si può ritenere che vi sia una competenza concorrente tra le due Autorità preposte, in chiave funzionale alla tutela degli interessi protetti[38]. Se l'interesse leso è la riservatezza del dato, interviene il Garante Privacy; se invece è violata la disciplina di PSD2 (violazione della regola del consenso contrattuale; mancanza dei presidi necessari per assicurare la *strong authentication*, ecc.) interviene Banca d'Italia.

L'avere rafforzato con PSD2 i poteri ispettivi del Garante Privacy[39] rende, peraltro, il ragionamento sin qui svolto rilevante anche sotto il profilo dell'*enforcement*, dal momento che le ispezioni possono diventare il "braccio armato" del Garante, come da sempre lo sono per Banca d'Italia.

Ma perché tutto ciò possa in concreto funzionare occorre che le autorità si attengano al principio di leale cooperazione tra loro, in modo da assicurare efficacia ed effettività all'azione coordinata e, per l'effetto, bilanciare al meglio gli interessi diversi ma comunque meritevoli di protezione.

Ove, invece, si ravvisasse per qualche verso un "contrasto reale" tra le due normative, un tale contrasto non potrebbe che essere risolto a livello

[38] Nel senso di ammettere anche un doppio procedimento e un doppio binario sanzionatorio ormai si orienta peraltro tutta la giurisprudenza di legittimità che si è pronunciata più volte di recente sul diverso tema del *cumulo dei procedimenti e ne bis in idem*, in caso di procedimento di opposizioni a sanzioni irrogate da Banca d'Italia e Consob. La scelta della giurisprudenza è stata nel senso di non escludere, in linea di principio, la possibilità di sanzionare diversamente illeciti per loro natura capaci di ledere contemporaneamente interessi diversi a cui garanzia sono preposte autorità diverse, purché sia rispettato il principio di *proporzionalità* delle sanzioni secondo il quale esse devono essere parametrate alla gravità del comportamento, ma non devono eccedere quanto necessario al fine di garantire la finalità della norma. Questo principio, che richiede la necessità, adeguatezza e proporzionalità della sanzione rispetto al fine, assume dunque assoluta centralità, divenendo il parametro per valutare il limite oltre il quale una qualsiasi disposizione non persegue più il proprio obiettivo.

[39] La centralità della figura del Garante quale perno intorno al quale ruota la disciplina della circolazione dei dati personali è ribadita nel Regolamento nell'art. 58, in cui sono riepilogate le funzioni delle quali è titolare il Garante, con riferimento a poteri di indagine, correttivi, autorizzativi e consultivi accompagnate dal significativo riconoscimento della legittimazione ad "intentare un'azione o agire in sede giudiziale o, ove del caso, stragiudiziale in caso di violazione del presente regolamento per far rispettare le disposizioni dello stesso". Per un approfondimento, v. V. Cuffaro, *cit.*, p. 1118.

europeo, mediante Standard tecnici condivisi o Linee Guida congiunte emanate da EBA ed EDPB.

Abstact
La Direttiva sui servizi di pagamento (PSD2) innova profondamente la disciplina bancaria per garantire maggiore efficienza, concorrenza e trasparenza nell'offerta di servizi di pagamento. La principale innovazione è rappresentanta dall'open banking, che apre il mercato dei servizi di pagamento ai nuovi operatori. Altra innovazione significativa è il divieto di surcharge, che si estende al di là del settore in cui era già regolato nel Codice dei consumatori. Queste nuove regole pongono un problema di sovrapposizione tra diversi silos verticali e orizzontali. Il presente documento affronta la questione della ripartizione delle competenze tra le Autorità. In particolare, si concentra sul rapporto tra BANKIT, AGCM, Privacy.

Parole Chiave: Riparto; competenze; intersezioni; sovrapposizioni; silos.

Abstact
The Directive on payment services (PSD2) deeply innovates banking rules to guarantee greater efficiency, competition and transparency in the offer of payment services. The main innovation consists of open banking which opens the market for payment services to new operators. Another relevant reform is the prohibition of a credit surcharge which extends beyond the sphere in which it was already regulated in the Consumer Code. These new rules pose an overlapping problem between different vertical and horizontal silos. This paper deals with the issue of the division of competences between the Autorithies. In particular, it focuses on the relationship between BANKIT, AGCM, Privacy.

Keywords: Overlapping; surcharge; competence; Authorities; privacy.

Simone Mezzacapo

L'inquadramento normativo della PSD2, tra 'dark side' del nuovo framework regolamentare UE dei servizi di pagamento e 'singolarità' dei pagamenti delle Pubbliche Amministrazioni

Sommario: 1. Inquadramento normativo e collocazione ordinamentale della disciplina di settore cui alla PSD2, anche alla luce del coordinamento con altre disposizioni UE e nazionali in materia – 2. La riperimetrazione dell'ambito di applicazione del *framework* armonizzato UE dei servizi di pagamento nel mercato interno e il *dark side* demarcato dal relativo *negative scope* – 3. La 'questione' del trattamento regolamentare dei servizi di pagamento che riguardano Pubbliche Amministrazioni.

1. *Inquadramento normativo e collocazione ordinamentale della disciplina di settore cui alla PSD2, anche alla luce del coordinamento con altre disposizioni UE e nazionali in materia.*

Il presente contributo intende affrontare l'inquadramento normativo dei servizi di pagamento disciplinati dalla cosiddetta PSD2[1] e più specificamente l'individuazione del ruolo sistemico e della 'collocazione' delle relative disposizioni nell'ambito del più complesso e articolato ordinamento giuridico e *acquis* UE e nazionale.

Circa il contenuto sostanziale della PSD2 c'è un punto che mi preme particolarmente mettere in evidenza, ossia che benché la PSD2 'dica molte cose' – ovvero realizzi un organico ed esteso intervento regolatorio in materia di prestazione e utilizzo di servizi di pagamento nel mercato interno dell'UE – tuttavia 'non dice tutto' (!).

La Direttiva reca infatti 'solo' diposizioni dirette alla regolazione

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

armonizzata di alcuni aspetti della materia e che si collocano, tra l'altro, in rapporto di specialità rispetto a numerose altre norme pure rilevanti in *subjecta materia* 'disseminate' nell'ordinamento UE e nazionale. Oltre ovviamente, e *in primis*, alle disposizioni del *Codice Civile* e sulla tutela dei 'dati personali', si pensi ad esempio, tra le tante, alle norme sul *surcharge* e sulle spese in genere pure contenute nelle disposizioni di cui alla Direttiva 2011/83/UE del 25 ottobre 2011 sui diritti dei consumatori[2] e al 'nostro' *Codice del Consumo*[3]. A livello di fonti UE si hanno presenti specificamente, tra le varie, le norme del Regolamento (UE) n. 260/2012 del 14 marzo 2012 sui requisiti tecnici e commerciali per i bonifici e gli addebiti diretti in euro[4] e quelle del Regolamento (CE) n. 593/2008 del 17 giugno 2008 sulla legge applicabile alle obbligazioni contrattuali (Roma I)[5], in particolare con riferimento alle tutele ivi previste a favore dei consumatori.

La PSD2 in pratica oltre a non disporre una regolazione completa del fenomeno 'pagamento', per altro verso non interviene di certo in un *legal vacuum*. Da un lato, a livello generale questa s'inserisce, stabilendo appunto un *corpus* di norme speciali di settore, nel complessivo ordinamento giuridico ed *acquis* ad essa preesistente; dall'altro, la stessa specificamente ridefinisce numerosi elementi strutturali della cornice regolamentare dei servizi di pagamento nel mercato interno dell'UE, quale precedentemente tracciata dalla Direttiva UE adottata nella stessa materia nel 2007 (la c.d. PSD1)[6] – quindi abrogata a decorrere dal 13.1.2018 e sostituita dalla PSD2 (cfr. art. 114 PSD2) – e che ha costituto la *legal foudation* del mercato unico dei pagamenti *retail*, avendo tra l'altro questa codificato, per la prima volta, alcuni principi fondamentali in materia, quali quelli della parità tra pagamenti *cross-border* e nazionali, della promozione della libera (e maggiore) concorrenza nel settore (introducendo ad esempio a tal

[2] Direttiva 2011/83/UE del Parlamento europeo e del Consiglio, del 25 ottobre 2011, sui diritti dei consumatori, recante modifica della Direttiva 93/13/CEE del Consiglio e della Direttiva 1999/44/CE del Parlamento europeo e del Consiglio e che abroga la Direttiva 85/577/CEE del Consiglio e la Direttiva 97/7/CE del Parlamento europeo e del Consiglio.
[3] Cfr. Decreto Legislativo 6 settembre 2005, n. 206 Codice del consumo, a norma dell'articolo 7 della legge 29 luglio 2003, n. 229.
[4] Cfr. Regolamento (UE) n. 260/2012 del Parlamento europeo e del Consiglio, del 14 marzo 2012, che stabilisce i requisiti tecnici e commerciali per i bonifici e gli addebiti diretti in euro e che modifica il regolamento (CE) n. 924/2009.
[5] Cfr. Regolamento (CE) n. 593/2008 del Parlamento europeo e del Consiglio, del 17 giugno 2008, sulla legge applicabile alle obbligazioni contrattuali (Roma I).
[6] Direttiva 2007/64/CE del Parlamento europeo e del Consiglio, del 13 novembre 2007, relativa ai servizi di pagamento nel mercato interno, recante modifica delle Direttive 97/7/CE, 2002/65/CE, 2005/60/CE e 2006/48/CE, che abroga la Direttiva 97/5/CE.

fine il primo *framework* armonizzato UE per gli Istituti di Pagamento, così da promuoverne il ruolo di *new entrants* nel settore), della libertà di scelta degli utenti (anche al fine della maggiore mobilità della domanda), della trasparenza informativa, della tutela forte degli utenti (rilevanti ad esempio al riguardo le relative norme armonizzate in materia di valute, *fees*, diritto al rimborso e responsabilità dei Prestatori di Servizi di Pagamento – PSPs).

Ne consegue l'esigenza di coordinare quello che la PSD2 'dice' con il disposto di altri plessi normativi e ordinamentali. Rileva al riguardo innanzitutto, ad esempio, la nostra disciplina civilistica del diritto delle obbligazioni pecuniarie: quest'ultima infatti, così come avvenne invero già con la PSD1, pur essendo incidentalmente interessata delle disposizioni della PSD2, tuttavia non è – o almeno non direttamente – modificata dalla PSD2, nel senso che benché quest'ultima intenda recare una disciplina organica e armonizzata dei servizi di pagamento nell'UE, tuttavia non si occupa direttamente della materia della disciplina delle obbligazioni pecuniarie. Ciò posto non può mancarsi d'individuare l'esistenza di alcuni *spillover effects* della PSD2 anche in quest'ambito, ovvero di non secondari, benché indiretti, effetti regolatori della PSD2 anche sulla disciplina dell'adempimento delle obbligazioni pecuniarie.

Così come avvenuto già con la PSD1, la PSD2 reca infatti una disciplina armonizzata 'solo' dei «servizi di pagamento» e delle «operazioni di pagamento», intese in particolare queste ultime quali atti (disposti dal pagatore o per suo conto o dal beneficiario) con cui sono 'collocati' (ovvero 'versati'), trasferiti o ritirati (ovvero 'prelevati') dei 'fondi'[7] e ciò «indipendentemente da eventuali obblighi sottostanti tra pagatore e beneficiario» (cfr. art. 4, punto 5 della PSD2).

Le disposizioni della PSD2 appaiono quindi volutamente 'neutrali' rispetto alla qualificazione giuridica del 'pagamento' negli ordinamenti degli Stati Membri e al rispettivo diritto delle obbligazioni pecuniarie, sicché le relative norme rimangono tuttora di sola fonte nazionale ed estranee, salva tuttavia una sempre maggiore influenza indiretta – *rectius* «portata regolatoria indiretta»[8] – della crescente armonizzazione UE in materia, quale avviata con la PSD1, prima, e proseguita con la PSD2, ora. Ad esempio,

[7] Ossia *ex* art. 4, punto 25) della PSD2: «banconote e monete, moneta scritturale o moneta elettronica quale definita all'articolo 2, punto 2), della direttiva 2009/110/CE».

[8] Cfr. A. Sciarrone Alibrandi, *L'adempimento dell'obbligazione pecuniaria tra diritto vivente e portata regolatoria indiretta della Payment services directive 2007/64/CE*, in *Il nuovo quadro normativo comunitario dei servizi di pagamento. Prime riflessioni* in «Quaderni di Ricerca Giuridica della Consulenza Legale» a cura di M. Mancini e M. Perassi, n. 63, Dicembre 2008, pp. 69 e ss.

nelle disposizioni della PSD2 il legislatore UE non prende posizione in merito alla dibattuta questione se il 'pagamento' è un *atto giuridico* o *negozio giuridico*, la soluzione di questa e di analoghe questioni rimangono quindi integralmente affidate alla nostra normativa (civilistica) nazionale e rinviate quindi, per quanto riguarda il punto di vista del diritto UE, ai diversi ordinamenti nazionali.

Abbiamo quindi molti e significativi aspetti del fenomeno 'pagamento' che nonostante gli obiettivi espliciti e impliciti della PSD2 di volere attuare un'armonizzazione forte in materia rimangono però ancora oggi non pienamente armonizzati in tutto il mercato interno.

Per altro verso invece il recepimento della PSD2 ha dato luogo in diversi casi a vere e proprie antinomie rispetto alle disposizioni di contigui o comunque connessi plessi normativi, nonché a problemi di coordinamento tra attribuzioni e competenze tra le diverse Autorità di regolamentazione e vigilanza.

Ad esempio sul tema del coordinamento con le nome di cui al nuovo *framework* armonizzato UE in materia di protezione dei dati personali e condizioni di liceità del loro 'trattamento', a cui pure già si è accennato, devo dire che le questioni di coordinamento in materia derivano forse principalmente dal fatto che benché il GDPR[9] fosse praticamente 'maturo' per poter essere approvato in concomitanza con l'approvazione della PSD2, la PDS2 è stata invece emanata a fine 2015 e il GDPR invece circa a metà del 2016, da cui il non perfetto allineamento tra i due plessi normativi da molti, anche oggi, messo in evidenza.

Ciò posto, per quanto riguarda il profilo dell'inquadramento, e quindi del coordinamento, della PSD2 nell'ambito dell'ordinamento giuridico nel suo complesso, vale rilevare che la PSD2 costituisce, come anticipato, solo una parte (benché importante) della disciplina del fenomeno dalla stessa regolamentato; la fattispecie 'pagamento' è infatti in realtà intercettata da diversi plessi normativi.

Già a livello di fonti UE, ad esempio, un primo riferimento da tenere presente è il Regolamento (UE) 2015/751 sulle c.d. *interchange fees* per le 'operazioni di pagamento basate su carta' (IFR)[10]. Oltre alla relativa affinità di materia, quest'ultimo Regolamento e la PSD2 fanno infatti parte insieme dell'iniziativa legislativa in materia di pagamenti di cui al c.d. EU *Payment*

[9] Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27.4.2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la Direttiva 95/46/CE (Regolamento Generale sulla Protezione dei Dati – GDPR).

[10] Regolamento (UE) 2015/751 del Parlamento europeo e del Consiglio, del 29.4.2015, relativo alle commissioni interbancarie sulle operazioni di pagamento basate su carta.

Legislative Package pubblicato dalla Commissione Europa nel 2013. Il successivo *iter* legislativo UE – durato circa due anni – si è concluso appunto con l'adozione dell'IFR e della PSD2.

Con l'emanazione dell'IFR sono stati, in particolare, codificati tutta una serie di principi UE enucleati negli ultimi dieci anni circa di *enforcement antitrust* nel settore delle carte di pagamento; in pratica le disposizioni dell'IFR codificano sostanzialmente le valutazioni e gli esiti dei *leading cases Visa*[11] e *Mastercard*[12]. L'IFR è composto da due insiemi principali di norme, una prima parte, forse la più nota, è quella che riguarda l'armonizzazione delle discipline nazionali in materia di *interchange fees*[13], la seconda, non meno importante, contiene un elenco di *business rules* da rispettarsi da parte di intermediari e *merchants* in materia di pagamenti basati su carte[14].

Da non dimenticare poi che la PSD2 è strettamente interconnessa, quanto meno per materia, con la meno famosa *Payment Accounts Directive* (PAD) del 2014[15]. Benché infatti la PAD sia invero generalmente considerata la 'sorella povera' della PSD2, in realtà è una Direttiva molto importante in chiave di disciplina sistemica della materia, e che si colloca 'a monte' della PSD2, perché armonizza alcuni aspetti fondamentali di quello che è uno dei principali elementi anche di tutta la disciplina di cui alla PSD2, ossia il *conto di pagamento*, che è l'elemento cardine sul quale è costruita tutta la disciplina del mondo dei servizi di pagamento. La PAD in particolare è dedicata all'armonizzazione degli aspetti relativi alla trasparenza delle spese sui servizi *core* connessi a un conto di pagamento, alla promozione della concorrenza tramite la facilità di *switching*, e quindi di portabilità dei conti, e al diritto all'accesso ai conti di pagamento con 'caratteristiche di base' per le fasce di popolazione svantaggiate. Tutta la PAD è in definitiva

[11] Decisione della Commissione dell'8.12.2010, C(2010) 8760 final (caso COMP/39.398 - Visa MIF) e successiva decisione sempre della Commissione del 26.2.2014, C(2014) 1199 final (caso AT.39398 – VISA MIF).

[12] Cfr. Decisione della Commissione del 19.12.2007, C (2007) 6474 def. (casi COMP/34.579 – MasterCard, COMP/36.518 – EuroCommerce, COMP/38.580 – Commercial Cards).

[13] Cfr. artt. 3 – 5 dell'IFR ai sensi dei quali sono, tra l'altro, stabiliti i famosi *cap* armonizzati dello 0,2% per le operazioni di pagamento basate su carte di debito e 0,3% per le operazioni di pagamento basate su carte di credito, salve alcune deroghe e opzioni nazionali.

[14] Sia consentito al riguardo il rinvio a S. Mezzacapo, *La nuova disciplina UE dei limiti alle* interchange fees *e delle* business rules *in materia di 'pagamenti basati su carte', tra regolamentazione strutturale del mercato interno e promozione della concorrenza*, in «Diritto della Banca e del Mercato Finanziario», n. 3, 2017, pp. 455 – 528.

[15] Direttiva 2014/92/UE del Parlamento europeo e del Consiglio del 23.7.2014, sulla comparabilità delle spese relative al conto di pagamento, sul trasferimento del conto di pagamento e sull'accesso al conto di pagamento con caratteristiche di base.

intesa ad assicurare una maggiore mobilità da parte degli utenti dei conti di pagamento e dei servizi di pagamento in generale, realizzando quindi chiaramente un intervento pro-concorrenziale che funge da base per assicurare in genere la possibilità di una elevata mobilità della domanda quale elemento fondamentale anche del mercato dei servizi di pagamento come disciplinati dalla PSD2[16].

Sulle concordanze e discordanze tra i principii e le disposizioni della PSD2 e quelli di altri plessi normativi, oltre a quelli da ultimo richiamati rilevano altresì il *corpus* delle norme *antitrust*, il *Codice del consumo*[17] e, non ultimo, il *Codice delle comunicazioni elettroniche*[18], quest'ultimo per tutto quello che riguarda segnatamente il fenomeno dei *mobile payments*, ovvero per tutto quanto riguarda le nuove possibilità, sviluppate e promosse dalla PSD2, di poter usare, ad esempio, il credito telefonico come provvista di fondi per effettuare operazioni di pagamento. In pratica, mentre tra le tradizionali tipologie di fondi che possono essere 'trasferite' nell'ambito delle operazioni di pagamento sono state fin ora annoverate le monete metalliche, le banconote, la moneta scritturale e la moneta elettronica, con la PSD2 viene chiaramente ammessa e regolamentata anche la possibilità di utilizzare, entro certi limiti, anche il credito telefonico, che sussume così quasi a nuova forma di *moneta scritturale* di natura non bancaria. Nell'ottica PSD2 il fenomeno del *mobile payment* entra nell'ambito del relativo perimetro regolamentare per finalità *in primis* di tutela del consumatore e di promozione della concorrenza.

Altro, non meno importate, *corpus* normativo nazionale che va ad intersecarsi con le disposizioni della PSD2 è il c.d. *Codice del terzo settore*[19]. Benché a prima vista possa sembrare che quest'ultimo 'appartenga' ad un ambito disciplinare molto lontano da quello della PSD2, tuttavia tra le varie cose che la PSD2 ora consente di fare in regime di esenzione dalla relativa disciplina – definendo, in modo molto più chiaro e soprattutto armonizzato a livello UE, i limiti dell'esenzione stessa – vi è anche l'utilizzabilità del credito telefonico per effettuare donazioni[20]. Pertanto quando pagamenti della

[16] Anche in materia sia consentito il rinvio a S. Mezzacapo, *La nuova disciplina nazionale dei conti di pagamento alla luce dell'armonizzazione attuata con la Payment Accounts Directive*, in *Banca borsa, tit. cred.*, n. 6, 2017, pp. 795, 816 e 820.

[17] Decreto Legislativo 6 settembre 2005, n. 206, Codice del consumo, a norma dell'articolo 7 della legge 29 luglio 2003, n. 229.

[18] Decreto Legislativo 1 agosto 2003, n. 259, Codice delle comunicazioni elettroniche.

[19] Decreto Legislativo 3 luglio 2017, n. 117, Codice del Terzo settore, a norma dell'articolo 1, comma 2, lettera b), della legge 6 giugno 2016, n. 106.

[20] Come indicato nel considerando (16) della PSD2 «*In order to ease the burden on entities that collect charitable donations, payment transactions in relation to such donations should also be*

specie sono effettuati nel quadro di un'attività di beneficenza, per effettuare *erogazioni liberali* destinate agli *enti del terzo settore* che esercitano determinate *attività caritatevoli*, oltre al rispetto delle condizioni per l'esenzione della disciplina dei servizi di pagamento, vengono in evidenza tutta una serie di tematiche che riguardano direttamente la disciplina specifica di settore, *rectius* nel nostro caso del 'terzo settore'. Per dirne una, l'individuazione della lista dei potenziali beneficiari delle donazioni tramite credito telefonico (art. 2, comma 2, lettera n), punto 2) del D.lgs. 27 gennaio 2010, n. 11, come modificato dal D.lgs. 15 dicembre 2017, n. 218).

Per quanto riguarda invece gli obiettivi di *policy* della PSD2, benché questi siano già oggetto di ampia analisi negli altri contributi, vale rilevare che, al di là dell'obiettivo generale della «ulteriore integrazione di un mercato interno dei servizi di pagamento», gli obiettivi stessi possono essere schematicamente declinati nei seguenti: 1) modernizzare il *framework* UE rispetto all'evoluzione tecnologica e regolamentare di nuovi servizi (*e.g.* tramite la nuova disciplina dei c.d. *Third Party Payment Services Providers*[21] o TPPs); 2) rafforzare il *level playing field*, la concorrenza tra PSPs e al tempo stesso la *consumer protection*; 3) rimuovere alcune ambiguità e lacune normative, segnatamente attraverso una più chiara ridefinizione del *negative scope* della disciplina del settore dei servizi di pagamento in senso stretto; 4) assicurare che i pagamenti elettronici siano *safer and more secure* (es. attraverso specifici requisiti e regole tecniche in materia di *common and secure*

excluded. Member States should, in accordance with national law, be free to limit the exclusion to donations collected in favour of registered charitable organisations. The exclusion as a whole should apply only where the value of payment transactions is below a specified threshold in order to limit it clearly to payments with a low risk profile». In particolare, ai sensi dell'art. 3 della PSD2 sono pertanto escluse dal suo ambito di applicazione: «*payment transactions consisting of the non-professional cash collection and delivery within the framework of a non-profit or charitable activity*» (cfr. art. 3 (d)); «*payment transactions by a provider of electronic communications networks or services provided in addition to electronic communications services for a subscriber to the network or service: […] (ii) performed from or via an electronic device and charged to the related bill within the framework of a charitable activity […]; provided that the value of any single payment transaction […] does not exceed EUR 50 and: — the cumulative value of payment transactions for an individual subscriber does not exceed EUR 300 per month, or — where a subscriber pre-funds its account with the provider of the electronic communications network or service, the cumulative value of payment transactions does not exceed EUR 300 per month*» (cfr. art. 3 (l)).

[21] Un *genus* questo che nella nuova tassonomia regolamentare (ri)definita dalla PSD2 si compone di due *species* di nuovi PSPs: 1) i prestatori di servizi di «disposizione di ordine di pagamento» (c.d. *Payment Initiation Services Providers* o PISPs) di cui all'art. 4, punto 18 della PSD2) i prestatori di servizi di «informazione sui conti» (c.d. *Account Information Service Providers* o AISPs) di cui all'art. 4, punto 19, Dir. 2015/2366.

communication e *strong customer authentication*[22], nonché apposite norme in materia di responsabilità dei PSPs – cfr. artt. 73, 74, 88 -93 della PSD2); 5) introdurre specifici presidii di *consumer protection* (quali ad esempio i requisiti prudenziali per i *Third Party Payment Services Providers*), le regole in materia di trasparenza, spese, regime di responsabilità dei PSPs, rimborsi, riduzione a massimo 50 Euro della franchigia addebitabile al pagatore in caso di operazioni di pagamento non autorizzate (salvi i casi di frode o negligenza grave)[23], operazioni di pagamento con importo non noto in anticipo[24]; 6) standardizzare alcuni aspetti tecnici e assicurare interoperabilità, anche tramite l'emanazione in numerosi ambiti di *Guidelines* dell'EBA ovvero di vere e proprie *norme tecniche di regolamentazione* elaborate dell'EBA e approvate dalla Commissione europea con proprio regolamento; 7) promuovere l'efficienza e la riduzione del costo dei servizi di pagamento; 8) estendere, rispetto alla PSD1, l'ambito di applicazione del diritto armonizzato UE in materia di servizi di pagamento.

2. *La riperimetrazione dell'ambito di applicazione del* 'framework' *armonizzato UE dei servizi di pagamento nel mercato interno e il* 'dark side' *demarcato dal relativo* 'negative scope'

Per i profili che più direttamente rilevano in funzione del tema assegnatomi, interessa in questa sede procedere ad analizzare più in dettaglio proprio quest'ultimo punto, ossia il fatto che la PSD2 amplia, modifica e ridefinisce, in modo significativo, l'ambito di applicazione della disciplina armonizzata UE in materia.

Ad un aspetto, tra l'altro tra i più noti, è stato già accennato, la PSD2 definisce infatti un nuovo *framework* legale, d'ispirazione pro concorrenziale, per imprese quali i TPPs (nella loro possibile duplice veste di PISP e di AISP), le quali sono in questo modo attratte *in scope*, ossia nell'ambito della cornice regolamentare UE dei servizi di pagamento da cui prima rimanevano invece estranee, essendo la relativa attività in precedenza considerata, a tal fine, come *unregulated*. In particolare, i PISP e gli AISP nella logica e *policy*

[22] Cfr. *Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with Regard to Regulatory Technical Standards for Strong Customer Authentication and Common and Secure Open Standards of Communication*.
[23] Cfr. art. 74, *id.*
[24] Cfr. art. 75, *id.*

approach pre-PSD2 erano essenzialmente considerati e trattati come dei meri fornitori di *servizi tecnici* distinti da quelli di pagamento in senso proprio, mentre oggi, stante anche la loro diffusione ed evoluzione, sono stati fatti rientrare nel novero dei veri e propri PSPs regolamentati[25]. Tra gli innumerevoli corollari di questo *policy change* indicativa appare, ad esempio, la conseguente chiara, esplicita e inequivoca 'messa al bando' – almeno in linea di principio – della controversa pratica del c.d. *screen scraping*, con conseguente obbligo d'ora in poi per tali TPPs di identificarsi presso i PSPs di radicamento dei conti di pagamento ogniqualvolta accedono *online* ai conti stessi 'per conto' dei propri clienti (cfr. artt. 66 e 67 della PSD2 e relative norme tecniche di regolamentazione).

A livello sistemico, la mia impressione è che, per effetto di tale nuovo trattamento regolamentare dei TPPs e della regolamentazione espressa e dettagliata dei rapporti tra questi e i PSPs 'di radicamento' (dei conti di

[25] In particolare, al riguardo il *framework* di cui alla PSD2 è basato, tra l'altro, sulla considerazione che dopo l'adozione della PSD1 «si sono diffusi nuovi tipi di servizi di pagamento, specialmente nel settore dei pagamenti tramite Internet. In particolare, si sono evoluti i servizi di disposizione di ordine di pagamento nel settore del commercio elettronico. Tali servizi di pagamento svolgono un ruolo nei pagamenti in detto settore mediante un software che fa da ponte tra il sito web del commerciante e la piattaforma di *online banking* della banca del pagatore per disporre pagamenti via Internet sulla base di bonifici. Inoltre, gli sviluppi tecnologici degli ultimi anni hanno portato anche alla nascita di una serie di servizi accessori, ad esempio servizi di informazione sui conti. Tali servizi forniscono all'utente di servizi di pagamento informazioni *online* aggregate su uno o più conti di pagamento, detenuti presso un altro o altri prestatori di servizi di pagamento, a cui si ha accesso mediante interfacce *online* del prestatore di servizi di pagamento di radicamento del conto. L'utente di servizi di pagamento può così disporre immediatamente di un quadro generale della sua situazione finanziaria in un dato momento. Anche tali servizi dovrebbero essere trattati nella presente Direttiva al fine di garantire ai consumatori una protezione adeguata relativamente ai dati di pagamento e contabili nonché la certezza giuridica legata allo status di prestatore di servizi di informazione sui conti. I servizi di disposizione di ordine di pagamento consentono al prestatore di servizi di disposizione di ordine di pagamento di assicurare al beneficiario che il pagamento è stato disposto così da incentivare il beneficiario a consegnare i beni o a prestare il servizio senza indebiti ritardi. Tali servizi offrono una soluzione a basso costo per i commercianti e i consumatori e consentono a questi ultimi di fare acquisti *online* anche senza carte di pagamento. Poiché non sono attualmente soggetti alla Direttiva 2007/64/CE, i servizi di disposizione di ordine di pagamento non sono necessariamente soggetti alla vigilanza di un'autorità competente e non devono rispettare i requisiti di cui alla Direttiva 2007/64/CE. Ciò solleva una serie di questioni giuridiche, ad esempio sul piano della tutela dei consumatori, della sicurezza e della responsabilità nonché della concorrenza e delle questioni legate alla protezione dei dati, con particolare riguardo alla protezione dei dati degli utenti di servizi di pagamento in conformità delle norme dell'Unione sulla protezione dei dati. È quindi opportuno che le nuove disposizioni affrontino tali aspetti» (Considerando 27 – 29 della PSD2).

pagamento), la PSD2 crei 'in vitro' un nuovo mercato *upstream* del *servicing* dei conti di pagamento, ovvero della 'fornitura e amministrazione' dei conti stessi, in cui operano appunto i PSPs 'di radicamento' dei conti, i quali finiscono così per assurgere, anche giuridicamente, a *facilities necessarie* per l'operatività nei connessi mercati *downstream* che su questi si basano, da cui l'importanza della pure sopra ricordata *Payment Accounts Directive* del 2014 per quanto riguarda la disciplina giuridica dei conti di pagamento, nonché l'inizio forse del progressivo tramonto nel mercato interno dell'UE del modello della 'banca universale', almeno per come oggi strutturato, a favore di modelli più aperti e meno integrati[26].

Sempre in linea con la logica dell'ampliamento dell'ambito di applicazione dell'*acquis* armonizzato UE in materia di servizi di pagamento, altro elemento a volte non adeguatamente valorizzato, ma altamente innovativo della PSD2, è costituto dal fatto che questa interviene altresì ad imporre obblighi di trasparenza anche alle operazioni di pagamento non in Euro laddove soltanto uno dei PSP «sia situato nell'Unione, per ciò che riguarda le parti dell'operazione di pagamento effettuate nell'Unione» (cfr. art. 2, par. 4 della PSD2), assoggettando quindi alla relative disposizioni anche le c.d. operazioni *one-leg* che erano invece fuori ambito di applicazione della disciplina UE di settore quale definita dalla PSD1[27]. Si è parlato in questo caso di potenziale applicazione extraterritoriale del diritto dell'Unione in materia; io devo dire tuttavia che non condivido questa osservazione, ciò perché a ben vedere l'applicazione delle disposizioni della PSD2 anche alle operazioni *one-leg* è invero limitata alle sole parti dell'operazioni stesse eseguite nell'Unione, mantenendosi in questo modo la territorialità intra-UE del suo ambito di applicazione.

Ciò posto, il *focus* principale di questa analisi sul punto vuole essere il fatto che la PSD2 rimodula profondamente e dettagliatamente anche il c.d. *negative scope* della disciplina UE di settore e nel rimodularlo sostanzialmente

[26] Sia consentito al riguardo il rinvio a S. Mezzacapo, *Competition Policy Issues in EU Retail Payment Business: the New PSD2 Regulatory Principle of Open Online Access to Information from 'Payment Accounts' and Associated 'Payment Transactions'*, in "European Competition Law Review, Vol. 39, Issue 12 [(2018) 39 E.C.L.R., Issue 12], pp. 536 – 538 e 543.

[27] Al riguardo è stato ritenuto opportuno che le disposizioni della PSD2 «in materia di trasparenza e di requisiti informativi a carico dei prestatori di servizi di pagamento e in materia di diritti e obblighi inerenti alla prestazione e all'uso di servizi di pagamento si applichino, ove opportuno, anche alle operazioni in cui uno dei prestatori di servizi di pagamento è situato al di fuori dello Spazio economico europeo (SEE), al fine di evitare approcci divergenti nei vari Stati membri a danno dei consumatori. Ove opportuno, tali disposizioni dovrebbero essere estese alle operazioni in tutte le valute ufficiali tra prestatori di servizi di pagamento situati nel SEE» (Considerando 8 della PSD2).

interviene in senso restrittivo; ovvero la PSD2 provvede a meglio definire e limitare i casi e le condizioni di esclusione dell'applicazione della disciplina UE dei servizi di pagamento come aggiornata dalla stessa PSD2, con il risultato di ampliare in pratica anche per questa via, per così dire indiretta, l'ambito di applicazione positivo delle regole di settore.

È infatti mia opinione al riguardo che al fine del corretto inquadramento sistemico della PSD2 sia invero essenziale *in primis* esplorare ed esaminare proprio la sua parte 'meno evidente', ovvero concentrare inizialmente l'attenzione su quello che definirei il '*dark side*' del quadro normativo, e di vigilanza, definito dalla PSD2 in materia di servizi di pagamento.

In pratica, mi pare che per poter cogliere e delineare a pieno il portato normativo e la collocazione ordinamentale delle varie disposizioni della PSD2, sia particolarmente utile soffermarsi innanzitutto ad analizzare non tanto la parte 'visibile' e 'prescrittiva' della PSD2, quanto piuttosto ciò di cui PSD2, volutamente e dichiaratamente, non si occupa e che rimane quindi 'nell'ombra' del relativo *framework* regolamentare, ovvero quel frastagliato e disomogeneo insieme di fattispecie e aspetti che, benché strettamente connessi e/o attigui alla materia dei 'servizi di pagamento', tuttavia la PSD2 lascia intenzionalmente fuori dall'ambito di applicazione delle relative disposizioni di settore, in quanto ritenuti appunto più opportunamente da collocare nel suo *negative scope*.

Un *dark side* che, in quanto tale, rimane inoltre, di norma, distante e non direttamente osservabile anche dal punto di vista proprio delle Autorità preposte alla vigilanza sul settore dei servizi di pagamento.

È un aspetto questo che, rispetto all'approccio regolamentare precedente, proprio la PSD2 mi pare però che miri a voler in qualche misura mitigare, incrementando in particolare in alcuni casi la 'visibilità' delle relative Autorità di vigilanza anche su questo 'lato oscuro' del settore in esame.

Mi preme infatti in questa sede segnalare che la PSD2 segna invero una significativa innovazione in materia in quanto, nel perimetrare meglio il *negative scope* della relativa disciplina armonizzata UE, prevede un articolato elenco di casi di esclusione espressa dell'applicazione delle relative disposizioni (cfr. art. 3), ma in alcuni di questi casi stabilisce al contempo degli obblighi di notifica nei confronti dell'Autorità di vigilanza di settore (es. per il caso delle esclusioni relative ai *limited networks* – cfr. art. 37 della PSD2).

In pratica, pur stabilendo che alcune fattispecie debbano rimane al di fuori dal relativo 'recinto regolamentare', la PSD2 prescrive ora però che in alcuni casi e a certe condizioni le Autorità di settore debbano poter osservare anche ciò che accade al di là, ma comunque in prossimità, dei confini

dell'area dei servizi di pagamento regolamentati in senso stretto.

Tale ridefinizione ai sensi della PSD2 del *negative scope* della disciplina di settore ha come obiettivo fondamentale quello di contribuire a una maggiore certezza giuridica in materia, a beneficio così degli ulteriori obiettivi del rafforzamento della tutela degli utenti dei servizi di pagamento, da un lato, del *level playing field* e della rimozione delle distorsioni della concorrenza per i PSP nel mercato interno, dall'altro. Il problema a cui con la PSD2 s'intende così porre rimedio è connesso in particolare al fatto che anche la PSD1 conteneva invero diverse ipotesi di esclusione dall'applicazione delle relative disposizioni, tuttavia l'estensione e il contenuto del risultante *negative scope* sono stati variamente declinati e/o intesi nei diversi Stati membri: alcuni Stati membri hanno interpretato le esenzioni in modo più restrittivo, mentre altri le hanno interpretate in modo più elastico, sicché di fatto le attività o servizi che potevano essere svolti in regime di esenzione oppure no sono variati significativamente a secondo degli Stati membri. Inoltre anche lo stesso sviluppo del settore dei pagamenti elettronici e le rapide innovazioni tecniche in materia hanno evidenziato alcuni limiti della precedente struttura regolamentare che, in alcuni casi, hanno lasciato spazio ad una applicazione non sempre coerente e scarsamente armonizzata della disciplina UE della materia e delle ipotesi di esenzione di cui al relativo *negative scope*[28].

[28] Risulta ad esempio che, dall'adozione del dicembre 2007 della PSD1, «*the retail payments market has experienced significant technical innovation, with rapid growth in the number of electronic and mobile payments and the emergence of new types of payment services in the market place, which challenges the current framework. (4) The review of the Union legal framework on payment services and, in particular, the analysis of the impact of* [PSD1] […] *and the consultation on the Commission Green Paper of 11 January 2012, entitled, 'Towards an integrated European market for card, internet and mobile payments', have shown that developments have given rise to significant challenges from a regulatory perspective. Significant areas of the payments market, in particular card, internet and mobile payments, remain fragmented along national borders. Many innovative payment products or services do not fall, entirely or in large part, within the scope of* [PSD1] […]. *Furthermore, the scope of* [PSD1] […] *and, in particular, the elements excluded from its scope, such as certain payment-related activities, has proved in some cases to be too ambiguous, too general or simply outdated, taking into account market developments. This has resulted in legal uncertainty, potential security risks in the payment chain and a lack of consumer protection in certain areas. It has proven difficult for payment service providers to launch innovative, safe and easy-to-use digital payment services and to provide consumers and retailers with effective, convenient and secure payment methods in the Union. In that context, there is a large positive potential which needs to be more consistently explored.* […] (6) *New rules should be established to close the regulatory gaps while at the same time providing more legal clarity and ensuring consistent application of the legislative framework across the Union. Equivalent operating conditions should be guaranteed, to existing and new players on the market, enabling new means of payment to reach a broader market, and ensuring a high level of consumer protection in the use of those payment services across the Union as a whole. This should generate*

In aggiunta a ciò, a differenza di quanto stabilisce ora la PSD2, ai sensi della PSD1 non erano previsti meccanismi formali di interlocuzione o interpello con le Autorità competenti in merito all'applicazione a specifici casi concreti delle norme di settore e/o delle relative ipotesi di esenzione, pertanto le valutazioni in merito erano, e in larga parte ancora sono, lasciate al *self-assessment* dei soggetti interessati, da cui un ulteriore contributo alla scarsa uniformità nel mercato interno delle pratiche e delle condotte degli operatori[29].

Ciò posto, giova innanzitutto mettere in evidenza che il *focus* della PSD2 è sui *servizi pagamenti elettronici*, quindi in generale sono da collocare nel relativo *negative scope*, volendo generalizzare, tutte le operazioni di trasferimento di fondi basate su strumenti 'cartacei' o 'in contanti' (*i.e.* banconote o monete, ciò considerato anche per «che per il contante esiste già un mercato unico dei pagamenti»)[30], fatte salve alcune limitate eccezioni, come ad esempio nel caso dei servizi per il prelievo di contante offerti da gestori di sportelli automatici (ATM) indipendenti ai quali, pur essendo in linea di principio esclusi dall'applicazione della PSD2, si applicano tuttavia alcune disposizioni di trasparenza di cui alla PSD2 stessa, così da «assicurare la chiarezza circa le commissioni sui prelievi»[31] (cfr. art. 3, lett. o), della PSD2)[32].

---

efficiencies in the payment system as a whole and lead to more choice and more transparency of payment services while strengthening the trust of consumers in a harmonised payments market » (Considerando 3, 4 e 6 della PSD2).

[29] È stato osservato in particolare che «*Service providers seeking to benefit from an exclusion from the scope of* [… PSD1 …] *often have not consulted authorities on whether their activities are covered by, or excluded from, that Directive, but have relied on their own assessments. This has led to a differing application of certain exclusions across Member States. It also appears that some exclusions may have been used by payment service providers to redesign business models so that the payment activities offered would be outside the scope of that Directive. This may result in increased risks for payment service users and diverging conditions for payment service providers in the internal market. Service providers should therefore be obliged to notify relevant activities to competent authorities so that the competent authorities can assess whether the requirements set out in the relevant provisions are fulfilled and to ensure a homogenous interpretation of the rules throughout the internal market. In particular, for all exclusions based on the respect of a threshold, a notification procedure should be provided in order to ensure compliance with the specific requirements. (20) Moreover, it is important to include a requirement for potential payment service providers to notify competent authorities of the activities that they provide in the framework of a limited network on the basis of the criteria set out in* [… PSD2 …] *if the value of payment transactions exceeds a certain threshold. Competent authorities should assess whether the activities so notified can be considered to be activities provided in the framework of a limited network*» (Considerando 19 e 20 della PSD2).

[30] Cfr. Considerando 23 della PSD2.

[31] Considerando 18 della PSD2.

[32] In particolare, è stabilito che la PSD2 non si applica «ai servizi di prelievo di contante offerti da prestatori tramite ATM per conto di uno o più emittenti della carta che non siano parti del

Più specificamente, coerentemente altresì con la premessa iniziale secondo cui la PSD2 armonizza il diritto dei servizi di pagamento, ma non si occupa del diritto 'obbligazioni pecuniarie', la prima tradizionale categoria di operazioni di pagamento che espressamente rimangono nel *negative scope* della PSD2 sono quelle «effettuate esclusivamente in contante» con *traditio* diretta dei fondi dal pagatore al beneficiario e quindi «senza alcuna intermediazione» (art. 3, lett. a), PSD2).

Men che meno rientrano quindi nell'ambito di applicazione della PSD2 tutte quelle attività di «trasporto materiale, a titolo professionale, di banconote e monete, ivi compresa la raccolta, il trattamento e la consegna» (art. 3, lett. c), della PSD2), un'esclusione questa che riguarda ad esempio la «attività di società che gestiscono il contante in transito (CIT - Cash-in-Transit companies) e [… le …] società di gestione del contante (CMC - Cash Management Companies) allorché le attività in questione si limitano al trasporto fisico di banconote e monete»[33].

Sono inoltre espressamente escluse (così come lo erano già ai sensi della PSD1), anche tutte quelle 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» (quali ad esempio la c.d. 'questua domenicale'), nonché le operazioni di cambio di valuta di tipo *cash in/cash out*, ossia quelle operazioni «in contante contro contante nell'ambito delle quali i fondi non siano detenuti su un conto di pagamento» (art. 3, lett. d) e f), della PSD2).

La PSD2 interviene inoltre a confermare il trattamento regolamentare da riservare al c.d. servizio di *cash back*, il quale anche se invero ancora non diffuso in Italia è invece molto utilizzato all'estero, soprattutto nell'ambito della grande distribuzione organizzata, stabilendo in particolare che questo continua a dover essere collocato nell'ambito del *negative scope* della disciplina UE dei servizi di pagamento in senso proprio. Al riguardo, così come già previsto ai sensi della PSD1, anche la PSD2 prescrive infatti che il relativo *framework* normativo non si applichi appunto a servizi, come quello in parola, «in cui il beneficiario fornisce contante al pagatore nel contesto di un'operazione di pagamento, a seguito di una richiesta esplicita

contratto quadro con il cliente che preleva denaro da un conto di pagamento, a condizione che detti prestatori non forniscano altri servizi di pagamento elencati nell'allegato I [… della stessa PSD2 …]. Ciononostante, al cliente sono fornite le informazioni in merito a qualsiasi commissione sui prelievi di cui agli articoli 45, 48, 49 e 59 [… della PSD2 …] prima che esegua il prelievo nonché al momento del ricevimento dei contanti alla fine dell'operazione, dopo il prelievo».

[33] Cfr. Considerando 12 della PSD2.

dell'utente di servizi di pagamento immediatamente precedente l'esecuzione dell'operazione di pagamento attraverso un pagamento destinato all'acquisto di beni o servizi» (art. 3, lett. e), della PSD2 – enfasi aggiunta).

Inoltre sono 'strutturalmente' escluse dall'ambito della PSD2, tutte quelle operazioni di pagamento basate su strumenti 'cartacei' di vario tipo – quali assegni, cambiali, *voucher, travelers's cheque*, vaglia postali – con i quali viene ordinato ad un PSP di «mettere fondi a disposizione del beneficiario» (cfr. art. 3, lett. g), della PSD2)[34], fermo restando che è in ogni caso ritenuto opportuno che «le buone prassi in materia si ispirino ai principi enunciati» nella PSD2[35].

Altra innovazione importante recata dalla PSD2 in materia di *negative scope* della disciplina di settore riguarda la disciplina dell'attività degli 'agenti commerciali'. In particolare viene fatta maggiore chiarezza e soprattutto assicurata maggiore uniformità rispetto alla PSD1 riguardo alle condizioni al ricorrere delle quali in ambito UE è da ritenersi che le operazioni di pagamento effettuate tramite 'agenti commerciali' siano da considerare escluse dall'ambito di applicazione delle disposizioni sui servizi di pagamento e gli agenti stessi non debbano quindi assumere la qualità di prestatori di servizi di pagamento in senso proprio.

Il tema è particolarmente sensibile, sia perché l'esclusione in parola ai sensi della PSD1 è stata applicata in modo significativamente difforme e secondo prassi divergenti nei diversi Stati Membri[36], sia perché intercetta un aspetto cardine della disciplina del commercio elettronico. Risulta specificamente che in alcuni casi l'applicazione della esenzione in parola è stata consentita alle 'piattaforme di commercio elettronico' secondo modalità 'abnormi' rispetto alla lettera e allo spirito della PSD1, con

[34] In particolare sono escluse dall'ambito di applicazione della PSD2 le operazioni di pagamento basate su uno dei seguenti tipi di documenti: «i) assegni cartacei disciplinati dalla Convenzione di Ginevra, del 19 marzo 1931, che stabilisce una legge uniforme sull'assegno bancario (chèque); ii) assegni cartacei analoghi a quelli di cui al punto i) e disciplinati dalla normativa degli Stati membri che non sono parte della Convenzione di Ginevra, del 19 marzo 1931, che stabilisce una legge uniforme sull'assegno bancario (chèque); iii) titoli cambiari su supporto cartaceo ai sensi della Convenzione di Ginevra, del 7 giugno 1930, concernente la legge uniforme sulla cambiale e il vaglia cambiario; iv) titoli cambiari su supporto cartaceo analoghi a quelli di cui al punto iii) e disciplinati dalle normative degli Stati membri che non sono parte della Convenzione di Ginevra, del 7 giugno 1930, che stabilisce una legge uniforme sulla cambiale e sul vaglia cambiario; v) voucher su supporto cartaceo; vi) assegni turistici su supporto cartaceo; vii) vaglia postali su supporto cartaceo conformemente alla definizione dell'Unione postale universale».

[35] Cfr. Considerando 22 della PSD2.

[36] Cfr. Considerando 11 della PSD2.

conseguente inadeguato presidio dei rischi per i consumatori e distorsioni della concorrenza[37].

Secondo l'approccio della PSD2 in materia la condizione primaria ed essenziale per la corretta applicazione dell'esenzione in parola è che un agente commerciale non deve mai detenere, o comunque essere in possesso o avere sotto il suo controllo giuridico, i fondi dei clienti; ove questa condizione sia soddisfatta è quindi, financo, consentito all'agente commerciale di agire per conto di tutte e due le parti di una operazione commerciale (come appunto certe piattaforme di commercio elettronico). Laddove invece l'agente commerciale detenga o controlli i fondi dei clienti, allora l'esenzione è applicabile solo se l'operazione di pagamento è effettuata tramite un agente che agisce per conto di una sola delle due parti dell'operazione (*i.e.* solo per conto del pagatore o del beneficiario – cfr. art. 3, lett. b) della PSD2).

Un ulteriore ambito in cui la PSD2 interviene a fare chiarezza riguarda l'appartenenza al relativo *negative scope* dei *c.d.* servizi tecnici 'di supporto' a quelli di pagamento in senso stretto, realizzando segnatamente rispetto alla PSD1 una restrizione dell'estensione di questa ipotesi di esenzione. Viene infatti al riguardo sostanzialmente disposto un *carve out* rispetto a tale categoria di servizi dei PIS e degli AIS: questi ultimi infatti, come detto, a differenza di quanto accadeva nel contesto pre-PSD2 vengono ora ad essere invece inclusi a tutti gli effetti nell'elenco dei veri e propri servizi di pagamento (cfr. art. 3, lett. j), della PSD2)[38].

Inoltre la PSD2 provvede a ridefinire in modo sostanziale, e segnatamente in senso restrittivo, le condizioni dell'esclusione relativa ai c.d. *limited networks*; ciò principalmente perché le evidenze di mercato hanno mostrato che «le attività di pagamento soggette [… a tale esclusione ai sensi della PSD1 in realtà …] spesso implicano volumi e valori di pagamento significativi e offrono ai consumatori centinaia o migliaia di prodotti e servizi diversi», determinando così diffusi casi di operatività in regime di applicazione dell'esclusione in parola in contrasto però, o comunque non

[37] Ovvero ad esempio anche alle piattaforme di commercio elettronico «che agiscono come intermediari per conto dei singoli acquirenti e dei singoli venditori senza un reale margine nella negoziazione o conclusione della vendita o dell'acquisto di beni o servizi» (Considerando 11 della PSD2).

[38] Come ivi disposto la PSD2 non si applica «ai servizi forniti da 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 della riservatezza, 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 ad esclusione dei servizi di disposizione di ordine di pagamento e dei servizi di informazione sui conti».

coerenti, con la *ratio* e le finalità per le quali l'esclusione stessa era stata originariamente prevista, con conseguente inadeguato presidio dei rischi per gli utenti e distorsioni concorrenziali tra PSPs e imprese che operano invece beneficiando di tali casi di esclusione dalla regolamentazione del settore dei servizi di pagamento[39].

In particolare, proprio al fine di mitigare tali rischi è meglio esplicitato nella PSD2 il principio di fondo che l'applicazione dell'esclusione in questione non possa più essere invocata laddove gli specifici strumenti di pagamento, su cui i relativi servizi sono basati, perdano il requisito essenziale della utilizzabilità «solo in modo limitato», dal punto di vista merceologico o della ubicazione geografica dei punti vendita, trasformandosi piuttosto in uno strumento «ad uso generale»[40]; come avverrebbe, ad esempio, laddove uno stesso strumento di pagamento possa essere utilizzato «all'interno di più di una rete limitata» o per «l'acquisto di una gamma illimitata di beni e servizi», oppure nel caso in cui questo non sia più esclusivamente «regolamentato da un'autorità pubblica nazionale o regionale, per fini sociali o fiscali specifici allo scopo di acquistare beni o servizi specifici»[41].

Come pure sopra accennato, altra significativa innovazione è costituita dal fatto che nell'occasione è stato altresì ritenuto opportuno introdurre un obbligo per i relativi prestatori di servizi di notificare alle Autorità competenti una descrizione dei servizi dagli stessi offerti in applicazione di tale esenzione relativa ai *limited networks* – con specificazione inoltre di quale esclusione, tra quelle contemplate all'art. 3, lettera k), punti i) e ii), della PSD2, sia stata considera nel caso di specie applicabile – così che le medesime Autorità provvedano, con decisione motivata, a stabilire se i servizi così prestati possano essere effettivamente considerati come prestati nel quadro di un *limited network*[42] e, in caso contrario, ne informino prontamente il prestatore di servizi (cfr. art. 37, par. 2 della PSD2).

Infine, un ulteriore elemento molto importante del *negative scope* della PSD2, anche per le sue dirette implicazioni in ottica *Fintech*, è costituito dalla dettagliata riperimetrazione della c.d. *telecom exemption* di cui all'art. 3, lett. l), della stessa PSD2, allo specifico fine di meglio precisarne il contenuto e al contempo di restringerne la potenziale ampiezza (*i.e.* con riguardo all'importo e all'oggetto delle operazioni escluse), viste anche le disomogenee prassi nazionali seguite dagli Stati Membri durante la 'vigenza' della PSD1[43].

[39] Cfr. Considerando 13 della PSD2.
[40] Cfr. Considerando 13 e 14 della PSD2.
[41] Cfr. Considerando 13 della PSD2.
[42] Cfr. Considerando 20 della PSD2.
[43] Anche al riguardo è stata riscontrata infatti una certa ambiguità della formulazione

È stabilito in particolare che al ricorrere di alcune condizioni – riferite cumulativamente all'importo (ridotto) del pagamento e al tipo di operazione – la disciplina della PSD2 non si applichi a determinate operazioni di pagamento effettuate «da parte di un fornitore di reti o servizi di comunicazione elettronica […] in aggiunta a servizi di comunicazione elettronica per un abbonato alla rete o al servizio», chiarendo così in quali casi è legittimamente possibile effettuare pagamenti, in regime di esclusione appunto dal *framework* PSD2, direttamente tramite un operatore di telecomunicazione (c.d. *operator billing*) o acquisti con addebito diretto sulla bolletta telefonica dell'utente di servizi di telecomunicazione (c.d. *direct to phone-bill purchases*)[44].

Al fine di salvaguardare gli interessi degli utenti e il sistema di riserve di attività del settore dei servizi di pagamento, l'applicabilità dell'esclusione in parola è segnatamente circoscritta a talune operazioni di pagamento ritenute «a basso profilo di rischio»[45], ossia alle sole operazioni di pagamento per l'acquisto o consumo di «contenuti digitali», «servizi a tecnologia vocale», oppure effettuate «nel quadro di un'attività di beneficenza» o per «l'acquisto di biglietti», ferme le ulteriori due generali condizioni cumulative che il valore di ciascuna di queste operazioni di pagamento «non superi 50 EUR» e in ogni caso che «il valore complessivo delle operazioni di pagamento […della specie …] non superi, per un singolo abbonato, 300 EUR mensili», questo sia nel caso di addebito in fattura sia nel caso di utilizzo del credito prepagato dell'utente (cfr. art. 3, lett. l), punti i) e ii), della stessa PSD2).

Un particolare tratto innovativo del *policy change* così attuato in materia è che, nel precisare e per certi aspetti restringere l'ammissibilità e applicabilità di tale esclusione, viene in ogni caso per altro verso testualmente ed espressamente 'sdoganata' a livello UE la possibilità di acquistare 'biglietti', tipicamente biglietti elettronici e relativi solamente alla prestazione di servizi[46], utilizzando per il pagamento il proprio credito

della esclusione ai sensi della PSD1 che ha favorito una sua applicazione disomogenea nei diversi Stati membri, con conseguente «mancanza di certezza giuridica per gli operatori e i consumatori e consentendo in alcuni casi ai servizi di intermediazione di pagamento di considerarsi ricompresi, in modo illimitato, nell'esclusione dall'ambito di applicazione della» PSD1 (Considerando 15 della PSD2).

[44] Cfr. Considerando 15 della PSD2.

[45] Considerando 16 della PSD2.

[46] Al riguardo è stato in particolare considerato che il riferimento alle operazioni di pagamento per l'acquisto di biglietti elettronici è strumentale a «tenere conto degli sviluppi nei pagamenti in cui, in particolare, i clienti possono ordinare, pagare, ottenere e convalidare biglietti elettronici da qualsiasi luogo e in qualsiasi momento utilizzando telefoni cellulari o altri dispositivi. I biglietti elettronici consentono e facilitano la prestazione di servizi che i

telefonico prepagato o tramite addebito in bolletta, fermi i limiti d'importo sopra indicati, possibilità questa che in Italia è stata, e per certi profili è ancora, abbastanza controversa, anche a causa delle ambiguità normative derivanti dalla congiunta applicazione delle disposizioni proprie del settore delle comunicazioni elettroniche e delle relative limitazioni (cfr. D.lgs. 1 agosto 2003, n. 259 – Codice delle comunicazioni elettroniche).

3. *La 'questione' del trattamento regolamentare dei servizi di pagamento che riguardano Pubbliche Amministrazioni*

Ciò detto, al fine di definire un più compiuto inquadramento ordinamentale della PSD2, mi preme infine svolgere di seguito alcune considerazioni circa l'ulteriore – e meno indagato – aspetto del rapporto tra la disciplina armonizzata UE dei servizi di pagamento, quale da ultimo ridefinita dalla PSD2, e le regole che governano i pagamenti della Pubblica Amministrazione.

E' dato infatti al riguardo osservare che in Italia in sede di recepimento della PSD1, nel 2010, si ritenne opportuno inserire nelle disposizioni transitorie del D. lgs. 11/2010 di recepimento la norma speciale di cui al relativo comma 6 dell'art. 37, ai sensi della quale si dispose che i «servizi di pagamento che riguardano amministrazioni pubbliche […, come individuate dall'art. 1, co. 2, del D.lgs. 165/2001 …], vengono adeguati alle disposizioni del presente decreto […, attuative appunto della PSD1 …] secondo le modalità e i tempi indicati con decreto del Ministro dell'economia e delle finanze, sentita la Banca d'Italia».

In punto di fatto e di diritto, ne risulta che in pratica le operazioni di pagamento delle pubbliche amministrazioni sono state da allora così mantenute in una sorta di *negative scope* nazionale della disciplina armonizzata UE dei servizi di pagamento o, quantomeno, in una condizione di limbo normativo.

Il suddetto decreto ministeriale attuativo recante le 'modalità e i tempi' di adeguamento *in parte qua* alle disposizioni della PSD1 non è stato infatti poi emanato, e quindi per diversi anni si è rimasti in una situazione di incertezza giuridica (almeno a detta di alcuni) circa l'*an* e gli

clienti potrebbero altrimenti acquistare sotto forma di biglietto cartaceo e comprendono il trasporto, l'intrattenimento, il parcheggio auto e l'ingresso ad eventi, ma escludono i beni fisici. Essi riducono in tal modo i costi di produzione e distribuzione connessi con i canali tradizionali di emissione di biglietti cartacei e aumentano la convenienza per il cliente grazie a modi semplici e nuovi di acquisto dei biglietti» (Considerando 16 della PSD2).

eventuali *quando* e *quomodo* dell'applicazione del nuovo *framework* UE in materia anche ai servizi di pagamento che riguardano le PP.AA.. Sono state formulate sul punto opinioni diverse e diametralmente opposte, ossia che in mancanza del decreto ministeriale in parola la nuova disciplina di cui al D.lgs. 11/2010 si applicasse *tout court* e senza deroghe o eccezioni, ovvero che in mancanza di tale decreto attuativo la disciplina stessa invece non si applicasse alle PP.AA..

Con l'entrata in vigore del decreto legislativo n. 218 del 2017[47] di recepimento della PSD2 si può dire che tale questione ermeneutica, e la maggior parte delle relative incertezze giuridiche in materia, sono state in ogni caso finalmente risolte per 'cessazione della materia del contendere', quanto meno a decorrere dal 1° gennaio 2019.

Giusta infatti la «constatata insussistenza di ragioni ostative per l'applicazione integrale delle disposizioni della PSD2 alle pubbliche amministrazioni»[48], nell'ambito delle varie modifiche apportate da D.lgs. 218/2017 al D.lgs. 11/2010 è stata disposta anche l'integrale abrogazione del relativo art. 37 con effetto «dalla data di entrata in vigore» dello stesso D.lgs. 218/2017, ad eccezione tuttavia proprio del comma 6 dell'art. 37 del D.lgs. 11/2010 che invece «è abrogato a decorrere dal 1° gennaio 2019» (cfr. art. 2, co. 39, del D.lgs. 218/2017).

Pertanto, una delle innovazioni ordinamentali, forse a *prima facie* meno evidenti, ma di certo tra le più rilevanti in chiave sistemica, realizzate con il recepimento della PSD2 è che dal 1° gennaio 2019 cessa ogni dubbio circa il fatto che anche PP.AA. sono da qualificare quali 'ordinari' utenti di servizi di pagamento, nonché in merito all'applicazione quindi anche ai servizi della specie prestati a favore delle PP.AA. del *framework* armonizzato UE in *subjecta materia*, salvi alcuni limitati 'adattamenti' tecnici che non costituiscono però deroghe ai relativi principi e regole.

È questo un aspetto che può sembrare un po' di 'nicchia', di interesse per i soli addetti ai lavori, ma che in realtà ha valenza generale riguardando l'amplissima platea di soggetti che a vario titolo hanno rapporti con le PP.AA. come pagatori o come beneficiari di un pagamento, perché tra i vari aspetti disciplinati dalla PSD2 c'è anche quello delle spese connesse alla

[47] Decreto Legislativo 15 dicembre 2017, n. 218, recante recepimento della Direttiva (UE) 2015/2366 relativa ai servizi di pagamento nel mercato interno, che modifica le Direttive 2002/65/CE, 2009/110/CE e 2013/36/UE e il regolamento (UE) n. 1093/2010, e abroga la Direttiva 2007/64/CE, nonché adeguamento delle disposizioni interne al regolamento (UE) n. 751/2015 relativo alle commissioni interbancarie sulle operazioni di pagamento basate su carta.
[48] Ministero dell'Economica e delle Finanze, Dipartimento della Ragioneria Generale dello Stato e Dipartimento del Tesoro, Circolare n. 22 del 15 giugno 2018, p. 2.

prestazione di servizi di pagamento.

Ciò posto, tale abrogazione differita, a decorrere dal 1° gennaio 2019, del comma 6 dell'art. 37 del D. lgs. 11/2010 trova essenzialmente la sua *ratio* nella necessità di consentire alle Pubbliche amministrazioni (centrali e locali) e ai relativi prestatori terzi di servizi di tesoreria o di cassa (tipicamente la Banca d'Italia, le banche e Poste Italiane S.p.A.)[49] di adeguarsi al fatto che, quanto meno da tale data, non vi è più alcun dubbio che il *framework* regolamentare di cui alla PSD2 (e al D. lgs. 11/2010) si applichi anche nei rapporti tra le Pubbliche amministrazioni e i relativi prestatori di servizi di pagamento.

La puntuale *compliance* col *framework* UE in parola non è infatti comunque del tutto esente da alcune questioni interpretative connesse, ad esempio, alle «peculiarità del servizio di tesoreria (o cassa), […alla individuazione degli …] aspetti che possono incidere sul rapporto intercorrente tra la pubblica amministrazione e il suo tesoriere/cassiere, […nonché alle soluzioni …] per consentire la corretta applicazione dei principi»[50] della PSD2.

Tra le principali ricadute di questa innovazione vi è *in primis* quella della necessità di effettuare un'accurata *due diligence*, e ove necessario un coerente adeguamento, di tutte le 'convenzioni di tesoreria e di cassa' in essere tra Pubbliche Amministrazioni e relativi tesorieri/cassieri al fine di assicurarne la conformità allo spirito e alla lettera della PSD2.

Il differimento dell'abrogazione al 1° gennaio 2019 è quindi innanzitutto specificamente funzionale a consentire un'ordinata opera di revisione e adeguamento delle convenzioni di tesoreria/di cassa.

L'adeguamento dei tali contratti dovrà avvenire in diversi modi, a secondo del tipo di adeguamenti che si rendessero necessari.

In linea di principio, soprattutto per quanto riguarda gli aspetti normativi delle convenzioni in parola, si ritiene che la maggior parte delle modifiche da apportare ai contratti della specie non dovrebbero implicare modifiche significative, *rectius* 'sostanziali'[51], del rapporto contrattuale tra la P.A. e il rispettivo cassiere/tesoriere

In questo caso, pertanto, per la modifica del contenuto dei contratti ben si potrà far affidamento su eventuali clausole di adeguamento automatico

[49] Ministero dell'Economica e delle Finanze, Dipartimento della Ragioneria Generale dello Stato e Dipartimento del Tesoro, Circolare n. 22 del 15 giugno 2018, p. 2.
[50] Ministero dell'Economica e delle Finanze, Dipartimento della Ragioneria Generale dello Stato e Dipartimento del Tesoro, Circolare n. 22 del 15 giugno 2018, p. 2.
[51] Cfr. art. 106, comma 4, del Decreto legislativo 18 aprile 2016, n. 50 (Codice dei contratti pubblici).

allo *ius superveniens* già contenute nelle convenzioni in esame. In mancanza di siffatte clausole espresse, considerato che eventuali modifiche contrattuali sarebbero nel caso comunque motivate dall'esigenza di adeguare le convenzioni medesime alle norme sopravvenute, «si reputa sufficiente un adeguamento delle convenzioni in essere ai sensi dell'art. 106, comma 1, del D. Lgs. n. 50/2016 […, recante il Codice dei contrati pubblici, …] da effettuare entro il 1° gennaio 2019»[52], ossia che le convenzioni in parola possono essere modificate senza bisogno di una nuova procedura di affidamento.

Se invece dal punto di vista delle Pubbliche Amministrazioni interessate le modifiche da apportare alle convenzioni fossero da ritenere sostanziali, in quanto determinano una 'alterazione considerevole' degli 'elementi essenziali' del contratto, allora l'unica opzione per assicurare la dovuta *compliance* con la PSD2 è quella di provvedere ad effettuare una nuova procedura di affidamento di servizi secondo i termini e le condizioni modificate, da completarsi anch'essa in tempo utile rispetto al termine del 1° gennaio 2019.

Dal punto di vista del diritto sostanziale, tra le regole armonizzate UE sui servizi di pagamento da applicarsi anche nei rapporti con le PP.AA. vi è altresì la fondamentale regola del c.d. 'T+1' in materia di 'tempi di esecuzione' massimi tra ricezione di un ordine di pagamento e l'accredito del relativo importo, ossia della riduzione ad un solo giorno lavorativo del tempo massimo entro il quale i *fondi* devono essere "girati" al PSP del beneficiario. In particolare, ai sensi dell'art. 83 della PSD2 (cfr. art. 20del D.lgs. 11/2010), il PSP di un soggetto pagatore deve assicurare che l'importo di una operazione di pagamento di cui gli sia stata ordinata l'esecuzione sia reso disponibile a favore del suo beneficiario (*rectius* venga accreditato sul conto del PSP del beneficiario) «entro la fine della giornata operativa successiva» a quella in cui il relativo ordine di pagamento è stato ricevuto dal PSP di cui si è avvalso il pagatore. Termine massimo questo che per le sole «operazioni di pagamento disposte su supporto cartaceo» può essere tuttavia convenzionalmente esteso dalle parti «di una ulteriore giornata operativa».

Al riguardo si è posto il problema di come applicare correttamente tale regola del 'T+1' alle operazioni di pagamento disposte dalle PP.AA., ovvero quando la P.A. assume il ruolo di pagatore, in quanto il mandato di pagamento emesso da una P.A. anche se 'materialmente' ricevuto dal relativo tesoriere/cassiere non è però da questo immediatamente eseguibile, ma deve essere preliminarmente sottoposto ad un ulteriore 'trattamento' da parte dello stesso tesoriere/cassiere, il quale deve eseguire infatti una serie

[52] Ministero dell'Economica e delle Finanze, Dipartimento della Ragioneria Generale dello Stato e Dipartimento del Tesoro, Circolare n. 22 del 15 giugno 2018, p. 3.

di attività complesse, controlli e verifiche che difficilmente possono essere completati in un solo giorno lavorativo[53].

Ciò posto, rispetto all'opzione di non applicare la regola del 'T+1' nel caso dei mandati di pagamento della PP.AA., si è ritenuto invece preferibile mantenere la piena applicazione della regola stessa, salva la possibilità di ricorrere ad un adattamento interpretativo, ovvero una *fictio iuris*. In pratica, considerato appunto che il mandato di pagamento non è immediatamente eseguibile appena materialmente ricevuto dal tesoriere/cassiere, si ritiene allora legittimo poter nel caso convenire, in via contrattuale, che il mandato si consideri giuridicamente 'ricevuto' (*i.e.* ai fini e per gli effetti della individuazione del *dies a quo* per il computo del termine del 'T+1' o del 'T+2') la 'giornata operativa' successiva a quella di sua effettiva ricezione materiale (di fatto) da parte del tesoriere/cassiere.

In altri termini è considerato lecito poter convenire contrattualmente che il tesoriere/cassiere abbia un determinato lasso di tempo per completare le operazioni necessarie a rendere un mandato di pagamento eseguibile e che solo una volta completate queste operazioni, o comunque scaduto il termine per queste stabilito, trovi quindi ordinaria applicazione la regola generale del 'T+1' (ovvero del 'T+2' in caso di operazioni di pagamento disposte su supporto cartaceo). Il lasso di tempo 'fisiologico' per lo svolgimento di tali operazioni preliminari da svolgersi da parte del tesoriere/cassiere è stato inoltre a sua volta quantificato in massimo un'ulteriore 'giornata operativa'[54].

[53] In particolare, come osservato il servizio di tesoreria/cassa affidato dalle pubbliche amministrazioni «alle banche/Poste è un servizio articolato che non si esaurisce nella mera messa esecuzione di operazioni di incasso e pagamento, ma prevede una serie di ulteriori obblighi e adempimenti a carico dei tesorieri/cassieri, discendenti dall'applicazione di norme di rango primario o secondario […]. Sotto questo profilo, pertanto, all'atto della ricezione dell'ordine di pagamento, cioè del mandato emesso dalla pubblica amministrazione e contente la disposizione di pagamento, lo stesso ordine non può essere considerato immediatamente e direttamente trasferibile alle procedure di pagamento. Ciò in quanto detto trasferimento presuppone che siano stati effettuati e positivamente conclusi i controlli e le verifiche affidate al tesoriere, che non si esauriscono nella mera verifica della liquidità disponibile e/o della firma da parte del soggetto cui è assegnato il potere di spesa, ma possono riguardare la capienza dello stanziamento di bilancio, la verifica dei vincoli di destinazione dei finanziamenti, la presenza delle codifiche previste dalla legge», Ministero dell'Economica e delle Finanze, Dipartimento della Ragioneria Generale dello Stato e Dipartimento del Tesoro, Circolare n. 22 del 15 giugno 2018, p. 4.

[54] Risulta in particolare che, anche grazie all'utilizzo della nuove tecnologie informatiche, i tempi per lo svolgimento di questi adempimenti e controlli sono sempre più ridotti e possono essere normalmente contenuti in una giornata lavorativa; in «concreto, proprio tenendo conto dell'informatizzazione in corso, che per molte pubbliche amministrazioni condurrà all'esclusivo uso dell'OPI telematico entro la fine del 2018, si ritiene che, ove necessario per esigenze di carattere organizzativo e/o procedurale dei tesorieri/cassieri, gli adempimenti cui

In questo modo è sostanzialmente rispettata a pieno la *ratio* e l'obiettivo della regola di cui all'art. 83 della PSD2, ossia assicurare che il PSP del pagatore esegua prontamente (*i.e.* entro la fine della giornata operativa successiva) un ordine di pagamento ricevuto dal pagatore, adattando però alle specificità del caso le modalità tecnico operative della relativa *compliance*.

Anche riguardo alla principale e centrale innovazione ordinamentale introdotta dalla PSD2 del suddetto principio dell'accesso aperto e condiviso *online* ai conti di pagamento da parte dei TPPs, si è posto il tema del *se* e *come* le relative regole debbano applicarsi al caso dei conti della specie di cui siano titolari le Pubbliche Amministrazioni. In particolare la questione ermeneutica verte sul fatto se ai *conti di tesoreria* delle PP.AA. si applichino in via ordinaria, oppure no, anche le disposizioni della PSD2 ai sensi delle quali in linea di principio i *conti di pagamento* che siano accessibili *online* (nel senso di accesso *Internet based*) da parte dei relativi titolari devono essere resi accessibili, sempre per via telematica, anche a favore dei TPPs (ove questi agiscano in base al 'consenso esplicito' e 'per conto' dei titolari dei conti stessi), nonché le relative 'norme tecniche di regolamentazione' in materia di *strong customer authentication* e di *common and secure open standards of communication*[55].

La soluzione interpretativa che – almeno allo stato – è apparsa più adeguata e coerente col nuovo *framework* regolamentare della PSD2 e la 'singolarità' del rapporto che intercorre tra le PP.AA. e i loro tesorieri/cassieri è stata che il *conto di tesoreria* non si configuri, e non sia quindi qualificabile pienamente, come un *conto di pagamento accessibile online* ai sensi e per gli effetti tipici della PSD2. Sicché l'orientamento prevalente è nel senso che i *conti di tesoreria* delle PP.AA. non rientrino a tutti gli effetti nell'ambito di applicazione di tali nuove disposizioni della PSD2 in materia di *open and shared access* da parte dei TPP ai conti di pagamento e quindi che, al

gli stessi sono tenuti possano far 'slittare' in avanti il termine di ricezione [… di una mandato di pagamento emesso da una P.A. …] – rispetto alla data in cui il mandato pervenuto materialmente [.. al tesoriere/cassiere…] – al massimo di una giornata operativa, lasciando un'ulteriore giornata operativa per l'esecuzione delle disposizioni di pagamento su supporto cartaceo […]. Tali aspetti vanno ovviamente regolati all'interno della Convenzione per il servizio di tesoreria/cassa, tenendo conto che di tratta di un'opportunità ammissibile sotto il profilo operativo, ma lasciata all'accordo tra i due contraenti, nei limiti sopra fissati», Ministero dell'Economica e delle Finanze, Dipartimento della Ragioneria Generale dello Stato e Dipartimento del Tesoro, Circolare n. 22 del 15 giugno 2018, p. 4.

[55] Cfr. 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.

contempo, nelle comunicazioni tra PP.AA. e relativi tesorieri/cassieri non si applicano neanche le disposizioni della PSD2, e delle pertinenti norme tecniche attuative, sui requisiti e *standard* di comunicazione e di sicurezza[56].

A mio avviso tale approdo ermeneutico trova supporto e giustificazione tra l'altro nel fatto che effettivamente le PP.AA. in realtà non accedono direttamente al proprio *conto di tesoreria*, essendo piuttosto tale accesso 'mediato' da speciali procedure dedicate, sicché il conto stesso a ben vedere non sarebbe accessibile *online* nel senso avuto presente nell'ambito e ai fini della PSD2 o comunque è accessibile secondo modalità talmente specifiche da essere strutturalmente diverse da un ordinario accesso di un utente al proprio conto di pagamento tramite *internet banking*. Inoltre, altre specificità dei conti di tesoreria delle PP.AA. sono costituite dal fatto che, di norma, a fine giornata i fondi in giacenza sui conti stessi sono riversati nei conti di *Tesoreria Unica* presso la Banca d'Italia, fermo restando però che in ogni caso il servizio di tesoreria o di cassa resta affidato al tesoriere/cassiere che gestisce, tramite procedure dedicate, il rapporto finanziario con la Banca d'Italia[57].

In definitiva, avuto anche riguardo alle disposizioni del *Testo unico delle leggi sull'ordinamento degli enti locali*[58] in materia, può dirsi che l'oggetto proprio del servizio di tesoreria/cassa a favore delle PP.AA. determina in realtà la configurazione del servizio stesso quale 'servizio complesso' soggetto a norme speciali, segnatamente in ampia parte diverso da quello di mera fornitura e amministrazione, da parte di un PSP di radicamento del conto, di un conto di pagamento per un pagatore (cfr. art. 4, punto 17), della PSD2).

[56] In tal senso è stato in particolare ritenuto che «in virtù del rapporto intercorrente tra la pubblica amministrazione e il suo tesoriere/cassiere, i conti di tesoreria non rientrano nel novero dei conti di pagamento accessibili *online*, così come definiti dalla PSD2 e dal relativo decreto di recepimento e pertanto non sono applicabili a tali conti le fattispecie […dell'accesso ai conti di pagamento da parte di prestatori dei nuovi servizi regolamentati dalla PSD2 di 'disposizione di ordini di pagamento' e/o di 'informazione sui conti' di pagamento …]. Similmente, nel colloquio fra pubblica amministrazione e tesoriere/cassiere, non trovano applicazione le disposizioni relative ai requisiti di sicurezza per i pagamenti elettronici», quali pure ridefiniti ai sensi della PSD2 e dei relativi *Regulatory Technical Standards* (Ministero dell'Economica e delle Finanze, Dipartimento della Ragioneria Generale dello Stato e Dipartimento del Tesoro, Circolare n. 22 del 15 giugno 2018, p. 5).

[57] Cfr. Legge 29 ottobre 1984, n. 720, Istituzione del sistema di tesoreria unica per enti ed organismi pubblici; art. 35 del Decreto-legge 24 gennaio 2012, n. 1, Disposizioni urgenti per la concorrenza, lo sviluppo delle infrastrutture e la competitività (convertito con modificazioni dalla L. 24 marzo 2012, n. 27); Decreto ministeriale del 4 agosto 2009, n. 59457, recante nuove modalità di regolamento telematico dei rapporti tra tesorieri e cassieri degli Enti ed organismi, di cui alla tabella A allegata alla legge 29 ottobre 1984, n. 720, e la Tesoreria dello Stato.

[58] Cfr. artt. 208 e ss. del Decreto Legislativo 18 agosto 2000, n. 267.

In tale prospettiva il tesoriere/cassiere non sembra poter essere quindi integralmente equiparato ai sensi e per gli effetti propri della PSD2 ad un PSP di radicamento del conto, né essere quindi soggetto al relativo obbligo, ove ne ricorrano i presupposti, di consentire l'accesso dei TPPs ai conti dallo stesso amministrati (cfr. artt. 67 e 67 della PSD2).

Un ultimo aspetto che mi pare importante analizzare è quello della disciplina delle spese applicabili nella prestazione dei servizi di pagamento, in particolare per quanto attiene ai profili: *i)* della 'ripartizione' delle spese; *ii)* del c.d. *surcharging* per l'utilizzo di un determinato strumento di pagamento; *iii)* dell'applicazione di 'deduzioni' sull'importo delle operazioni di pagamento a titolo di copertura delle spese.

Al riguardo vale ricordare che con l'emanazione della PSD2, e col relativo recepimento nazionale ai sensi del D.lgs. 218/2017, è stata innanzitutto ulteriormente rinforzata la *policy* di fondo che l'opzione normativa più opportuna ed efficiente – in quanto «agevola il trattamento completamente automatizzato dei pagamenti»[59] – è che di regola il beneficiario e il pagatore debbano sostenere ciascuno *solo* le spese ad essi (eventualmente) direttamente addebitate dai rispettivi PSPs (cfr. art. 62, par. 2, della PSD2), ossia che in materia di addebito delle spese dei servizi di pagamento debba essere in linea di principio applicata la c.d. *regola SHA* (spese condivise)[60].

Circa il profilo dell'eventuale applicazione di spese per l'utilizzo di un determinato strumento di pagamento, il *framework* di cui alla PSD2 è invece basato sulla considerazione che in generale era opportuna una revisione dell'approccio in materia di pratiche di *sucharging* già definito nella PSD1 (cfr. 52, par. 3), unitamente ad una sua maggiore armonizzazione a livello di regolamentazione nazionale delle pratiche stesse. In particolare è stato a tal fine tenuto presente, da un lato, che la diversità di prassi nazionali riscontrate in materia ha «portato a un'estrema eterogeneità del mercato dei

[59] Considerando n. 65 della PSD2.

[60] In particolare, le disposizioni in materia della PSD2 sono basate sull'assunto che è «opportuno prevedere che, di norma, le spese siano prelevate direttamente al pagatore e al beneficiario dai rispettivi prestatori di servizi di pagamento. L'importo di eventuali spese applicate può anche essere pari a zero in quanto è opportuno che le disposizioni della presente direttiva non influiscano sulla pratica secondo cui il prestatore di servizi di pagamento non addebita ai consumatori l'accreditamento sui loro conti. Analogamente, a seconda dei termini del contratto, il prestatore di servizi di pagamento può addebitare solo al beneficiario (commerciante) le spese di utilizzo del servizio di pagamento, nel qual caso non vengono imposte spese al pagatore. È possibile che i sistemi di pagamento applichino spese nella forma di una commissione di sottoscrizione. Le disposizioni sull'importo trasferito o su eventuali spese applicate non hanno alcun impatto diretto sulla determinazione dei prezzi tra i prestatori di servizi di pagamento o eventuali intermediari» (Considerando 65 della PSD2).

pagamenti nell'Unione e confond[e] i consumatori, in particolare nel settore del commercio elettronico e in un contesto transfrontaliero» e, dall'altro, che il citato Regolamento (UE) 2015/751 ha stabilito, giusto prima dell'approvazione della PSD2, anche dei *cap* armonizzati alle *interchange fees* per i pagamenti basati su carte (ossia per tipi di pagamenti per i quali i beneficiari tipicamente applicano il *surcharging* proprio per compensare i costi a loro carico per l'accettazione dei pagamenti stessi)[61], prevedendo tuttavia, al relativo art. 11, apposite disposizioni proprio in materia di libertà di 'orientamento' dei «consumatori verso l'uso di un qualsiasi strumento di pagamento preferito dal beneficiario»[62].

Ciò posto, benché nella prima parte dell'art. 62, par. 3, della PSD2 sia stato sostanzialmente 'rifusa' la prima parte del par. 3 dell'art. 52 della PSD1, tuttavia è stato ora inoltre disposto che ferma la libertà del «beneficiario di imporre una spesa o di proporre una riduzione al pagatore o di orientarlo in altri modi verso l'uso di un determinato strumento di pagamento», in ogni caso le spese a tal fine eventualmente addebitate al pagatore non devono mai superare «i costi diretti sostenuti dal beneficiario per l'utilizzo dello specifico strumento di pagamento».

Una specificazione quest'ultima che, nello stabilire ora un criterio uniforme in materia di *surcharcing*, è direttamente collegata proprio alle intervenute limitazioni nel frattempo imposte alle *interchange fees* ai sensi del Regolamento (UE) 2015/751 da cui si attende un effetto di forte riduzione dei costi per il beneficiario dell'accettazione di pagamenti basati sulle carte cui si applicano le limitazioni stesse.

Inoltre il collegamento con i *cap* alle *interchange fees* di cui al Regolamento (UE) 2015/751 è ancora più diretto laddove la PSD2 (al relativo art. 62, par. 4) introduce ora quello che risulta essere un vero e proprio divieto di *surcharge* a livello UE quanto meno «per l'utilizzo di strumenti di pagamento le cui commissioni interbancarie sono oggetto del capo II del regolamento (UE) 2015/751 e per i servizi di pagamento cui si applica il regolamento (UE) n. 260/2012» che stabilisce invece 'i requisiti tecnici e commerciali per i bonifici e gli addebiti diretti in euro'.

Infine, così come pure già previsto dalla PSD1, è altresì consentito agli Stati membri di adottare regimi regolamentari più stringenti in materia di *surcharging*, potendo questi ulteriormente «vietare o limitare il diritto del beneficiario di imporre spese tenendo conto della necessità di incoraggiare

[61] Cfr. Considerando 66 della PSD2.

[62] Cfr. Mezzacapo, *La nuova disciplina UE dei limiti alle* interchange fees *e delle* business rules *in materia di 'pagamenti basati su carte', tra regolamentazione strutturale del mercato interno e promozione della concorrenza*, cit., pp. 523 e 524.

la concorrenza e di promuovere l'uso di strumenti di pagamento efficienti».

Giusta tale ultima opziona nazionale, la scelta operata dal legislatore italiano in sede di recepimento della PSD1, e ulteriormente rafforzata in occasione del recepimento della PSD2, è stata proprio nel senso di generalizzare il divieto di *surcharge*, stabilendo quindi un regime in materia molto più restrittivo di quello UE (cfr. art. 3, del D. Lgs. 11/2010)[63].

A livello nazionale il divieto di *surcharge* è altresì previsto e ribadito, benché qui in chiave prettamente di tutela dei consumatori, dall'art. 62, co. 1, del *Codice del Consumo* secondo cui ai «sensi dell'articolo 3, comma 4, del decreto legislativo 27 gennaio 2010, n. 11, i professionisti non possono imporre ai consumatori, in relazione all'uso di determinati strumenti di pagamento, spese per l'uso di detti strumenti, ovvero nei casi espressamente stabiliti, tariffe che superino quelle sostenute dal professionista».

Circa la possibilità per i PSP coinvolti nell'esecuzione di un'operazione di pagamento di applicare 'deduzioni' a titolo di addebito di spese sull'importo effettivamente trasferito al beneficiario, una pratica questa invero «di fatto comune nell'ambito dei servizi di tesoreria/cassa delle banche a favore di amministrazioni pubbliche»[64], la PSD2 ribadisce che ciò deve essere vietato perché è «essenziale, per il trattamento completamente integrato e automatizzato dei pagamenti e per la certezza giuridica rispetto all'adempimento di eventuali obblighi sottostanti tra gli utenti di servizi di pagamento, che la totalità dell'importo trasferito dal pagatore sia accreditata sul conto del beneficiario», ferma la possibilità per il solo beneficiario di autorizzare il proprio PSP a dedurre le proprie spese, e queste soltanto, dandone di volta in volta dettagliata informativa al beneficiario stesso[65]. E' quindi al riguardo stabilito l'obbligo – in linea di principio – per tutti i PSPs coinvolti nell'effettuazione di una operazione di pagamento di trasferire «la totalità dell'importo dell'operazione» stessa, con contestuale e speculare

[63] In particolare l'art. 3, co. 4 del D. Lgs. 11/2010, come da ultimo novellato dal D. Lgs. 218/2017, stabilisce che il «beneficiario non può applicare a carico del pagatore spese relative all'utilizzo di strumenti di pagamento», sicché ne risulta che, in ossequio al principio generale in materia di spese, il beneficiario di un pagamento deve sostenere integralmente le spese allo stesso nel caso addebitate (dai PSPs di cui avvale) per il caso di utilizzo di strumenti di pagamento (diversi dal contante) e non può (ri)addebitarle al pagatore. Rispetto alla precedente formulazione dell'art. 3 del D.Lgs. 11/2010 la novella ha anche eliminato la precedente facoltà attribuita alla Banca d'Italia di stabilire (con proprio regolamento) eventuali deroghe al divieto «tenendo conto dell'esigenza di promuovere l'utilizzo degli strumenti di pagamento più efficienti ed affidabili»

[64] Ministero dell'Economica e delle Finanze, Dipartimento della Ragioneria Generale dello Stato e Dipartimento del Tesoro, Circolare n. 22 del 15 giugno 2018, p. 6.

[65] Cfr. Considerando 80 della PSD2.

divieto per gli stessi di «trattenere spese sull'importo trasferito», salva la suddetta facoltà a favore del solo beneficiario del pagamento e i relativi obblighi informativi a carico del relativo PSP (cfr. art. 81 della PSD2).

La *ratio* sottostante è sempre costituita dal principio per cui di regola il beneficiario e il pagatore debbono sostenere ciascuno *solo* le spese ad essi (eventualmente) direttamente addebitate dai rispettivi PSPs.

Nel caso delle PP.AA., in stretto punto di diritto la dovuta *compliance* con tali principi e regole in materia di addebito di spese richiede che tutti tali aspetti siano espressamente e coerentemente regolamentati nell'ambito delle relative convezioni di tesoreria/cassa, cosa che fino ad oggi è stata fatta in modo disomogeneo, integrando le convenzioni stesse degli elementi eventualmente mancanti e modificando se del caso le pattuizioni in conflitto.

Dal punto di vista invece delle ricadute sistemiche il portato diretto di tali disposizioni è che d'ora in avanti anche le PP.AA. dovranno corrispondere in modo esplicito e trasparente il prezzo dei servizi di pagamento alle stesse prestati dai relativi PSPs, dovendo pertanto «iscrivere nei propri bilanci stanziamenti specifici e adeguati ai quali imputare gli oneri»[66] conseguenti alla piena applicazione alle PP.AA. anche per questi aspetti del nuovo *framework* normativo dei servizi di pagamento definito dalla PSD2, giusta anche la menzionata abrogazione (ai sensi dell'art. 2, co. 39, del D.lgs. 218/2017) «a decorrere dal 1° gennaio 2019» del comma 6 dell'art. 37 del D. lgs. 11/2010.

Abstract

L'articolo mira a chiarire la collocazione e il ruolo sistemici, nell'ordinamento UE e nazionale, della più recente disciplina armonizzata UE dei servizi di pagamento nel mercato interno. A tal fine, l'analisi è principalmente focalizzata sulla ridefinizione, ai sensi della PSD 2, dell'ambito di applicazione di tali norme di settore e, soprattutto, sul relativo *dark side*, quale risultante quest'ultimo dalle disposizioni sul *negative scope* delle norme stesse. Specifica attenzione è infine riservata all'analisi dell'applicazione dei principi e delle regole del nuovo *framework* UE in materia con talune specificità dei servizi di pagamento che riguardano le pubbliche amministrazioni nazionali.

Parole chiave: PSD2, Servizi di pagamento, T*elecom exemption*, Reti limitate, Pagamenti delle pubbliche amministrazioni, Conti di tesoreria, Tempi di esecuzione, Regola SHA, S*urcharge*.

Abstract

The article aims at clarifying the systemic positioning and role, within the EU and Italian legal framework, of the latest EU harmonized regulation of payment

[66] Ministero dell'Economica e delle Finanze, Dipartimento della Ragioneria Generale dello Stato e Dipartimento del Tesoro, Circolare n. 22 del 15 giugno 2018, p. 6.

services in the internal market. To this end, the analysis is mainly focused on the redefinition, pursuant to PSD 2, of the scope of application of such sector rules and, primarily, on the relating 'dark side', the latter resulting from the provisions on the 'negative scope' of the same rules. Specific attention is finally reserved to the analysis of the application of the rules and principles of said new EU regulatory framework with certain 'singularities' of payment services involving Italian national public administrations.

Keywords: PSD2, Payment services, T*elecom exemption*, Limited networks, Payments of public administrations, Treasurer's accounts, Execution time, SHA rule, Surcharge.

Vito Meli

Opportunità e sfide per la concorrenza nella disciplina dei servizi di pagamento

Sommario: 1. Alcuni elementi di contesto e le opportunità per la concorrenza – 2. Il bilanciamento di interessi in Antitrust – 3. Che tipo di bilanciamento di interessi? – 4. Le sfide per le Autorità di concorrenza – 5. Conclusioni.

1. *Alcuni elementi di contesto e le opportunità per la concorrenza*

Il mio intervento non si dilungherà sull'analisi della PSD2, non potendo io aggiungere nulla a quello che hanno già detto e diranno i relatori molto più qualificati di me su questa materia.

Cercherò invece di delineare le categorie analitiche che l'Autorità di concorrenza applicherebbe nell'affrontare eventuali questioni di propria competenza connesse all'implementazione della PSD2.

Ma consentitemi prima di ricapitolare alcuni elementi, a tutti noti, che servono per introdurre le riflessioni sulla tutela e la promozione della concorrenza.

Da un lato, il recepimento e l'attuazione della PSD2 si inseriscono in un momento di grande interesse intorno allo sviluppo delle *fintech* e al fenomeno dei *big data*.

Le società che combinano la tecnologia con l'offerta di servizi finanziari sono quelle che possono trovare linfa vitale nelle innovazioni introdotte dalla PSD2, come vedremo oltre. Spesso tali società sono associate alle *start-up*, che pure costituiscono un tema di grande attualità. Tuttavia, la mia impressione è che le *fintech* che potrebbero lasciare il segno modificando il mercato si debbano individuare fra soggetti quali Apple, Google, Amazon, Facebook, AliBaba, ecc., ovvero fra imprese che non sono più *start-up* da molto tempo. E probabilmente anche fra imprese già del settore, quali

[*] Le opinioni espresse non impegnano in alcun modo l'Autorità di appartenenza.

Mastercard, che stanno puntando molto sull'innovazione.

Tali società, però, chiamano in causa il fenomeno dei *big data*, ovvero l'acquisizione e la valorizzazione di volumi enormi di dati, rinnovati di continuo, che vengono utilizzati in modo intelligente anche tramite algoritmi specifici. Tutte queste grandi realtà, infatti, sfruttano fra le altre cose l'immensa mole di informazioni accumulate con le rispettive attività e da queste, ovvero dai *big data*, traggono un vantaggio competitivo spesso essenziale per il loro successo e non facile da colmare per i concorrenti. Uno dei campi nei quali la profilazione dei clienti e l'accumulazione di informazioni circa le abitudini e altre caratteristiche degli stessi è più fecondo è proprio quello dei pagamenti elettronici, in quanto le transazioni commerciali sono rivelatrici di un'immensa mole di informazioni preziose.

Sicché, non si può discutere delle implicazioni concorrenziali della PSD2 senza tenere conto di questi altri due temi, quello delle *fintech* e dei *big data*, data l'interconnessione delle questioni.

Ma il recepimento della PSD2 si inserisce anche in un contesto di bassa redditività delle banche. Superata la fase più acuta della crisi dovuta agli NPL, molti commentatori sostengono che il problema di bassa reddittività delle banche non sia più riconducibile ad un fenomeno congiunturale, ma che esso oramai abbia assunto carattere strutturale, in una situazione di tassi di interesse comunque ancora bassi. Sulla redditività del sistema bancario nell'anno in corso abbiamo avuto segnali contraddittori e non mi vorrei addentrare in un'analisi che altri possono fare meglio di me. Credo però che non si possa negare che essa costituisca un tema di particolare rilievo, e che i bilanci delle banche potrebbero beneficiare significativamente del contributo dei servizi di pagamento.

Per il sistema bancario, quindi, il rilevante tasso di crescita del settore dei pagamenti, in forte espansione anche grazie all'*e-commerce* ed alla dinamica indotta dalle innovazioni tecnologiche, e la circostanza che tale tasso di crescita potrebbe essere ulteriormente accelerato dagli effetti della PSD2, costituiscono un'importante opportunità, anche per migliorare la propria redditività, oltre che per approfondire la relazione con il cliente.

Allo stesso tempo però è già stato osservato che il fenomeno delle *fintech* e i nuovi scenari introdotti dalla PSD2 possono generare un rischio di disintermediazione per le banche.

Infatti, è noto che la PSD2 regola l'ingresso di nuovi soggetti, in particolare le cosiddette 'terze parti' (TPP-*Third Party Providers*) e stimola la prestazione di nuovi servizi. Nel far ciò impone al sistema bancario di 'aprire' i conti correnti detenuti dai propri clienti; le banche dovranno consentire

l'accesso ai conti da parte dei TPP e questi potranno disporre pagamenti e fornire informazioni, se autorizzati dai clienti. Potranno così essere definiti e creati nuovi servizi ed anche i servizi di pagamento già esistenti potranno essere svolti da soggetti diversi e potranno essere frammentati in una serie di segmenti, ciascuno eventualmente svolto da un operatore diverso. In pratica, più di oggi, potrà essere inviato denaro e potranno essere effettuati pagamenti, anche via *chat* o comunque con lo smartphone, con effetti istantanei. Con il significativo abbattimento delle barriere all'ingresso nuovi operatori potranno intervenire in tali servizi. Essi potranno essere grandi e piccoli, ma è facile immaginare che un ruolo importante potranno giocarlo le grandi imprese che già operano nei mercati digitali, ovvero quelle alle quali abbiamo già fatto riferimento.

Non è del tutto intuitivo capire come la segmentazione fra svariati soggetti di servizi in precedenza svolti *end-to-end* dallo stesso operatore possa risultare più efficiente, ma da un lato occorre considerare che grazie all'innovazione i vecchi servizi potranno assumere nuove caratteristiche che li rendono completamente diversi nella loro funzionalità (si pensi al bonifico istantaneo) dall'altro, occorre semplicemente riconoscere che se la frammentazione dei servizi si afferma, ebbene vi devono essere ragioni di efficienza intrinseca che lo consentono, altrimenti il fenomeno difficilmente si verificherebbe.

Tutto ciò potrà condurre all'intensificarsi della concorrenza nel settore dei pagamenti, con possibili effetti benefici sul benessere dei consumatori e sull'efficienza, in termini di minori costi dei servizi, maggiore varietà degli stessi e più possibilità di scelta fra le imprese presenti sul mercato. Le Autorità di concorrenza non possono quindi che guardare con favore le prospettive che si aprono con la PSD2.

Pertanto, il nuovo contesto di fatto e giuridico che si potrà realizzare con la PSD2 e con i fenomeni cui si è accennato offre alle banche rinnovate opportunità in termini di recupero di redditività, ma anche nuovi rischi. Al riguardo voglio anche ricordare che la presenza di operatori non bancari nei servizi di pagamento non è certamente un fenomeno recente e che quindi non siamo in presenza di una novità assoluta. E consentitemi anche di rammentare che solo pochi anni fa si discuteva dell'imminente affermazione delle società telefoniche in una molteplicità di settori, fra cui quello dei pagamenti grazie alle sim prepagate, e che tale previsione non ha avuto quasi alcun seguito.

Inoltre, quanto all'effettiva penetrazione in ambito bancario/finanziario degli operatori innovativi e, in generale, delle relazioni *online* e delle nuove

tecnologie, le evidenze in possesso dell'Autorità Antitrust sembrano un po' in controtendenza, dato che conducono a ridimensionare fortemente l'attualità di tali fenomeni, che assumerebbero rilievo molto di più in prospettiva che nei comportamenti odierni.

Infatti, in relazione alla valutazione delle recenti concentrazioni bancarie connesse alla costituzione dei gruppi di credito cooperativo, l'Autorità ha svolto, tramite una società specializzata, una ricerca di mercato volta, fra l'altro, ad indagare le abitudini di consumo della clientela bancaria, anche al fine di approfondire la conoscenza dei mercati rilevanti.

L'indagine ci ha rappresentato un quadro piuttosto diverso dalle nostre aspettative, risultando che i consumatori sono, in media, molto tradizionali e che le *fintech,* allo stato, restano un fenomeno abbastanza confinato a mercati e clienti molto limitati. In sostanza, i consumatori accettano sempre di più la relazione *online*, ma sempre riservandosi la possibilità di mantenere un rapporto con uno sportello bancario (fisico), tanto che non rinunciano al servizio di prossimità, scegliendo di detenere necessariamente almeno un rapporto con un operatore vicino all'abitazione o al luogo di lavoro. Il fenomeno, peraltro, risulta comune, nell'esperienza dell'Autorità, ad altri mercati, nei quali pure sono state svolte indagini di mercato *ad hoc*. Ovviamente, l'indagine dell'Autorità ha fotografato l'oggi, non il domani. E quindi si può comunque affermare che il fenomeno *fintech* è importante, ma a tendere dato che, per ora, esso incide poco sulle dinamiche competitive dei mercati bancari e finanziari.

Quindi, per riassumere, dalla PSD2 e dallo sviluppo delle *fintech* e dei *big data* ci si attende un incremento della competizione, con la comparsa di nuovi soggetti e nuovi servizi. Tale prospettiva è vista con gran favore dalle Autorità di concorrenza, ma è anche fonte di opportunità e rischi per il mondo bancario.

A questo punto, prima di proseguire parlando delle ricadute che questi fenomeni potranno avere sull'attività dell'Autorità, consentitemi una deviazione e lasciate che mi soffermi brevemente sul titolo di questo convegno, che trovo particolarmente appropriato nel richiamare la necessità di un bilanciamento di interessi.

2. *Il bilanciamento di interessi in Antitrust*

Apparentemente, ovvero in un'opinione abbastanza diffusa, in tema di bilanciamento di interessi l'Autorità Antitrust non ha molti margini di manovra: estremizzando, essa applicherebbe le regole di concorrenza nell'ambito di un modello para-giurisdizionale, lasciando ad altre istituzioni il compito di intervenire, eventualmente, a mo' di contrappeso.

Non voglio dire che questo non accada mai. Si pensi al caso nel quale la tutela della concorrenza produca nel breve periodo l'uscita di una o più imprese dal mercato, con il conseguente intervento di sussidi di disoccupazione o di altri interventi che potremmo definire 'compensativi'. Ecco, in casi come questo le Autorità Antitrust agiscono tenendo conto specificamente dell'interesse pubblico riconducibile alla concorrenza e, quindi, lato sensu all'efficienza, mentre altri soggetti intervengono per garantire il soddisfacimento di altri interessi pubblici, quali il sostegno ai lavoratori ed alle famiglie nelle situazioni di crisi aziendale.

Tuttavia, in genere la prassi antitrust ha in sé anche molte possibilità di bilanciamento di interessi. Anzi in taluni casi si tratta di veri e propri obblighi. Ed è per questa ragione che sempre più la prassi antitrust si affida nelle proprie decisioni anche all'analisi economica.

Tutte le tre tipiche fattispecie antitrust – ovvero il controllo preventivo delle operazioni di concentrazione e la repressione delle intese illecite e degli abusi di posizione dominante – o contengono esplicitamente nel dettato normativo la possibilità di effettuare bilanciamenti delle restrizioni concorrenziali con i benefici complessivi di efficienza, oppure, come nel caso della repressione degli abusi di posizione dominante, questo tipo di valutazione viene oramai effettuata per prassi di derivazione comunitaria.

In particolare mi riferisco, nel caso delle concentrazioni, al Regolamento 139/2004 che fra le altre cose prevede che la valutazione dei singoli casi debba essere effettuata tenendo conto anche «dell'evoluzione del progresso tecnico ed economico purché essa sia a vantaggio del consumatore». E mi riferisco, nel caso delle intese, all'art. 101.3 del TFUE che esonera dal divieto le intese che, pur restrittive, «contribuiscano a migliorare la produzione o la distribuzione dei prodotti o a promuovere il progresso tecnico o economico, pur riservando agli utilizzatori una congrua parte dell'utile che ne deriva». Quanto alla figura dell'abuso di posizione dominante, basti citare tutti i molteplici casi nei quali – per prassi comunitaria – le Autorità di concorrenza che intervengono a sanzionare comportamenti escludenti da parte di imprese in posizione dominante nei confronti dei concorrenti,

devono dimostrare che questi ultimi non sono meno efficienti del soggetto dominante, effettuando il c.d. *as efficient test*.

Nell'ambito poi dell'attività consultiva dell'Autorità il bilanciamento di interessi è costante, nel senso che l'Autorità ha la facoltà discrezionale di attivare i propri poteri consultivi e quindi può decidere, anche in base al bilanciamento di interessi pubblici rilevanti, se attivarli o meno.

3. *Che tipo di bilanciamento di interessi?*

Sono fermamente convinto quindi che nel valutare sotto il profilo antitrust le questioni che potranno sorgere nell'ambito dei sistemi di pagamento a valle dell'implementazione della PSD2 l'Autorità sarà molto attenta ad effettuare gli opportuni bilanciamenti di interessi.

Occorre però esplicitare gli interessi che si devono considerare, definendone il perimetro. E' pacifico che sempre di più sia la normativa che la prassi antitrust comunitaria intendono tutelare la concorrenza avendo riguardo all'interesse ultimo dei consumatori finali. In passato e/o in altri contesti giuridici, la prassi antitrust ha spesso dato per presupposto che, in ultima analisi, la protezione dei concorrenti garantisse la tutela dei consumatori finali. In tali contesti le Autorità di concorrenza si sono comportate di conseguenza, applicando il paradigma dettato da una teoria economica oggi superata. Attualmente questa presunzione non può più esservi e si possono proteggere i concorrenti solo laddove sia possibile presumere (appunto, sulla base di ragionamenti economici) che, in ultima analisi, ciò produca benefici anche per i consumatori.

4. *Le sfide per le Autorità di concorrenza*

Tornando quindi alla PSD2, come si diceva ci si può attendere un incremento della concorrenza, dovuta all'ingresso dei nuovi operatori e allo sviluppo di nuovi servizi, e ci si può aspettare l'insorgere di questioni che possano anche coinvolgere direttamente le competenze dell'Autorità. Mi riferisco ovviamente a comportamenti che non siano riconducibili esclusivamente alla competenza dell'Autorità di vigilanza.

Naturalmente, non è possibile prevedere quali sono le questioni che

si potrebbero porre, né, tanto meno, è possibile anticipare la posizione che l'Autorità Antitrust potrebbe assumere, e se anche lo fosse non me ne sarebbe consentito parlarne. Però credo sia utile ragionare sul tipo di questioni si potrebbero porre e sulle categorie logiche e giuridiche che l'Autorità potrebbe adoperare nel valutarle. Tenendo sempre presente che tale valutazione non potrebbe non considerare il bilanciamento di interessi di cui si è detto e nel far ciò si muoverebbe secondo i principi delineati.

Come si diceva, è facilmente prevedibile che l'apertura di una serie di servizi a nuovi operatori possa condurre a tensioni, anche di specifica competenza Antitrust. Del resto, già in passato sono pervenute all'Autorità alcune denunce da parte di operatori che ritenevano di essere ostacolati dalle banche nel loro ingresso nel mondo dei pagamenti. L'incerto inquadramento normativo di tali attività nell'ambito della PSD, insieme ad altre considerazioni, aveva condotto l'Autorità a non intervenire. Ora, con la PSD2, si è fatta chiarezza e risulta pacifico che una serie di servizi possano essere forniti e che vi debba essere la collaborazione delle banche.

Pertanto, eventuali ostacoli del mondo bancario all'ingresso dei nuovi operatori, oltre a poter condurre a valutazioni dell'Autorità di vigilanza, potrebbero astrattamente configurare illeciti antitrust laddove si trattasse di comportamenti concordati fra le banche, che potrebbero ricadere nel divieto di intese restrittive della concorrenza. In questi casi la valutazione delle Autorità di concorrenza è piuttosto 'standardizzata' e difficilmente sarebbe possibile qualunque tipo di bilanciamento di interessi: la collusione esplicita volta all'esclusione dei concorrenti è una fattispecie vietata grave che molto molto difficilmente potrebbe trovare giustificazioni in termini di beneficio ai consumatori tali da consentire di riconoscerne la liceità.

Sempre con specifico riferimento esclusivamente ai profili di concorrenza, diverso è il caso di eventuali ostacoli all'ingresso dei nuovi operatori (o allo svolgimento di nuovi servizi) posti individualmente dalle banche. Tipicamente i comportamenti unilaterali sono sottoposti allo scrutinio antitrust solo se realizzati da soggetti in posizione dominante, potendo in questi casi costituire degli abusi. Al riguardo rileva osservare che, salvo specifiche situazioni locali o specifici mercati del prodotto, nessuna banca in Italia detiene una posizione dominante e ciò condurrebbe ad escludere che eventuali comportamenti individuali possano ricadere nella figura dell'abuso di posizione dominante. C'è anche da osservare, però, la particolare posizione che ciascuna banca detiene in relazione all'accesso al conto dei propri clienti, assimilabile per certi versi alla già acclarata posizione di monopolio che detengono gli operatori telefonici nella terminazione delle

chiamate. Pertanto – pur senza considerare gli strumenti dell'Autorità relativi alla repressione delle pratiche scorrette – non si può escludere che eventuali comportamenti individuali possano essere ricondotti anche alla figura dell'abuso di posizione dominante, sebbene non mi risultano precedenti analoghi in questo settore e pertanto non ci muoveremmo nell'ambito di una fattispecie classica, bensì ci troveremmo a dover affrontare un tema nuovo, certamente controverso.

D'altro canto, come abbiamo visto, i nuovi entranti nei mercati dei servizi di pagamento potrebbero essere anche soggetti già dotati, in altri settori, di significativi vantaggi competitivi. Mi riferisco alle cosiddette *over the top* già menzionate, le quali potrebbero far leva sul potere di mercato che detengono altrove per entrare nei servizi di pagamento. Naturalmente, lo sfruttamento dei vantaggi competitivi acquisiti in altri mercati è un fenomeno che nella stragrande maggioranza dei casi non produce effetti restrittivi sotto il profilo antitrust. Tuttavia, la situazione è ben diversa se il nuovo entrante detiene nel mercato di provenienza una posizione di dominanza. In tali casi, vi possono essere i presupposti per valutare l'ipotesi dell'abuso di posizione dominante. Senza entrare nel dettaglio di un tema che dà abbastanza da discutere alla comunità antitrust, mi limito a segnalare che proprio la definizione della posizione di mercato di soggetti quali Google, Facebook ed Amazon pone delle questioni di non immediata soluzione.

Se, da un lato, vi sono precedenti comunitari che hanno in qualche modo 'sistematizzato' la posizione di alcuni di tali operatori, definendo i mercati rilevanti ed individuando l'eventuale posizione di dominanza in essi detenuta, vi è ancora dibattitto su come inquadrare nell'analisi antitrust non l'attività specifica di ciascuno di tali operatori bensì l'enorme volume di informazioni che essi detengono, i *big data*, che può avere una valenza trasversale nei mercati. Questo sarà uno dei temi da approfondire in futuro, e sarà certamente trattato anche dall'indagine conoscitiva che l'Autorità sta svolgendo insieme all'Agcom ed al Garante per la privacy.

Infine, credo sia da segnalare che dal mondo bancario provengono anche voci che lamentano una presunta disparità di trattamento degli enti creditizi a favore dei nuovi operatori, asimmetria che farebbe operare la concorrenza in una situazione di squilibrio. Tipicamente, gli interventi dell'Autorità volti a garantire che i mercati siano caratterizzati da un *level playing field* sono interventi di *advocacy*, ovvero sono pareri resi ai soggetti competenti (legislatore o regolatore che sia). Si tratta dunque di un'attività diversa dagli interventi di *enforcement*, basati sui poteri istruttori dell'Autorità, dei quali si è discusso in precedenza. Nell'ambito delle segnalazioni l'Autorità ottiene

un notevole successo con i propri interlocutori: le statistiche ci dicono che in media i nostri pareri sono accolti favorevolmente, e quindi sono attuati, complessivamente in oltre il 50% dei casi, ma per alcune categorie di segnalazione il tasso di successo sale anche oltre il 75% dei casi.

Dal punto di vista metodologico, in relazione all'eventuale opportunità di attivare i poteri di segnalazione dell'Autorità per questo tipo di vicende, mi sembra utile condividere una riflessione che ci conduce nuovamente alla necessità di un bilanciamento di interessi.

Nell'esprimere i propri pareri sulle regole che definiscono le caratteristiche dei mercati e dei soggetti che vi operano, l'Autorità Antitrust tiene sempre in conto le esigenze che hanno originato la configurazione di determinate regole ed effettua una valutazione di proporzionalità. Con ciò voglio dire che la necessità di garantire il *level playing field* riguarda più propriamente i mercati, non i soggetti che vi operano, ovvero per chi svolge la stessa attività devono in generale valere le stesse regole. Ma se un soggetto svolge anche altre attività, esso potrà essere sottoposto anche ad altre regole, eventualmente più stringenti.

Calato nella realtà in esame, ciò significa che è ben possibile che le banche – che operano nella raccolta, oltre che nei servizi di pagamento – siano sottoposte a regole prudenziali più onerose di quelle degli intermediari finanziari (come peraltro avviene da moltissimo tempo) proprio in ragione delle diverse attività che esse svolgono. Naturalmente, con ciò non si vuole dirimere la questione in un modo o in un altro; sarà da valutarsi se effettivamente vi siano regole specifiche e non proporzionali che rendono i mercati dei servizi di pagamento dei terreni di gioco non piani, partendo sempre dal presupposto che per i medesimi servizi dovrebbero valere le medesime regole.

5. *Conclusioni*

In conclusione, la PSD2 e i fenomeni collegati lasciano intravedere grandi opportunità per la concorrenza, che si dovrebbe intensificare, assicurando ai clienti prezzi più bassi e servizi innovativi e migliori. Le opportunità per la concorrenza potranno anche trasformarsi in sfide per le Autorità Antitrust, nella misura in cui si misureranno sul campo di gioco soggetti estremamente diversi, ovvero banche e *fintech*, le quali potranno essere piccole *start-up*, ma anche soggetti molto grandi, dotati di un proprio rilevante potere di

mercato, acquisito in altri settori. Alcune delle possibili ricadute antitrust di tale confronto rientrano nelle figure tipiche del diritto della concorrenza; altre potranno richiedere nuove analisi, sulle quali peraltro la comunità antitrust già riflette e produce i primi risultati.

Per quanto riguarda le banche, che sono poi le vere protagoniste dei mercati dei servizi di pagamento, abbiamo visto che si prospettano opportunità e rischi. È stato evidenziato da più parti il ritardo con il quale i *player* tradizionali si starebbero muovendo in questi ambiti, con il conseguente rischio di essere rimpiazzati dai nuovi operatori. D'altro canto, se si chiede alle banche di calarsi nelle nuove dinamiche concorrenziali, di fare fronte alle sfide poste dai nuovi operatori e dalle nuove tecnologie (ad esempio aprendo i conti correnti all'accesso delle terze parti), se si chiede loro essenzialmente di intraprendere un percorso di efficientamento e di svecchiamento, ebbene dall'altro lato, occorrerebbe anche rinunciare all'atteggiamento emerso in talune occasioni che porta a richiedere al sistema bancario di farsi carico di interessi pubblici – certamente meritori – ma che sono appunto pubblici e che non possono essere caricati sulle spalle delle imprese private, se non realizzando effetti distorsivi nei mercati, con il rischio anche di imporre il pagamento dei relativi costi a determinate categorie di consumatori invece che alla fiscalità generale.

Abstract

L'entrata in vigore della PSD2 e i fenomeni collegati – con l'ingresso sui mercati dei pagamenti di nuovi attori e lo sviluppo di nuovi servizi – consentono di prevedere grandi opportunità per la concorrenza. La competizione si intensificherà e assicurerà ai clienti prezzi più bassi, servizi innovativi e migliori. Tuttavia, le opportunità per la concorrenza potranno anche trasformarsi in sfide per le Autorità Antitrust, nella misura in cui si misureranno sul campo di gioco soggetti estremamente diversi, ovvero banche e fintech, le quali potranno essere piccole start-up, ma anche soggetti molto grandi, dotati di un proprio rilevante potere di mercato, acquisito in altri settori. Alcune delle possibili ricadute di tale confronto rientrano nelle figure tipiche del diritto della concorrenza, quali la repressione delle intese restrittive e degli abusi di posizione dominante. Altre potranno richiedere nuove analisi, ad esempio sulla definizione dei mercati rilevanti. Anche i poteri di advocacy potranno essere chiamati in causa nella misura in cui si determineranno situazioni distorsive della concorrenza.

Parole chiave: PSD2, Concorrenza, Servizi di pagamento, Autorità Antitrust, Fintech.

Abstract

The entry into force of PSD2 and of several phenomena related to it – that will result both in the appearance of new actors in the payment market and

in the development of new services – is likely to create great opportunities for competition. The competition will intensify, thus providing customers with lower prices and better, more innovative services. Nevertheless, the opportunities for competition could become challenges for the Antitrust Authorities. The new actors are bound to differ significantly. Fintech firms could be small start-ups or larger institutions with a significant market power, previously acquired in other sectors. Some of the possible effects of the interaction between banks and Fintech fall within the established patterns of competition law: for example, the repression of restrictive practices and the abuse of a dominant position. Other cases will probably require further analysis; namely, those relating to the definition of relevant markets. Furthermore, should scenarios of market distortion occur, even advocacy powers could be invoked.

Key words: PSD2, Competition, Payment services, Antitrust Authority, Fintech.

Daniele De Paoli

PSD2 e privacy

Sommario: 1. Il problematico disallineamento della disciplina Privacy e PSD2 – 2. Le novità del GDPR e possibili soluzioni per un migliore coordinamento – 3. La centralità della sicurezza e la nuova disciplina dei '*data breach*' – 4. I primi riscontri empirici e riflessioni conclusive.

1. *Il problematico disallineamento della disciplina Privacy e PSD2*

Il Garante per la Protezione dei Dati Personali è impegnato in questo periodo nella complessa fase di implementazione delle nuove norme europee, più faticosa del previsto anche per i fenomeni di disallineamento delle molteplici normative, fra cui quella riguardante la Direttiva PSD2 (Dir. 2015/2366), già trattati dai relatori intervenuti prima di me.

La questione è stata affrontata anche dal Coordinamento delle Autorità europee, che ha operato nel tentativo di superare le difficoltà che si incontrano nella lettura di alcune disposizioni della Direttiva PSD2 in rapporto con il Regolamento UE 2016/679 (c.d. GDPR), dal 25 maggio pienamente efficace.

Pensiamo ad esempio ad alcune 'scivolate', come la definizione dei dati implicati nelle operazioni di pagamento come dati di tipo 'sensibile', che è sicuramente un errore dal punto di vista giuridico, e che dimostra l'assenza di dialogo fra parti importanti dell'apparato comunitario.

Altro elemento di possibile confusione è quello relativo al consenso. Qui è opportuno distinguere tra consenso contrattuale, che è dovuto e previsto, e c.d. consenso privacy, che non sarebbe necessario in situazioni di trattamento nelle quali sono in gioco dati che possono essere trattati dai vari titolari del trattamento anche sulla base della clausola del c.d. legittimo interesse del titolare del trattamento, previsto dal nuovo Regolamento all'art. 6, par. 1, lett. f).

È interessante ricordare come l'Autorità sia venuta a conoscenza, meno

* Il presente scritto, pur rivisto dall'autore, conserva il carattere colloquiale dell'intervento originale al convegno.

di un anno fa, di questo problema del disallineamento. Il tema è stato posto al Garante dall'ABI che aveva la necessità di informare gli associati in merito alle nuove disposizioni (se chiedere un altro consenso, se e come aggiornare le informative ecc.). Ma tutto questo è avvenuto mentre in modo affrettato si stava concludendo il percorso di recepimento italiano della Direttiva PSD2, tanto che le sollecitazioni dell'ABI al Garante sono arrivate lo stesso giorno in cui veniva adottato il Decreto di recepimento della PSD2.

Come Autorità, in questo contesto, non potevamo fare molto. Abbiamo comunque interessato la Presidenza del Consiglio e il MEF e abbiamo fatto capire che sarebbe stato importante ridiscutere sui vari tavoli competenti il tema giustamente posto dagli operatori.

È utile sottolineare che la vicenda del disallineamento, in ambito italiano, è avvenuto in vigenza del Codice privacy del 2003.

In tale quadro normativo l'Autorità Garante aveva il potere di esprimere pareri - obbligatori anche se non vincolanti - solo rispetto alla normazione secondaria (regolamenti, decreti ministeriali, ecc.).

2. *Le novità del GDPR e possibili soluzioni per un migliore coordinamento*

Una significativa novità, che sottolineo per indicare un orizzonte nuovo che si apre per l'Autorità, è data dal fatto che le nuove norme prevedono l'interlocuzione con il Garante anche in fase di produzione di fonti primarie. Quindi un rapporto con il Parlamento, o con il Governo nel momento in cui elabora, ad esempio, decreti legislativi, molto più intenso e articolato di quanto avvenuto finora. Tutto ciò dovrebbe permettere di meglio 'costruire' la normativa, soprattutto quando ci troviamo in presenza di plessi normativi complessi, intersecati con altre normative (proprio come nel caso della PSD2).

Ovviamente sono disposizioni che stanno vivendo le prime settimane di applicazione, come vediamo rispetto a due situazioni in fase di elaborazione normativa e finite in questi giorni al centro dell'attenzione mediatica.

Parlo, da un lato, del progetto legislativo che mira ad introdurre forme più incisive di controllo per i lavoratori pubblici, riguardo alla loro presenza sui posti di lavoro, attraverso l'utilizzo anche di dati di tipo biometrico, dall'altro della generalizzazione dell'utilizzo della videosorveglianza negli asili nido e nelle case di cura.

Tornando al nostro tema, al di là dei problemi interpretativi, mi concentrerei sugli aspetti della disciplina privacy del nuovo Regolamento

che possono incidere ed essere interessanti per verificare l'azione che gli attori di questa catena complessa della PSD2 (banche, nuovi operatori dei sistemi di pagamenti, intermediari vari, ecc.) si troveranno ad intraprendere.

3. *La centralità della sicurezza e la nuova disciplina dei* 'data breach'

L'elemento centrale al quale noi presteremo particolare attenzione è sicuramente l'elemento della 'sicurezza'. Sono in gioco grandi quantità di dati, dati che coinvolgono pesantemente le persone, il portafoglio delle persone, perché - come ha precisato il dottor Meli - le banche devono aprire i conti correnti dei propri clienti. Questa espressione corrisponde a quello che realmente si verifica e che dovrà necessariamente avvenire con una serie di presidi di sicurezza adeguati, tali da impedire che non si apra il conto di fronte a chi non è il titolare o comunque colui che esprime la volontà di avvalersi di quel servizio.

Questa è una tipica problematica di sicurezza e non a caso è uno dei perni su cui ruota il Regolamento. Anche la magica parola *accountability* – responsabilizzazione - di fatto si declina in una sequenza di domande del tipo: sono in grado nel momento in cui tratto dati così delicati, così significativi, di garantire un livello di sicurezza che limiti il più possibile *hackeraggi*, interventi illeciti interni o esterni, non danneggi il cliente, non comporti un danno d'immagine ecc.?

La tradizione precedente della disciplina di protezione dati si è basata, per quanto riguarda le misure di sicurezza, nell'esperienza italiana, sul rispetto delle indicazioni contenute nel famoso Allegato B annesso al Codice privacy che fissava le 'misure minime' di sicurezza che il titolare del trattamento doveva adottare, almeno per non incorrere in sanzioni penali. Mediamente il titolare del trattamento si accontentava di questo.

Questo meccanismo è stato in passato criticato, anche perché mai aggiornato nel corso degli ultimi 15 anni, ma aveva ovviamente una sua praticità di utilizzo: dato un set minimo di misure, le applico e sono tranquillo.

Adesso, se ci riferiamo all'art. 32 del Regolamento europeo sulla sicurezza, il terreno comincia a mancare, perché il riferimento è fatto a categorie assolutamente generali: l'adeguatezza, l'aggiornamento, lo stato dell'arte, la verifica della resilienza dei sistemi, ecc..

Cosa significa questo, in concreto, nel mondo dei nuovi servizi di pagamento? A che punto posso considerarmi in regola?

Questa è la frontiera sulla quale ognuno si trova per evitare il rischio del *data breach* (art. 33), cioè la violazione dei dati personali.

4. *I primi riscontri empirici e riflessioni conclusive*

Al riguardo, abbiamo i primi dati delle denunce di *data breach* fatte a 4-5 mesi dall'adozione delle nuove regole.

In precedenza, la segnalazione delle violazioni di dati personali non era presente nella legislazione italiana, più precisamente l'obbligo gravava, per effetto di un'altra disposizione comunitaria, solo sulle imprese di telecomunicazione.

Il Regolamento generalizza l'obbligo di denuncia dei casi di violazione dei dati personali a tutti i titolari del trattamento.

Sono arrivate finora 400 segnalazioni.

C'è un po' di tutto (*hackeraggi*, furti di *devices* o altri strumenti contenenti dati personali, errori umani). Teniamo presente che circa un anno fa, in era pre-GDPR, uno dei più grossi gruppi bancari italiani ci aveva segnalato una violazione di dati che, partita da un'ipotesi di perdita dati di circa 200 mila correntisti, fortunatamente solo dati anagrafici, in realtà, completate le verifiche, si era estesa fino ad un totale di 700.000 soggetti. E, cosa interessante, il buco non si era verificato nel perimetro interno dell'istituto di credito interessato, ma presso una società esterna responsabile del trattamento, alla quale erano stati affidati incarichi tutto sommato abbastanza limitati. A causa della debole struttura informatica di questo soggetto, si è però aperta una 'porta' (informatica) che ha determinato la fuoriuscita delle informazioni.

Questa è una situazione che segnalo perché, rispetto all'aspetto sicuramente positivo dell'ingresso di nuovi soggetti e dell'offerta di nuove possibilità previste dalla PSD2, con questa realtà dobbiamo fare i conti. Se è già difficile controllare soggetti più strutturati, più tradizionalmente abituati ad avere cura dei propri dati come sono le banche, sicuramente l'attenzione deve essere moltiplicata nei confronti di soggetti nuovi che entrano su questo mercato, magari senza adeguate cautele.

A margine del discorso sui *data breach* possiamo poi ricordare una tematica che nel campo dei dati finanziari è estremamente rilevante, quella dei furti di identità. Un tema di cui nessuno ama parlare perché nessuno vuole ammettere che sono stati persi dati con i quali si sono sottoscritti

contratti, ecc. La casistica è però tuttora diffusa soprattutto nell'ambito del credito al consumo.

Un altro tema sul quale bisognerà maturare riflessioni ed esperienza è il modo col quale il trattamento dei dati da parte degli attori, anche nuovi, si rapporterà all'esercizio dei diritti degli interessati. Su questo punto particolare attenzione va prestata al nuovo diritto alla portabilità dei dati personali che apre nuove prospettive per gli interessati anche nella logica di favorire il passaggio da un operatore ad un altro in chiave anticoncorrenziale.

Vi ringrazio per l'attenzione.

Abstract

Nel breve intervento sono stati sottolineati innanzitutto alcuni aspetti che evidenziano il disallineamento (almeno a livello terminologico) fra la Direttiva PSD2 ed il coevo Regolamento generale sulla protezione dei dati (GDPR). Situazione già rilevata dalle Autorità europee di protezione dei dati, specie con riferimento all'uso improprio della categoria del consenso.

In chiave applicativa, si evidenzia poi come la principale preoccupazione sia quella di assicurare un'alta qualità dei dati trattati, in un contesto in cui occorre soprattutto prevenire i furti di identità ed evitare le perdite (dolose o colpose) di dati. Il nuovo Regolamento europeo pone infatti particolare attenzione alla prevenzione dei rischi dei c.d. data breach.

Parole chiave: Regolamento generale sulla protezione dei dati, GDPR, PSD2, Consenso, Violazione dei dati personali, Data breach, Privacy, Sicurezza dei dati.

Abstract

The short speech analyses some aspects that highlight the misalignment (at least at the terminological level) between the PSD2 directive and the General Data Protection Regulation (GDPR), already addressed by the European Data Protection Authorities, with specific reference to the use of the notion of consent. From a practical point of view, it highlights the main concern of the Authority: ensuring the high quality of the processed data, while preventing the identity theft and the loss of data due to fraud or negligence. The new European Regulation pays particular attention to the prevention of the risks of the so-called data breach.

Keywords: General data protection regulation, GDPR, PSD2, Consent, Personal data breach, Privacy, Data security.

Domenico Gammaldi

La sicurezza degli strumenti e del mercato dei pagamenti

Sommario: 1. I prodromi normativi e tecnologici della PSD2 – 2. Dalla PSD1 alla PSD2: il *fil rouge* del quadro regolamentare – 3. Il ruolo e il contributo della *European Banking Authority.*

1. *I prodromi normativi e tecnologici della PSD2*

Il presente contributo mira a sviluppare, nell'ambito del delicato rapporto fra innovazione e regolamentazione, il tema della sicurezza degli strumenti e del mercato dei pagamenti. Nell'affrontarlo vorrei contestualizzare alcune scelte operate dalla Direttiva PSD2 nella più ampia evoluzione che ha interessato il mercato dei pagamenti negli ultimi anni, nei quali ha trovato realizzazione l'Area Unica dei Pagamenti europei (la SEPA), e il quadro regolamentare definito dalla Direttiva sulla sicurezza cibernetica. Peraltro, la definizione della normativa PSD2 e IFR ha visto forti progressi proprio nel semestre italiano di Presidenza dell'Unione europea.

La relazione fra innovazione e regolamentazione nell'ambito dei pagamenti è legata all'accelerazione che l'evoluzione tecnologica applicata ai servizi finanziari ha registrato negli ultimi anni e che ha inciso profondamente sull'ecosistema dei pagamenti che, avendo le caratteristiche proprie di una economia di rete, vede coinvolti in un unico disegno tutti gli attori, finanziari e non finanziari.

Occorre però individuare con maggior dettaglio a quale ecosistema ci si voglia riferire e per farlo partirei da due definizioni molto generali di pagamenti e tecnologia.

I 'pagamenti' possiamo definirli come un trasferimento di fondi con il quale un pagatore (o debitore) estingue un'obbligazione nei confronti di un beneficiario (o creditore). I sistemi di pagamento e regolamento, all'interno dei quali si completa il processo, svolgono dunque un ruolo importante

* L'autore desidera ringraziare i colleghi della Banca d'Italia che lo hanno aiutato a preparare questo intervento con un costante e proficuo confronto di idee.

per la stabilità e l'efficienza del sistema finanziario e per l'economia nel suo complesso e la stessa conduzione della politica monetaria presuppone l'esistenza di infrastrutture affidabili ed efficienti.

I pagamenti, e in particolare quelli elettronici connessi all'*e-commerce*, si basano su processi complessi anche se sempre più spesso il pagamento, in quanto servizio finanziario, viene percepito dagli agenti economici come un aspetto accessorio, marginale, rispetto alla transazione 'commerciale' che lo genera.

Si parla di 'diluizione' del servizio nel processo più ampio che parte dal bene da acquisire. Il cliente sceglie 'come' pagare nell'ambito delle diverse modalità che vengono prospettate dal venditore del bene; il pagamento completa una transazione commerciale ma la scelta del consumatore è 'condizionata' da 'cosa' ha comprato e con quale 'modalità' (se in un negozio fisico piuttosto che su un sito di *e-commerce* o tramite una app su un *device mobile*), non da un asettico confronto fra strumenti/soluzioni.

Forse ci siamo sempre concentrati su cosa comprare e sulla disponibilità di fondi piuttosto che sulla modalità di pagamento, ma oggi vi è un *gap* sempre più grande fra complessità del processo di pagamento e conoscenza dello stesso processo da parte dell'utente.

Credo che solo gli addetti ai lavori si rendano pienamente conto di quale complessità vi sia nell'inserire, su una applicazione o un sito, il numero di una carta di credito, un codice di sicurezza, un *touch* su 'invia' che ci impegna a pagare.

La Tecnologia, con la T maiuscola, nella definizione che ne dà il vocabolario «indica le tecniche utilizzate per produrre oggetti e migliorare le condizioni di vita dell'uomo: non si tratta quindi solo di realizzazioni concrete, ma anche di procedure astratte. La tecnologia ha un legame molto stretto con la scienza, di cui non è un semplice aspetto applicativo. La storia della tecnologia si intreccia con la storia dell'umanità: in particolare negli ultimi secoli il progresso tecnologico ha iniziato a correre a velocità sempre maggiori».

Oggi la tecnologia è Diversificata, Disponibile e Diffusa: la diversificazione è connessa alla pluralità di operatori che offrono i vari servizi di pagamento, non solo le banche ma anche gli istituti di pagamento, i soggetti che offrono servizi per iniziare i pagamenti o quelli di accesso ai conti; la disponibilità del servizio implica una connessione 24 ore su 24, tutti i giorni dell'anno; la diffusione è legata alla numerosità di *device* con i quali è possibile operare (*tablet*, *smartphone*, Internet, *smartwatch*), ma anche alla continua proposizione di nuove soluzioni o di nuove applicazioni di tecnologie note.

Siamo di fronte ad un contesto complesso in cui è difficile individuare

esattamente il perimetro regolamentare; tale individuazione, se troppo rigida o estesa, potrebbe non rendere immediatamente evidenti i possibili benefici dell'innovazione.

2. *Dalla PSD1 alla PSD2: il* fil rouge *del quadro regolamentare*

Un giovane imprenditore, nel corso di un suo intervento, riconduceva alle previsioni della PSD1 l'emergere di un contesto regolamentare che aveva ampliato gli spazi per l'avvio di attività imprenditoriali nell'ambito del segmento pagamenti; da 'regolatore' è stata una grande soddisfazione, spesso le affermazioni sono di tutt'altro tenore. Tutti si lamentano che la regolamentazione blocca l'innovazione. La PSD1 è stata una scommessa 'regolamentare' vinta: la proposta del 2005 viene approvata nell'aprile 2007 e il primo *smartphone*, ovvero il modo per avviare un'innovativa interazione con il cliente/consumatore, è dell'agosto dello stesso anno. Il quadro regolamentare è riuscito a gestire, non senza qualche affanno, dieci generazioni di *device*, grazie alla tecnica normativa adottata e alla capacità dei regolatori di ottimizzare gli spazi interpretativi consentiti; spero che anche la PSD2 riesca a dare risposte all'evoluzione futura.

La PSD2 ha nella sua impostazione elementi di auto-aggiustamento laddove ha previsto un ruolo attivo dell'EBA per l'emanazione di un quadro regolamentare di secondo livello (*regulatory technical standards* e linee guida) armonizzato fra tutti i paesi dell'Unione: in tal modo si è data una risposta sia alla maggiore competitività, in quanto sono stati ridotti gli spazi di 'disallineamento' normativo, sia all'evoluzione tecnologica, potendo l'EBA intervenire sulle regole da lei stessa definite.

La PSD2 fa parte di un ecosistema regolamentare che parte dalla SEPA e trova il suo completamento nel Regolamento IFR [Reg. (UE) n. 575/2013 del Parlamento Europeo e del Consiglio, del 23 giugno 2013, relativo ai requisiti prudenziali per gli enti creditizi e le imprese di investimento] e nella Direttiva NIS [Dir. (UE) 2016/1148 del Parlamento Europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi dell'Unione] per gli aspetti di *cybersecurity*.

L'innovazione pone al centro del dibattito fra i regolatori l'opzione se agire sui soggetti o sulle attività; la PSD2, ancor più della precedente PSD1, è un grande contenitore in cui non viene fatta una scelta definitiva ma si decide di agire sia sui soggetti sia sulle attività, intervenendo anche su aspetti

tecnologici, quali le previsioni in materia di API (A*pplication Programming Interfaces*), per facilitare la nascita di un contesto competitivo.

Il *fil rouge* che sottende le scelte regolamentari operate dalla Direttiva è favorire lo sviluppo tecnologico in un contesto di certezza, fiducia e sicurezza in cui la definizione dei servizi di pagamento è neutra sotto il profilo tecnologico per consentire «lo sviluppo di nuovi tipi di servizi di pagamento, garantendo pari condizioni operative ai prestatori di servizi di pagamento esistenti e ai nuovi prestatori» (considerando 33, PSD2).

Questa neutralità tecnologica però non deve esimere dal verificare se le potenzialità legate alle nuove tecnologie non possano facilitare l'adozione di presidi regolamentari innovativi. Può aiutarci un'esemplificazione. Tutta la regolamentazione sul reporting, per l'esigenza delle Autorità di disporre di dati, negli anni si è evoluta dall'invio di moduli cartacei a soluzioni informatizzate. La disponibilità di soluzioni tecnologiche innovative per la gestione dei processi, quali la DLT, possono far ipotizzare scenari in cui vi sia un accesso diretto delle Autorità alle informazioni sui cc.dd. nodi della *chain*, con un diverso costo del *reporting*.

Altra riflessione è sul concetto di standard e anche in questo caso un'esemplificazione può aiutare. La SEPA è 'uno' standard, ma non è 'lo' standard; sottolineo l'articolo indeterminativo e non determinativo. Oggi tutti gli operatori per effettuare bonifici adottano lo standard messo a punto dall'EPC ma il regolamento SEPA non preclude l'esistenza, a certe condizioni di un altro standard. Questa possibilità, se da un lato si pone in contrasto con il principio dell'integrazione del mercato, dall'altro è il 'lievito' dell'innovazione dove, almeno in una prima fase, un certo grado di frammentazione è fisiologico.

La PSD2 ha due grandi anime: i diritti, dei prestatori e degli utilizzatori dei servizi di pagamento, e la sicurezza, che è funzionale ai diritti in quanto è il primo presidio alle tutele; per comprenderle appieno occorre richiamare alcuni tratti della PSD1.

Nel suo impianto, la prima Direttiva ha definito un quadro regolamentare univoco per i servizi di pagamento per assicurare maggiore tutela agli utenti e aumentare la trasparenza, per sviluppare l'utilizzo degli strumenti di pagamento alternativi al contante e ampliare il novero degli operatori offerenti i servizi. In questa impostazione, definisce i servizi di pagamento, i soggetti che possono offrirli e, nel contempo, i criteri di massima per l'individuazione di soggetti e servizi esclusi. Le modalità applicative venivano rimesse alle Autorità nazionali.

Nel definire gli istituti di pagamento come una nuova categoria di

intermediari, la PSD1 introduceva un elemento che si poneva in forte discontinuità con il passato. Per questi operatori il sistema di vigilanza era reso compatibile con un oggetto sociale 'ibrido', non esclusivamente finanziario; difatti, pur in presenza di regole di natura prudenziale applicabili ai soggetti, introduceva un controllo per attività, focalizzato sui servizi di pagamento.

Nonostante la forte accelerazione dell'innovazione tecnologica con sempre più ampie modalità di offerta di servizi, vi è stata una sostanziale tenuta del *framework* regolamentare anche grazie agli interventi 'applicativi' delle Autorità nazionali che, nel contempo, hanno indotto qualche elemento di disarmonia nel quadro regolamentare.

Accanto a queste disarmonie, un elemento di criticità sussisteva nell'ambito dei presidi di sicurezza, la cui scelta era di fatto demandata agli operatori; al riguardo tuttavia, le Autorità di vigilanza e sorveglianza, tramite un intervento congiunto, hanno costituito un comune tavolo di lavoro (il *Securepay Forum*) per dare indicazioni agli operatori sui presidi di sicurezza da attivare; tali indicazioni sono alla base delle regole definite dalla seconda Direttiva.

3. *Il ruolo e il contributo della* European Banking Authority

La revisione del quadro regolamentare ha portato a un ampliamento della disciplina in tema di requisiti di sicurezza e la rivisitazione operata dalla PSD2 ha tenuto conto dell'evoluzione dei canali, degli strumenti e delle modalità di interazione con la clientela in un ecosistema digitale.

In questa rivisitazione un ruolo centrale è stato assegnato all'EBA, chiamata, più in generale, a delineare e mantenere aggiornato il quadro normativo di secondo livello e ad assicurare il coordinamento tra le diverse Autorità nazionali.

La sicurezza dei pagamenti elettronici, e non solo, è funzionale e propedeutica alle tutele previste a favore degli utilizzatori dei servizi di pagamento; all'EBA la PSD2 assegna quattro mandati in materia di sicurezza: a) definire *Regulatory Technical Standards (RTS)*, direttamente applicabili negli Stati membri, in materia di *strong customer authentication*, ed emettere linee guida su b) la sicurezza preventiva per limitare la vulnerabilità dei processi (*operational security*), c) la gestione degli incidenti su larga scala (*incident reporting*) e d) l'analisi ex-post delle frodi (*fraud reporting*).

Vorrei ora richiamare brevemente i contenuti delle disposizioni EBA.

I *Regulatory Technical Standards* riguardano sia le procedure di autenticazione del cliente sia le modalità di comunicazione sicura con i *Third Party Providers* (TPP). Per l'autenticazione si richiede l'uso di procedure di autenticazione forte a due fattori con elementi dinamici in maniera che, se questi vengono catturati durante la fase autorizzativa del pagamento, non possono essere usati per attivare pagamenti fraudolenti verso altri beneficiari (de-sensibilizzazione delle credenziali utente). L'accesso ai conti di pagamento da parte dei TPP viene disciplinato da una regolamentazione che potremmo definire 'tecnica': i prestatori di servizi di pagamento detentori del conto del cliente, (ASPSP, *Account Servicing Payment Service Provider*) devono mettere a disposizione dei TPP una interfaccia tecnologica, documentata, con adeguati requisiti prestazionali e di sicurezza nonché munita di procedure di autenticazione del cliente. I TPP, soggetti a licenza, hanno il diritto di utilizzare l'interfaccia per eseguire operazioni dietro consenso del cliente. Tale accesso è subordinato: i) alla presentazione da parte dei TPP di certificati digitali che li identificano in fase di avvio della connessione e che li qualificano come operatori con licenza PSD2 e ii) al rispetto dei presidi operativi e di sicurezza predisposti dall'ASPSP sull'interfaccia.

Le linee guida sulla *Operational Security* richiedono agli intermediari la messa a punto di una serie di misure di sicurezza di natura preventiva (*risk management, identification/protection degli asset, continuos monitoring, Business Continuity*); nell'impostazione tipica delle linee guida non si fissano regole e standard ma si richiamano *best practices* ampiamente diffuse tra gli operatori e, in larga parte, già adottate nell'attuale quadro regolamentare.

Il documento sull'*Incident Reporting* affronta il tema della classificazione e del reporting degli incidenti di sicurezza rilevanti che possono determinare la perdita di dati sensibili, funzionali per l'avvio di azioni fraudolente, e pone le basi per un più efficace monitoraggio, e conseguente reazione. Per la segnalazione sono definiti due livelli di gravità (*Lower impact, Higher impact*) rispetto a varie dimensioni di impatto (es: numero delle transazioni coinvolte, possibili perdite, rischio reputazionale, etc..); l'evento è giudicato rilevante, e quindi da segnalare (*major incident*), o in caso di alto impatto su una dimensione, oppure in presenza di impatto minore su almeno tre dimensioni.

La condivisione fra le Autorità di eventi malevoli o accidentali che propagandosi potrebbero minare la sicurezza del sistema, consente alle Autorità di rafforzare le analisi di sicurezza e il pronto avvio di azioni per mitigare il rischio di contagio.

Le linee guida per il *Fraud Reporting* definiscono il quadro dell'*infosharing* sulle frodi relative a strumenti di pagamento che i PSP devono notificare

alle Autorità nazionali in una logica di monitoraggio del fenomeno e di analisi dei trend.

L'attenzione degli operatori si è concentrata in particolare sugli RTS, forse perché definiscono anche il perimetro delle modalità operative con cui le terze parti (PISP, *Payment Initiation Service Provider* e AISP, *Account Information Service Provider*) potranno accedere ai conti, l'elemento più dirompente nell'assetto del mercato degli operatori dei pagamenti. Minore attenzione è stata posta alle linee guida, ancorché solo una lettura unitaria dei quattro mandati e delle implicite interrelazioni che vi sono offre una visione olistica della sicurezza che la normativa vuole assicurare all'ecosistema dei pagamenti.

Concludendo il tema della relazione fra innovazione e sicurezza nella PSD2, gli elementi di novità da aver presente sono la previsione di un forum, l'EBA, dove le Autorità europee possono confrontarsi sulle norme e sulle evoluzioni del mercato per meglio valutarne le implicazioni e per assicurare un *level playing field* non solo sui mercati nazionali ma anche fra i diversi sistemi in una economia aperta.

Occorre nel tempo assicurare la capacità dei regolatori di applicare in maniera uniforme il quadro regolamentare all'operatività concreta e verificare l'attualità delle norme definite che, interagendo con soluzioni tecnologiche, possono avere un elevato tasso di obsolescenza.

Non si può fissare uno 'standard' normativamente; il regolatore deve dichiarare gli interessi pubblici da tutelare e i principi che l'operatore deve rispettare nelle proprie scelte: obiettivi e principi non si modificano per l'innovazione tecnologica, quello che cambia è il grado di rischio ovvero la sua rilevanza e quindi vanno ripensati e adattati i relativi presidi.

Con la PSD2, e in senso lato anche con la NIS e la GDPR, si è rafforzato il quadro regolamentare a presidio della sicurezza per consentire agli operatori di cogliere le opportunità dell'innovazione in un contesto in cui la competizione non è fra tecnologie ma fra i diversi servizi offerti.

Abstract

In questo articolo si affronta il tema della sicurezza degli strumenti di pagamento e si discute il delicato rapporto esistente fra regolamentazione e innovazione. Specifica attenzione viene dedicata alle soluzioni individuate dalla PSD2 per assicurare che le norme sull'offerta di servizi di pagamento favoriscano il progresso tecnologico preservando la sicurezza dei trasferimenti di denaro. L'analisi si concentra sul ruolo centrale assegnato dalla Commissione Europea alla European Banking Authority e sui meccanismi con cui quest'ultima definisce e aggiorna la

normativa di secondo livello, assicurando il coordinamento tra le diverse Autorità nazionali.
Parole Chiave: PSD2, Concorrenza, Servizi di pagamento, Sicurezza, EBA, Regolamentazione, Innovazione tecnologica.

Abstract
This article addresses the issue of the security of payment instruments and discusses the delicate relationship between regulation and innovation. It specifically focuses on the solutions identified by the PSD2 to ensure that the rules on the provision of payment services favor technological progress while preserving the security of money transfers. The analysis emphasizes the central role assigned by the European Commission to the European Banking Authority and focuses on the mechanisms with which the latter defines and updates second level legislation, ultimately ensuring coordination between the various national Authorities.

Keywords: PSD2, Competition, Payment services, Security, European Banking Authority, Regulation, Technological innovation.

Bruna Szego

I nuovi prestatori autorizzati

Sommario: 1. Introduzione – 2. Chi sono i TPP e quali servizi offrono? – 3. Quali regole? – 4. I rapporti con le banche e le sfide del futuro.

1. *Introduzione*

All'inizio del 2019 è stata attuata in Italia la nuova Direttiva sui servizi di pagamento, la *Payment Service Directive* (c.d. PSD2). I suoi obiettivi sono chiari: modernizzare il mercato europeo dei pagamenti a beneficio dei consumatori e dell'industria; rendere i pagamenti elettronici meno costosi, più efficienti e più sicuri; favorire la concorrenza. Sono obiettivi certamente ambiziosi; operatori e autorità sono chiamati a perseguirli in un contesto – quale il settore finanziario e in particolare quello dei pagamenti – caratterizzato dalla rapida evoluzione tecnologica, che modifica le modalità di prestazione dei servizi tradizionali e favorisce lo sviluppo di servizi nuovi.

Ed è proprio in quest'ultimo ambito – quello dello sviluppo dei servizi nuovi – che si situa il tema del mio intervento. Una delle novità più rilevanti della nuova Direttiva è infatti l'aver disciplinato una nuova categoria di prestatori di servizi di pagamento, i cosiddetti *Third Party Providers* (TPP). Si tratta di soggetti che – differentemente da tutti gli altri già regolati dalla Direttiva – non gestiscono somme di denaro della clientela ma informazioni relative a conti di pagamento.

Chi sono e cosa fanno i TPP? Quali regole sono previste per loro e quali i rapporti con le banche? Quali sfide per il prossimo futuro ne derivano, per i TPP stessi, le banche e le Autorità di vigilanza? Cercherò di rispondere a queste domande.

* Un ringraziamento particolare a Mariakatia Di Staso e Elena Cocchi per i preziosi consigli su una versione preliminare di questo scritto.

2. *Chi sono i TPP e quali servizi offrono?*

I TPP possono prestare due differenti tipologie di servizi: il servizio di disposizione di ordini di pagamento (*Payment Initiation Service* - PIS) e il servizio di informazione sui conti (*Account Information Service* – AIS).

Secondo la definizione della Direttiva, il PIS è il servizio «che dispone l'ordine di pagamento su richiesta dell'utente di servizi di pagamento relativamente a un conto di pagamento detenuto presso un altro prestatore di servizi di pagamento». Chi lo presta - il cosìddetto *Payment Initiation Service Provider*, PISP - si interpone tra il pagatore e il suo conto di pagamento *online* e dispone l'ordine di pagamento verso un terzo beneficiario. Il pagatore può quindi eseguire un pagamento *online* con addebito diretto sul proprio conto. Per l'erogazione del servizio, il PISP dispone l'ordine di pagamento a valere sul conto *online* del pagatore, radicato presso un altro intermediario, tipicamente una banca (*Account Servicing Payment Service Provider* – ASPSP o prestatore di servizi di pagamento di radicamento del conto).

Con il servizio di *Account Information* si forniscono invece all'utente dei servizi di pagamento informazioni consolidate su uno o più conti di pagamento detenuti presso un altro prestatore di servizi di pagamento o presso più prestatori di servizi di pagamento. Il prestatore di questo servizio (*Account Information Service Provider* - AISP), in sostanza, mette a disposizione del cliente che ha conti accessibili *online*, informazioni relative a tutti i suoi conti di pagamento, anche quando essi sono radicati presso diversi soggetti. L'utente di servizi di pagamento è quindi in grado di avere una visione complessiva della propria situazione finanziaria, immediatamente e in qualsiasi momento, senza necessità di contattare singolarmente i vari prestatori di pagamento dove i conti sono radicati.

La PSD2 ha quindi 'riconosciuto' sul piano normativo l'esistenza di questi servizi; ma quali sono le esigenze che hanno portato al loro sviluppo? È perché regolarli in modo uniforme in Europa?

La nascita e lo sviluppo di questi servizi sono strettamente collegati al diffondersi dell'utilizzo di internet per acquistare beni e servizi (*e-commerce*) e, parallelamente, per effettuare pagamenti. L'interposizione del PISP rende il pagamento *online* più rapido e potenzialmente meno costoso per il cliente: il PISP, di fatto, crea un '*link*' tra il pagatore e il *merchant online* attraverso l'*online banking* del pagatore stesso. Ne beneficia il pagatore, che può acquistare *online* i prodotti desiderati senza necessità di disporre di una carta di credito; basta un conto di pagamento. Ne beneficia il *merchant*, che 'risparmia' le commissioni applicate sui pagamenti con carta

di credito, riceve conferma immediata dell'avvenuto avvio dell'operazione di pagamento. In sintesi: pagamenti *online* più rapidi, meno costosi, collegati allo sviluppo *dell'e-commerce* e che a loro volta vi danno impulso.

Il servizio di informazione sui conti invece aggrega informazioni sui differenti conti facenti capo a uno stesso soggetto e le riorganizza secondo criteri prescelti dall'utente (ad esempio, per categorie di spesa); in questo modo favorisce la consapevolezza degli utenti con riferimento alla propria condizione finanziaria e la loro pianificazione di spesa.

Quanto al secondo aspetto – perché regolare questi servizi in modo uniforme in Europa - l'analisi di impatto svolta dalla Commissione a corredo della proposta segnalava la presenza di molteplici benefici attesi dalla nuova disciplina. A fronte di maggiori oneri che i TPP avrebbero dovuto sopportare, connessi con il rispetto delle nuove regole, venivano stimati – soprattutto per i PISP – un bacino di utenza potenziale molto ampio e significativi risparmi di costi per i *merchants*[2]. Inoltre, faceva premio risolvere le incertezze relative alle regole applicabili, al regime di tutela della clientela, alle responsabilità dei TPP e delle banche.

In particolare, in assenza di regole gli utenti potevano non essere adeguatamente informati sulle caratteristiche e i rischi del servizio prestato o non ricevere adeguate garanzie sulla correttezza del trattamento dei propri dati. Erano altresì esposti alle conseguenze di problemi tecnici o utilizzi fraudolenti connessi alla prestazione di questi servizi, senza che vi fossero specifici meccanismi di tutela. Le banche presso cui erano radicati i conti di pagamento, dal canto loro, si trovavano esposte a responsabilità non chiaramente definite con elevati rischi legali, reputazionali e operativi, questi ultimi connessi ad eventuali accessi non autorizzati ai sistemi informatici. Infine, i TPP potevano vedersi negato dalle banche l'accesso alle informazioni necessarie per la prestazione del servizio (con conseguenze negative sullo sviluppo del proprio business) ed erano anch'essi esposti a rischi legali non agevolmente valutabili.

La PSD2, nell'operare un'ampia revisione della disciplina sui servizi di pagamento, ha perciò ricondotto al proprio interno anche i nuovi servizi e ha provato a soddisfare le esigenze di tutela degli interessi in gioco con l'intento di favorire lo sviluppo del business; per questo, ha creato un *framework* comune che, da un lato, mira ad assicurare un più elevato livello di trasparenza e sicurezza delle operazioni e, dall'altro, impone una

[2] Si veda Commissione Europea, Commission Staff Working Document: Impact Assessment Accompanying the PSD2 and Interchange Fees Regulation proposal (Bruxelles, 24.7.2013) disponibile su <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013SC0288&from=EN> (ultimo accesso 10.10.2018).

'collaborazione forzata' dei prestatori di servizi tradizionali (essenzialmente le banche) così che questi mettano a disposizione dei TPP il set informativo necessario per operare.

3. *Quali regole?*

Nel nuovo quadro i TPP sono soggetti regolamentati, sottoposti al controllo dell'autorità di vigilanza. Esaminerò più da vicino il regime cui essi sono sottoposti, per gli aspetti di competenza della Banca d'Italia: la disciplina prudenziale e quella in materia di trasparenza.

Di seguito per semplicità mi riferirò al caso di nuovi operatori che esercitano in via esclusiva le attività di PIS e AIS, tralasciando i casi in cui queste attività sono svolte congiuntamente ad altri servizi di pagamento. Per i soggetti già operanti in questo mercato la Direttiva prevede una disciplina transitoria, che è stata in seguito meglio precisata dall'*European Banking Authority* (EBA): i soggetti che già offrivano i servizi di PIS e AIS quando è entrata in vigore la PSD2 (12 gennaio 2016) possono continuare a operare ma dovranno chiedere l'autorizzazione a partire dalla data in cui diverranno applicabili le norme tecniche di regolamentazione dell'EBA in materia di sicurezza (ossia a decorrere dal 14/09/2019).

La PSD2 è stata recepita in Italia con il decreto legislativo 15 dicembre 2017, n. 218, che ha apportato modifiche ai due corpi normativi nei quali sono disciplinati i servizi di pagamento: il testo unico bancario (TUB) e il decreto legislativo 27 gennaio 2010, n. 11. I servizi di disposizione di ordini di pagamento e di informazione sui conti sono oggi inclusi tra le attività riservate a banche, IMEL e istituti di pagamento. Il regime applicato a questi soggetti, in linea con le indicazioni del legislatore europeo, è ricalcato su quello previsto per i prestatori di servizi di pagamento 'tradizionali' ma con alcune differenze importanti, che tengono conto delle specificità del loro business.

PISP e AISP sono stati inquadrati come istituti di pagamento; essi possono dunque operare solo dopo essere stati autorizzati dalla Banca d'Italia. L'autorizzazione è rilasciata quando l'operatore soddisfa una serie di requisiti, che rappresentano un sottoinsieme di quelli richiesti per gli altri istituti di pagamento. Per gli AISP in particolare non sono previsti requisiti patrimoniali minimi commisurati ai rischi assunti; mentre per i PISP questi requisiti sono pari al capitale minimo iniziale fissato dalla Banca d'Italia (pari a 50 mila euro). Il trattamento è semplificato perché – se non

svolgono anche altri servizi di pagamento tradizionali – i TPP non entrano mai in possesso dei fondi dei clienti. Supplisce all'assenza di un requisito patrimoniale l'obbligo di dotarsi di una polizza di assicurazione della responsabilità civile per i danni arrecati nell'esercizio dell'attività[3].

Il valore assicurato, secondo criteri definiti dall'EBA, deve tener conto del profilo di rischio dell'impresa, della dimensione del business (rappresentato dal valore delle transazioni per i PISP e dal numero di clienti per gli AISP), della circostanza che l'attività sia svolta congiuntamente ad altre attività di pagamento o industriali[4].

Per entrambe le tipologie di operatori, sono richiesti requisiti di *fit* and *proper* per i membri degli organi di amministrazione e controllo; per scelta del legislatore europeo, invece, il controllo sui soggetti che detengono partecipazioni qualificate nel capitale è previsto solo per i PISP e non anche per gli AISP.

Un ruolo centrale nella regolamentazione prudenziale di questi soggetti è senza dubbio l'adeguatezza degli assetti organizzativi e di controllo: i TPP devono essere in grado di identificare, valutare e mitigare i rischi relativi alla prestazione dei servizi, in particolare quelli relativi alla sicurezza. Gli intermediari devono dotarsi di (i) una specifica politica per il governo dei rischi operativi e di sicurezza; (ii) procedure per la gestione e il controllo di questi rischi; (iii) sistemi per la prevenzione e il monitoraggio degli incidenti di sicurezza; nonché (iv) procedure per l'archiviazione, il monitoraggio, la tracciabilità e la limitazione dell'accesso ai dati sensibili relativi ai pagamenti.

Sul fronte della trasparenza, la PSD2 conserva pressoché inalterato l'impianto delle regole previsto dalla PSD1, che si fonda su obblighi di informazione in tutte le fasi del rapporto con il cliente: prima della stipula del contratto (o dell'esecuzione dell'operazione), in corso di rapporto e nella fase immediatamente successiva all'esecuzione dell'operazione. Anche qui, occorre distinguere tra PISP e AISP.

Ai primi si applicano le stesse regole di trasparenza previste per i prestatori di servizi di pagamento 'tradizionali', con alcuni aggiustamenti per includere negli obblighi di informazione i riferimenti al servizio che questi svolgono (ad esempio, con riguardo alle modalità attraverso le quali l'utente può prestare e revocare il consenso alla disposizione dell'ordine di

[3] Per i PISP, la polizza copre i rischi derivanti dal compimento di operazioni di pagamento non autorizzate e dalla mancata o inesatta esecuzione di ordini di pagamento; per gli AIPS quelli derivanti dall'accesso fraudolento alle informazioni del conto di pagamento o dall'uso non autorizzato di queste.

[4] Si tratta di una forma di copertura che nell'ordinamento italiano è adottata, ad esempio, per gli agenti in attività finanziaria e i mediatori creditizi; sinora essa era assente nella regolamentazione prudenziale dei soggetti sottoposti alla supervisione della Banca d'Italia.

pagamento e comunicare al PISP eventuali operazioni disposte o eseguite non correttamente).

Per gli AISP, invece, la Direttiva prevede un regime semplificato, che si fonda sull'applicazione solo di alcune regole relative alle informazioni precontrattuali, in ragione delle peculiarità del servizio offerto. A livello nazionale, nel dare attuazione a questa semplificazione, si è previsto che le informazioni sul servizio che essi svolgono possano essere rese in forma libera, ossia anche con modalità diverse da quelle previste per gli altri servizi di pagamento (foglio informativo e documento di sintesi o copia del contratto idonea per la stipula). Non si applicano, inoltre, le regole in materia di contratti e gli obblighi di natura organizzativa, che la disciplina nazionale prevede per gli altri servizi di pagamento. Ad esempio, per i contratti relativi a questi servizi non è richiesta la forma scritta; né gli AISP sono tenuti ad adottare procedure interne per la gestione dei reclami attinenti a questioni di trasparenza (è invece richiesto che gli AISP siano in grado di gestire i reclami riguardanti la sicurezza dei pagamenti)[5].

Si tratta, in sintesi, di una calibrazione delle regole per assicurare un approccio proporzionato che tiene conto delle specificità dei nuovi servizi.

4. *I rapporti con le banche e le sfide del futuro*

L'accesso alle informazioni e l'interazione tra il TPP e il soggetto presso cui è radicato il conto di pagamento devono avvenire nel rispetto degli standard di sicurezza e secondo le modalità disciplinati da norme tecniche europee direttamente applicabili. È questo forse uno degli snodi più interessanti e, senza dubbio, delicati dell'impianto previsto dalla PSD2.

I TPP non gestiscono conti di pagamento; per la prestazione dei propri servizi rimangono sostanzialmente dipendenti dai soggetti presso cui è radicato il conto, sostanzialmente le banche. La PSD2 compie una scelta ben precisa, per ragioni essenzialmente di concorrenza, e impone quella che ho già definito una 'collaborazione forzata'. Gli intermediari presso cui è radicato il conto sono tenuti a consentire ai TPP, subordinatamente

[5] Si vedano l'articolo 114-septiesdecies del TUB e la Sezione VI del documento di consultazione riguardante le modifiche alle disposizioni della Banca d'Italia in materia di "Trasparenza delle operazioni e dei servizi bancari e finanziari. Correttezza delle relazioni tra intermediari e clienti", disponibile su <https://www.bancaditalia.it/compiti/vigilanza/normativa/consultazioni/2018/direttiva-2015-66ue/Documento_consultazione.pdf> (ultimo accesso 10.10.2018).

al consenso da parte del titolare del conto, di accedere alle informazioni necessarie per prestare i propri servizi. L'accesso deve essere consentito a condizioni non discriminatorie: ad esempio, la banca non potrebbe applicare ad un'operazione di pagamento eseguita tramite un PISP condizioni diverse da quelle applicate alla stessa operazione, ma eseguita direttamente dal cliente sulla piattaforma *online* della banca stessa. Ai TPP è richiesto di identificarsi mediante apposite certificazioni digitali, limitarsi a chiedere le informazioni strettamente necessarie, garantire l'uso corretto e riservato delle credenziali dell'utente. Non mi addentrerò negli aspetti più tecnici, in parte ancora in via di definizione a livello europeo. Il tema dell'accesso alle informazioni offre un concreto esempio di intervento regolamentare in un'area ascrivibile *lato sensu* al *Fintech*, dove si confrontano, talora scontrandosi, le spinte all'innovazione e le esigenze di tutela tipiche del settore finanziario. Con il quadro normativo ancora in via completamento, non è possibile fare, sul piano applicativo, valutazioni attendibili degli effetti che la nuova normativa potrà avere sul mercato bancario e dei pagamenti in generale. Alcune riflessioni di ordine generale sono comunque possibili.

Per le banche gli effetti opereranno verosimilmente su due fronti. Un primo, più immediato, di adeguamento alle prescrizioni normative per la predisposizione dell'infrastruttura tecnologica, che dovrà consentire il dialogo tra i sistemi delle banche e quelli dei TPP in modo sicuro. Saranno necessari investimenti; dovranno essere assicurati presidi adeguati per la gestione dei maggiori rischi di sicurezza *cyber*. Le banche dovranno presidiare i rischi che si presenteranno nell'impianto e nella manutenzione dell'infrastruttura tecnologica per l'interazione con i TPP, anche quando dovessero avvalersi di soggetti terzi. L'adeguatezza dei processi di governo e controllo, la disponibilità di competenze adeguate diventano fattori cruciali.

Una seconda ricaduta, di carattere più strategico, è legata alle possibili pressioni concorrenziali. Le banche saranno chiamate a scegliere il ruolo che intendono assumere rispetto alle potenzialità di sviluppo di questi servizi. Da mere esecutrici materiali dell'operazione, i cui margini tendono progressivamente a comprimersi, le banche potrebbero divenire driver dell'innovazione, attraverso l'offerta di servizi a più elevato valore aggiunto e quindi più remunerativi e competitivi.

Per i TPP la sfida maggiore è guadagnare la fiducia degli utenti. Sotto questo profilo, l'investimento in adeguati sistemi di governo dei rischi operativi e di sicurezza per limitare il rischio di frodi e di incidenti, è un tassello fondamentale per ampliare la base di utenti. Occorre peraltro trovare un punto di equilibrio nel *trade off* esistente tra l'esigenza di rispettare il

livello di sicurezza richiesto per lo svolgimento di questi servizi e quella di assicurare comunque la facilità di utilizzo per il cliente.

C'è un ultimo aspetto da rimarcare: i 'nuovi servizi' si configurano per loro natura come strumentali. L'appetibilità per i potenziali utenti è quindi strettamente connessa all'ottenimento di servizi a valore aggiunto, rispetto ai quali il servizio di disposizione di ordini di pagamento o di informazione sui conti è solo una componente.

In questa direzione vanno le iniziative che sino ad oggi sono state portate all'attenzione della Banca d'Italia. Non sono state ancora avanzate richieste di autorizzazione; si è trattato piuttosto di interlocuzioni preliminari, che confermano come l'interesse verso le potenzialità di questi nuovi servizi attragga una platea diversificata di attori: *start-up* e operatori consolidati, di natura sia finanziaria sia industriale, con background, dimensioni e target di clientela diversi. In tutti i progetti industriali presentati, l'esercizio del servizio di PIS o di AIS si configura come strumentale allo sviluppo di servizi più complessi, a più elevato valore aggiunto.

Ad esempio, le informazioni acquisite tramite il servizio di AIS sono utilizzate per la personalizzazione dei contratti di offerta di prodotti e servizi erogati sia da società del gruppo sia da partner industriali oppure integrate nella valutazione del merito di credito per l'offerta di servizi finanziari, come la concessione di finanziamenti.

In ogni caso la diffusione dei nuovi servizi nel mercato dei pagamenti italiano ed europeo è oggetto di stime ancora approssimative: non sono ancora disponibili, infatti, dati ufficiali sulla diffusione di questi nuovi servizi sia tra i TPP, sia tra le banche. Tuttavia, benché sia prematuro trarre conclusioni, ad oggi, i segnali indicano che lo sviluppo di questo mercato è strettamente connesso all'instaurazione di forme di collaborazione tra banche, nuovi prestatori e industria. Quanto più diversificata, ampia e integrata sarà la collaborazione, tanto più proficue potranno essere le iniziative.

La PSD2 pone significative sfide anche per la Banca d'Italia nella sua veste di supervisore degli istituti di pagamento, inclusi i nuovi operatori, sia per i profili di stabilità sia di tutela della clientela.

Per i nuovi operatori, il primo tavolo di confronto sarà rappresentato dalla valutazione di eventuali istanze di iscrizione all'albo degli istituti di pagamento. L'analisi dei piani industriali e dell'adeguatezza degli assetti di governo e organizzativi ha un ruolo cruciale nell'assicurare la sostenibilità del business nel tempo e la sua conduzione secondo criteri di prudenza. La Banca d'Italia può contare sull'esperienza maturata sino a oggi nella valutazione delle istanze degli istituti di pagamento. Quest'esperienza andrà

integrata e adattata alle differenti caratteristiche di questi nuovi soggetti, per i quali il fattore tecnologico rappresenta un elemento di forza ma anche la principale vulnerabilità.

La regolamentazione prudenziale dei TPP, pur modulata su quella degli altri soggetti finanziari, presenta specificità che richiederanno un adattamento dei modelli di supervisione. Se la valutazione dell'adeguatezza dei requisiti di capitale rappresenta un elemento imprescindibile dell'attività di supervisione delle banche, degli IP e degli IMEL, per i TPP il focus si sposta sugli assetti organizzativi e sui processi. Il contenimento del rischio operativo, soprattutto quello legato a frodi e incidenti di sicurezza, la capacità del management di adottare le misure necessarie per rimuovere eventuali carenze riscontrate diventano centrali. Per la valutazione, la Banca d'Italia si avvarrà del tradizionale set delle informazioni di vigilanza, integrato da informazioni sugli incidenti di sicurezza, sulle frodi o ricavabili dagli esposti della clientela, che agevolano l'identificazione di potenziali vulnerabilità e la calibrazione di eventuali interventi correttivi.

Inoltre, il rafforzamento del dialogo con gli operatori rappresenta per l'autorità una leva importante per monitorare il mercato, individuare i progetti più innovativi e favorirne così l'evoluzione anche in coerenza con gli sviluppi che si stanno osservando a livello internazionale.

Con riguardo ai profili di tutela della clientela, l'autorità di vigilanza è chiamata ad assicurare che, a fronte della crescente digitalizzazione e della forte spinta innovativa che caratterizzano il mercato dei pagamenti, il sistema di protezione resti nella sostanza inalterato. In ambito internazionale, questo tema è oggetto di attenzione nel filone della tutela dei consumatori di prodotti finanziari nell'era 'digitale', nell'agenda dell'OCSE.

I servizi offerti dai TPP sono prestati *online* e dunque, di regola, non richiedono la presenza fisica degli operatori sul territorio; essi inoltre presuppongono l'instaurazione e lo sviluppo di relazioni complesse sia con la clientela, sia con altri intermediari. In virtù della loro posizione di terzietà PISP e AISP si interpongono, per l'aspetto dispositivo o informativo, nel rapporto contrattuale tra l'intermediario che gestisce il conto e l'utente che ne è titolare solo in forza del consenso espresso da quest'ultimo. E' quindi importante che l'utente sia informato e consapevole dei contenuti e delle modalità di svolgimento di questi servizi, abbia chiari il ruolo e la responsabilità dei diversi operatori coinvolti, i propri diritti. Appare dunque cruciale che alla verifica del rispetto sostanziale degli obblighi informativi si accompagnino iniziative per accrescere la conoscenza e la consapevolezza degli utenti.

Per mantenere inalterato il livello di protezione degli utenti, il quadro

regolamentare dovrebbe assicurare la 'neutralità tecnologica' e quindi essere in grado di adattarsi ai cambiamenti prodotti dall'innovazione; per il supervisore, la sfida riguarda soprattutto le tecniche e le procedure per i controlli di trasparenza che dovranno anche tenere conto della necessaria interazione tra i prestatori dei nuovi servizi e gli intermediari che gestiscono i conti sui quali, ad esempio, possono essere addebitati i costi di questi servizi. Alcuni degli attuali modelli di business, anche a scopo promozionale, non prevedono tuttavia alcun addebito di commissioni all'utente ma solo al *merchant*, beneficiario del pagamento.

In ogni caso è necessario un approccio europeo e uno stretto coordinamento tra autorità, specialmente in ragione delle modalità virtuali con cui i nuovi servizi vengono prestati. Il loro sviluppo e la loro integrazione nel mercato unico richiedono che le regole comuni siano applicate con criteri omogenei per realizzare nel concreto il *level playing field*. Per questa via passa infatti l'eliminazione delle barriere che ancora si frappongono alla fruizione di servizi finanziari *cross border*, ancor più se innovativi, soprattutto da parte dei consumatori, come evidenziato nel 2017 dalla Commissione europea nel *Consumer financial services action plan*.

Abstract

Una delle novità più rilevanti della nuova Direttiva sui servizi di pagamento è l'aver disciplinato una nuova categoria di prestatori di servizi, i *Third Party Providers* (TPP). Si tratta di soggetti che – differentemente da tutti gli altri già regolati dalla Direttiva – non gestiscono somme di denaro della clientela ma informazioni relative a conti di pagamento. Chi sono e cosa fanno i TPP? Quali regole sono previste per loro e quali i rapporti con le banche? Quali sfide per il prossimo futuro ne derivano, per i TPP stessi, le banche e le Autorità di vigilanza? Questo scritto risponde a queste domande.

Parole chiave: TPP, PIPS, AISP, Servizi di Pagamento, Prestatori di Servizi di Pagamento, Third Party Providers, Open Banking.

Abstract

Rules on third party providers (TPPs) are one of the most important changes introduced by the new European directive on payment services. Differently from all other service providers already envisaged by European law, TPPs do not manage clients' money but only information on payment accounts. Who are they and what do they do? What kind of rules does the directive set for them and how is the relationship with the banking sector shaped? What are the major challenges in the near future for TPPs, banks and supervisory authorities? This paper addresses these issues.

Keywords: TPPs, PIPS, AISP, Payment Services, Payment Servicers, Third Party Providers, Open Banking.

ROMA TRE
UNIVERSITÀ DEGLI STUDI

Il volume raccoglie i contributi presentati nell'incontro di studio *"Innovazione e regole. Il bilanciamento degli interessi nella PSD2 – Dir 2015/2366/UE"*, frutto di un'organizzazione congiunta della Banca d'Italia e del Dipartimento di Giurisprudenza dell'Università degli Studi Roma Tre, e svoltosi presso l'Università di Roma Tre il 12 ottobre 2018.

Esso costituisce un momento di riflessione sui temi della Direttiva sui servizi di pagamento del mercato interno (PSD2), attraverso una serie di interventi finalizzati all'approfondimento della nuova cornice regolamentare -che fissa diritti e obblighi dei prestatori e degli utenti dei servizi di pagamento- e al confronto sulle questioni più rilevanti poste dalla normativa europea.

I contributi raccolti provengono da rappresentanti dell'Accademia, della Banca centrale nella sua funzione di Vigilanza sugli intermediari e di Sorveglianza sul sistema dei pagamenti e delle Autorità di controllo coinvolte nell'applicazione della Direttiva. La trattazione è suddivisa in due parti, la prima volta a tentare un inquadramento delle novità normative e delle principali criticità giuridiche in un'ottica sistematica; la seconda incentrata sul tema delle interserzioni del nuovo quadro regolamentare con il diritto della concorrenza, della privacy, con la tutela dell'utente e la promozione dei presidi di sicurezza.

Maria Cecilia Paglietti è ricercatrice di Diritto privato comparato del Dipartimento di Giurisprudenza dell'Università di Roma Tre, abilitata alle funzioni di professore associato di Diritto privato e di Diritto comparato. Ha scritto libri e saggi in materia di accesso alla giustizia, diritto dei consumatori, diritto della risoluzione alternativa delle controversie, diritto dei cosmetici. Dal 2013 è titolare del corso "Clinica legale in diritto dei risparmiatori".

Maria Iride Vangelisti è responsabile della divisione Strumenti e servizi di pagamento nel Dipartimento Mercati e sistemi di pagamento della Banca d'Italia. Si occupa di sistemi di pagamento dal 1995 e ha partecipato a gruppi di lavoro internazionali presso la Banca dei regolamenti internazionali e la Banca centrale europea. Ha scritto con Riccardo De Bonis "Moneta. Dai buoi di Omero ai Bitcoin" (Il Mulino, 2019).

Roma TrE-Press
2020