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.