DALLA PSD ALLA PSD2: INNOVAZIONE TECNOLOGICA E OPEN BANKING

Maddalena Rabitti, Università degli Studi Roma Tre
Antonella Sciarrone Alibrandi, Università Cattolica del Sacro Cuore

UNIVERSITÀ CATTOLICA del Sacro Cuore

Agenda

- I servizi di pagamento come settore precursore del FinTech
- Le ragioni del passaggio da PSD a PSD2
- Le questioni di fondo della PSD2
- I principi cardine della PSD2
- La scelta dell'open banking e il paradigma delle API
- Il rapporto fra PSD2 e GDPR: un problema aperto

I servizi di pagamento come settore precursore del FinTech

- Primo comparto interessato da:
  - forme di **innovazione tecnologica** (es.: electronic payments, e-money) sperimentate prima all'interno del sistema bancario e poi da soggetti esterni (IMEL e IP), in ampio anticipo sull'odierno utilizzo di tecnologie abilitanti con impatto su prodotti, servizi, modelli di business (FinTech definito come «innovazione finanziaria abilitata da tecnologie digitali»)
  - forme di **disruption** (nel 2009 bitcoin nasce come «fenomeno eversivo» rispetto al sistema) ma anche di **cooperation e integration** (si pensi all'orizzonte futuro delle valute digitali emesse da banche centrali), che pongono la questione del confine fra servizi finanziari in senso tradizionale e nuovi servizi
  - un **intervento normativo (PSD2)** che, con approccio nuovo e ricadute sull'intero sistema finanziario, affronta questioni legate alla frantumazione della tradizionale catena del valore per effetto di nuove forme di attività e nuovi operatori focalizzati su specifici segmenti della filiera

UNIVERSITÀ CATTOLICA del Sacro Cuore

Le ragioni del passaggio da PSD a PSD2

- Nei sette anni intercorrenti fra PSD (2007/64) e PSD2 (2015/2366) si è assistito, per effetto dell'innovazione tecnologica, all'ingresso sul mercato di nuovi operatori e nuovi servizi che restavano fuori dal perimetro applicativo della PSD (e dalla riserva di attività in essa prevista)
- In assenza di regole ad hoc si è assistito anche all'emersione di nuovi rischi relativi a:
  - Mancanza di level playing field fra operatori
  - Accesso ai dati degli utenti e utilizzo dei medesimi
  - Sicurezza delle transazioni/frodi/pagamenti non autorizzati
- A distanza di quattro anni da PSD2 (e prima ancora della sua piena attuazione) ci sono già molte altre innovazioni nel campo dei pagamenti (ad es. DLT e blockchain): tensione immanente fra dinamismo dell'innovazione e staticità della regolazione

UNIVERSITÀ CATTOLICA del Sacro Cuore

Le questioni di fondo della PSD2

- Come promuovere capacità di innovazione degli operatori (new comer ma anche incumbent) assicurando adeguata tutela agli interessi «classicamente» tutelati dalla regolazione del sistema finanziario (concorrenza, efficienza, stabilità, protezione degli utenti)?
- Come regolare il rapporto fra operatori/servizi «tradizionali» del settore (banche, IP, IMEL) presso cui è radicato un conto di pagamento – oggi denominati Account Servicing Payment Service Provider, ASPSP - e operatori/servizi (Account Information Service Provider, AISP, e Payment Initiation Service Provider, PISP) ad alto tasso di innovazione, senza necessità per l'utente di radicare un nuovo conto potendo accedere a conti preesistenti?
- Come rispondere all'accresciuto bisogno di sicurezza dell'utente?

I principi cardine della PSD2

- Ampliamento della riserva di attività (licensed Third Party Providers: TPP) nel segno del principio di proporzionalità (level playing field)
  - 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 di servizi (same business, same risks, same rules)
- Rispetto del principio di neutralità tecnologica
  - non vanno definite con rigidità le modalità tecnologiche con cui i singoli servizi devono essere erogati e i dati in possesso degli ASPSP devono essere messi a disposizione delle TPP
- Scelta della soluzione dell'open banking e adozione del paradigma delle Application Programming Interfaces, API
- Autenticazione forte del cliente e standard di comunicazione sicuri tra ASPSP e TPP

UNIVERSITÀ CATTOLICA del Sacro Cuore

La scelta dell'open banking e delle API: soluzioni operative e giuridiche

- La scelta di open banking della PSD2 che consente ai diversi provider l'accesso alle informazioni legate ai conti di pagamento attraverso le API è stata molto dibattuta a livello internazionale:
  - Dubbi sulla unidirezionalità dei flussi informativi
  - Dubbi sulla sua effettiva, piena neutralità tecnologica
- E' una scelta che lascia spazio (creando opportunità) a:
  - diverse soluzioni operative (iniziative di legislatori nazionali, come quella UK, e iniziative di standardizzazione di tipo cooperativo che nascono dal mercato come quella italiana di Cbi)
  - diverse soluzioni giuridiche a fronte della non necessità di una relazione contrattuale fra ASPSP e TPP ma solo di una infrastruttura tecnologica (anche in assenza di contratto fra operatori tale relazione si conforma – ad es. in termini di responsabilità per pagamenti non autorizzati – sulla base di PSD2 ma la presenza di un contratto può portare a una configurazione più personalizzata della relazione)

UNIVERSITÀ CATTOLICA del Sacro Cuore

Il rapporto fra PSD2 e GDPR/1

- Open banking è modello fondato su accesso ai dati dell'utente e condivisione di tali dati, con forte impatto sul profilo della sicurezza, della profilazione della clientela per disparate finalità e anche della stabilità del sistema bancario (il che spiega il recente interesse del FSB in ottica di competition con i Tech Giants, nuovi latifondisti digitali)
- Profilo della tutela dei dati non si esaurisce all'interno di PSD2 (ove pure ci sono regole specifiche di settore) ma coinvolge GDPR (2016/679), ponendo una serie di questioni ancora aperte che richiedono il coordinamento fra diversità autorità di settore anche a livello europeo (EBA e European Data Protection Board)
- Sono attese a breve Linee guida della Commissione

UNIVERSITÀ CATTOLICA del Sacro Cuore

Il rapporto fra PSD2 e GDPR/2: il consenso

- Il rapporto fra PSD2 e GDPR pone una serie di questioni ancora aperte innanzitutto sul tema del consenso
  - Rapporto fra consenso PSD2 (consenso di natura contrattuale) e consenso GDPR (nella prospettiva dei diritti fondamentali)
  - Un solo consenso vale per entrambe le discipline? Dipende dalle finalità del trattamento
  - Rapporto tra black-list prevista da PSD2 e consenso dato ai sensi del GDPR
  - La posizione delle cd. parti silenti (ossia i beneficiari dei pagamenti i cui dati circolano anch'essi)
  - Non coincidenza della nozione di dati sensibili per la PSD2 e di dati sensibili per il GDPR

UNIVERSITÀ CATTOLICA del Sacro Cuore

Il rapporto tra PSD e GDPR/3: l'accountability

- Il passaggio dall'adempimento «formale» del consenso a una strategia «sostanziale» di azione che consiste nell'adozione di presidi organizzativi e procedure adeguate a prevenire i rischi connessi all'attività di prestazione di servizi di pagamento e al trattamento dei dati personali dei clienti
- Il principio dell'accountability nel contesto del GDPR: al titolare del trattamento viene demandato di decidere in autonomia modalità e limiti del trattamento dei dati e viene imposto di organizzarsi con procedure e controlli idonei all'obiettivo di prevenzione dei rischi che possono derivare dal trattamento dei dati
- La Valutazione d'impatto sulla protezione dei dati (art. 35 GDPR), necessaria in presenza di rischi specifici anche legati alla tecnologia

UNIVERSITÀ CATTOLICA del Sacro Cuore

Conclusioni

- I tre pilastri della PSD2 da leggere in termini di vincolo/opportunità:
  - Sicurezza dei dati dell'utente e protezione dell'accesso (necessità di integrare gli RTS EBA attraverso un modello robusto di consent model e di accountability)
  - Semplicità di adozione e integrazione delle API
  - Definizione di uno schema di compensi per le banche che resta sostenibile il business model e risponda alle esigenze di revenues