

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 ASPSP⁴ - 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 internazionale⁶.

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 personali⁸. 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 pagamento⁹.

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'API¹⁰. 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 coinvolti¹¹. 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 connotarlo¹².

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 Unito¹³) che determina regole tecniche di comunicazione comuni ai soggetti prestatori dei servizi di pagamento, siano essi ASPSP o TPP. La seconda, invece, ruota attorno a soluzioni di sistema provenienti dal mercato (come è accaduto in Italia¹⁴). 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 nazionali¹⁵.

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 TPP 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 Transformation 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

