271

17 gennaio 2017

Istituto Bruno Leoni
idee per il libero mercato

IBL Focus

Pagamenti online: serve più sicurezza, ma anche flessibilità

Di Giacomo Lev Mannheimer

Introduzione

Negli ultimi dieci anni, la percentuale di cittadini dell'Unione Europea che compiono abitualmente acquisti *online* è grossomodo raddoppiata.[1] Internet ha stravolto le abitudini d'acquisto delle persone, non solo in termini quantitativi, ma anche dal punto di vista delle aspettative delle persone nei confronti dei sistemi di vendita: dai supermercati aperti 24 ore su 24 all'obbligo del POS in tutti gli esercizi commerciali, segnali della 'rincorsa' del commercio *offline* ai benefici dell'e-commerce sono visibili ovunque.

Il processo di armonizzazione tra l'esperienza di acquisto *online* e quella *offline*, tuttavia, non è a senso unico. Ci sono aspetti dell'e-commerce – e in particolare quelli legati alla sicurezza delle transazioni – su cui da anni il legislatore, a Roma e soprattutto a Bruxelles, sta cercando di mettere mano per rendere l'esperienza d'acquisto in tutto e per tutto equiparabile a quella *offline*.

Quando acquistiamo un prodotto con la nostra carta di credito, l'esercente adempie il suo obbligo d'identificazione secondo criteri e gradi diversi secondo il bene acquistato, il suo valore, l'eventualità che ci conosca personalmente. In altre parole, difficilmente ci viene chiesto di esibire un documento acquistando un caffè nel nostro bar di fiducia, mentre è molto probabile che ciò accada acquistando un gioiello o un'automobile.

Gli acquisti *online*, dal punto di vista dell'identificazione dell'acquirente, pongono evidentemente alcuni problemi che li distinguono nettamente dagli esempi sopracitati. Tuttavia, negli ultimi anni, la tecnologia ha fatto passi avanti tali – anche nel campo della sicurezza delle transazioni *online* – da rendere possibile ipotizzare sistemi d'identificazione dell'acquirente altrettanto flessibili e 'naturali': l'utilizzo dei dati di acquisto dei singoli utenti (siti preferiti, orari, metodi di pagamento), insieme ad alcune caratteristiche biometriche (impronte digitali, stile di battitura sulla tastiera, firma), permette di simulare con grande efficacia l'esperienza di acquisto *offline*.

In ragione di tali progressi, desta alcune preoccupazioni il modo con cui la Commissione Europea ha inteso regolare la sicurezza delle transazioni nella proposta di direttiva sui servizi di pagamento che ha elaborato nei mesi passati: cioè attraverso un unico sistema, valido per tutti, rigido e insensibile alle caratteristiche dei singoli acquisti.

1 Dati Eurostat.

Giacomo Lev Mannheimer è Fellow dell'Istituto Bruno Leoni.

Credere che applicare lo stato dell'arte di una materia indistintamente a tutti coloro che ne sono interessati sia la migliore forma di regolazione è un difetto assai comune del legislatore, che in questo modo disincentiva la concorrenza e la ricerca di soluzioni migliori; farlo in un settore, come quello dell'economia digitale, che più di ogni altro oggi vive di continua innovazione, significa rallentare e inibire l'adeguamento dell'e-commerce a sistemi di frode *online* sempre più sofisticati, e dunque paradossalmente finire per diminuire la sicurezza degli acquisti.

Come vedremo, la soluzione adottata dalla Commissione Europea non è peraltro l'unica possibile, ma esistono alternative che – senza compromettere, ma anzi aumentando la sicurezza – non ledono in modo così evidente la libertà di scambio, la concorrenza e l'innovazione.

La nuova direttiva sui servizi di pagamento

Il 23 dicembre 2015 è stato pubblicato sulla Gazzetta ufficiale dell'Unione Europea il testo della direttiva 2015/2366, cioè la nuova direttiva sui servizi di pagamento nell'Unione Europea (cosiddetta *Payment Services Directive 2*, di seguito "PSD2"), proposta dalla Commissione europea nel luglio 2013 e passata negli anni successivi attraverso *l'iter* di approvazione del Parlamento prima e del Consiglio dell'Unione Europea poi.

La pubblicazione in Gazzetta della PSD2 ha comportato l'abrogazione dell'omologa direttiva 2007/64/CE (cosiddetta *Payment Services Directive 1*, di seguito "PSD1"), che per quasi dieci anni aveva regolato il mercato interno dei pagamenti al dettaglio. Quest'ultima, dalla sua approvazione sino ad oggi, ha contribuito notevolmente a formare regole, procedure e prassi comuni a tutte le banche e le società che prestano servizi di pagamento all'interno dell'Unione Europea, definendo ad esempio i termini massimi per l'esecuzione dei bonifici bancari e degli accrediti, le condizioni per il rimborso in caso di pagamenti non autorizzati o irregolari, gli obblighi di rendicontazione gratuita delle operazioni effettuate dai clienti, eccetera. Più in generale, tutte le forme di pagamento elettronico emerse nel mercato dell'UE in questi anni (basti pensare ai sistemi di pagamento di Amazon, eBay, o Facebook) hanno dovuto adeguarsi a quanto previsto dalla PSD1 ormai dieci anni fa.

Obiettivo dichiarato della PSD2 è completare il sentiero già tracciato dalla PSD1, nel tentativo di armonizzare il quadro regolamentare europeo – oggi frammentato dalle notevoli e numerose differenze nel recepimento della direttiva ora abrogata – e di rafforzare la tutela degli utenti dei servizi di pagamento, aumentando in particolare il livello di sicurezza di quelli elettronici.[2] Negli ultimi dieci anni, infatti, il mercato dei pagamenti *online* ha subito una notevole evoluzione, sia nel peso economico delle transazioni effettuate, sia nelle tecnologie adottate; di qui l'esigenza, da parte della Commissione europea, di aggiornare la normativa del settore.

Le principali novità introdotte dalla nuova direttiva riguardano l'estensione dell'ambito di applicazione della disciplina in tema di trasparenza delle condizioni e dei requisiti informativi a operazioni parzialmente al di fuori dell'UE, la rimodulazione delle esenzioni dagli obblighi di trasparenza previsti dalla direttiva stessa, il divieto di *surcharge* (cioè dell'applicazione di commissioni aggiuntive nel caso di utilizzo di carte di pagamento), l'abbassamento a 50 euro della franchigia che un utente può essere obbligato a pagare in caso di operazioni non autorizzate, nuove modalità di controllo della disponibilità di fondi (*fund checking*), l'istitu-

2 V. PSD2, considerando (6) e ss.

zione di un registro centrale – in capo all'Autorità Bancaria Europea (EBA) – per rafforzare la trasparenza del funzionamento degli istituti di pagamento autorizzati, e l'introduzione di nuovi servizi di pagamento.[3]

Proprio quest'ultimo punto merita un approfondimento e costituisce l'oggetto del presente studio. Prima di affrontarlo direttamente, però, è necessaria una breve premessa per comprendere il contesto nel quale esso sarà esaminato.

I PISP, tra prassi e regole

Negli ultimi anni, come anticipato, il mercato dei pagamenti è stato letteralmente travolto dall'evoluzione tecnologica. Come altri mercati parimenti trasformati dalla digitalizzazione – basti pensare ai trasporti o agli alloggi turistici – gli *incumbents* del settore hanno spesso finito per ostacolare l'ingresso di *competitors* innovativi, facendo leva su norme, prassi e relazioni consolidatesi nel tempo, piuttosto che tentare di adeguarsi innovando rispettivamente normative e servizi offerti – o comunque hanno iniziato a farlo con colpevole ritardo. Nel caso di specie, le banche e le altre istituzioni finanziarie hanno iniziato a subire la concorrenza di servizi innovativi di pagamento, legati a fondi di denaro gestiti interamente *online*, senza alcun legame con il sistema bancario.

Il risultato, nel settore dei pagamenti come negli altri citati, è stato il generarsi di una profonda spaccatura tra *incumbents* e *competitors*, i cui servizi sono spesso molto apprezzati dai consumatori e ignorati dal legislatore, con la conseguenza – nel caso di specie – di generare possibili rischi per la sicurezza e per la trasparenza dei loro utenti.

Si pensi, ad esempio, ad alcuni dei più diffusi servizi di intermediazione di pagamenti *online*. Diverse aziende del settore *fintech*, cosiddette *Third Party Providers* (di seguito "TPP"), offrono già da qualche anno la possibilità di aggregare saldi di diversi conti correnti su un unico 'portafoglio virtuale', effettuando pagamenti direttamente dai conti collegati senza alcun controllo su di essi da parte degli istituti di credito emittenti. In altre parole, tali piattaforme consentono all'utente di effettuare pagamenti da un conto bancario senza passare attraverso i sistemi di controllo e di tutela del consumatore (ad esempio la richiesta di password, PIN, codici token, ecc.) previsti obbligatoriamente per la banca in cui sono detenuti i fondi, bensì prelevandoli direttamente. I gestori di questi servizi, cosiddetti *Payment Initiation Service Providers* (di seguito "PISP"), costituiscono oramai una fetta importante del mercato dei pagamenti dell'UE, anche se non in Italia, senza che alcuna norma ne regoli l'utilizzo: il rischio di frodi informatiche, dalle conseguenze potenzialmente rilevanti, è pertanto assai elevato.

Nella consapevolezza che si tratti di un fenomeno ineludibile, la Commissione Europea ha correttamente avviato un progetto di riforma della normativa sul mercato dei pagamenti che non solo regoli, ma che anzi incentivi i PISP. La PSD2, infatti, non si limita a includere il riconoscimento giuridico degli intermediari di servizi bancari in grado di addebitare direttamente i pagamenti sul conto corrente dei propri utenti senza l'ulteriore autorizzazione dell'istituto bancario corrispondente, ma stabilisce l'obbligo, da parte dell'istituto bancario da cui proviene il pagamento, di garantire al PISP l'accesso al conto *online* dell'utente, fermo restando il divieto per quest'ultimo di entrare in possesso dei fondi del pagatore.[4] In

3 Cfr. M. Folcia-F. Cascinelli-G. Zanetti-S. Marcozzi, *Pillola di PSD2 n°3: le principali novità normative introdotte*, PwC, 2016.

4 PSD2, art. 66, par. 4.

pratica, con l'approvazione della PSD2, i gestori dei 'portafogli virtuali' in grado di accedere direttamente ai conti bancari degli utenti, senza ulteriori richieste autorizzative da parte delle banche in cui quei conti sono depositati, potranno operare senza correre il rischio di non rispettare la normativa in materia.

Ciò potrebbe favorire frodi da parte di soggetti che, presentandosi come intermediari di pagamenti *online*, utilizzino illecitamente i dati dei propri clienti, senza che le banche in cui sono detenuti i fondi possano in alcun modo intervenire per bloccare le transazioni. Per questa ragione, la direttiva specifica che tali servizi debbano prevedere sistemi di sicurezza che limitino il loro accesso ai fondi dei clienti per una specifica transazione alla volta.

La PSD2, grazie a queste caratteristiche, è potenzialmente in grado di sanare notevolmente la frattura tra *incumbents* e *competitors* emersa negli ultimi anni. Oggi, infatti, secondo quanto previsto dalla PSD1, banche e altri istituti di pagamento non sono tenuti a fornire a soggetti intermediari l'accesso diretto ai conti dei propri clienti. Questa è una tra le ragioni per cui, ad esempio, un servizio come PayPal – che consente di effettuare transazioni *online* senza condividere i dati della propria carta di credito con il destinatario del pagamento – non può autorizzare un pagamento direttamente dal conto bancario collegato alla carta di credito utilizzata, ma necessita pur sempre la previa effettuazione di un bonifico bancario dall'istituto emittente al relativo conto PayPal.

Ciò ha favorito l'emersione di quei PISP che forniscono il medesimo servizio direttamente, senza il consenso degli istituti di credito, e che oggi, grazie alla PSD2, potranno farlo 'alla luce del sole'. Il fine della norma, tuttavia, non è solo quello – formale – di ricondurre i PISP al rispetto della normativa vigente, bensì anche e soprattutto quello di associare ad essi gli obblighi ulteriori previsti dalla direttiva in materia di trasparenza e sicurezza dei consumatori. Proprio su quest'ultimo punto, come vedremo, l'apprezzabile tentativo della Commissione Europea di regolare il fenomeno senza svilirne le potenzialità rischia di scontrarsi con un sistema di controlli sbilanciato e controproducente.

Lo strong customer authentication

Come si evince in tutta evidenza dal paragrafo precedente, l'esigenza di non imbrigliare la semplicità degli acquisti *online* e la sperimentazione di servizi innovativi rischia di scontrarsi con quella di regolarne l'utilizzo garantendo la massima sicurezza agli utenti nel 'dialogo' tra banche e terze parti coinvolte nel pagamento. Per impedire questo rischio, la Commissione Europea ha chiesto all'Autorità Bancaria Europea (di seguito "EBA") di definire *standard* tecnici adeguati, che tenessero conto di questo potenziale conflitto.[5] In particolare, all'EBA è stato chiesto di formulare una proposta sul sistema di verifica dell'identità di chi effettua transazioni con i PISP, così da scongiurare l'eventualità che il mancato controllo da parte degli istituti bancari dia luogo a frodi.

Nell'agosto 2016, l'EBA ha pubblicato un primo Consultation Paper sul tema,[6] sottolineando l'importanza di garantire un sistema di autenticazione degli utenti 'forte' (*strong customer authentication* nel testo, di seguito "SCA") da parte dei PISP, così come esplicitamente richiesto dalla PSD2. Quest'ultima, nel richiedere all'EBA di formulare una proposta relativa al sistema da richiedere ai PISP per esercitare i propri servizi, specifica le caratteristiche che

5 V. PSD2, art. 98.

6 V. https://www.eba.europa.eu/documents/10180/1548183/Consultation+Paper+on+draft+RTS+on+SCA+and+CSC+%28EBA-CP-2016-11%29.pdf.

dovrebbe possedere un sistema 'forte', descrivendolo come un sistema di autenticazione

> basato 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 concepito in modo tale da tutelare la riservatezza dei dati di autenticazione.[7]

La definizione utilizzata nella PSD2 riprende una comune classificazione delle credenziali di autenticazione che abitualmente vengono richieste agli utenti dai sistemi di pagamento *online*, generalmente suddivise nelle seguenti categorie:

- *Knowledge*, come password o codici PIN, talvolta accompagnati da ulteriori richieste di individuare in tempo reale immagini o sequenze alfanumeriche. Le credenziali *knowledge* sono statiche, forniscono livelli di sicurezza normalmente deboli e possono facilmente essere violate.
- *Possession*, come e-Token, carte e chiavi USB 'intelligenti', spesso basati su *one-time password* generate da algoritmi e verificate da un server in remoto una volta che il cliente ha effettuato l'accesso ai suoi dati, così utilizzandole. Ovviamente, questi dispositivi hanno il difetto di poter essere persi, rubati, o danneggiati.
- *Inherence*, come impronte digitali, analisi della retina e altre caratteristiche biometriche, oppure verifiche della voce, delle dinamiche di pressione dei tasti, della velocità di battitura, eccetera.
- *Behavioral*, come dispositivi registrati, fedeltà dei clienti, posizione geografica, comportamenti di acquisto e tutte le altre forme di 'esperienza' nell'acquisto da parte del venditore, che possono contribuire a formare indizi, se non sull'identità dell'acquirente, quantomeno – in senso opposto – nel sollevare dubbi in caso di frode o di furto d'identità.

Come abbiamo visto, lo SCA è una procedura di autenticazione basata sull'utilizzo di almeno due credenziali tra *knowledge*, *possession* e *inherence*, di cui almeno una non riutilizzabile (come codici temporanei inviati via token o sms). Non solo: a questi requisiti, l'EBA stabilisce che i PISP debbano includere nelle piattaforme che autorizzano pagamenti anche elementi grafici di collegamento dinamico che associno le transazioni a una somma ben precisa e a un beneficiario altrettanto preciso, per evitare che l'autenticazione venga utilizzata per scopi diversi rispetto a quello originario.[8] In altre parole, ogni specifico acquisto tramite PISP dovrebbe essere autorizzato singolarmente, in modo che risulti esplicita, per ogni transazione, l'entità della somma pagata e il suo beneficiario.

La proposta dell'EBA è, dunque, quella di rendere obbligatoria, per i gestori di piattaforme che permettono il pagamento diretto di somme *online*, senza l'intermediazione di un istituto bancario, l'adozione di sistemi di autenticazione che richiedano a chi esegue la transazione almeno due codici o altre prove che garantiscano un'identificazione sicura, mentre oggi – vale la pena ricordarlo – non vi è alcun requisito di questo genere, poiché la direttiva in vigore non regola il funzionamento dei PISP.

Alla pubblicazione del Consultation Paper l'EBA ha fatto seguire un periodo di due mesi

7 V. PSD2, art. 4 (30).

8 V. PSD2, art. 97.

per permettere a banche, istituzioni e altri *stakeholders* di esprimere la propria opinione sulle caratteristiche del sistema di autenticazione da far adottare obbligatoriamente ai PISP proposto. Diversi attori tra quelli coinvolti hanno espresso perplessità sulla proposta, in quanto lo SCA – così come progettato dall'EBA – renderebbe le procedure di pagamento *online* certamente più sicure di quanto siano oggi, ma anche eccessivamente macchinose.

Dubbi sono emersi anche nel Parlamento europeo, dove eurodeputati di rappresentanza politica eterogenea hanno rilevato diversi aspetti critici connessi agli standard tecnici della PSD2 individuati dall'EBA.[9] Oltre all'assenza di una soglia di esenzione della loro applicazione per transazioni minori, la maggior parte delle criticità emerse riguardano – anche in questo caso – l'assenza di criteri concernenti il tasso di rischio di ciascuna transazione per determinare forme flessibili e non arbitrarie di adozione della PSD2, transazione per transazione.

Un'alternativa flessibile allo SCA

I dubbi emersi durante la consultazione aperta dall'EBA sono stati riassunti e avvalorati da uno studio indipendente prodotto qualche mese fa da una società di consulenza, Clever Advice, relativo agli effetti che comporterebbero sugli acquisti e sui consumi *online* le caratteristiche dello SCA, come proposto dall'EBA.[10] Secondo tale analisi, circa il 25% degli acquisti *online*, già oggi, resterebbero incompiuti a causa dell'eccessiva farraginosità dei processi di autenticazione degli acquirenti. Le persone, in altre parole, rinuncerebbero a un acquisto *online* su quattro, secondo la ricerca, per la difficoltà o la farraginosità delle richieste di password, PIN, token e altri codici e sistemi identificativi.

La predisposizione di meccanismi particolarmente stringenti, specialmente per soggetti come i PISP che, ad oggi, non sono obbligati a prevederne affatto, penalizzerebbe – secondo lo studio – lo sviluppo del mercato digitale europeo, e particolarmente le piccole imprese, poiché i consumatori troverebbero certamente più vantaggioso effettuare l'iscrizione solo a pochi grandi portali intermediari (come Amazon, ad esempio) per effettuare i propri acquisti *online*, rinunciando – per l'eccessiva complessità della procedura di autenticazione per ogni singolo acquisto – ad effettuare la medesima procedura su tutti i siti web dei singoli venditori dei beni e servizi cui sono interessati. Non solo: ad essere penalizzati sarebbero anche i consumatori, la cui libertà di scelta sarebbe *de facto* limitata da un eccesso di tutela non richiesta nei loro confronti. Infine, paradossalmente, imporre un procedimento rigido e unitario a tutte le operazioni di pagamento, indipendentemente dalle loro caratteristiche e dal fattore di rischio ad esse associato, potrebbe rivelarsi perfino dannoso, nel lungo termine, per la prevenzione delle frodi. Infatti, la forza di una tecnica di prevenzione si deteriora sempre nel tempo, a causa del continuo adattamento dei truffatori alle diverse tecnologie. Non fornire alcun incentivo allo sviluppo di soluzioni di autenticazione innovative, bensì applicare un unico *standard* a tutte le transazioni *online* dell'Unione Europea, sarebbe in questo senso un 'regalo' ai truffatori, che potrebbero utilizzare su larga scala i metodi individuati per aggirare lo SCA.

Oggi, il quadro normativo dell'Unione Europeo non stabilisce alcun parametro per valutare

9 V. https://polcms.secure.europarl.europa.eu/cmsdata/upload/6f88b464-7412-468a-a554-a91e-65de8cc2/PSD2%20RTS%20scrutiny%20brf%20v10.pdf.

10 Lo studio è disponibile all'indirizzo https://www.ecommerce-europe.eu/app/uploads/2016/09/Suggestions-to-improve-European-Online-Payments-Regulation.pdf.

il tasso di sicurezza da utilizzare come base per valutare l'efficienza delle misure di prevenzione attuate da ciascun fornitore di servizi di pagamento. In altre parole, i diversi sistemi di autenticazione oggi utilizzati dalle diverse piattaforme di pagamento non sono valutati per l'effettiva capacità di prevenire frodi, ma secondo una valutazione del tutto teorica. Anche il sistema individuato dall'EBA, che vorrebbe applicarlo a tutte le piattaforme di pagamento, è cioè il risultato di una valutazione basata forse sulla sensazione che la somma di meccanismi di autenticazione particolarmente stringenti (almeno due di cui uno non riutilizzabile, come abbiamo visto) possa e debba costituire la risposta universale ai problemi di sicurezza degli acquisti *online*, ma non certo sull'evidenza scientifica. Questo, tuttavia, è un consueto errore di presunzione da parte del decisore pubblico, che si illude che il modo migliore per gestire un fenomeno sia farlo con un unico metodo, a prescindere dalle singole caratteristiche dei suoi singoli componenti.

Ciò che lo studio di Clever Advice propone – e che costituisce anche la proposta di fondo di quasi tutti i contributi critici emersi durante la consultazione aperta dall'EBA – è invece di misurare il tasso di frodi effettivamente compiute nelle transazioni effettuate in un determinato arco di tempo dai diversi gestori di piattaforme di pagamento, così da determinare un parametro quantitativo che consenta di stabilire la capacità di ogni gestore di gestire i rischi della propria piattaforma, così come l'efficacia delle singole misure di prevenzione. A seconda del 'punteggio' raggiunto in relazione al tasso di frodi individuato come medio, ogni gestore avrebbe la facoltà di adottare sistemi di controllo più o meno stringenti. In questo modo, il gestore di una piattaforma che dimostri di contenere il numero di frodi molto al di sotto della media, anche se applicando metodi basati solamente sul comportamento degli utenti, potrebbe essere esentato dal dover richiedere codici o password ai propri utenti. Si pensi, ad esempio, a una piattaforma di consegna di cibo *online*: si può supporre che a una persona che tutti i venerdì ordini una pizza allo stesso ristorante possa non essere richiesta, ogni venerdì, una combinazione di codici alfanumerici, anche in funzione del fatto che un'eventuale truffa comporterebbe una perdita economica molto minore di quella che genererebbe l'applicazione di regole così stringenti a un acquisto *online* altrimenti così semplice. Al contrario, i sistemi di controllo dovrebbero essere molto più pervasivi per acquisti tipicamente una tantum (si pensi a un gioiello, o a un televisore), con valore economico molto alto, su siti in cui l'utente sembra non avere mai effettuato alcun accesso.

Secondo questo diverso modello, la sicurezza degli utenti sarebbe garantita non da un sistema universale efficiente solo in teoria e presumibilmente assai limitante la fluidità degli acquisti *online*, ma dai risultati effettivi raggiunti dai diversi sistemi di controllo in concorrenza fra loro. I PISP, d'altro canto, sarebbero incentivati a sviluppare soluzioni e prodotti innovativi per limitare le frodi *online*, a fronte del beneficio di poter adottare sistemi più semplici in funzione dei risultati raggiunti.

Tale metodo, denominato Targeted Authentication (TA), consente di adottare un approccio mirato, da parte di ciascuna tecnica di autenticazione, rispetto al rischio potenziale di ciascuna transazione. È, in questo senso, l'esatto opposto dello SCA: un sistema flessibile, dinamico, basato sul risultato e non sulla teoria. Le tecniche di TA, infatti, consentono di valutare in tempo reale il rischio di ogni transazione, secondo algoritmi dotati di autoapprendimento, così da essere in grado di monitorare caratteristiche biometriche e comportamentali impensabili nei sistemi statici previsti dallo SCA (orari e posizioni di acquisto, tipologia di beni acquistati di recente, ecc.). Inoltre, il TA tiene in considerazione il fattore di rischio di ciascuna operazione, a partire dal suo valore economico, per non irrigidire inutilmente l'esperienza di acquisto. Di conseguenza, tali tecniche prevedono sistemi di autenti-

cazione molto complessi in caso di pagamenti di somme alte o per beni non comunemente acquistati, mentre semplificano il procedimento in caso di acquisti di valore modesto o secondo metodi di acquisto adottati di frequente dal singolo utente.

Conclusioni

La PSD2 costituisce indubbiamente un quadro di riferimento moderno e innovativo per l'economia digitale nell'Unione Europea, incentivando la semplificazione e l'uniformità degli acquisti *online*. L'esigenza – doverosa – di garantire la sicurezza dei pagamenti offre tuttavia aree di potenziale miglioramento. Lo SCA – come previsto dall'EBA – dovrebbe certamente essere un'opzione disponibile, ma all'interno di un contesto in cui ai PISP sia permesso di offrire tecniche di autenticazione alternative. Viceversa, lo SCA si traduce in un procedimento gravoso, soprattutto per le PMI, che influirebbe negativamente sull'esperienza degli utenti, aumentando il tasso di abbandono dai procedimenti di acquisto e frenando le opportunità di investire in soluzioni di prevenzione innovative.

Come si è visto, esistono tecniche sofisticate, nel campo del Targeted Authentication, in grado di offrire livelli di protezione pari, se non superiori, a quelle tradizionali, senza tuttavia complicare eccessivamente l'esperienza di acquisto *online*, e aumentando significativamente il tasso di conversione dei processi di pagamento *online* in acquisti veri e propri.

Tali tecniche, all'interno della PSD2, sono previste soltanto per la gestione dei rischi di acquisti transnazionali, tramite rilevazione e profilatura degli utenti nei pagamenti con carte di credito. Viceversa, il TA dovrebbe essere esteso a tutte le transazioni, come strumento di valutazione dell'efficacia dei diversi sistemi di autenticazione per consentire quantomeno un'applicazione flessibile – e orientata al risultato effettivo di contrasto alle frodi – dello SCA.

Istituto Bruno Leoni
idee per il libero mercato

IBL Focus

Chi Siamo

L'Istituto Bruno Leoni (IBL), intitolato al grande giurista e filosofo torinese, nasce con l'ambizione di stimolare il dibattito pubblico, in Italia, promuovendo in modo puntuale e rigoroso un punto di vista autenticamente liberale. L'IBL intende studiare, promuovere e diffondere gli ideali del mercato, della proprietà privata, e della libertà di scambio. Attraverso la pubblicazione di libri (sia di taglio accademico, sia divulgativi), l'organizzazione di convegni, la diffusione di articoli sulla stampa nazionale e internazionale, l'elaborazione di brevi studi e briefing papers, l'IBL mira ad orientare il processo decisionale, ad informare al meglio la pubblica opinione, a crescere una nuova generazione di intellettuali e studiosi sensibili alle ragioni della libertà.

Cosa Vogliamo

La nostra filosofia è conosciuta sotto molte etichette: "liberale", "liberista", "individualista", "libertaria". I nomi non contano. Ciò che importa è che a orientare la nostra azione è la fedeltà a quello che Lord Acton ha definito "il fine politico supremo": la libertà individuale. In un'epoca nella quale i nemici della libertà sembrano acquistare nuovo vigore, l'IBL vuole promuovere le ragioni della libertà attraverso studi e ricerche puntuali e rigorosi, ma al contempo scevri da ogni tecnicismo.

Istituto Bruno Leoni – Piazza Cavour 3 - 10123 Torino – Italy
T: +39 (011) 1978 1215 – F: +39 (011) 1978 1216 – www.brunoleoni.it – info@brunoleoni.it