COMITATO PAGAMENTI ITALIA

RESOCONTO RIUNIONE COMITATO PAGAMENTI ITALIA (CPI) – Codise

Il 26 gennaio 2016 si è tenuta presso la Banca d'Italia una riunione straordinaria del Comitato Pagamenti Italia, aperta alla partecipazione di membri del Codise (Comitato per la continuità operativa della piazza finanziaria italiana)
La prima parte della sessione ha avuto ad oggetto la consultazione EBA relativa al *Discussion Paper* sulla bozza di standard tecnici sull'autenticazione forte del cliente e i requisiti per la comunicazione sicura ai sensi della PSD2.
La seconda parte della riunione ha riguardato la consultazione BRI sulla resilienza *cyber* per le infrastrutture dei mercati finanziari.
hanno partecipato, oltre a rappresentanti della Banca d'Italia (BI)[1], esponenti di ABI, AbiLab, Banca Sella, Banco Popolare, BancoPosta, BNL, Borsa Italiana, BPER, Cabel, Cariparma, CBI, CCG, Cedacri, Consob, Consorzio Bancomat, Consorzio Triveneto, Credem, CSE, Deutsche Bank, E-Mid, Equens, Fineco, Iccrea, Intesa San Paolo, Ivass, Mediobanca, MEF, Monte dei Paschi di Siena, Monte Titoli, MTS, Poste Italiane, Sia, Unibanca, Unicredit.
Il dibattito è stato preceduto, nella prima sessione, da una presentazione tenuta dal dott. Giambelluca e dalla dott.ssa Costanza Iacomini in tema di evoluzioni normative in materia di sicurezza nei pagamenti *retail*; la seconda sessione di discussione è stata preceduta da una presentazione tenuta dall'ing. Sciusco sulla Guida "*on cyber resilience for financial market infrastructures*".

PRIMA SESSIONE

Nel corso della **prima sessione** sono stati discussi alcuni dei quesiti presenti nel Discussion Paper dell'EBA, riguardanti 5 aree tematiche:

1) i **requisiti per l'autenticazione forte** del cliente quando questi acceda al proprio conto online, dia inizio ad un pagamento elettronico o esegua azioni che possano implicare un rischio di frode o di altri abusi nei pagamenti[2];
2) le **esenzioni nell'applicazione dell'autenticazione forte**, basate sul livello di rischio specifico del servizio di pagamento, sul valore e/o la ricorrenza della transazione, sul canale di pagamento utilizzato[3];

---

[1] Per Banca d'Italia erano presenti al tavolo dei relatori il dott. Gammaldi, il dott. Giambelluca, la dott.ssa Costanza Iacomini e l'ing.Sciusco.

[2] Cfr. domande:

(Q1) Quali azioni svolte dall'utente on-line, oltre all'accesso al conto e alla disposizione dei pagamenti, meritano di essere incluse tra le "azioni che comportano rischi di frode" da assoggettare ad autenticazione forte?
(Q4) Quali problematiche può comportare il rispetto del requisito dell'"indipendenza" degli elementi nell'autenticazione forte?
(Q5) Quali sfide o difficoltà intravedete nell'implementazione del requisito dell'autenticazione legata all'importo e al beneficiario della transazione?

[3] Cfr. domande:

(Q7-Q8) Quali casistiche ritenete necessario che siano prese in considerazione come esenzioni dall'applicazione dell'autenticazione forte?

3) i requisiti che le misure di sicurezza devono soddisfare per tutelare la **riservatezza e l'integrità delle credenziali di sicurezza** personalizzate degli utenti di servizi di pagamento[4];
4) i **requisiti per standard aperti di comunicazione comuni e sicuri** ai fini dell'identificazione, dell'autenticazione, della notifica e della trasmissione di informazioni, nonché dell'attuazione delle misure di sicurezza, tra banche, Payment Initiation Service Providers, Account Information Service Providers, pagatori, beneficiari e altri prestatori di servizi di pagamento[5];
5) le possibili **sinergie con il Regolamento e-IDAS** sull'identità digitale[6].

Con riguardo al **primo punto**, R. Stasi (AbiLab) fa notare che l'autenticazione forte richiama casistiche già disciplinate dalle recenti linee guida dell'EBA sugli *internet payments* e che l'elemento di maggiore novità per gli operatori, che i nuovi standard tecnici EBA dovranno gestire in base alla PSD2, consiste nel cd. "*dinamic linking*" collegato all'importo e al beneficiario della transazione. In questo caso, è stata auspicata una attenta valutazione dei reali rischi insiti nelle diverse tipologie di pagamenti al fine di apprestare misure appropriate al tipo di transazione e alle particolari caratteristiche delle stesse, come ad esempio l'importo, evitando di realizzare tutele eccessive per transazioni a più basso rischio .
Altri partecipanti, tra cui S. Stefanelli (Cedacri), hanno sottolineato come l'aumento delle misure richieste per potere fruire di determinati servizi possa costituire un ostacolo alla fruibilità e accessibilità delle transazioni. In tale ottica, risulterebbe necessario gestire il *trade off* tra sicurezza e flessibilità: apprestare controlli più sicuri a tutela dell'identità digitale dei soggetti può comportare una certa refrattarietà, nell'utente, all'uso dello strumento digitale e pertanto andrebbe utilizzato un approccio realmente proporzionale al rischio insito nello strumento stesso.
È stata in tale sede prospettata l'opportunità di valorizzare il più possibile la responsabilità del soggetto che presta il servizio: ove si prevedesse una correlazione tra discrezionalità nell'adozione delle misure e responsabilità patrimoniale del prestatore dei servizi di pagamento, sarebbe esso stesso a preoccuparsi di rendere il servizio più sicuro, facendo gravare meno il problema sull'utente finale.
E' stata inoltre enfatizzata l'opportunità, ai fini della sicurezza del sistema, di rafforzare i presidi di identificazione dei diversi soggetti che in esso operano, anche mediante l'estensione dei controlli a soggetti che non rientrano, ad oggi, direttamente nel campo di applicazione della PSD2.
A tal proposito, è stato fatto presente (G. Giambelluca) che una delle novità della PSD2 consiste proprio nell'ampliamento dell'ambito applicativo a operatori tecnologici, come i cd. Third Party Provider (TPP) che offrono servizi di accesso ai conti, e nella previsione di regole per la comunicazione sicura tra tutti i soggetti che intervengono nel processo di pagamento, inclusi i TPP. Si va dunque nella direzione auspicata della creazione di un ambiente controllato per tutte le relazioni inter-PSP, che rappresenta un'importante base di partenza per l'offerta di servizi sicuri agli utenti.

---

[4] Cfr. domande:
(Q12) Conoscete soluzioni innovative che possano garantire la protezione delle credenziali dell'utente nelle diverse ipotesi di utilizzo (es. enrolment)?
(Q14) In quale fase del processo di pagamento sono maggiori i rischi per la riservatezza e l'integrità delle credenziali?
[5] Cfr. domande:
(Q16) Quali requisiti dovranno essere fissati nella normativa EBA per conseguire gli obiettivi di armonizzazione/innovazione e favorire al contempo l'adozione degli standard per la comunicazione sicura da parte di tutti gli attori coinvolti?
(Q17) Siete a conoscenza di standard di riferimento, già diffusi o in via di sviluppo, utilizzabili per la comunicazione sicura?
[6] Cfr. domande:
(Q19) Ritenete che i servizi di identità digitale offerti da e-Id provider in conformità al Regolamento e-IDAS, possano costituire una soluzione concreta per facilitare gli adempimenti PSD2 (autenticazione forte, protezione credenziali, comunicazione sicura, ecc…)?

In merito al quesito che richiede quali difficoltà si intravedano nella implementazione dell'autorizzazione forte legata all'importo e al beneficiario della transazione, il rappresentante del Credito Emiliano (S. Chiriatti) evidenzia come non sempre sia possibile, per i nuovi strumenti richiesti dall'utenza e che si affacciano sul mercato, tenere conto dei requisiti richiesti, a causa delle concrete tecnologie disponibili; per esempio, per alcuni strumenti non sarebbe possibile l'inserimento di codici diversi da quelli numerici e ciò rende di fatto impraticabile la introduzione di requisiti alfabetici, pure richiesti dalla normativa per la codifica del beneficiario.
Sempre in merito allo stesso quesito, è stato da più parti evidenziato, e in particolare dal rappresentante del consorzio CBI, che andrà chiarito come applicare il requisito dell'autenticazione collegata a importo e beneficiario della transazione nel caso dei pagamenti aggregati disposti dalle imprese, che prevedono di norma l'autorizzazione di un unico flusso dispositivo.

Riguardo al **secondo punto di discussione**, partendo dalle ipotesi di esenzioni già evidenziate dallo stesso *Discussion Paper*, gli interventi hanno sollecitato la necessità di :

- esentare dagli obblighi normativi alcuni pagamenti di piccolo importo;
- tenere in considerazione la condotta dei pagatori a fini di esenzione e stilare black list e white list;
- valutare alcuni casi di accesso ai conti e addebito diretto (es. SDD B2B);
- rafforzare le analisi dei rischi delle transazioni per tenere conto concretamente soltanto di quelle per le quali sussistano pericoli di frode.

Con riferimento a tale ultimo punto, in particolare, è stato fatto presente che i presidi antifrode, che controllano il comportamento abituale del cliente, sono stati, in molti casi, più efficaci dei sistemi di autenticazione forte: gli algoritmi che controllano i comportamenti sono considerati validi sostituti e possono evitare sovrapposizioni. L'aspetto della *risk analysis* è emerso infatti come punto di particolare attenzione e argomento in evoluzione nell'ambito delle politiche di sicurezza**.**
In merito al *direct debit,* è stata segnalata da BI (Giambelluca) la eventualità di un chiarimento interpretativo per definire se ad esso potrà applicarsi la normativa in esame; altre attività, come quella della firma del mandato all'addebito, potranno invece essere classificate tra le azioni a rischio frode soggette a autenticazione forte, come già previsto nelle vigenti Linee Guida dell'EBA sugli *internet payments*.
Complessivamente è emersa, in tema di esenzioni, la richiesta da parte dei PSP di un certo grado di flessibilità, per lasciare la possibilità a chi amministra questi strumenti di autenticazione di poterli utilizzare efficacemente.

Il **terzo punto di discussione** muove dall'art 97 comma 3 della Direttiva, il quale prevede che gli Stati membri provvedano a che siano realizzate misure di sicurezza adeguate a tutelare la riservatezza e l'integrità delle credenziali di sicurezza personalizzate degli utenti di servizi di pagamento.
La discussione, ancora una volta, ha fatto emergere la preoccupazione che la ricerca di maggiori livelli di sicurezza si traduca in una perdita di flessibilità: le esigenze di sicurezza e flessibilità potrebbero essere coniugate attraverso un approccio realmente proporzionato al rischio differenziando i presidi di sicurezza in relazione alla tipologia, alla funzione e ai destinatari (consumatori e non consumatori).
Riguardo al quesito relativo alla conoscenza di soluzioni innovative e alle fasi in cui si concentrano i maggiori rischi a riservatezza e integrità dei dati, è stato fatto notare come andrebbero rafforzate al massimo le misure in capo all'utente e definiti con chiarezza i rapporti tra PSP e utilizzatore finale in caso di mancata attivazione dei presidi.
Al fine di tutelare la riservatezza delle credenziali degli utenti, è emersa l'esigenza preminente di definire gli ambiti di intervento e i poteri dei TPP, anche dal punto di vista strettamente tecnico, e di tenere conto dei rischi che la circolazione di credenziali attraverso un soggetto terzo può

comportare. Sebbene la tecnologia permette di focalizzare, sulla base di alcuni parametri, i punti in cui si annidano i maggiori rischi, non sempre è facile individuare le vullnerabilità in presenza di soggetti terzi che si frappongono tra l'utilizzatore e il PSP. Anche dal lato del cliente, non sempre è facile comprendere alcune logiche connesse ai nuovi servizi di accesso ai conti: si è richiamata pertanto la necessità di rafforzare la consapevolezza dei rischi connessi a tali nuovi paradigmi di mercato, anche attraverso una maggiore trasparenza nei rapporti contrattuali.
In tale contesto, è stato fatto notare (Giambelluca) che anche l'educazione finanziaria può svolgere un ruolo fondamentale. È stato inoltre sottolineato come la PSD2 ricerchi un adeguato bilanciamento tra l'esigenza, da un lato, di certezza/trasparenza delle responsabilità nei rapporti tra PSP e clienti e, dall'altro, di rispetto del principio di non discriminazione dei nuovi operatori, per evitare che possano essere create barriere o ostacoli per il solo fatto che il pagamento venga da un TPP.
Tra i problemi summenzionati, è stato evidenziato (AbiLab) come la diffidenza da parte dei PSP nei confronti dei TPP fosse anche dovuta alla mancanza di controlli in capo a questi soggetti: per il futuro saranno richieste le stesse garanzie di tutela previste per qualunque PSP e dovrebbero, in particolare, essere monitorati gli schemi contrattuali che vincoleranno tali soggetti alle banche ed altri PSP.
In tema di riservatezza e tutela della integrità dei dati, il rappresentante di Cariparma ha evidenziato l'opportunità che EBA chiarisca in che termini sia utilizzabile il "dato biometrico" a fini di sicurezza/autenticazione delle transazioni.

Il **quarto punto di discussione** si riferisce all'art 98 della Direttiva, il quale prevede che l'EBA definisca **requisiti per standard aperti di comunicazione comuni e sicuri** ai fini dell'identificazione, dell'autenticazione, della notifica e della trasmissione di informazioni tra banche, *Payment Initiation Service Providers*, *Account Information Service Providers*, pagatori, beneficiari e altri prestatori di servizi di pagamento.
Si tratta di requisiti che devono da un lato garantire una comunicazione sicura e dall'altro evitare di creare nuove frammentazioni: tali requisiti costituiranno la base per lo sviluppo degli standard di comunicazione da parte degli organismi competenti.
E' stato richiesto ai partecipanti, tra l'altro, se essi fossero a conoscenza di standard di riferimento, già diffusi o in via di sviluppo, utilizzabili per la comunicazione sicura.
Il Consorzio AbiLab ha fatto presente come sia importante individuare nel mercato la *governance* dei soggetti deputati a realizzare tali standard. Nel corso della discussione è stato evidenziato il rischio che il mercato non prenda in carico questa attività, anche a causa dei tempi ristretti a disposizione e dell'assenza di incentivi. Si è dunque sottolineata l'esigenza che l'EBA individui in maniera chiara i requisiti necessari per la definizione dei medesimi, in modo da agevolarne la redazione.
Il rappresentante di Unicredit (F. Bonora) ha notato in tale sede come per individuare uno standard di comunicazione sicura sarebbe importante separare standard tecnici, protocolli di comunicazione e sistemi di sicurezza che rientrano nel modello operativo dell'impresa. Non sarebbe irrilevante definire se l'adozione di un linguaggio *xml* sia sufficiente a garantire la comunicazione oppure debba essere necessario adottare protocolli e standard anche avendo a riferimento le esperienze di altri settori.
Il dott. Gammaldi ha evidenziato il fatto che i requisiti rappresenteranno dei "principi – matrice" su cui innestare basare lo standard, il quale deve avere però capacità di auto-modificarsi nel tempo, così da evitare anacronismi e una "over-regolamentazione". Ciò premesso, da un lato i principi dovrebbero contenere almeno delle informazioni utili o condivise per poi definire gli standard, dall'altro gli standard dovrebbero avere delle regole di autoregolamentazione, ovvero delle proprie regole di autocorrezione nel tempo (per esempio attraverso entità come l'*ISO*).
Il rappresentante di CSE (Tinti) ha precisato l'esigenza per i PSP di "esplodere" i servizi utilizzabili da terze parti per i servizi evoluti di pagamento: EBA dovrebbe individuare un set minimo di servizi

che il PSP dovrebbe essere obbligato a esporre alle terze parti o agli altri attori per poter adempiere alla normativa; in questo modo verrebbe garantito un set minimo di operazioni al mercato e un livello minimo di sicurezza con cui esporre queste informazioni, che dovrebbe anche consentire l'identificazione del TPP da parte dell'utente bancario al momento di accesso allo strumento che viene messo a disposizione. Ci si immagina pertanto una lista di servizi che presuppongono una tassonomia condivisa e livelli minimi di requisiti accedibili.
Il rappresentante di *Deutsche Bank* (Toso) ha evidenziato infine su questo argomento cosa a suo avviso debba intendersi per sicurezza, ovvero "identità dell'originatore e protezione del messaggio"; ciò premesso , data l'opportunità di potere riconoscere se l'operazione sia stata prodotta direttamente ovvero intermediata, queste informazioni dovrebbero essere previste come requisiti riconoscibili e vincolanti. Essi dovrebbero infatti non essere discrezionali: dovrebbe trattarsi di certificati con cui proteggere la comunicazione e ogni soggetto "potrebbe applicare" il suo certificato.

Con riguardo al **quinto punto**, l'attenzione si è focalizzata sulle potenziali sinergie tra la normativa contenuta nel Regolamento e-IDAS e qualle riguardante la sicurezza e l'autenticazione dei pagamenti. Ci si è dunque chiesti se i sistemi di identità digitali disciplinati dal Regolamento possano essere utili in termini di sicurezza e in tal caso se essi possono impattare sui requisiti che EBA sta definendo.
Nel corso della discussione si è preliminarmente distinto (Stasi-AbiLab) tra il servizio di identificazione e quello in argomento: l'identificazione risponde in sé a finalità di conoscenza del cliente e pertanto attiene più alla relazione col cliente stesso; la sicurezza invece si riferisce allo strumento: **gli ambiti possono anche coincidere laddove si usi lo strumento dell'identità digitale in funzione di sicurezza**. Tale distinzione vale anche per SPID, il nuovo Sistema Pubblico di Identità Digitale, che risponde a finalità di identificazione e non è detto che possa essere utilizzata da tuti i PSP anche in funzione di sicurezza in quanto tale utilizzo è comunque sempre subordinato a valutazioni di business e di rischio.
Secondo la dott.ssa Azzolini (BNL), considerato che l'impianto normativo in discussione andrà in attuazione nel 2018, la massima raccomandazione sarebbe quella di individuare un *framework* di responsabilità che consenta di stare sul mercato in modo aperto e competitivo.
Il dott. Gammaldi in proposito ha spiegato come la PSD1 abbia dovuto rincorrere alcune soluzioni tecnologiche e di processo e come in tal caso i rischi possano essere di due tipi: che le modalità di autenticazione prodotte dalla normativa siano in contrasto con gli standard creando ambiguità; che si manifesti un possibile contrasto tra normativa europea e normativa nazionale e ne derivino problemi di conformità. I tempi della normativa possono essere molto lunghi rispetto all'evoluzione della tecnologia se si considera che già dalla firma della normativa PSD2 alla pubblicazione sono trascorsi diversi mesi a cavallo tra il 2014 e il 2015 e che successivamente sono richiesti 18 mesi per l'attuazione. L'impegno del regolatore e della BI in particolare nel semestre di Presidenza italiana è stato soprattutto quello di tener conto, nella predisposizione delle norme e nella disciplina dei casi concreti, della rapidità di rinnovamento e obsolescenza e della tecnologia.

SECONDA SESSIONE

La seconda sessione ha riguardato la consultazione BRI sulla resilienza cyber per le infrastrutture dei mercati finanziari e ha rappresentato l'occasione per un più ampio dibattito sulle tematiche di cyber resilience.

Il Committee on Payments and Market Infrastructures (CPMI) e la International Organisation of Securities Commissions (IOSCO) hanno pubblicato, per una consultazione pubblica (scadenza 23 febbraio 2016), una guida per migliorare la resilienza a fronte di minacce cyber delle Financial

Market Infrastructures, sul presupposto che il livello di resilienza operativa delle FMI, compresa quella cyber, può essere un fattore decisivo nella resilienza totale del sistema finanziario e dell'economia in generale.
Considerato che la guida non impone requisiti aggiuntivi rispetto ai CPMI-IOSCO Principles for Financial Market Infrastructures (PFMI) e che vi vengono definiti principi e non regole, nel dibattto è stato evidenziato che il principale riferimento normativo in materia cyber resilience continua a essere rappresentato dalla regolamentazione di sorveglianza e vigilanza nazionale (Circ. 285 e Linee Guida SMP in materia di continuità operativa delle infrastrutture di mercato) che richiama il rischio cyber nell'ambito della gestione del rischio operativo e della continuità di servizio. La Guida intende rendere operanti tali principi non attraverso uno strumento cogente ma demandando alle Autorità il presidio della coerenza complessiva di tutta la filiera. Il dott. Gammaldi ha fatto presente che l'applicazione in concreto della Guida CPMI-IOSCO può richiedere la re-interpretazione di alcuni principi; per esempio, con riguardo ai tempi di ripristino di cui al principio 17 appare necessario considerare minacce cyber estreme ma plausibili e porre in essere le azioni necessarie per costruire una capacità di ripartenza entro due ore da un evento distruttivo (in coerenza con il principio 17 dei PFMI). La guida, pur riconoscendo le difficoltà di raggiungere tale obiettivo, sottolinea come siano già disponibili opzioni tecniche e organizzative che potrebbero essere implementate per soddisfare la conformità con il requisito.
Il rappresentante di Banca Intesa ha auspicato, accanto alle iniziative private, un intervento delle autorità pubbliche che tenga conto e metta a fattor comune quanto già si è cominciato a sviluppare a livello privatistico.
A tale proposito, il dott. Gammaldi ha richiamato l'importanza su questo tema della direttiva europea NIS, in corso di emanazione, che attribuisce un ruolo centrale al partenariato pubblico-privato per lo scambio di informazioni e best practice nell'ambito della sicurezza delle reti e dell'informazione. L'approccio su tale materia del legislatore europeo riconosce un ruolo di primo piano alle strategie nazionali per la cybersecurity; al riguardo è stato ricordato che la Banca d'Italia attua una stretta collaborazione con i vari attori istituzionali coinvolti. In fase di recepimento della NIS, saranno presidiati alcuni aspetti al fine di evitare sovrapposizioni normative e mantenere la coerenza con le norme di settore. Indipendentemente dagli interventi che si renderanno necessari per l'attuazione della direttiva NIS, in Banca d'Italia si è avviata una riflessione in materia di info-sharing nell'ambito del settore finanziario.
P. Francescucci (Unicredit) ha messo in evidenza come l'applicazione della guida potrebbe comportare adempimenti, anche non indifferenti, per le imprese: in primo luogo, per fronteggiare un cyber attack, che determini interruzione alla continuità, è necessario che le aziende si dotino di competenze specifiche e definiscano una chiara responsabilità dei ruoli all'interno dell'organizzazione in tema di cyber-security; in secondo luogo, il problema delle interdipendenze tra fornitori critici rende auspicabile avviare quanto prima un tavolo congiunto ove il regulator possa incidere significativamente.
Il dott. Gammaldi ha fatto presente che le interdipendenze che vengono a crearsi tra infrastrutture e normative di diversi settori rappresentano una complessità da tenere sotto controllo. È importante individuare la tipologia di interdipendenze (finanziarie o tecnologiche), in che modo la norma possa regolamentare questi aspetti con un livello di dettaglio tale da non essere inappropriata o a rischio obsolescenza.
R. Stasi (AbiLab) e la rappresentante di Intesa sono intervenuti in merito ai potenziali impatti dei nuovi principi sugli assetti preesistenti e sulle relazioni con l'attuale normativa di vigilanza.
A chiusura della presentazione il dr. Gammaldi ha infine inteso evidenziare come il rischio cyber, non nuovo per il settore e per le autorità competenti, ha assunto nel contesto di mondo fortemente interconnesso e di economie di rete una rilevanza maggiore per: i) l'aumento esponenziale dei dati e dei servizi digitali (anche di pagamento); ii) l'aumento della complessità dei sistemi che condividono non solo interdipendenze ma anche vulnerabilità nel cyberspace; iii) la crescente

diversificazione e sofisticazione della minaccia cyber. In questo contesto va inquadrata la guida sulla cyber resilience.