Giugno 2016

Sicurezza dei pagamenti via internet: l'aggiornamento della Circolare Banca d'Italia n.285/2013 in recepimento degli Orientamenti dell'Autorità Bancaria Europea

Avv. Damiano Di Maio

Introduzione

Con la pubblicazione, in data 17 maggio 2016, del 16° aggiornamento della Circolare n. 285 del 17 dicembre 2013 recante "Disposizioni di vigilanza per le banche" (G.U. n. 127 del 1 giugno 2016 – Supplemento Ordinario n. 17), l'Autorità di vigilanza italiana ha provveduto a recepire le previsioni regolamentari elaborate dall'Autorità Bancaria Europea (di seguito per brevità, l'ABE) finalizzate ad accrescere il livello di sicurezza dei pagamenti via internet, nell'ambito di una cornice normativa comune su base europea.

Con il predetto aggiornamento si prefigurano una serie di nuovi adempimenti che impatteranno trasversalmente sull'organizzazione e sull'operatività dei soggetti destinatari delle previsioni in esso contenute, in attesa peraltro che venga recepita

nell'ordinamento italiano[1] la Direttiva (UE) 2015/2366 del 25 novembre 2015 (di seguito, Direttiva PSD2)[2] recante la rinnovata disciplina relativa ai servizi di pagamento nel mercato interno, che abroga[3] la Direttiva 2007/64/CE (di seguito Direttiva PSD).

Il presente contributo si propone pertanto di illustrare sinteticamente le principali novità intervenute nel *corpus* normativo delle richiamate Diposizioni di vigilanza, al fine di individuarne i concreti effetti sui modelli di *business* e di governo dei processi per gli operatori economici coinvolti, anche alla luce delle problematiche emerse e delle indicazioni fornite dalla Banca d'Italia in sede di resoconto alle consultazioni.

1. Gli Orientamenti dell'Autorità Bancaria Europea sulla sicurezza dei pagamenti via internet recepiti nella disciplina di vigilanza

La pubblicazione sul sito dell'ABE lo scorso 5 marzo, degli "Orientamenti finali sulla sicurezza dei pagamenti via internet" [4] del 19 dicembre 2014 (di seguito, per brevità, gli Orientamenti) si inserisce all'interno di un quadro normativo europeo, quello della disciplina relativa ai servizi di pagamento nel mercato interno, recentemente oggetto di importanti modifiche[5].

Per quanto concerne l'impostazione adottata dall'ABE nella formulazione dei predetti Orientamenti, a seguito dei risultati emersi in sede di consultazione[6], l'Autorità di vigilanza europea optava per un approccio *two-step*, fondato:

a) sull'elaborazione ed implementazione di linee guida che replicano il contenuto delle raccomandazioni della Banca Centrale Europea[7] del 31 gennaio 2013 e che rappresentano, come indicato dalla Banca d'Italia, *"il documento a fronte del quale le banche centrali, nell'esercizio della propria funzione di sorveglianza sui sistemi e sugli*

[1] Ai sensi del combinato disposto di cui ai commi 1 e 2 dell'art. 118 della Direttiva PSD2, gli Stati membri adottano, pubblicano le misure necessarie per conformarsi alla Direttiva e applicano tali misure a partire dal 13 gennaio 2018.
[2] Entrata in vigore il 13 gennaio 2016.
[3] A decorrere dal 13 gennaio 2018, secondo quanto previsto dall'art. 114 comma 1 della Direttiva PSD2.
[4] Cfr. ABE/GL/2914/12 "Orientamenti finali sulla sicurezza dei pagamenti via internet emanati ai sensi dell'art. 16 del Regolamento istitutivo dell'ABE n. 1093/2010, disponibili all'indirizzo: https://www.eba.europa.eu/documents/10180/1004450/EBA_2015_IT+Guidelines+on+Internet+Payments.pdf/b9c5dee9-78bd-47c5-a80c-4d2f3f8a1de2.
[5] Cfr.: Introduzione.
[6] Cfr.: EBA "Consultation Paper on the implementation of draft EBA Guidelines on the security of internet payments prior to the transposition of the revised Payment Services Directive (PSD2)", 20 ottobre 2014.
[7] Disponibili all'indirizzo: https://www.ecb.europa.eu/pub/pdf/other/recommendationssecurityinternetpaymentsoutcomeofpcfinalversionafterpc201301en.pdf.

strumenti di pagamento, valutano la conformità agli standard di sicurezza dei pagamenti via internet[8] *"*;

b) sulla implementazione futura di requisiti più stringenti una volta attuata la Direttiva PSD2[9].

1.1 Ambito di applicazione soggettivo

Ai sensi del Titolo I punto 2 degli Orientamenti, risultano destinatari della rinnovata normativa regolamentare i prestatori di servizi di pagamento per come definiti dall'art. 1 della Direttiva PSD:

a) gli enti creditizi ai sensi dell'articolo 4, punto 1, lettera a), della direttiva 2006/48/CE;

b) gli istituti di moneta elettronica ai sensi dell'articolo 1, paragrafo 3, lettera a), della direttiva 2000/46/CE;

c) gli uffici postali che hanno il diritto di prestare servizi di pagamento a norma del diritto nazionale;

---

[8] Cfr: Banca d'Italia, documento per la consultazione, "Recepimento in Italia degli orientamenti dell'ABE in materia di sicurezza dei pagamenti tramite canale internet", disponibile all'indirizzo https://www.bancaditalia.it/compiti/vigilanza/normativa/consultazioni/2015/recepimento-orientamenti-abe/index.html.

[9] Cfr. EBA/GL/2014/12 Final Guidelines, p.3 *"Given that the negotiations on the revision of the existing Payment Services Directive (PSD) were ongoing, and that SecuRe Pay had already consulted on the substance of the guidelines, the CP sought input solely from stakeholders with regard to how the potentially higher security standards required by the forthcoming PSD 2 as of 2017/18 should be catered for by the EBA: through a one-step approach in which the EBA anticipates and 'frontloads' future requirements from the implementation date of the guidelines on 1 August 2015 onwards, or a two-step approach that will see the guidelines implemented as consulted on 1 August 2015, with potentially more stringent requirements necessary under the PSD 2 being implemented at a later stage, as set by the PSD 2.*
The EBA received 45 responses to the CP, including a response from the EBA's Banking Stakeholder Group (BSG). The majority of responses stated that they would be able to agree with the two-step approach, although a significant number of these respondents did so only as a second-best solution, should their first choice — the EBA delaying the issuing of the guidelines until the transposition of the PSD 2 — not come to pass. Two responses expressed a preference for the one-step approach. A large minority of responses were against either option and proposed instead that the EBA should not issue the guidelines at all and instead wait until the transposition of the PSD 2 and its security requirements in 2017/18.
The EBA has assessed the responses and concludes that, due to the continually high levels of fraud observed on internet payments, a delay in the implementation of the guidelines until the transposition of the PSD 2 in 2017/18 is not a plausible option. Furthermore, given the preferences expressed by respondents, the EBA concludes that a one-step approach is not desirable. The EBA is therefore issuing the final guidelines with the substance as consulted, i.e. a
conversion of the original SecuRe Pay recommendations, with an implementation date of 1 August 2015, and the implementation of any potentially more stringent requirements under the PSD 2 at a later stage — by the date set in the PSD 2".

d) gli istituti di pagamento ai sensi della Direttiva PSD;

e) la Banca centrale europea e le banche centrali nazionali ove non agiscano in quanto autorità monetarie o altre autorità pubbliche;

f) gli Stati membri o le rispettive autorità regionali e locali ove non agiscano in quanto autorità pubbliche.

Volgendo lo sguardo alla disciplina italiana, le modifiche impattano in particolare le banche e le capogruppo di gruppi bancari, gli istituti di pagamento e gli istituti di moneta elettronica e gli intermediari finanziari di cui al Titolo V del Testo Unico Bancario (TUB) autorizzati alla prestazione di servizi di pagamento e/o all'emissione di moneta elettronica, iscritti ai relativi albi e inoltre Bancoposta.

1.2 Ambito di applicazione oggettivo

Con riferimento all'ambito di applicazione oggettivo, ovvero i servizi di pagamenti via internet attratti dalle, per utilizzare il termine dell'ABE, *"aspettative minime"* individuate negli Orientamenti[10], il punto 7 del Titolo I li individua, indipendentemente dal dispositivo di accesso utilizzato, nelle fattispecie di seguito elencate:

- carte, per tali intendendosi l'esecuzione dei pagamenti con carta via Internet, compresi i pagamenti con carta virtuale, così come la registrazione dei dati relativi alle carte di pagamento per l'utilizzo in *"soluzioni di tipo "Wallet"*;
- bonifici, per tali intendendosi l'esecuzione dei bonifici via Internet;
- mandato elettronico, per tale intendendosi l'emissione e la modifica dei mandati elettronici di addebito diretto;
- moneta elettronica, per tale intendendosi i trasferimenti di moneta elettronica tra due conti di moneta elettronica via Internet.

Restano escluse - per espressa previsione degli Orientamenti - alcune fattispecie tra le quali emergono i pagamenti le cui istruzioni sono trasmesse per posta, per telefono, posta vocale o utilizzando la tecnologia basata su SMS; per tale ultima fattispecie, peraltro, gli intermediari avevano avanzato dubbi sulla loro esclusione in quanto foriera di possibili effetti distorsivi sulla concorrenza, che tuttavia la Banca d'Italia in sede di resoconto alla consultazioni parrebbe aver escluso, asserendo che *"le ipotesi di esenzione sono definite dal legislatore UE con l'obiettivo di realizzare un bilanciamento tra servizi di pagamento riservati a intermediari autorizzati e fattispecie*

[10] Aspettative minime che *"non inficiano la responsabilità dei prestatori di servizi di pagamento di monitorare e valutare i rischi connessi alle loro operazioni di pagamento, sviluppare proprie politiche di sicurezza dettagliate e porre in essere adeguate misure di sicurezza, emergenza, gestione degli incidenti e continuità operativa, che siano commisurate ai rischi inerenti ai servizi di pagamento prestati"*, come precisato al punto 6 del Titolo I degli Orientamenti.

escluse dall'ambito di applicazione in ragione di alcune loro particolari caratteristiche[11]*".*

1.3 Contenuto sostanziale degli Orientamenti: fattispecie di maggior rilievo

Con riferimento al contenuto sostanziale degli Orientamenti, il Titolo II individua tre macro aree di disciplina che verranno di seguito illustrate nei loro aspetti più rilevanti: la prima impatta sull' assetto organizzativo dell'intermediario che deve essere in grado di prevenire, monitorare e controllare i rischi connessi all'ambiente di sicurezza dei pagamenti via internet; la seconda prevede tutta una serie di misure specifiche che nella concreta operatività dell'intermediario impattano sui rischi di sicurezza dei pagamenti via internet; la terza detta indicazioni sulla condotta degli intermediari, *latu sensu* riassumibile nei concetti di educazione finanziaria ed assistenza nel rapporto con i clienti.

1.3.1 L'assetto organizzativo per la prevenzione, il monitoraggio ed il controllo dei rischi connessi all'ambiente di sicurezza dei pagamenti via internet

Primo e fondamentale adempimento richiesto dagli Orientamenti (Titolo II punto 1) per strutturare un assetto organizzativo idoneo consiste, nella redazione, attuazione e riesame[12], di una formale policy di sicurezza per i servizi di pagamento via internet, che deve essere approvata dall'alta dirigenza e finalizzata a definire gli obiettivi di sicurezza e la propensione al rischio, mediante l'individuazione di ruoli e responsabilità dei vertici aziendali.

Nell'ambito dell'attività commerciale dell'intermediario, è richiesta poi una valutazione documentata dei rischi sia nella fase antecedente all'avvio dell'offerta dei servizi, che nel continuo, con frequenza regolare.

Elemento fondamentale per valutare la tenuta dei presidi di gestione del rischio adottati nella policy e attuati mediante le soluzioni tecnologiche utilizzate dall'intermediario, è l'incidente relativo alla sicurezza[13], la cui gestione deve essere documentata da una o

---

[11] Banca d'Italia, Resoconto della consultazione, *"Recepimento in Italia degli orientamenti dell'ABE in materia di sicurezza dei pagamenti tramite canale internet"*, p. 2.

[12] Il riesame viene richiesto *"(…) in linea con l'Orientamento 2.4* [del Titolo II]", che distingue due tipologie di revisione degli scenari di rischio: la prima, fondata su tre fattispecie e che si rende necessaria al verificarsi dell'evento: i) dopo gli incidenti gravi che interessano i servizi, ii) prima di un cambiamento importante delle infrastrutture o delle procedure iii) quando nuove minacce sono individuate attraverso attività di monitoraggio dei rischi.
La seconda è invece prevista come revisione generale che dovrebbe essere fatta almeno una volta l'anno.

[13] Tra cui vi è espressamente ricompreso il reclamo del cliente in materia di sicurezza (cfr. punto 3 degli Orientamenti).

più procedure che descrivano i *flussi informativi interni* verso l'alta dirigenza e i *flussi informativi esterni* verso le autorità competenti per l'ipotesi gravi incidenti[14].

Sempre nell'ottica di garanzia di flussi informativi e cooperazione nella gestione di gravi incidenti relativi alla sicurezza dei pagamenti, l'Autorità di vigilanza richiede ai prestatori di servizi di acquiring di intervenire sui contratti stipulati con gli operatori commerciali online che conservano, elaborano o trasmettono i dati sensibili relativi ai pagamenti, prevedendo un obbligo di cooperazione alla cui violazione l'intermediario dovrebbe *"(...) procedere all'applicazione* [dell']*obbligo contrattuale"*[15] o alla risoluzione del contratto; alle medesime conseguenze dovrebbe giungersi nell'ipotesi in cui, sempre nel rapporto contrattuale tra i soggetti sopra indicati, gli operatori commerciali online non attuino le misure relative al controllo e alla mitigazione dei rischi individuati negli Orientamenti da 4.1 a 4.7 al fine di evitare il furto dei dati sensibili relativi ai pagamenti attraverso i loro sistemi.

Sul punto non sono mancati i dubbi espressi dagli intermediari in sede di resoconto alle consultazioni, che hanno evidenziato come:

i) l'imposizione ai prestatori di servizio di pagamento dell'obbligo di inserire la clausola di cooperazione in caso di gravi incidenti di sicurezza, "[sarebbe risultata] *eccessivamente costosa rispetto ai potenziali benefici, in assenza di efficaci strumenti per assicurarne il rispetto*[16]*"*;

ii) l'inserimento delle clausole che obbligano l'esercente al rispetto delle misure di cui ai punti da 4.1 a 4.7 avrebbe presentato *"(...) criticità sia per il contenuto estremamente tecnico delle stesse*[17]*"* che per la circostanza che le regole di sicurezza potrebbero richiedere la necessità di aggiornamenti frequenti ed urgenti che mal si concilierebbero con le tempistiche in materia di modifica unilaterale dei contratti ex art. 126-sexies del TUB[18].

---

[14] Il grave incidente è definito, ai sensi del Titolo I punto 12 degli Orientamenti, come *"un incidente che ha o può avere un impatto significativo sulla sicurezza, sull'integrità e sulla continuità dei sistemi di pagamento dei prestatori di servizi di pagamento e/o sulla sicurezza dei dati sensibili sui pagamenti o dei fondi. La valutazione della rilevanza dovrebbe prendere in considerazione il numero di clienti potenzialmente interessati, l'importo a rischio e l'impatto su altri prestatori di servizi di pagamento o altre infrastrutture di pagamento"*.

[15] Cfr. Titolo II, punto 3.4 degli Orientamenti.

[16] Banca d'Italia, Resoconto della consultazione, *"Recepimento in Italia degli orientamenti dell'ABE in materia di sicurezza dei pagamenti tramite canale internet"*, p. 7.

[17] Banca d'Italia, Resoconto della consultazione, *"Recepimento in Italia degli orientamenti dell'ABE in materia di sicurezza dei pagamenti tramite canale internet"*, p. 7.

[18] Articolo 126-sexies TUB (Modifica unilaterale delle condizioni)

1. Ogni modifica del contratto quadro o delle condizioni e informazioni a esso relative fornite all'utilizzatore ai sensi dell'articolo 126-quater, comma 1, lettera a), è proposta dal prestatore dei servizi di pagamento secondo le modalità stabilite dalla Banca d'Italia, con almeno due mesi di anticipo rispetto alla data di applicazione prevista.

Ciò nondimeno, la Banca d'Italia, con riguardo al succitato punto i), ha chiarito la necessità di disciplinare contrattualmente gli obblighi di cooperazione poiché rappresentano un *"fattore di rilievo per l'innalzamento dei livelli di sicurezza nel settore dei pagamenti via internet*[19]*"*; con riferimento al successivo punto ii) l'Autorità di vigilanza ha precisato che i principi richiamati *"(…) hanno natura esemplificativa e generale*[20]*"* e pertanto la loro concreta imposizione seguirà ad una preventiva valutazione con riguardo all'effettivo livello di rischio del prestatore dei servizi di pagamento.

Avuto riguardo poi alle citate le misure relative al controllo ed alla mitigazione dei rischi, in estrema sintesi, l'ABE le individua nelle seguenti fattispecie:

- prospettazione di più livelli di difesa della sicurezza (difesa in profondità)[21];
- separazione dei compiti e dei ruoli negli ambienti della tecnologia dell'informazione[22];
- applicazione del principio del privilegio minimo[23] nell'accesso alle reti;
- creazione di "piste di controllo", ovvero registri e procedimenti di tracciabilità dei dati per limitare l'accesso ai dati sensibili relativi ai pagamenti e risorse critiche quali reti, sistemi, banche dati[24];

---

2. Il contratto quadro può prevedere che la modifica delle condizioni contrattuali si ritiene accettata dall'utilizzatore a meno che questi non comunichi al prestatore dei servizi di pagamento, prima della data prevista per l'applicazione della modifica, che non intende accettarla. In questo caso, la comunicazione di cui al comma 1, contenente la proposta di
modifica, specifica che in assenza di espresso rifiuto la proposta si intende accettata e che l'utilizzatore ha diritto di recedere senza spese prima della data prevista per l'applicazione della modifica.
3. Le modifiche dei tassi di interesse o di cambio possono essere applicate con effetto immediato e senza preavviso; tuttavia, se sono sfavorevoli per l'utilizzatore, è necessario che ciò sia previsto nel contratto quadro e che la modifica sia la conseguenza della variazione dei tassi di interesse o di cambio di riferimento convenuti nel contratto. L'utilizzatore
è informato della modifica dei tassi di interesse nei casi e secondo le modalità stabilite dalla Banca d'Italia.
4. Le modifiche dei tassi di interesse o di cambio utilizzati nelle operazioni di pagamento sono applicate e calcolate in una forma neutra tale da non creare discriminazioni tra utilizzatori, secondo quanto stabilito dalla Banca d'Italia.
5. Restano ferme, in quanto compatibili, le disposizioni di cui all'articolo 33, commi 3 e 4, del decreto legislativo 6 settembre 2005, n. 206.

[19] Banca d'Italia, Resoconto della consultazione, *"Recepimento in Italia degli orientamenti dell'ABE in materia di sicurezza dei pagamenti tramite canale internet"*, p. 7.

[20] Banca d'Italia, Resoconto della consultazione, *"Recepimento in Italia degli orientamenti dell'ABE in materia di sicurezza dei pagamenti tramite canale internet"*, p. 7

[21] Cfr.: Orientamenti, Titolo II punto 4.

[22] Cfr.: Orientamenti, Titolo II punto 4.1.

[23] Secondo cui *"Ogni programma e ogni utente privilegiato del sistema dovrebbe funzionare con la minor quantità di privilegi necessari per completare il lavoro"* (cfr.: nota 6 Orientamenti).

- applicazione del principio "Data minimisation", secondo cui la raccolta, il routing, l'elaborazione, la conservazione e la visualizzazione dei dati sensibili dovrebbero essere mantenute ad un livello di minimo assoluto;

- determinazione delle modalità di controllo, che coinvolgeranno:

    1) la funzione controllo dei rischi, la quale dovrà supervisionare i test periodici[25] sulle misure di sicurezza garantire la loro robustezza ed efficacia[26];

    2) la funzione internal audit, la quale dovrebbe verificare periodicamente le misure di sicurezza adottate proporzionalmente ai rischi per la sicurezza implicati e avvalendosi di soggetti esperti ed indipendenti rispetto allo sviluppo, alla realizzazione o alla gestione dei servizi di pagamento via internet prestati[27];

    3) la funzione di conformità, la quale, in sede di validazione di eventuali contratti di esternalizzazione, dovrà prestare particolare attenzione all'inclusione dei principi e degli orientamenti dell'ABE;

- tracciabilità di tutte le transazioni e processi di gestione del mandato elettronico[28] mediante, tra gli altri, l'inclusione nel servizio offerto di meccanismi di sicurezza per la registrazione dettagliata dei dati delle operazioni e dei mandati elettronici, fra cui il numero sequenziale dell'operazione, la marcatura temporale per i dati delle operazioni, le modifiche alla parametrizzazione, e l'accesso ai dati delle operazioni e dei mandati elettronici[29].

1.3.2 Le misure specifiche di controllo e sicurezza che impattano sui pagamenti via internet

Il secondo ambito di regolamentazione inserito nel Titolo II degli Orientamenti rileva in quanto oggetto di intenso confronto tra gli intermediari e la Banca d'Italia, per come documentato nel resoconto alle consultazioni, in relazione agli aspetti operativi per l'implementazione delle misure richieste.

---

[24] Cfr: Orientamenti, Titolo II punto 4.3.
[25] Sarà fondamentale che l'intermediario vada a strutturare il processo che regola i test e le eventuali modifiche che dovessero rendersi necessarie, per come richiesto dal Titolo II punto 4.5 degli Orientamenti *"(…) tutte le modifiche dovrebbero formare l'oggetto di un processo formale di gestione dei cambiamenti che garantisca che i cambiamenti siano correttamente ideati, sottoposti a prove, documentati e autorizzati. Sulla base dei cambiamenti effettuati e delle minacce alla sicurezza osservate, le prove dovrebbero essere ripetute regolarmente e comprendere scenari di attacchi potenziali pertinenti e noti"*.
[26] Cfr.: Orientamenti, Titolo II punto 4.5.
[27] Cfr.: Orientamenti, Titolo II punto 4.6.
[28] Cfr.: Orientamenti, Titolo II punto 5.
[29] Cfr.: Orientamenti, Titolo II punto 5.2.

In ragione di ciò, come in precedenza, si cercherà di fornire una lettura combinata tra detti Orientamenti ed i successivi chiarimenti della Banca d'Italia in sede di resoconto alle consultazioni, al fine di rappresentare un quadro della disciplina che possa raccordare gli adempimenti di matrice europea con quelli nazionali.

1.3.2.1 Identificazione inziale dei clienti e adempimenti di trasparenza

In particolare, il punto 6 del citato Titolo II degli Orientamenti, oltre richiamare l'attenzione degli intermediari sul rispetto degli obblighi di adeguata verifica dei clienti prima che i medesimi siano autorizzati ad accedere ai servizi di pagamento via internet,[30] richiede che i clienti confermino preventivamente la volontà di effettuare i pagamenti via internet utilizzando i servizi prima di potervi accedere; circa le modalità per ottemperare a detto Orientamento parrebbe essere ritenuto adeguato dalla Banca d'Italia l'inserimento nel contratto quadro di un riferimento alla possibilità di utilizzare la carta di credito per effettuare operazioni di pagamento su internet[31], fermo restando che *"(...) in ogni caso, sarà cura dell'intermediario adottare ogni misura utile a far sì che il cliente abbia piena consapevolezza di tale possibilità di utilizzo dello strumento*[32]*"*.

Con riguardo poi al punto 6.2 degli Orientamenti, vengono richieste tutta una serie di informazioni integrative rispetto alle previsioni della PSD[33], che i prestatori di servizi di pagamento dovrebbero fornire ai clienti e che di seguito si segnalano:

- informazioni chiare sui requisiti del cliente in termini di apparecchiature utilizzate dall'utente, software o altri strumenti necessari (per esempio software antivirus, firewall);
- orientamenti per l'uso corretto e sicuro delle credenziali di sicurezza personalizzate;
- una descrizione passo passo della procedura con la quale il cliente inoltra e autorizza un'operazione di pagamento e/o ottiene informazioni, inclusi gli esiti di ogni azione;
- orientamenti per l'uso corretto e sicuro di tutto l'hardware e il software fornito al cliente;

[30] Cfr.: Orientamenti, Titolo II, punti 6 e 6.1.
[31] Per come emerso nelle *"Osservazioni di Assofin al Documento di consultazione di Banca d'Italia"*, p. 5.
[32] Cfr.: Banca d'Italia, Resoconto della consultazione, *"Recepimento in Italia degli orientamenti dell'ABE in materia di sicurezza dei pagamenti tramite canale internet"*, p. 9.
[33] In particolare, gli Orientamenti precisano che le informazioni andranno ad integrare l'art. 42 della direttiva PSD che specifica le informazioni che il prestatore di servizi di pagamento deve fornire all'utente dei servizi di pagamento prima di stipulare un contratto per la fornitura dei servizi di pagamento (cfr. Orientamenti, punto 6.2, nota 12).

- le procedure da seguire in caso di perdita o furto delle credenziali di sicurezza personalizzate, o dell'hardware o del software del cliente per l'accesso o l'esecuzione delle operazioni;

- le procedure da seguire in caso di abuso riscontrato o sospetto;

- una descrizione delle responsabilità e degli oneri del prestatore di servizi di pagamento e del cliente, rispettivamente, per quanto riguarda l'uso del servizio di pagamento via Internet.

Sul punto, per quanto attiene ai possibili interventi da effettuare in ottemperanza alla normativa secondaria della Banca d'Italia in materia di Trasparenza delle operazioni e dei servizi bancari e finanziari e correttezza delle relazioni tra intermediari e clienti (di seguito, per brevità, Disposizioni di trasparenza) l'Autorità nazionale di vigilanza ha precisato che le citate informazioni di cui al punto 6.2 rappresentano *"(...) una specificazione del principio di carattere generale di cui all'*[orientamento] *6"* e che esse dovranno *"(...) essere rese nell'ambito dell'informazione preventiva di cui all'art 41 PSD così come recepito in Italia dal D.lgs. 11/2010 e dalle Disposizioni di Trasparenza"*.

Conseguentemente, parrebbe doversi prospettare un intervento di aggiornamento dei fogli informativi, in quanto le citate informazioni sembrerebbero rientranti nell'ambito delle *"caratteristiche e rischi tipici dell'operazione"* di cui alla Sezione II par. 3 delle Disposizioni di trasparenza, richiamate dalla Sezione VI, par. 4.1.1 relativa all'informativa pre-contrattuale in materia di Servizi di pagamento.

In particolare, occorre altresì precisare come la Banca d'Italia non parrebbe aver accolti i dubbi espressi nel *postion paper* dell'ABI del 12 ottobre 2015 circa *"(...) il rischio di fornire una tale quantità di informazioni la cui rilevanza non risulti immediatamente percepibile dalla clientela*[34]*"*.

Oltre a ciò, interventi vengono richiesti sul contratto quadro nella parte in cui si prevede che il prestatore dei servizi di pagamento possa bloccare una specifica operazione o lo strumento di pagamento per problemi di sicurezza, dovendo pattuire: i) il metodo e i termini della comunicazione al cliente ii) le modalità per contattare il prestatore dei servizi di pagamento per sbloccare l'operazione di pagamento via internet o il servizio; par tale ultimo profilo, la Banca d'Italia ha precisato come, *"(...) ove previste,* [le fattispecie relative al blocco di singole transazioni per problemi di sicurezza debbano essere] *comunque regolate in forma scritta*[35]*"* dovendosi evitare sovrapposizioni con la fattispecie del blocco dello strumento di pagamento per problemi di sicurezza,

[34] Cfr.: ABI *"Position Paper in risposta alla procedura di consultazione della Banca d'Italia sul "Recepimento in Italia degli Orientamenti dell'ABE in materia di sicurezza dei pagamenti tramite canale internet"*, p. 8.
[35] Cfr.: Banca d'Italia, Resoconto della consultazione, *"Recepimento in Italia degli orientamenti dell'ABE in materia di sicurezza dei pagamenti tramite canale internet"*, p. 10.

puntualmente disciplinata nel suo contenuto dalla disposizione di legge di cui all'art. 6 del d.lgs. 11/2010.

1.3.2.2 Autenticazione forte del cliente

Un secondo aspetto relativo alle misure specifiche e di sicurezza per i pagamenti via Internet concerne la disciplina dell'autenticazione forte del cliente[36], della quale i prestatori di pagamento dovrebbero avvalersi a protezione dell'inoltro dei pagamenti via internet e dell'accesso ai dati sensibili relativi ai pagamenti, ai sensi del Titolo II punto 7 degli Orientamenti.

L'obbligatorietà dell'utilizzo di siffatta procedura viene prevista secondo una tecnica di redazione tale per cui, fissato il principio generale dell'autenticazione forte del cliente, alcuni dei successivi punti (da 7.1 a 7.9) individuano le esenzioni da tale principio; esenzioni parametrate sulla base dell'ambito di applicazione oggettivo degli Orientamenti: bonifico/ mandato elettronico/ moneta elettronica/ e carte.

In particolare, nel condurre l'analisi sulle citate esenzioni, laddove le medesime non siano dettagliate esattamente dall'ABE (si pensi al punto 7.1 relativo ai bonifici), l'Autorità di vigilanza richiede agli intermediari di utilizzare misure alternative di identificazione per categorie di operazioni a basso rischio pre-identificate sulla base di analisi risk-based delle operazioni o che coinvolgono pagamenti di basso valore di cui alla direttiva sui servizi di pagamento[37].

---

[36] Definita, ai sensi del Titolo I, punto 12, degli Orientamenti come *"una procedura basata sull'impiego di due o più dei seguenti elementi - classificati nelle categorie della conoscenza, del possesso e dell'inerenza: i) qualcosa che solo l'utente conosce, per esempio una password statica, un codice, un numero di identificazione personale; ii) qualcosa che solo l'utente possiede, per esempio un token, una smart card, un cellulare; iii) qualcosa che caratterizza l'utente, per esempio una caratteristica biometrica, quale può essere un'impronta digitale. Inoltre, gli elementi selezionati devono essere reciprocamente indipendenti, ossia la violazione di un elemento non compromette l'altro o gli altri. Almeno uno degli elementi dovrebbe essere non riutilizzabile e non replicabile (eccettuata la categoria dell'inerenza) e non atto a essere indebitamente carpito via Internet. La procedura di autenticazione forte dovrebbe essere concepita in modo tale da proteggere la riservatezza dei dati di autenticazione"*.

[37] Cfr.: Titolo II, punto 7.5 degli Orientamenti, secondo cui *"I prestatori di servizi di pagamento che offrono servizi di acquiring dovrebbero richiedere ai loro operatori commerciali online di supportare soluzioni che permettano all'emittente di eseguire l'autenticazione forte del titolare della carta per le transazioni con carta via Internet. L'uso di misure di autenticazione alternative potrebbe essere preso in considerazione per categorie di operazioni a basso rischio pre-identificate, per esempio sulla base di un'analisi del rischio delle operazioni, o che coinvolgono pagamenti di basso valore, di cui alla direttiva sui servizi di pagamento"*.
In particolare l'ABI nel *"Postion paper in risposta alla procedura di consultazione della Banca d'Italia sul recepimento degli Orientamenti dell'ABE in materia di sicurezza dei pagamenti tramite canale internet"*, come evidenziava *"(...)in riferimento all'Orientamento 7.5, se l'intenzione è di richiedere la strong authentication sulla maggioranza delle transazioni, si prevedono rilevanti impatti sui servizi di acquiring, in quanto gli esercenti online saranno orientati a scegliere PSP che consentono maggiore flessibilità sulla gestione del protocollo 3D Secure"*.

In sede di recepimento, poi, la Banca d'Italia parrebbe essere stata chiara nel sottolineare che il principio dell'autenticazione forte trova applicazione generale e che i casi di esclusione sono identificati direttamente dagli Orientamenti; a tale riguardo e a titolo semplificativo, non è stata accolta, per esempio, la richiesta di escludere le carte aziendali e corporate dall'ambito di applicazione degli Orientamenti[38], piuttosto che quella di esentare dall'autenticazione forte la registrazione di una carta in un wallet[39] o, ancora, la richiesta di introdurre margini di flessibilità nel ricorso all'autenticazione forte, ammettendo la derogabilità al principio in base al quale almeno un degli elementi richiesti per l'autenticazione sia non riutilizzabile e non replicabile e non atto ad essere indebitamente carpito via internet[40].

L'importanza della procedura di autenticazione forte trova, da ultimo, conferma anche nel testo delle Disposizioni, laddove è previsto che *"(…) fermi restando i casi in cui gli Orientamenti prescrivono obblighi specifici (come nel caso dell'utilizzo dell' "autenticazione forte"), le banche applicano le disposizioni contenute negli Orientamenti secondo il principio di proporzionalità, cioè tenuto conto della dimensione e complessità operative, della natura dell'attività svolta, della tipologia dei servizi prestati*[41]*"*.

1.3.2.3 Registrazione del cliente e monitoraggio delle operazioni

Tra gli altri Orientamenti meritevoli di analisi si segnalano i numeri 8 e 10, recanti, rispettivamente, indicazioni in merito alla sicurezza della registrazione iniziale al servizio del cliente ed il monitoraggio delle operazioni volte a prevenire, rilevare e bloccare il traffico dei pagamenti fraudolenti prima dell'autorizzazione finale del prestatore del servizio di pagamento.

---

[38] Cfr.: Banca d'Italia, Resoconto della consultazione, *"Recepimento in Italia degli orientamenti dell'ABE in materia di sicurezza dei pagamenti tramite canale internet"*, p. 12.

[39] Cfr.: Banca d'Italia, Resoconto della consultazione, *"Recepimento in Italia degli orientamenti dell'ABE in materia di sicurezza dei pagamenti tramite canale internet"*, p. 14; occorre altresì precisare per chiarezza che le soluzioni di tipo "wallet" consistono in quelle *"(…) soluzioni che permettono al cliente di registrare i dati relativi a uno o più strumenti di pagamento, al fine di effettuare pagamenti con diversi operatori commerciali online"*, per come indicato al Titolo I punto 12 degli Orientamenti.

[40] Cfr.: Banca d'Italia, Resoconto della consultazione, *"Recepimento in Italia degli orientamenti dell'ABE in materia di sicurezza dei pagamenti tramite canale internet"*, p. 7.
Sull'importanza del principio generale dell'autenticazione forte del cliente la Banca d'Italia non parrebbe dunque aver accolto le argomentazioni emerse in sede di consultazioni in particolare da parte di Mastercard, che proponeva di riformulare il punto 7 fondando l'autenticazione forte del cliente *"sulla base di una analisi del rischio dell'operazione"*; tra gli argomenti a sostegno delle proprie richieste, l'operatore individuava sia l'approccio adottato nella legislazione statunitense dove *"(…) per la clientela non commerciale è sufficiente che le istituzioni finanziarie implementino un approccio multi livello in linea con il rischio relativo alle transazioni dei consumatori; esclusivamente per la cliente*[la] *commerciale è raccomandata (ma non obbligatoria)l'autenticazione forte (la cd. "autenticazione multi-fattore") per le transazioni via internet"*(p. 6 del Documento) che il principio di facilità di utilizzo per il consumatore basato (anche) sullo scenario della transazione.

[41] Circolare Banca d'Italia n.285/2013, Parte Prima, Titolo Quarto, Capitolo 4, Sezione VII "Principi organizzativi relativi a specifiche attività o profili di rischio", par. 1.

In particolare, l'articolato del punto 8 individua tre requisiti per la registrazione iniziale e la fornitura all'utente di strumenti di autenticazione e/o software per effettuare pagamenti:

i) procedure da effettuarsi in un ambiente sicuro e affidabile;

ii) procedure efficaci e sicure per la consegna delle credenziali personalizzate;

iii) autenticazione forte per le operazioni con carta indipendentemente da uno specifico acquisto su Internet; qualora sia disponibile l'attivazione durante lo shopping online, questa dovrebbe essere fatta reindirizzando il cliente verso un ambiente sicuro e affidabile.

Con riferimento al monitoraggio delle operazioni, l'Autorità di vigilanza europea richiede ai prestatori di servizi di pagamento di dotarsi di sistemi di rilevamento e prevenzione delle frodi per individuare operazioni sospette, tra gli altri, prima che il prestatore di servizi di pagamento autorizzi da ultimo le operazioni o i mandati elettronici e fondati, nella loro entità, complessità ed adattabilità sul rispetto della normativa in materia dei dati, nonché commisurati al risultato della valutazione dei rischi.

In sede di resoconto alle consultazioni, la Banca d'Italia ha precisato, tra l'altro, che: i) la valutazione dei rischi è rimessa agli intermediari i quali, per le finalità di cui all'Orientamento 8, potranno anche utilizzare statistiche aziendali[42]; ii) non è possibile identificare *ex ante* le azioni da intraprendersi a seguito dell'individuazione di una frode, rimettendo tale identificazione alla valutazione dei competenti organi aziendali sulla base della tipologia di frode accertata e della normativa eventualmente applicabile alla specifica violazione[43].

1.3.3. L'assistenza al cliente: sensibilizzazione, educazione e comunicazione

La terza ed ultima fattispecie afferente il contenuto sostanziale degli Orientamenti attiene al rapporto di assistenza cui sono tenuti gli intermediari nel rapporto con il cliente; in particolare, all'interno di tale fattispecie, si richiede ai prestatori dei servizi di pagamento di fornire supporto sia in una fase *ex ante*, mediante l'avvio di programmi di educazione e di sensibilizzazione dei clienti destinati a garantire la loro comprensione sulle necessità di proteggere le proprie credenziali di accesso gestendo la sicurezza del proprio dispositivo di accesso ai pagamenti a mezzo internet ed utilizzando il sito web autentico del prestatore dei servizi di pagamento[44], che in una fase *ex post* di possibili eventi patologici, per esempio illustrando in che modo il prestatore di servizi di

[42] Cfr.: Banca d'Italia, Resoconto della consultazione, *"Recepimento in Italia degli orientamenti dell'ABE in materia di sicurezza dei pagamenti tramite canale internet"*, p. 15.
[43] Cfr.: Banca d'Italia, Resoconto della consultazione, *"Recepimento in Italia degli orientamenti dell'ABE in materia di sicurezza dei pagamenti tramite canale internet"*, p. 16.
[44] Cfr.: Titolo II, punti 12.1, 12. 4 degli Orientamenti.

pagamento informerà il cliente circa (potenziali) operazioni fraudolente o metterà in guardia il cliente circa il verificarsi di attacchi[45].

2. I dubbi degli operatori in sede di recepimento e le indicazioni della Banca d'Italia: ulteriori profili di riflessione

Con riguardo agli ulteriori spunti di confronto emersi in sede di resoconto alle consultazioni, due in particolare meritano di essere sinteticamente illustrati: il primo, afferente al principio del *comply or explain*; il secondo relativo alla vincolatività delle Migliori Prassi, allegate agli Orientamenti e finalizzate ad orientare le condotte "operative" degli intermediari ad un'aderenza uniforme ai principi contenuti negli Orientamenti.

2.1 L'eliminazione del principio comply or explain e la non vincolatività delle Migliori Prassi.

Diversamente rispetto all'efficacia prescrittiva delle raccomandazioni della Banca Centrale Europea del 31 gennaio 2013, fondata sul principio del c.d. *comply or explain*, ossia sulla sussistenza di *"ampi margini di flessibilità nella scelta delle concrete modalità di attuazione che risultano rimesse, nella sostanza, alla scelta degli operatori*[46]*"* i quali *"possono* [giustificare] *le ragioni per le quali le misure di sicurezza raccomandate sono adottate con modalità equivalenti a quelle direttamente previste dalle raccomandazioni stesse*[47]*"*, gli Orientamenti dell'ABE fanno venire meno *"(...) la richiamata facoltà riconosciuta agli operatori*[48]*"*, con la conseguenza che *"i prestatori di servizi di pagamento sono chiamati ad un rispetto puntuale delle misure di sicurezza in essi contenute e delle modalità attuative ivi specificate*[49]*"*.

In estrema sintesi la Banca d'Italia, in sede di consultazione del provvedimento dell'ABE prevedeva la piena vincolatività sia degli Orientamenti che delle Migliori Prassi; su tale affermazione si sono concentrate gran parte delle richieste di modifica della normativa da parte degli intermediari, le cui principali criticità sottoposte all'Autorità di vigilanza italiana possono essere riassunte nelle seguenti:

1. possibili effetti rilevanti dell'eliminazione del margine di flessibilità legato al principio del "comply or explain" "[sull]*'autonoma valutazione delle scelte tecnologiche e procedurali per la sicurezza dei pagamenti via Internet da parte delle strutture coinvolte nei processi sottostanti*[50]*"* e consequenziale *"necessità*

[45] Cfr.: Titolo II, punto 12.1 degli Orientamenti.
[46] Cfr.: Banca d'Italia, documento per la consultazione, "*Recepimento in Italia degli orientamenti dell'ABE in materia di sicurezza dei pagamenti tramite canale internet"*, agosto 2015.
[47] *Ibidem.*
[48] *Ibidem.*
[49] *Ibidem.*
[50] Federcasse*, "Recepimento in Italia degli Orientamenti dell'ABE in materia di Sicurezza dei Pagamenti tramite canale Internet" – position paper in risposta alla procedura di consultazione della Banca*

per le stesse, di rianalizzare criticamente le attività e le progettualità realizzate, con un conseguente impatto sui tempi di adeguamento[51]*"*;

2. possibili effetti rilevanti sulla competitività degli operatori nazionali dell'anticipata introduzione a livello nazionale di misure di sicurezza (le Migliori Pratiche) che, in termini anche più stringenti, verranno introdotte solo successivamente a livello europeo mediante l'entrata in vigore della PSD2[52].

Per quanto concerne il principio del *comply or explain*, la Banca d'Italia ha ritenuto di non accogliere le richieste degli intermediari chiarendo che *"(...) la rimozione del principio del "comply or explain" rappresenta uno dei principali elementi di novità derivanti dall'incorporazione delle Raccomandazioni della Banca Centrale Europea negli Orientamenti dell'EBA, che, con tale trasposizione, si propone di accrescere il grado di armonizzazione e sicurezza nel settore dei pagamenti via internet*[53]*"* e tuttavia riconoscendo ad essi *"(...) un congruo periodo di tempo entro il quale implementare le disposizioni di recepimento degli Orientamenti*[54]*"*.

A tale ultimo proposito, nella nota esplicativa del 23 maggio relativa alle Disposizioni, è stato individuato al 30 settembre 2016 il termine per adeguarsi alle disposizioni; gli intermediari dovranno altresì trasmettere alla Banca d'Italia - entro il 30 ottobre 2016 - una relazione, approvata dall'organo con funzione di supervisione strategica, sugli interventi effettuati sulla struttura organizzativa e di controllo nonché sui sistemi informativi, al fine di assicurare il rispetto degli obblighi introdotti con le modifiche del 17 maggio 2016.

Con riguardo alle Migliori Prassi poi, in parziale accoglimento delle richieste pervenute, la Banca d'Italia rilevando che *"(...) la PSD2 disciplina gli obblighi di autenticazione*

---

d'Italia", p. 2; nello stesso senso anche l'ABI: *"(...) l'eliminazione del principio di "comply or explain" determinerebbe un'ulteriore analisi delle attività già realizzate e delle progettualità in corso presso le banche, con un conseguente impatto sui tempi di adeguamento"*, ABI *"Postion paper in risposta alla procedura di consultazione della Banca d'Italia sul recepimento degli Orientamenti dell'ABE in materia di sicurezza dei pagamenti tramite canale internet"*, p. 3.

[51] Federcasse, *"Recepimento in Italia degli Orientamenti dell'ABE in materia di Sicurezza dei Pagamenti tramite canale Internet" – position paper in risposta alla procedura di consultazione della Banca d'Italia"*, p. 2.

[52] In particolare si richiama quanto espresso a pag. 4 dall'ABI nel *"Postion paper in risposta alla procedura di consultazione della Banca d'Italia sul recepimento degli Orientamenti dell'ABE in materia di sicurezza dei pagamenti tramite canale internet": " (...) le MP non solo ad oggi rappresentano degli esempi di carattere generico difficilmente traducibili in modalità e prassi operative, ma si ritiene altresì che il disallineamento normativo derivante dalla loro adozione esclusivamente nel contesto italiano possa determinare una perdita di competitività per il settore nei confronti delle controparti europee, a causa degli ingenti investimenti che i PSP insediati in Italia dovrebbero sostenere ai fini dell'adeguamento ma ancor più in termini di customer experience e di impatti sulla clientela"*.

[53] Cfr.: Banca d'Italia, Resoconto della consultazione, *"Recepimento in Italia degli orientamenti dell'ABE in materia di sicurezza dei pagamenti tramite canale internet"*, p. 3.

[54] *Ibidem.*

della transazione con riferimento all'importo e al destinatario del pagamento, oggetto della MP 8, rimettendo all'EBA la definizione delle regole tecniche e dei casi di esenzione (…) nelle more del consolidamento del quadro normativo europeo, la cui completa attuazione sarebbe prevista non prima di ottobre 2018[55]*",* ha ritenuto di non renderle obbligatorie, fermo restando tuttavia *"(…) la possibilità per gli intermediari di tenerne conto al momento della definizione delle scelte da assumere per conformarsi al contenuto degli Orientamenti*[56]*"*.

Conclusioni

Il rinnovato impianto normativo descritto si pone in linea di continuità con gli interventi regolamentari che - a vario titolo - le Autorità di vigilanza europee stanno richiedendo di introdurre all'interno del quadro normativo regolamentare nazionale.

Ciò che maggiormente emerge dagli Orientamenti, alla luce, in particolare, dell'eliminazione del principio *comply or explain*, parrebbe essere una sempre maggiore pervasività delle regole - gerarchicamente sovraordinate - europee che, sebbene riducano i margini di azione dell'Autorità di vigilanza nazionale, necessitano pur sempre del loro intervento chiarificatore, al fine di creare basi comuni e regole uniformi entro cui gli intermediari possano accrescere il livello di competitività nell'offerta dei propri servizi.

[55] Cfr.: Banca d'Italia, Resoconto della consultazione, *"Recepimento in Italia degli orientamenti dell'ABE in materia di sicurezza dei pagamenti tramite canale internet"*, p. 4.
[56] Cfr.: Banca d'Italia, Resoconto della consultazione, *"Recepimento in Italia degli orientamenti dell'ABE in materia di sicurezza dei pagamenti tramite canale internet"*, p. 5; vedi anche Circolare Banca d'Italia n.285/2013, Parte Prima, Titolo Quarto, Capitolo 4, Sezione VII "Principi organizzativi relativi a specifiche attività o profili di rischio", par. 1 *"(…) In linea con quanto previsto dagli Orientamenti, è rimessa alla valutazione di ogni banca la scelta se attenersi anche agli esempi di Migliori Prassi di cui all'Allegato 1* [degli] *Orientamenti"*.