X CONVEGNO ANNUALE DELL'ASSOCIAZIONE ITALIANA DEI PROFESSORI UNIVERSITARI
DI DIRITTO COMMERCIALE "ORIZZONTI DEL DIRITTO COMMERCIALE"

"*L'EVOLUZIONE TECNOLOGICA E IL DIRITTO COMMERCIALE*"

Roma, 22-23 febbraio 2019

MARILENA RISPOLI FARINA

La Strong Customer Authentication e la responsabilità dei Prestatori dei servizi di pagamento

SOMMARIO: 1. 1. Introduzione: le direttive comunitarie sui servizi di pagamento. Profili generali. - 2.1 L'autenticazione forte del cliente e gli orientamenti dell'ABF. - 2.2 La soluzione proposta dal legislatore comunitario e cristallizzata nella Direttiva n. 2366. - 3. La responsabilità civile dei prestatori dei servizi di pagamento prima e dopo la Direttiva PSD 2. - 4. Conclusioni.

1. Introduzione: le direttive comunitarie sui servizi di pagamento. Profili generali.

La Direttiva 2015/2366/UE (cd. *Payment Service Directive 2*)[1] ha modificato, sotto molteplici profili, il sistema dei servizi di pagamento, sulla scia delle novità introdotte a livello internazionale ed europeo nel sistema dei servizi di pagamento e dell'evoluzione dell'industria dei sistemi di pagamento[2].

[1] DIRETTIVA (UE) 2015/2366 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 25 novembre 2015 relativa ai servizi di pagamento nel mercato interno, che modifica le direttive 2002/65/CE, 2009/110/CE e 2013/36/UE e il regolamento (UE) n. 1093/2010, e abroga la direttiva 2007/64/CE, in G.U.E, 23 dicembre 2015, L 337/35.
Dal riesame del quadro europeo e dalla consultazione pubblica sul Libro verde della Commissione del 2012"Verso un mercato europeo integrato dei pagamenti tramite carte, internet e telefono mobile", è emersa la necessità di adottare ulteriori misure e di apportare adeguamenti alla normativa sui servizi di pagamento, per rispondere meglio alle esigenze di un vero e proprio mercato unico dei pagamenti e contribuire a tutti gli effetti ad una migliore tutela della concorrenza, dell'innovazione e della sicurezza.

[2] Per un quadro dei problemi e dei cambiamenti: TRESOLDI C. (a cura di), *Economia dei sistemi di pagamento*, DarwinBooks, 2006.

La Direttiva, condivide con quella immediatamente antecedente (la n. 64 del 2007), lo scopo di assicurare all'industria dei servizi di pagamento un quadro giuridico, moderno e coerente, che garantisca parità di condizioni di accesso e regolamentazione per tutte le imprese che prestino servizi di pagamento, e nel contempo intende consentire a tutti i consumatori la possibilità di orientare la scelta del servizio, valendosi del contenimento dei costi che la disciplina comunitaria persegue, nonché dei vantaggi connessi al maggior livello di sicurezza ed efficacia rispetto agli standard esistenti a livello nazionale. Allo stesso tempo, la Direttiva si inquadra in un rafforzamento delle dinamiche di mercato e della concorrenza: attraverso la predisposizione di un dettagliato contenuto minimo del contratto il cliente può svolgere un esame comparativo delle offerte e il singolo prestatore del servizio è indotto a non praticare condizioni sfavorevoli che indurrebbero il cliente "consapevole" degli svantaggi a preferire un altro intermediario[3] (in particolare. cfr. i Considerando 53 - 75).
La Direttiva n.2366, (PSD2), come la prima PSD, ha posto l'accento in particolar modo sull'importanza dell'informazione nell'equilibrio generale della disciplina, al fine di consentire all'utente di operare scelte con cognizione di causa, spaziando tra le diverse possibilità consentite dagli ordinamenti europei che debbono adeguarsi ai requisiti indispensabili per garantire un livello minimo e sufficiente di tutela dell'utente sia al momento della stipula del contratto e della sua esecuzione, che per ogni singola operazione da questi effettuata (Considerando n. 54). I Prestatori dei servizi di pagamento, pertanto, dovrebbero fornire: informazioni chiare e di qualità elevata; proporzionate alla necessità degli utenti e comunicate in modo standardizzato; differenziate, a seconda che si tratti di informazioni concernenti singole operazioni o l'intero contratto quadro.
Le esigenze di trasparenza che vengono ribadite (le nuove disposizioni riproducono, infatti, sostanzialmente le medesime disposizioni in materia di obblighi di trasparenza) devono essere, allo stato attuale dello sviluppo dell'industria dei pagamenti, contemperate con quelle di economicità nella conduzione dell'impresa: motivo per il quale tutti gli Istituti di credito e, in generale, le imprese che erogano i servizi di pagamento si sono avvalse delle più moderne tecnologie al fine di assolvere quest'impegno.

2.1 L'autenticazione forte del cliente e gli orientamenti dell'ABF.
Tra i molteplici profili su cui interviene la PSD 2, sicuramente va annoverata l'introduzione di rigorosi requisiti di sicurezza relativamente agli ordini e

[3] Cfr. RISPOLI FARINA M., *Informazione e servizi di pagamento*, in *Analisi giuridica dell'economia*, I, 2015, p. 175 e ss.; RISPOLI FARINA M., *La direttiva PSD2: novità e continuità nella disciplina dei servizi di pagamento* in BRUNELLA RUSSO, (a cura di), *I servizi di pagamento nell'epoca della digitalizzazione*, *Atti del Convegno in onore di Giuseppe Restuccia*, Taormina 15-16 febbraio 2018, Cedam, 2019, p. 30 e ss.

al trattamento dei pagamenti elettronici. Requisiti che dovrebbero contribuire a ridurre i rischi di frode connessi a tutti i mezzi di pagamento, da quelli più tradizionali a quelli più recenti, ma in particolar modo per i servizi prestati *online*. Com'è noto, già sulla base della Direttiva 2007/64/CE (PSD), i Prestatori di servizi di pagamento erano tenuti ad applicare un sistema di *autenticazione del cliente*, un procedimento, cioè, che convalida l'identità dell'utente del servizio di pagamento o di un'operazione di pagamento, in modo tale da ridurre al minimo eventuali "intrusioni" non autorizzate all'interno dei conti di pagamento, evitando così furti di denaro e di dati personali.
Presidi di sicurezza, invero, che appaiono particolarmente rigorosi in riferimento alle operazioni a distanza, come i pagamenti effettuati online: in tal caso, è necessario un collegamento con il conto del soggetto beneficiario e del soggetto pagatore, al fine di proteggere, contemporaneamente, sia chi invia un pagamento, sia chi lo riceve.

Il concetto di autenticazione degli utenti vede la luce per la prima volta con la prima Direttiva pagamenti, all'art. 4, comma 1, n. 19)[4], ai sensi del quale la stessa è definita quale "*[…]procedura che consente al prestatore di servizi di pagamento di verificare l'uso di uno specifico strumento di pagamento, incluse le caratteristiche di sicurezza personalizzate*". Definizione molto ampia , che quindi poteva essere riempita con contenuti diversi ed eterogenei, motivo per il quale il legislatore della riforma ha preferito adottare una definizione diversa e maggiormente precisa, al fine di individuare tutte quelle operazioni che consentano di acquisire la sicurezza che gli *account* degli utenti (e quindi la relativa disponibilità di fondi), siano accessibili soltanto per i rispettivi titolari e non per terzi malintenzionati
Pertanto con la Direttiva n. 2366 , il legislatore europeo ha affiancato alla definizione di autenticazione, pressoché mutuata dalla precedente Direttiva, quella di autenticazione forte del cliente, definita come: "*un'autenticazione basata 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 concepita in modo tale da tutelare la riservatezza dei dati di autenticazione*".
Perché l'autenticazione possa definirsi "forte", è necessario quindi che, nel portare a compimento l'operazione di accesso, l'utente superi almeno due "ostacoli" tra quelli suindicati: non è chiaro, però se tali ostacoli possano riguardare la medesima categoria, (ad esempio soltanto la conoscenza e il

[4] Per il testo della Direttiva 2007/64/CE, vd. *https://eur-lex.europa.eu/legalcontent/IT/ALL/?uri=CELEX%3A32007L0064*

possesso, trascurando l'inerenza), oppure se ve ne debbano essere distribuiti due per ogni *step* (e cioè almeno due per la conoscenza, almeno due per quanto riguarda il possesso, e così via)[5]. L'interpretazione che appare preferibile è che il legislatore si sia "accontentato" di sistemi di accesso che richiedano almeno due delle tre categorie richieste.
Quindi possiamo dire che una significativa novità della riforma dei servizi di pagamento, posta in essere dalla PSD 2, è rappresentata dalla maggior precisazione riguardante gli obblighi per l'accesso forte, delineati non solo dal Considerando 4, ma anche dagli artt. 97 e 98 della Direttiva stessa, che sono poi stati recepiti nel nostro ordinamento nel decreto legislativo n. 218 del dicembre 2018.
L'art. 97 della nuova PSD 2 statuisce che gli Stati membri provvedano affinché i Prestatori dei Servizi di pagamento applichino l'autenticazione forte del cliente nei seguenti casi: i) quando il pagatore accede al suo conto di pagamento online; ii) quando il pagatore dispone un'operazione di pagamento elettronico; iii) quando effettua una qualsiasi altra operazione, rientrante nel *genus* dei servizi di pagamento, tramite un canale a distanza per il quale vi può essere un rischio di frode nei pagamenti o altre tipologie di abusi[6]. Ai sensi del paragrafo 2 di tale articolo, i Prestatori dei servizi di pagamento dovranno assicurarsi che sia creato un *link* dinamico tra l'operazione, il soggetto pagatore ed il beneficiario: in tal modo, sarà assicurata la tracciabilità del pagamento e si eviteranno, del resto, intrusioni non autorizzate. Inoltre, nell'atto comunitario è inserito anche il riferimento ai Prestatori del Servizio di informazione sui conti: anche per questi soggetti è disposto l'obbligo di accertarsi che chiunque acceda ai conti di pagamento debba necessariamente superare almeno due dei tre step previsti dalla *strong customer authentication*. Infine, l'ultimo paragrafo dell'art. 97 espressamente statuisce che il Prestatore del servizio di radicamento del conto (e cioè il *Provider* presso cui è radicato il conto di pagamento) debba necessariamente richiedere, sia al Prestatore del servizio di disposizione di ordini di pagamento, sia al Prestatore del Servizio di informazione sui conti, la procedura di accesso di autenticazione forte per evitare accessi abusivi al conto del proprio cliente.
La problematica dell'autenticazione "forte" nell'accesso ai sistemi di pagamento ha trovato spazio nelle decisioni dell'Arbitro Bancario

[5] Cfr. VANINI S., *L'attuazione in Italia della seconda Direttiva sui servizi di pagamento nel mercato interno: le innovazioni introdotte da d.lgs. 15 dicembre 2017, n. 218*, in *Le nuove leggi civili e commerciali*, 4, 2018, p. 866 e ss.
Per una rapida disamina in tema di PSD 2, cfr. CASCINELLI F. - PISTONI V. - ZANETTI G., *La Direttiva (UE) 2015/2366 relativa ai servizi di pagamento nel mercato interno*, in *dirittobancario.it*; MONTELLA P., *La Direttiva PSD 2: obiettivi della revisione e principali tratti di novità*, in *Innovazione e diritto*, p. 1 e ss.
[6] Tale statuizione è riprodotta *sic et simpliciter* dall'art. 10-bis del d.lgs. 217/2018.

Finanziario[7]. Quest'ultimo ha registrato una notevole inversione di tendenza rispetto agli ultimi anni rispetto alla posizione del consumatore che subiva l'utilizzo fraudolento dei propri strumenti di pagamento o che si vedeva sottratte le proprie credenziali di accesso ai sistemi di *home banking*: ad esemplificare, può rammentarsi una decisione del Collegio di Milano, la n. 1555 del 2010, che aveva rigettato il ricorso di una cliente che aveva incautamente lasciato il proprio bancomat, insieme alle credenziali di accesso, all'interno della propria vettura lasciata senza sicura inserita. L'arbitro, nonostante la signora avesse prontamente riferito di essere stata derubata anche del bancomat, ha ritenuto molto negligente il comportamento assunto dalla ricorrente, sulla quale grava l'obbligo di custodire con scrupolo e diligenza le credenziali di sicurezza dei propri dispositivi di pagamento. Ancora, nella decisione n. 2845 del 2011, veniva evidenziato e posto a carico del ricorrente, che si vedeva respingere il ricorso presentato dinanzi all'Arbitro, il sistema del cd. *lebanese loop*, mediante il quale un terzo malintenzionato riesce a clonare la carta inserita in un ATM ed a carpire con l'inganno i codici di autenticazione dall'ignaro utilizzatore (spiandolo mentre li digita sulla tastiera). In tal caso, il Collegio aveva ravvisato, ancora una volta, l'imprudenza dell'utilizzatore, il quale, in presenza di un estraneo, avrebbe forse dovuto porre più attenzione nell'inserimento del codice PIN.
La decisione del Collegio di Coordinamento dell'ABF. del 24 giugno 2014 (n. 3947), pur mostrando già un primo temperamento alla severità nell'analisi della posizione dell'utilizzatore degli strumenti di pagamento, pone la propria attenzione sulla mancata diligenza del ricorrente, il quale aveva lamentato l'utilizzo non autorizzato della propria carta bancomat per un ammontare di oltre 7 operazioni non autorizzate. In tal caso, infatti, l'orientamento dell'Arbitro è stato sì quello di riconoscere l'inversione dell'onere della prova a carico dell'intermediario resistente (come già statuito dalla Direttiva PSD), ma anche quella di riconoscere oneri di diligenza, nella custodia del dispositivo di pagamento e del relativo PIN, abbastanza gravosi per l'utente; di fronte alle doglianze di parte ricorrente circa una supposta clonazione della propria carta bancomat, l'Arbitro ha accolto le controdeduzioni di parte resistente, il quale ha prodotto in giudizio una documentazione inerente l'impossibilità di clonare le carte con il cd. microchip. Ciò, unito al fatto che i prelievi presuntivamente abusivi erano tutti stati effettuati in zone limitrofe alla residenza di parte ricorrente,

[7] In materia di servizi di pagamento e strumenti di pagamento possono consultarsi le numerose Decisioni dei Collegi ABF e del Collegio di coordinamento sul sito *www.arbitrobancariofinanziario.it.*
Su alcune tematiche specifiche e sulla portata conformativa degli orientamenti ABF in tema di servizi di pagamento cfr.: CORVESE C. - GIMIGLIANO G. (a cura di), *Profili interdisciplinari del commercio elettronico*, Pacini, Siena, 2016.

ha fatto propendere il Collegio ad imputare all'utilizzatore la colpa grave nel non aver custodito correttamente la carta di pagamento ed il relativo PIN.
Conformemente a quanto affermato dall'ABF, una sentenza del Tribunale di Milano del 26 settembre 2018, chiamato a decidere in secondo grado su una controversia avente ad oggetto la responsabilità civile della banca *ex* art. 12 del d.lgs. n. 11/2010, vecchio testo (applicabile *ratione temporis* dato che i fatti di cui è causa di riferiscono al 2015, antecedentemente all'entrata in vigore dell'attuale PSD 2) ha affermato, tramite presunzioni *ex* art. 2729 c.c., la piena responsabilità dell'utilizzatore di una carta che si asseriva essere stata rubata, ma senza i relativi codici di accesso. Il proprietario del bancomat, in sostanza, aveva affermato di aver correttamente adempiuto gli obblighi di corretta custodia del PIN inerente allo strumento di pagamento, ma che ciononostante la carta bancomat era stata clonata e utilizzata per prelievi non autorizzati dal proprio conto corrente. La banca convenuta, invece, resistendo in giudizio, aveva prodotto uno studio commissionato ad esperti del Politecnico di Torino, sulla base del quale deve dedursi che la clonazione e conseguente estrapolazione delle nuove carte bancomat, dotate di PIN, risulta pressoché impossibile: da ciò il Tribunale di Milano aveva desunto che, in effetti, il codice segreto a cinque cifre doveva essere stato incautamente custodito dal cliente insieme al Bancomat, disattendo completamente agli obblighi di diligente custodia degli stessi sancito dall'art. 7 del decreto. A seguito di ciò, il Tribunale ha deciso di rigettare *in toto* la richiesta di rimborso avanzata dal cliente alla propria banca.
Dagli esempi citati è possibile desumere come i Collegi dell'ABF fossero alquanto attenti a riconoscere la responsabilità dei danni provocati all'utilizzatore dello strumento di pagamento in capo al Prestatore del servizio di pagamento negando, il più delle volte, le richieste di rimborso formulate dai clienti, ai quali veniva imputato un comportamento negligente o, quanto meno, imprudente.

Le più recenti decisioni, in ordine temporale, assunte dall'Arbitro Bancario Finanziario, paiono orientarsi diversamente, in quanto considerati i progressi della tecnologia, esso appare sempre più propenso ad addossare il rischio di un utilizzo fraudolento dei sistemi di pagamento, e delle relative credenziali, in capo ai Prestatori dei servizi. Possiamo richiamare la decisione n. 17675/2017 del Collegio di Milano, laddove vengono citate le *Recommendations for the security of internet payments* emanate il 31 marzo 2013 dallo *European Forum on the Security of Retail Payments (Secure Pay)*, costituito presso la Banca Centrale Europea. Le citate *Recommedations,* nonostante risalgano a circa 6 anni fa, contenevano già indicazioni importanti sugli

accorgimenti da adottare dai Prestatore dei servizi di pagamento per assicurare il corretto funzionamento delle operazioni.
Raccomandazioni poi riprese dagli *Orientamenti in materia di sicurezza dei pagamenti tramite internet,* emanati dall'Autorità Bancaria Europea nel dicembre 2014 che statuiscono dei cd. "principi guida" e definiscono i requisiti minimi di sicurezza per i servizi di pagamento prestati via internet; requisiti minimi che costituiscono il canone di diligenza professionale cui i prestatori dovevano adeguarsi.
Tra tali "principi guida" si annovera quello che richiede ai prestatori di servizi di pagamento di garantire che l'operatività via internet e l'accesso ai "*sensitive payment data*" (come tali dovendosi classificare non solo le credenziali di accesso, ma anche quelle dispositive) siano protetti dalla "*strong customer authentication*". Le citate Raccomandazioni chiariscono poi che, affinché possa parlarsi di autenticazione forte, la procedura adottata dall'intermediario debba essere basata sull'impiego di due o più dei seguenti elementi: (i) qualcosa che il cliente conosce, (ii) qualcosa che il cliente possiede e (iii) qualcosa che caratterizza il cliente (per esempio una caratteristica biometrica) e *almeno uno di detti elementi deve essere non riutilizzabile, non replicabile e* non atto ad essere carpito via internet. Tale punto mi pare di notevole rilievo: a nulla serve introdurre differenti e costosi sistemi di protezione, se essi possono essere facilmente sottraibili tramite un messaggio di *phishing* dal quale il cliente, più o meno inesperto, può essere attirato a fornire le proprie credenziali.
Va ricordata in proposito un' altra decisione del 2017, la n. 15608, in cui il Collegio ABF aveva rilevato come fosse "inutile", nel caso di specie sottoposto alla sua attenzione, un sistema di autenticazione a due fattori, in quanto inadeguato alla protezione del soggetto, ritenendo non realizzatasi quella colpa grave del ricorrente, pur in presenza di un sistema a due fattori, conforme alle indicazioni del Collegio di Coordinamento (dec. 3498/2012). Il sistema di protezione a due fattori, dunque, non sempre risulta essere efficace, se inserito in un sistema informatico che comunque consente un accesso non autorizzato[8].
Si può rilevare che nella maggior parte delle decisioni fin qui prese dall'Arbitro, si afferma che sebbene sia stata adottata la misura di

[8] È il caso del cd. *man-in-the-browser*, efficacemente definito come: "*subdolo meccanismo di aggressione ha luogo attraverso un sofisticato metodo di intrusione caratterizzato da un effetto sorpresa capace di spiazzare l'utilizzatore, grazie alla perfetta inserzione nell'ambiente informatico originale e nella correlata simulazione di un messaggio che a chiunque non potrebbe apparire che genuino, posto che l'unica "differenza" consta, come si è detto, nell'acronimo del protocollo di trasferimento, individuato come un normale "http" e non già come un "https" protetto*".
Ne consegue che, anche laddove dovessero essere stati formalmente rispettato il precetto dell'autenticazione a due fattori, essa dovrebbe comunque essere rapportata al contesto informatico di riferimento.

protezione a due fattori, se l'operazione è oggetto di attacco fraudolento, poiché sul Prestatore del servizio di pagamento ricade il rischio di impresa, su di esso incombe anche la sopportazione dei costi derivanti dalle pratiche di rimborso *uti singuli,* così da realizzare una vera protezione del cliente. Dottrina e giurisprudenza, in presenza di un sostanziale squilibrio di posizioni tra l'utente e il Prestatore del servizio di pagamento, ritengono ragionevole che esso venga sanato con la presunzione di responsabilità dei danni provocati all'utilizzatore a carico del Prestatore del servizio di pagamento.
In un'ottica ben diversa da quella della già menzionata decisione del 2014, la decisione del Collegio di Coordinamento n. 16237 del 26 luglio 2018 ha statuito in maniera chiara quelli che sono gli obblighi, gravanti sull'intermediario, di protezione, *"[…] derivanti da un'interpretazione costituzionalmente orientata del combinato disposto degli artt. 1175 e 1375 c.c. data dalla giurisprudenza di legittimità."*. In sostanza, l'intermediario deve addossarsi il cd. rischio di impresa, gravante su chiunque eroghi servizi nei confronti di una clientela non sempre specializzata. Nel caso di specie, in particolare, l'intermediario è stato sanzionato per non essersi accorto del superamento del plafond della carta bancomat dell'utilizzatore, venendo meno proprio agli obblighi di diligenza e protezione contrattualmente previsti.
L'Arbitro Bancario Finanziario, quindi, dopo un periodo di iniziale scetticismo di fronte alle richieste di rimborso degli utenti, di cui si dichiarava spesso l'imprudenza, la negligenza o l'imperizia, ha in un certo senso anticipato quelle che sono state le novità, in tema di *Strong customer authentication*, recepite dapprima dal legislatore comunitario, e poi da quello nazionale, imputando sempre al Prestatore del servizio di pagamento la responsabilità dell'utilizzo fraudolento delle credenziali dei propri clienti.

2.2 La soluzione proposta dal legislatore comunitario e cristallizzata nella Direttiva n. 2366: le esenzioni dall'autenticazione forte.
L'art. 98 della Direttiva PSD 2 ha affrontato la problematica suindicata, conferendo alla Commissione europea il potere di adottare, previa presentazione di progetti di norme da parte dell'Autorità Bancaria Europea[9], atti delegati al fine di "*[…] specificare i requisiti dell'autenticazione forte del cliente, le esenzioni dalla sua applicazione e standard aperti di comunicazione comuni e sicuri."*[10].

[9] E a norma degli artt. 10 e ss. del Regolamento (UE) n. 1093/2010.
[10] Cfr. la bozza del Regolamento delegato della Commissione, datato 27.11.2017, e disponibile sul sito dell'Autorità Bancaria Europea.

La Banca d'Italia, con il 16° Aggiornamento delle Disposizioni di Vigilanza per le Banche (Circolare 285/2013), aveva individuato le problematiche concernenti i sistemi di accesso sicuro, in particolare la tutela della riservatezza e dell'integrità delle credenziali dei clienti. In particolare, l'Autorità, preso atto dell'enorme volume di contenzioso che aveva investito le sedi arbitrali, raccomandava di limitare il rischio *phishing* ed altre attività fraudolente che potessero mettere a rischio i fondi degli utilizzatori. Tra i pericoli individuati, annoveriamo il furto e la modifica delle credenziali di accesso involontariamente trasmesse dall'utente (*pishing message*, *fraudulent websites* o *malware* sul computer) ovvero inviate tramite canali di comunicazione alternativi, quali linea telefonica e tecnologie radio non adeguatamente protette.
La Commissione Europea, in data 27 novembre 2017, ha approvato il regolamento delegato concernente le norme tecniche di regolamentazione relative all'autenticazione forte: in primo luogo precisando le esenzioni da applicare per determinati tipi di operazioni; soffermandosi poi sui requisiti che le misure di sicurezza devono soddisfare per tutelare la riservatezza e l'integrità delle credenziali di sicurezza personalizzate[11] di tutti gli utenti e gli standard di sicurezza per tutti i soggetti coinvolti nello svolgimento di un'operazione di pagamento[12].
Al Capo II del Regolamento (precisamente, agli artt. 6, 7 e 8 del testo) sono esplicitati quegli elementi fondamentali che caratterizzano la *Strong customer Authentication* e di cui si è già richiamato in premessa: in particolare, i requisiti che devono possedere gli elementi classificati come "conoscenza" devono essere tali da non permettere a malintenzionati di venirne in possesso (si pensi ad interfacce web che memorizzano l'username o la password del cliente); l'art. 7, invece, stabilisce che i prestatori di servizi di pagamento adottano misure volte ad attenuare il rischio che gli elementi dell'autenticazione forte del cliente classificati come "possesso" siano illecitamente utilizzati da soggetti non autorizzati (pensiamo ad una *smart card* che, una volta inserita in un computer, possa

[11] Da qui la nostra attenzione, alla precedente nt. 5, alla tutela della *privacy*.
[12] Interessante notare l'art. 4, Capo I, del Regolamento adottato, che parla di un codice di autenticazione, univoco e non "spendibile" per più di una volta, generato da almeno due dei tre elementi fra conoscenza, possesso e inerenza, e che il cliente del servizio di pagamento deve utilizzare al fine di poter accedere al suo conto di pagamento online, disporre un'operazione di pagamento elettronico o effettuare qualsiasi azione tramite un canale a distanza che possa comportare un qualsivoglia rischio di frode.
Tale codice di autenticazione dovrà essere tale da non poter risalire a nessuno dei due elementi per l'autenticazione in possesso del cliente, e dovrà essere difficile da contraffare; è altresì previsto, ed è di evidenza comune per chiunque provi ad interfacciarsi con un sistema di *home banking*, un sistema per bloccare prima in via temporanea, e poi permanentemente, l'accesso all'interfaccia messo a disposizione del prestatore dopo un predeterminato numero di tentativi.

essere clonata da un *malware* ed all'occorrenza utilizzata); infine, per quanto riguarda gli elementi classificati come "inerenza", è previsto che i Prestatori di servizi di pagamento si assicurino che essi non possano essere surrettiziamente riprodotti (un dispositivo che catturi la scansione ottica di un individuo, potrebbe illecitamente trasmettere la "lettura" dei dati ad un altro pc in maniera fraudolenta).
Soprattutto, i Prestatori dei servizi di pagamento devono assicurarsi che laddove siano presenti dei dispositivi multifunzione per l'utilizzo combinato di due o più elementi, la compromissione dell'uno non infici anche l'altro.
Di notevole interesse, inoltre, risulta il Capo III del Regolamento, rubricato "Esenzioni dall'Autenticazione forte del cliente", comprendendo, quindi, tutti quei casi in cui i Prestatori del servizio di pagamento sono autorizzati a non rispettare la procedura di *Strong customer authentication*, come quando l'utente debba soltanto consultare il saldo di uno o più conti di pagamento, o consultare le movimentazioni concernenti il suo conto. La valutazione della Commissione europea, in questo caso, è stata quella di non considerare queste operazioni particolarmente pericolose, dato che l'utente, per accedere al proprio conto online, ha dovuto inserire almeno *username* e *password*; oppure, quando deve compiere una mera operazione ricognitiva del proprio saldo, senza disporre alcun pagamento (art. 10); l'autenticazione forte dovrà invece obbligatoriamente tornare ad applicarsi laddove l'utente volesse consultare il proprio saldo per la prima volta, ovvero dopo un lasso di tempo pari a 90 giorni.
Un'altra esenzione importante, posta a salvaguardare un Mercato che ha trovato ampio spazio tra i consumatori, è quello afferente alla tecnologia delle carte di debito e credito (o prepagate) *contactless*, le quali devono essere soltanto avvicinate al dispositivo POS del beneficiario al fine di autorizzare il pagamento. Ebbene, in tal caso è prevista la possibilità di non digitare il PIN (il quale, insieme al chip elettronico, costituisce una misura di autenticazione forte del cliente), purché siano rispettate una serie di condizioni (art. 11): i) l'importo dell'operazione non superi i 50 euro; ii) l'importo cumulativo delle precedenti operazioni *contactless* non superi la cifra di 150 euro totali; iii) il numero totale delle operazioni di pagamento senza digitazione del PIN sia stato pari o inferiore a cinque nella medesima giornata.
È chiara la finalità di tale esenzione: si vuole evitare che la carta di pagamento *contactless* venga utilizzata da soggetti i quali, una volta impossessatisi dello strumento, potrebbero utilizzarla più volte anche non conoscendo il PIN, date le peculiarità dello strumento, svuotando progressivamente il conto dell'ignaro pagatore.
Ancora, il Prestatore del servizio di pagamento non è tenuto ad applicare l'autenticazione forte del cliente se il pagatore dispone un'operazione di

pagamento presso un terminale di pagamento incustodito allo scopo di pagare il pedaggio o il parcheggio (art. 12 del Regolamento). In questo caso, la finalità di rendere più celeri le operazioni di transito, e gli importi solitamente ridotti delle transazioni, hanno suggerito alla Commissione europea di applicare l'esenzione anche a questo tipo di operazioni. Anche l'abitualità sembra in un certo senso "trascurata" da parte della Commissione: se un pagatore crea una serie di operazioni ricorrenti (dello stesso importo e a favore del medesimo beneficiario), il legislatore sembrerebbe non riconoscere, in tal caso, un pericolo per l'utilizzatore e, quindi, anche questo caso sembrerebbe rientrare nelle esenzioni di cui al Capo III del Regolamento (art. 14, par. 2). Si tratta di un sistema, cioè, di autenticazione mirata (cd. *targeted authentication*[13]), la quale si fonda, in sostanza, nell'analisi costante, continuativa ed in tempo reale dell'operazione di pagamento dalla quale dovrebbero essere estrapolati dati che permettono di identificare un determinato pagamento come a basso rischio di frode e, come tale, sicuro in quanto proveniente dal titolare de conto di pagamento.
In tal caso, il rischio di un utilizzo fraudolento dei conti di pagamento sembrerebbe arginato dal fatto che, nell'organizzare per la prima volta il *set* di operazioni da disporre abitualmente, sia comunque richiesta l'autenticazione forte del cliente.

3. La responsabilità dei prestatori dei servizi di pagamento prima e dopo la Direttiva PSD 2[14].

Alla luce dei mutamenti operati con la PSD 2 possiamo chiederci se possono rilevarsi cambiamenti per quel che concerne il regime della responsabilità civile dei Prestatori di servizi di pagamento. Il che può tradursi anche nella domanda: le modifiche hanno reso più semplice per i Prestatori dei servizi liberarsi dalla presunzione di responsabilità per i danni provocati agli utilizzatori degli strumenti di pagamento?

---

[13] Cfr. BERTI DE MARINIS G., *La disciplina dei pagamenti non autorizzati nel nuovo sistema delineato dal recepimento della direttiva PSD 2*, in *Diritto della banca e del mercato finanziario*, 4, 2018, p. 650 e ss.

[14] Amplissima la dottrina in materia: cfr. *La nuova disciplina dei servizi di pagamento*, Giappichelli, 2011, a cura di Marco Mancini, Marilena Rispoli Farina, Vittorio Santoro, Antonella Sciarrone Alibrandi, Onofrio Traiano; ma vedi anche BRESCIA MORRA C., *Il diritto delle banche*, II ed., Il Mulino, 2016; *Armonizzazione europea dei servizi di pagamento e attuazione della Direttiva 2007/64/CE*, a cura di Marilena Rispoli Farina, Vittorio Santoro, Antonella Sciarrone Alibrandi, Onofrio Troiano, Giuffrè, Milano, 2009; BONTEMPI P., *Diritto bancario e finanziario*, Giuffrè, Milano, 2016; Costi R., *L'ordinamento bancario*, Il Mulino, 2012; C*ommentario al Testo Unico Bancario*, a cura di Porzio M., Belli F., Losappio G., Rispoli Farina M., Santoro V., Giappichelli, Torino, 2010.

Vale ancora ricordare che gli artt. 10 e 11 del d.lgs. n. 11/2010, di attuazione della PSD, delineavano la responsabilità dei Prestatori di servizi di pagamento, i quali avevano l'obbligo di assicurarsi che "*tutti i dispositivi personalizzati forniti alla clientela non siano mai accessibili a soggetti diversi dal loro legittimo titolare*". In particolare, gli articoli citati prevedevano, in caso di disconoscimento dell'operazione da parte del loro autore, un rimborso immediato a favore dell'utilizzatore dei servizi, tranne che nel caso di motivato sospetto di frode e salva la possibilità, per l'intermediario, di dimostrare *ex post* che l'utilizzatore non aveva alcun diritto al rimborso[15].
L'art. 10, in particolare, prevedeva che, qualora l'utilizzatore dei servizi di pagamento negasse di aver autorizzato un'operazione già eseguita, o sostenesse che non fosse stata correttamente eseguita, era onere del Prestatore provare che l'operazione di cui trattasi aveva avuto l'esito sperato senza patire le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti. Parimenti, l'utilizzo di uno strumento di pagamento offerto dall'intermediario non rappresentava un automatico riconoscimento della legittimità dell'operazione o, al contrario, che il cliente avesse agito fraudolentemente o ancora che questi non avesse adempiuto, con dolo o colpa grave, agli obblighi di utilizzo conforme degli strumenti in suo possesso.

---

[15] FRAU R., *Operazioni di home banking disconosciute dal correntista e responsabilità semioggettiva della banca*, in Responsabilità civile e previdenza, 3, 2017, p. 855 e ss.
Reputiamo interessante porre la nostra attenzione sul commento fatto da FRAU alla decisione della Cassazione, I Sez. .Civ., n. 10638 del 23 maggio 2016, la quale, oltre a porre la propria attenzione sul tema della responsabilità civile dell'Intermediario, analizza un tema scarsamente dibattuto nella dottrina: la tutela dei dati personali *sic et simpliciter*. Intendiamo dire: nel momento in cui si rileva un accesso non autorizzato nei conti correnti personali (o di pagamento) di un determinato soggetto, la problematica non concerne soltanto il possibile utilizzo fraudolento delle disponibilità monetarie di un soggetto, ma anche la problematica concernente il furto dei dati personalissimi quali nome, cognome, indirizzo di residenza, etc., i quali hanno trovato una tutela iniziale grazie alla prima legge sulla privacy (la n. 676 del 1996), per poi concretizzarsi nel cd. Codice sulla privacy (d.lgs. 196/2003) ed infine nel Regolamento europeo sulla protezione dei dati personali n. 2016/679 (cd. GDPR).
L'art. 15 del d.lgs. 196/2003, prima della sua abrogazione, disponeva infatti che chiunque cagionasse ad altri un danno per illecito trattamento dei dati personali, ne dovesse rispondere in sede civile ai sensi dell'art. 2050 c.c.: la Cassazione, allora, nella vigenza di detto articolo, aveva statuito, nella sentenza 10638/2016, che laddove il cliente allegasse il danno ricevuto per l'effetto del furto delle proprie credenziali informatiche (considerate alla stregua di un dato personale come di quelli sopra esemplificati), alla controparte intermediaria spetterebbe l'onere di dimostrare che il furto è stato cagionato dalla trascuratezza, frode od errore del correntista.
In poche parole, la normativa ante PSD 2 configurava una sorte di responsabilità oggettiva radicatasi in capo al Prestatore del servizio di pagamento, il quale risponde per il semplice fatto di non aver, evidentemente, apposto quelle misure idonee ad impedire l'illecita apprensione altrui delle credenziali di pagamento del proprio cliente.

Con il d.lgs. 218/2017, di attuazione della direttiva PSD2, che fa un espresso riferimento ai nuovi *players* del Mercato dei Pagamenti (quali il Prestatore del servizio di disposizione di ordini di pagamento, o il Servizio di informazione sui conti), il legislatore ancor più chiaramente statuisce quell'onere della prova, gravante sui soggetti intermediari, e che implicitamente era possibile desumere dalla formulazione del vecchio testo: attualmente, infatti, l'art. 10, ult. cpv., del d.lgs.11/2010, così come modificato, sancisce che è onere del Prestatore di servizi di pagamento, compreso, se del caso, il Prestatore di servizi di disposizione di ordine di pagamento, fornire la prova della frode, del dolo o della colpa grave dell'utente, al fine di far ricadere su quest'ultimo i costi dell'operazione non autorizzata.
Il recepimento della Direttiva PSD 2 ha comportato anche la modifica dell'art. 11, il quale non si limita più a prevedere, genericamente, l'obbligo del rimborso[16] ma cerca di dare tempi certi entro i quali quest'ultimo dovrà avvenire: entro la medesima giornata in cui si è svolta l'operazione o, al più tardi, entro la giornata operativa successiva[17].
Inoltre (ed è questa una previsione di ordine logico, già sancita sotto la vigenza del vecchio testo) viene ribadita la possibilità, a favore del Prestatore di servizi chiamato ad effettuare il rimborso, di dimostrare, anche in un momento successivo al pagamento, che l'operazione a questi impartita è avvenuta correttamente (cioè, su disposizione del cliente intestatario dei fondi) con diritto di ripetere le somme già elargite.
L'utilizzatore del servizio di pagamento, infatti, nel sistema previgente non sopportava alcuna perdita in ragione dell'utilizzo illecito dello strumento in suo possesso, eccetto una franchigia, allora di un importo fino a 150 euro, per tutte quelle operazioni anteriori alla comunicazione dell'avvenuto furto o smarrimento dello strumento al Prestatore del servizio di pagamento. In virtù dell'introduzione della *Strong customer authentication*, invece, l'utilizzatore ha sempre diritto alla restituzione integrale dell'importo addebitatogli senza autorizzazione, laddove il Prestatore di pagamenti non

[16] Cfr. FRAU R., *Operazioni di home banking disconosciute*, cit., p. 866.
[17] La modifica occorsa all'articolo, a causa delle modifiche introdotte da PSD 2, ha tenuto anche in considerazione l'introduzione e la nascita di nuovi *players* del Mercato, quali il Prestatore di servizi di disposizione di ordine di pagamento ed il Prestatore di servizi di pagamento di radicamento del conto. È inoltre previsto, poi, sempre *ex* art. 11 del d.lgs. 11/2010, che laddove questi abbia dovuto rimborsare, per ragioni di celerità, il pagatore, ma l'operazione "incriminata" era da imputare solo e soltanto al Prestatore di servizi di disposizione di ordine di pagamento, allora quest'ultimo dovrà rimborsare il primo (ancora una volta) entro la medesima giornata in cui è avvenuto il rimborso al pagatore, o al più entro la giornata successiva.
Medesimo meccanismo di rimborso, ovviamente, se l'operazione non autorizzata è avvenuta dietro responsabilità del Prestatore di servizi di pagamento di radicamento del conto.

abbia adempiuto all'obbligo di esigere un'autenticazione forte del cliente. Anche il beneficiario del pagamento, inoltre, risponderà dell'utilizzo indebito dello strumento laddove non abbia adempiuto all'obbligo di richiedere l'autenticazione forte del pagatore.
Negli altri casi, salvo se abbia agito in modo fraudolento o non abbia adempiuto a uno o più degli obblighi di cui all'articolo 7, con dolo o colpa grave, (e cioè corretta custodia delle credenziali di autenticazione e comunicazione tempestiva di uso illecito delle stesse), il pagatore può sopportare, per un importo comunque non superiore a euro 50, la perdita relativa a operazioni di pagamento non autorizzate derivanti dall'utilizzo indebito dello strumento di pagamento conseguente al suo furto, smarrimento o appropriazione indebita.
È chiaro, quindi, che sotto questo aspetto, la garanzia costituita da un sistema di accesso forte consiste nell'estrema difficoltà che un sistema del genere possa essere violato. Per questo, il legislatore nazionale, sulla scorta di quello europeo, ha previsto a carico del Prestatore il rimborso immediato e integrale "*[…] in ogni caso al più tardi entro la fine della giornata operativa successiva a quella in cui prende atto dell'operazione o riceve una comunicazione in merito. Ove per l'esecuzione dell'operazione sia stato addebitato un conto di pagamento, il prestatore di servizi di pagamento riporta il conto nello stato in cui si sarebbe trovato se l'operazione di pagamento non avesse avuto luogo, assicurando che la data valuta dell'accredito non sia successiva a quella dell'addebito dell'importo*"; nel caso anche tali procedure, che di per sé dovrebbero essere le più sicure, fossero violate, il pagatore non sopporterà alcuna perdita.
Poiché tutti coloro che offrono un servizio di pagamento sono tenuti all'obbligo di operare attraverso interfacce web che consentano l'autenticazione forte del cliente, è diventato estremamente più facile per l'utilizzatore di tali strumenti ottenere il rimborso di quanto illecitamente sottrattogli; la responsabilità del Prestatore del servizio (o di eventuali altri soggetti collegati, come i Prestatori del servizio di radicamento del conto, o coloro che semplicemente forniscono informazioni ad esso collegate) è diventata completamente di tipo oggettivo, data l'estrema difficoltà che incontreranno detti soggetti nel fornire la prova del dolo o della colpa grave in capo all'utilizzatore.

4. Conclusioni.

Si può concludere osservando che le leggi comunitarie di ultima generazione si pongono con maggior rigore nell'ottica di tutelare il consumatore e in particolare l'utilizzatore del servizio di pagamento e il risparmio che i clienti depositano nei conti di pagamento ai fini di un loro utilizzo corretto e consapevole.

Il Prestatore del servizio di pagamento deve osservare i canoni di diligenza professionale, poiché nello svolgimento del contratto di *home banking* (dove ricopre un ruolo da protagonista, com'è ovvio, la *Strong authentication*), l'Azienda di credito, quale contraente professionale non è - e non può essere - all'oscuro dell'evoluzione tecnologica anche nell'ambito dei rimedi per combattere le frodi[18], ed è pertanto tenuta ad adeguarsi all'evoluzione dei nuovi sistemi di sicurezza, dovendo assumere come canone di comportamento quella "diligenza del buon banchiere"[19], la quale ha consentito, nel tempo, di giustificare una certa responsabilità da *status* in capo al Prestatore del servizio, che è quasi sempre, appunto, una banca.
Tuttavia, è chiaro che la necessarietà di dotarsi di sistemi di autenticazione forte (poiché, in caso contrario, a norma del novellato art. 12 del d.lgs. 11/2010, spetterebbe un rimborso integrale ed immediato a favore dell'utilizzatore fraudolentemente depauperato dei propri fondi) ci pone il quesito se ci troviamo ancora in un contesto di responsabilità cd. semi oggettiva, o oggettiva *tout court*, poiché sarà sempre più difficile dimostrare l'inottemperanza di un soggetto al quale, ad esempio, sono stati rubati dati biometrici di per sé non smarribili, come impronte digitali o fattezze del viso. In tal caso, allora, è lecito chiedersi: a chi va imputata l'operazione non autorizzata? Al soggetto Prestatore del servizio di pagamento, o all'utilizzatore? E nel caso in cui l'utilizzatore di un servizio convenisse in giudizio il Prestatore del servizio di pagamento, per vedersi riconosciuto l'indebito oggettivo, la banca convenuta, potrebbe forse citare in giudizio il realizzatore del *software* per l'autenticazione ad accesso forte, per rivalersi nei suoi confronti?
In effetti, nelle controversie nascenti tra l'utilizzatore di un *software* ed il fornitore del programma stesso, un aspetto fondamentale, sul quale la dottrina ha molto dibattuto, riguarda proprio la distribuzione dell'onere probatorio relativamente ai difetti del servizio di *home banking* ad all'inadempimento contrattuale. Da un punto di vista processuale, infatti, l'art. 2697 c.c., primo comma, impone a colui che fa valere in giudizio un diritto l'onere di provare i fatti che ne costituiscono il fondamento: di conseguenza, spetterebbe alla banca, nel nostro caso, dover dimostrare che il fallimento della procedura di autenticazione forte è dipesa dall'inadempimento del produttore del *software*[20]. Tuttavia, è noto come nel campo delle obbligazioni viga il principio secondo il quale una volta che il

[18] Cfr. FRAU R., *op. cit*., pag. 867 e s.
[19] Ampia la dottrina in materia che ha cercato di tratteggiare con maggior precisione tale imprescindibile qualità: come non ricordare i classici studi tra cui soprattutto FERRI G., *La diligenza del buon banchiere*, in *Banca, Borsa e Titoli di credito*, 1958, I, p. 1 e ss.
[20] Si veda in proposito CASALI P.G., *I contratti del software: qualificazione, responsabilità e garanzie*, in *I Contratti*, IV, 2014, p. 389 e ss. relativamente ai rapporti tra produttore ed utilizzatore di *software* di uso comune.

creditore ha allegato l'inadempimento altrui, incombe sul debitore l'onere di provare l'esatto adempimento dell'obbligazione[21] (e ciò anche ai sensi dell'art. 2697 c.c., secondo comma). Ciononostante, nel caso di specie da noi citato di compravendita del *software* di *home banking*, si ricorda che la violazione della garanzia per tali vizi si traduce in una responsabilità negoziale speciale e diversa rispetto a quella ordinaria *ex* artt. 1218 e 1453 c.c.: di conseguenza, in quest'ottica l'onere probatorio spetterebbe in capo alla banca utilizzatrice del programma (e non al fornitore del *software*) relativamente all'esistenza di quei difetti e delle conseguenze dannose che hanno condotto all'accesso non autorizzato ai fondi del pagatore. La banca (acquirente-utilizzatrice) come potrebbe allora tutelarsi?
Per provare le conseguenze dannose, potrebbe essere utile valersi in sede processuale delle decisione dell'ABF o della competente Corte territoriale di merito che ha accertato la violazione del sistema di accesso forte e che ha sancito il diritto alla restituzione dell'indebito a favore del cliente; per provare i difetti di fabbricazione, invece, basterebbe chiedere di effettuare una consulenza tecnica o, se non si vogliono attendere le lungaggini antecedenti l'inizio di un processo, chiedere un accertamento tecnico preventivo ai sensi dell'art. 696 c.p.c.
È questa, forse, una delle tante soluzioni cui la giurisprudenza di merito e, in ultima istanza, quella di legittimità, dovrà dare applicazioni concrete ed efficaci.

[21] Seppur pleonastico, è bene ricordare che ai sensi dell'art. 1223 del Codice civile, il risarcimento del danno per l'inadempimento o per il ritardo deve comprendere la perdita subita dal creditore (il cd. danno emergente) ed il mancato guadagno (cd. lucro cessante), purché siano conseguenza diretta ed immediata del danno subito.