Archivio selezionato: Dottrina

HOME BANKING, CAPTAZIONE DI CREDENZIALI DI ACCESSO DEI CLIENTI TRAMITE PHISHING E RESPONSABILITÀ DELLA BANCA

Responsabilita' Civile e Previdenza, fasc.3, 2015, pag. 911
Riccardo Frau -
Classificazioni: BANCA (Istituti di credito) - In genere
(*)Sommario 1. Il fatto. — 2. La cornice normativa di riferimento. — 3. Tecniche di captazione dei codici di accesso ai sistemi telematici di pagamento. — 4. Orientamenti dell'Arbitro Bancario Finanziario. — 5. Diligenza dell'operatore bancario e tratti di responsabilità oggettiva. — 6. Profili del danno non patrimoniale. — 7. Considerazioni conclusive.

1. IL FATTO

I cointestatari di un conto corrente chiamavano la banca a rispondere in giudizio, a titolo contrattuale ed extracontrattuale, dei danni risentiti a causa di alcune operazioni di *home banking* transitate sul loro conto, che venivano dagli stessi disconosciute. In particolare, gli attori chiedevano il rimborso invocando una responsabilità dell'intermediario in base agli artt. 31-33 del d.lgs. n. 196/2003 (c.d. Codice Privacy) e dell'art. 2050 c.c.

La banca, costituitasi in giudizio, contestava le richieste e chiedeva il rigetto della domanda, affermando l'idoneità dei propri sistemi di sicurezza, la loro rispondenza agli *standard* tecnici richiesti e deducendo, di contro, la scarsa cautela dei correntisti per l'aver rivelato a terzi le proprie credenziali informatiche di accesso al servizio di *home banking*.

Il Tribunale adìto ammetteva una CTU per la verifica dei sistemi di sicurezza adottati dall'intermediario e successivamente pronunciava la condanna al risarcimento a carico dell'azienda di credito, motivando come segue.

In primo luogo, veniva acclarata la natura delittuosa delle operazioni transitate sul conto degli attori, anche perché non contestata dalla convenuta, data la modalità e la tempistica delle stesse, susseguitesi in un brevissimo arco di tempo e artatamente limitata, ciascuna di esse, al massimale consentito per ogni singola operazione.

La parte centrale della motivazione ruota intorno alla risultanze della consulenza tecnica, diffusamente richiamata nel corpo della sentenza, specie in ordine alle possibili tecniche di captazione delle credenziali informatiche necessarie per l'attivazione del servizio di *home banking*. Il CTU, infatti, preliminarmente riteneva di escludere alcune tecniche di intrusione informatica, quali il c.d. MITM (acronimo di *Man In The Middle*) ovvero il c.d. MITB (*Man In The Browser*) (1) e optava invece, date le caratteristiche tecniche della frode, per un caso di *phishing*: in altre parole, a parere del consulente, i correntisti erano stati vittima di un messaggio di posta elettronica ingannevole, in quanto in apparenza proveniente dalla stessa banca con cui intrattenevano il conto. Detto messaggio, asseritamente inviato dal servizio di assistenza per i clienti, aveva indotto i medesimi a rispondere indicando i propri codici di accesso al servizio, che erano stati poi utilizzati dai truffatori per prelevare indebitamente le somme (2).

Ciò posto, la CTU sollevava il tema della inadeguatezza dei sistemi di sicurezza dell'intermediario rispetto agli *standard* necessari per il servizio in esame, che lo stesso consulente riteneva essere al di sotto delle tipologie correnti negli istituti di credito più evoluti. In particolare, la perizia evidenziava il fatto che il servizio veniva qui accordato ai clienti a fronte di una *password* « statica », in quanto consegnata ai correntisti ad inizio del rapporto (sebbene con facoltà dei medesimi di modificarla in seguito), dove invece la maggior parte del sistema bancario, all'epoca dei fatti, risultava ormai orientata sulle c.d. OTP (*one time password*), vale a dire delle *password* dinamiche (o « usa e getta »), generate dal gestore al momento dell'operazione bancaria richiesta e aventi immediata scadenza, in modo da non poter essere più riutilizzate da soggetti terzi, anche se

illecitamente carpite.

A ben vedere, questo passo risultava di preminente rilievo nella decisione del giudice, il quale, da tali assunti, derivava il convincimento, espressamente declinato in sentenza, che fosse stata integrata una responsabilità di natura contrattuale *ex* art. 1176, comma 2, c.c., in quanto la procedura adottata dall'intermediario convenuto non poteva ritenersi improntata alla diligenza professionale esigibile in relazione alla specifica attività esercitata. A sottolineare questo profilo sta infatti il passo in cui il giudicante afferma che la banca convenuta risultava gravemente in difetto « *per non essersi adeguata agli* standard *di sicurezza dei sistemi informatici, non avendo adottato, nel servizio di* home banking*, quel sistema di autenticazione basato su OTP, che all'epoca dei fatti costituiva uno* standard *consolidato per la tutela dei clienti di banche dal* phishing *e dai programmi spia*" ».

Per tale effetto, l'intermediario bancario veniva condannato al rimborso delle somme abusivamente prelevate dal conto degli attori, con rivalutazione a far data dagli episodi contestati. Veniva altresì liquidata in via equitativa, a titolo di danno non patrimoniale, la somma di 800 Euro ciascuno.

Il caso in esame ripropone quindi il tema della responsabilità dell'azienda di credito per danno ai correntisti derivante da frode informatica, che inizia a registrare una consistente casistica sia nella giurisprudenza che nelle decisioni di alcuni organismi di composizione (segnatamente, l'Arbitro Bancario Finanziario), tanto da giustificare qualche ulteriore approfondimento in questa sede.

2. LA CORNICE NORMATIVA DI RIFERIMENTO

La sentenza in esame offre l'occasione per ripercorrere il tema della responsabilità della banca per l'abusiva utilizzazione delle credenziali informatiche del correntista nell'ambito del servizio di *home banking*(3), più volte oggetto di trattazione su queste pagine (4). La ripresa di questo tema, tuttavia, si rivela di particolare interesse non solo ai fini di un aggiornamento del dibattito, ma anche per constatare come la giurisprudenza di merito sia giunta a risultati simili utilizzando tuttavia percorsi logico-giuridici alquanto differenti: nel precedente più risalente (Trib. Palermo, 12 gennaio 2010), infatti, la condanna dell'intermediario bancario era stata fondata sulla normativa relativa al trattamento dei dati personali (5), mentre detto tratto risultava assente nella più recente pronuncia richiamata (Trib. Verona, 2 ottobre 2012), la quale optava per una configurazione in chiave esclusivamente negoziale della responsabilità, facendo leva, in particolare, sulla disciplina del mandato *ex* art. 1856 c.c.

Ciò posto, per quanto preliminarmente attiene al tema della responsabilità da trattamento dei dati (6), si ricorda che la richiamata decisione del giudice palermitano, alla luce del rinvio operato dall'art. 15, d.lgs. n. 196/2003, al regime delle attività pericolose *ex* art. 2050 c.c. (7), aveva condannato l'istituto di credito, quale titolare del trattamento, al risarcimento dei danni per non aver impedito agli abusivi utilizzatori di introdursi illecitamente nel sistema telematico del cliente, consentendo così la captazione dei suoi codici di accesso (8) e le conseguenti illegittime disposizioni di bonifico. In tale frangente, si faceva ricorso, inoltre, all'art. 31 del citato decreto legislativo, il quale impone che i dati personali oggetto di trattamento siano custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi, ivi compreso quello di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Per ciò che concerne, di contro, la configurazione in termini di responsabilità negoziale, il precedente del giudice veronese evidenziava che l'intermediario, nei rapporti con il cliente, risponde secondo le regole del mandato (dato l'espresso richiamo operato, al riguardo, dall'art. 1856 c.c. in tema di esecuzione di incarichi bancari) e che la diligenza cui essa è tenuta va considerata con particolare rigore, rinviando, in proposito, alla consolidata opinione che emerge

dalla giurisprudenza di legittimità (9). In particolare, la pronuncia riprendeva alcuni passi testuali della S.C., ricordando che deve essere verificata l'adozione, da parte dell'istituto bancario, delle misure idonee a garantire la sicurezza del servizio, dato che la diligenza posta a carico del professionista ha natura tecnica e deve essere valutata tenendo conto dei rischi tipici della sfera professionale di riferimento ed assumendo quindi, come parametro, la figura dell'accorto banchiere (10).

Per completare il tema sul possibile inquadramento della responsabilità, si evidenzia infine come non venga richiamato, nella decisione che si annota, un riferimento normativo di un certo rilievo in materia, che, se da un lato è ben presente nelle decisioni dell'Arbitro Bancario Finanziario (come nel seguito si vedrà), d'altro canto non ha finora registrato particolari riscontri in giurisprudenza: ci si riferisce, in particolare, al disposto del d.lgs. 27 gennaio 2010, n. 11 (11), che, oltre a stabilire l'obbligo del prestatore del servizio di pagamento di assicurare che i dispostivi personalizzati forniti dai gestori non siano accessibili a soggetti diversi dal legittimo titolare, detta alcune disposizioni specificamente indirizzate a ripartire le responsabilità derivanti dall'utilizzazione del servizio stesso. In particolare, all'art. 10 si prevede che, qualora l'utente neghi di aver autorizzato un'operazione di pagamento già effettuata, l'onere di provare la genuinità della transazione va a ricadere sostanzialmente sul prestatore del servizio. Nel contempo, il successivo art. 11 obbliga quest'ultimo ad una rifusione sostanzialmente immediata, in caso di operazione disconosciuta dal cliente, tranne che nel caso di motivato sospetto di frode (12), fermo restando, tuttavia, il diritto del prestatore di servizi di procedere, in seguito, allo storno dell'operazione di rimborso ove la paternità dell'operazione sia da confermare in capo al correntista. Non pare dubbio che un meccanismo così concepito configuri, a carico dell'intermediario che predispone il servizio di *home banking*, un regime di responsabilità piuttosto stringente (su cui si tornerà nel seguito).

Sul lato opposto, per ciò che attiene all'utilizzatore, vengono precisati, all'art. 7 stesso decreto, alcuni canoni di condotta, sia in tema di tempestiva comunicazione dell'altrui utilizzo indebito dello strumento, sia in relazione all'adozione delle misure idonee a garantire la sicurezza dei dispositivi personalizzati che ne consentono l'utilizzo.

Il quadro di cui sopra ha poi ricevuto un ulteriore contributo di precisazione dal provvedimento della Banca d'Italia del 5 luglio 2011 (13), il quale, alla sezione IV, si occupa espressamente degli obblighi e delle responsabilità dell'utilizzatore di servizi di pagamento, in relazione alle modalità di fruizione dei medesimi. La norma si rivela di particolare interesse per il livello di dettaglio con cui vengono regolamentati, da un lato, i livelli di sicurezza dei dispositivi messi a disposizione della clientela e, dall'altro, i canoni di cautela cui gli utilizzatori devono attenersi (14).

3. TECNICHE DI CAPTAZIONE DEI CODICI DI ACCESSO AI SISTEMI TELEMATICI DI PAGAMENTO

Posto che, ad avviso del decidente, la diligenza esigibile dall'operatore bancario deve essere di tipo professionale e tecnico, detto tratto avrebbe imposto all'intermediario l'adozione di misure idonee a garantire la sicurezza dei servizi erogati. A questo proposito, la pronuncia annotata si sofferma operando una comparazione fra i presìdi adottati nel caso concreto e quelli — più evoluti — disponibili nella prassi bancaria e giunge ad un giudizio di inidoneità dei primi, dal quale fa conseguentemente derivare la responsabilità per danni dell'azienda di credito.

Il tratto giustifica una più approfondita riflessione in ordine ai possibili fenomeni di sottrazione delle credenziali di accesso ai sistemi di *home banking*. In particolare, la sentenza, sulla base della considerazioni del consulente tecnico, propende per una frode attuata mediante la fattispecie del c.d. *phishing*(15), espressione con cui si compendiano una pluralità di tecniche di captazione di dati e codici personali, su cui conviene brevemente soffermarsi.

Secondo alcuni riferimenti (16), il *phisherman* (o *phisher*) è il soggetto specializzato nella sottrazione di numeri di carte di credito, di bancomat e — per quanto qui maggiormente rileva —

di credenziali di accesso all'*internet banking*, per la quale vengono utilizzate modalità differenti (17). Se, da un lato, è frequente il ricorso a messaggi di posta elettronica ingannevoli, apparentemente inviati da istituti di credito, con i quali si richiede al cliente la digitazione dei codici personali, adducendo svariati motivi (controlli di sicurezza o altro), d'altro canto si registra anche la tecnica di introdurre occultamente sulla postazione informatica del correntista un programma-spia (18), che ne cattura le *password*. Una volta ottenuti detti codici, il terzo accede quindi abusivamente al sistema e dispone uno o più bonifici in favore di un altro soggetto, collaboratore del *phisherman*, il quale avrà il compito di dirottarlo ancora su altro destinatario (preferibilmente all'estero), trattenendo una commissione per il suo intervento.

A ben vedere, il caso portato in decisione sembra concernere la prima delle due ipotesi citate, in quanto i correntisti, prima dei prelevamenti contestati, avevano ricevuto un messaggio di posta elettronica apparentemente inviato dal servizio assistenza della loro banca, che li invitava a digitare le credenziali informatiche di accesso al servizio. Nel rispondere, i clienti avevano peraltro inconsapevolmente fornito la *password* ai terzi abusivi prenditori.

La recente giurisprudenza delle Corti penali, sebbene non ancora numerosa, mostra una crescente attenzione a questo fenomeno, nel tentativo di un appropriato inquadramento giuridico del medesimo e delle responsabilità ad esso collegate.

Al riguardo, pare innanzitutto utile richiamare la pronuncia secondo la quale la condotta in esame consiste nel carpire, mediante abusivo inserimento nel sistema informatico o mediante false e-mail dirette ai clienti delle banche o delle poste, i dati significativi dei rapporti di conto corrente intrattenuti dagli stessi, dati che vengono successivamente utilizzati in modo fraudolento per « clonare » carte di credito e/o di pagamento o per disporre *on line* operazioni di trasferimento di denaro su conti correnti nella disponibilità dei criminali, con successivo prelevamento di contanti e conseguente dispersione del denaro fraudolentemente sottratto. Sul piano giuridico, il decidente aveva qui ritenuto che la condotta fosse ascrivibile alla fattispecie della truffa (19).

Un ulteriore contributo giunge dalla sentenza in cui, nel premettere che il *phishing* consiste nell'illecita intrusione via internet, da parte di terzi soggetti, nei sistemi informatici concernenti servizi *home banking* per utenti titolari di conti correnti bancari, si afferma come detto comportamento integri, di per sé, i reati di accesso abusivo informatico (20) e falsificazione del contenuto di comunicazioni informatiche di cui agli art. 615-*ter* e 617-*sexies* c.p. A tale proposito, la sentenza soggiunge che, qualora detta attività venga svolta con la collaborazione di soggetti operanti in Paesi stranieri, essa concreta i reati di associazione a delinquere, con l'aggravante di reato transnazionale, di accesso abusivo informatico e di falsificazione di comunicazioni informatiche (21).

Con specifico riguardo all'apporto della richiamata figura del collaboratore, si ritiene inoltre che sia penalmente responsabile del delitto di riciclaggio colui che, con più azioni in esecuzione del medesimo disegno criminoso, senza essere concorso nel reato presupposto, accetta il rischio — ovvero agisce nella piena consapevolezza — della probabile origine delittuosa di denaro, che si impegna a fare transitare sul proprio conto corrente bancario e, quindi, a trasferire verso soggetti terzi e ciò anche con riferimento alla possibilità che la propria condotta sia idonea ad ostacolare l'attività di accertamento della provenienza delittuosa delle somme ricevute (22). Altra giurisprudenza introduce tuttavia una distinzione, quando afferma, da un lato, che, ove il ricettatore o riciclatore sia consapevole dell'attività illecita del *phisher* ed assicuri a questi il proprio apporto, lo stesso risponde di concorso nell'attività delittuosa del secondo; di contro, nel caso in cui il medesimo sia inconsapevole del disegno criminoso complessivo, non sussisterebbe il concorso doloso nel reato presupposto, bensì la sua responsabilità per i reati di riciclaggio o ricettazione a titolo di dolo eventuale (23).

Ciò posto, la fenomenologia esaminata va peraltro posta a confronto con il più ampio novero delle tecniche, che, a vario titolo, integrano il c.d. furto di identità (e, in particolar modo, il furto di

identità digitale) (24). Per stare ad una prima definizione, esso potrebbe essere individuato come la condotta illecita volta a ottenere indebitamente denaro o altri vantaggi, utilizzando le generalità di altra persona. Il fenomeno ha registrato, peraltro, una tale diffusione, specie in ambito finanziario, da giustificare diversi recenti interventi legislativi.

In primo luogo, si ricorda infatti che, a seguito del d.lgs. 11 aprile 2011, n. 64, sono stati inseriti nel d.lgs. 13 agosto 2010, n. 141, fra gli altri, gli artt. 30-*bis* e 30-*ter*.

L'art. 30-*bis*, da un lato, soggiunge ulteriori elementi dal punto di vista definitorio, dal momento che distingue fra due sottotipi di furto di identità e precisamente:

a) *impersonificazione totale*: occultamento totale della propria identità mediante l'utilizzo indebito di dati relativi all'identità e al reddito di un altro soggetto. L'impersonificazione può riguardare l'utilizzo indebito di dati riferibili sia ad un soggetto in vita sia ad un soggetto deceduto;

b) *impersonificazione parziale*: occultamento parziale della propria identità mediante l'impiego, in forma combinata, di dati relativi alla propria persona e l'utilizzo indebito di dati relativi ad un altro soggetto, nell'ambito di quelli di cui alla lettera *a*).

L'art. 30-*ter*, dal canto suo, prevede la costituzione di un sistema pubblico di prevenzione delle frodi nel settore del credito al consumo, istituendo un archivio centrale informatizzato, cui aderiscono vari operatori finanziari.

La figura del furto di identità trova ormai riscontro anche nelle decisioni della giurisprudenza in ambito finanziario, ad esempio relativamente al caso del nominativo di un ignaro soggetto segnalato « a sofferenze » nel sistema, dopo che era stato concesso a terzi, ma a suo nome, un finanziamento, dietro esibizione dei suoi documenti di identità, in precedenza furtivamente sottrattigli (25). La S.C. ha peraltro avuto modo di precisare, al riguardo, che, nell'ipotesi di furto di identità con utilizzazione, da parte del reo, di un documento altrui in nulla alterato o modificato, al fine di aprire conti correnti ed emettere assegni, la riconoscibilità dell'abuso è da ritenere *in re ipsa* e da presumere fino a prova contraria. Sarebbe qui a carico della banca, quindi e non del danneggiato, l'onere di fornire la prova della scusabilità del suo errore per la somiglianza fra le due persone o per altra causa (26).

Un'altra novella normativa che merita una segnalazione, infine, è la modifica dell'art. 640-*ter* c.p., il cui comma 3, inserito dall'art. 9, d.l. 14 agosto 2013, n. 93 (conv. con modifiche nella l. 15 ottobre 2013, n. 119), prevede un aumento di pena se la frode informatica venga commessa con *furto o indebito utilizzo dell'identità digitale di uno o più soggetti*. Alla luce di questo richiamo, si registrano, di recente, alcune opinioni sul possibile inquadramento del *phishing* sotto questa fattispecie normativa (27).

4. ORIENTAMENTI DELL'ARBITRO BANCARIO FINANZIARIO

Come visto, la sentenza in esame ha ritenuto che la prevista consegna, all'attivazione del servizio di *home banking*, di un codice utente e una prima *password* di accesso fossero da ritenere cautele insufficienti, a fronte dei presìdi più evoluti disponibili per questa attività. In altre parole, il giudice giunge a sancire l'inadeguatezza del sistema predisposto dall'intermediario, in quanto di livello inferiore rispetto agli strumenti comunemente utilizzati dal sistema e allo stato dell'evoluzione tecnologica.

Su questo tema, i riferimenti di giurisprudenza risultano, per la verità, alquanto rari (28) e non sempre dedicano un approfondimento al dettaglio tecnico dei presìdi adottati o esigibili (29). Il profilo, di contro, sembra emergere, con maggiore frequenza, in alcune recenti decisioni dell'Arbitro Bancario Finanziario (30), in cui si pongono a confronto, da un lato, i requisiti di cautela posti a carico dell'intermediario e, dall'altro, gli obblighi di diligenza nella custodia dei

codici d'accesso da parte del cliente, con specifico richiamo alla più recente normativa del settore.

Data la numerosissima serie di provvedimenti e considerato il taglio di questo contributo, ci si dovrà limitare, in questa sede, a selezionare alcuni richiami, parsi fra quelli di maggior rilevanza ai fini dell'inquadramento della problematica in esame.

A tale proposito, in una prima fase, parallelamente alla responsabilità della banca, non di rado veniva evidenziato anche il profilo della colpa concorrente del cliente per negligente custodia dei codici di accesso (31), fino a ridurre, in alcuni casi in misura significativa, la richiesta di rimborso, quando accertato che il medesimo aveva fornito incautamente a terzi i propri codici personali (32).

Dopo l'emanazione del d.lgs. n. 11/2010, si registra, invece, una prassi che vede progressivamente aumentare le pronunce di condanna integrale nei confronti degli intermediari, anche a fronte della predisposizione di presìdi di sicurezza molto avanzati (33). Ciò anche in forza dell'assetto impresso alla materia dal citato provvedimento, che impone, come visto, un rimborso sostanzialmente immediato in favore dell'utilizzatore, salva la prova di una sua compartecipazione nella frode, che resta però a carico del prestatore del servizio. A volte, oltre al richiamo alla normativa citata, si registra anche l'affermazione (analoga a quella riportata nell'annotata sentenza) secondo la quale il grado di diligenza cui l'impresa bancaria è tenuta va individuato in quello professionale *ex* art. 1176, comma 2, c.c.

Oltre all'argomentazione relativa al nuovo assetto giuridico della materia (non a caso, le decisioni dell'Organismo di composizione fanno ampio richiamo al d.lgs. n. 11/2010), tuttavia, la svolta interpretativa dell'Arbitro Bancario Finanziario deriva anche da un ulteriore ordine di motivazioni, che meglio si coglie mediante un richiamo testuale di alcuni passi delle decisioni più recenti.

A questo proposito, si osserva infatti che « L'evidente squilibrio che le predette disposizioni determinano nel rapporto fra prestatore e utilizzatore di un servizio di pagamento trovano una loro giustificazione, per così dire, “social-commerciale”, nitidamente ricostruita in una pronuncia del Collegio di Roma, ad avviso del quale “la disciplina è evidentemente ispirata al principio del “rischio d'impresa”, e cioè all'idea secondo la quale è razionale far gravare i rischi statisticamente prevedibili legati ad attività oggettivamente “pericolose”, che interessano un'ampia moltitudine di consumatori o utenti, sull'impresa, in quanto quest'ultima è in grado, attraverso la determinazione dei prezzi di vendita dei beni o di fornitura del servizio, di ribaltare sulla massa dei consumatori e degli utenti il costo dell'assicurazione di detti rischi. Si tende, in altri termini, a “spalmare” sulla moltitudine degli utilizzatori il rischio dell'impiego fraudolento di carte di credito e strumenti di pagamento, sì da evitare che esso gravi esclusivamente e direttamente sul singolo pagatore » (34). Particolarmente incisivo si rivela poi il tratto in cui si afferma che « la menzionata disciplina configura quindi in capo all'intermediario, per la quota eccedente la franchigia, una sorta di “responsabilità oggettiva” (...) che può essere superata solo dalla prova, da esso fornita, del dolo o della colpa grave del cliente, al quale allora potranno essere attribuiti i danni per l'uso illecito dello strumento » (35).

Gli obblighi della banca, inoltre, secondo alcune delle decisioni dell'Autorità citata, si spingerebbero fino a ricomprendere un approfondito monitoraggio delle operazioni disposte su internet dalla clientela: « La condotta dell'intermediario appare, inoltre, priva della necessaria diligenza anche con riguardo ad ulteriori e connessi obblighi derivanti dalla propria posizione contrattuale, con particolare riguardo al costante e scrupoloso monitoraggio delle transazioni *on line* da parte dei correntisti (già più volte richiamato da questo Collegio; cfr., per tutte, dec. n. 1477/2011); tale dovere, infatti, consente all'intermediario di verificare il regolare andamento delle operazioni e di segnalare quelle che appaiono anomale, come è avvenuto nel caso di specie, tenuto conto che — per i bonifici di cui si discute — si tratta di operazioni effettuate in un ristretto lasso temporale e nei confronti del medesimo beneficiario, ponendosi in contraddizione con la usuale operatività del conto del ricorrente (36) ». In questo tratto, gli orientamenti dell'Arbitro Bancario Finanziario paiono più rigidi della giurisprudenza di merito, posto che, in alcuni precedenti, si era

escluso che in capo all'azienda di credito sussista un onere di questo tipo, tenuto anche conto che molte di tali operazioni vengono disposte a sportelli bancari chiusi (37).

A margine di tali posizioni, su cui a breve si tornerà, meritano di essere segnalate alcune ulteriori indicazioni provenienti dagli orientamenti dell'Autorità.

Quanto alle possibili modalità di captazione informatica dei codici di accesso, viene presa in considerazione anche la tecnica, particolarmente evoluta ed insidiosa, del c.d *man-in-the browser*, mediante il quale viene inserito nell'ambiente informatico originale e nella correlata simulazione un messaggio-esca che a chiunque apparirebbe come genuino (38).

Di rilievo, inoltre, pare il passo, riportato in altra pronuncia, in cui si segnala che eventuali clausole di esonero da responsabilità dell'intermediario contenute nel contratto di servizio non avrebbero effetto, in quanto onerose ai sensi dell'art. 1341 c.c. e vessatorie ai sensi delle norme di protezione del consumatore (39). Fra l'altro, a parere della citata Autorità, eventuali pattuizioni tese ad esonerare il prestatore del servizio da responsabilità per dolo o colpa grave incorrerebbero nel divieto posto dall'art. 1229 c.c. (40).

Si assiste quindi ad un assetto in cui i Collegi tendono a configurare una responsabilità dell'intermediario in tutti i casi in cui non si riesca a dimostrare il dolo o la colpa grave del cliente. Al riguardo, non viene ritenuta sufficiente una difesa della banca che si limiti a sostenere l'affidabilità dei propri sistemi di controllo sul servizio di *home banking*(41). Va detto, peraltro, che talvolta riaffiora nelle decisioni il richiamo ad una responsabilità concorrente del correntista *on line*, specie quando non abbia seguito le ordinarie cautele nella protezione del proprio computer (ad esempio, con idonei *software* antivirus) (42).

La ricognizione di cui sopra evidenzia come l'Arbitro Bancario Finanziario tenda a seguire percorsi argomentativi in parte non coincidenti con quelli della giurisprudenza corrente, posto che quest'ultima si è fin qui mostrata meno incline, almeno per la fattispecie in esame, ad aderire alla tesi di una responsabilità oggettiva della banca fornitrice del servizio di *home banking*. Il tratto giustifica pertanto qualche ulteriore approfondimento relativamente alla diligenza del banchiere, cui spesso si richiamano sia i giudici (ivi compreso quello di Milano che si annota), sia l'organismo di composizione.

5. DILIGENZA DELL'OPERATORE BANCARIO E TRATTI DI RESPONSABILITÀ OGGETTIVA

La sentenza che si annota, come visto, afferma che l'intermediario, nei rapporti con il cliente, deve osservare canoni di diligenza professionale, in relazione alla natura dell'attività esercitata, con espresso richiamo all'art. 1176, comma 2, c.c. A seguire, la motivazione evidenzia che la banca, nel contratto di *home banking*, ha la veste di contraente qualificato, che, non ignaro delle modalità di frode mediante *phishing* da tempo note nel settore, è tenuto ad adeguarsi all'evoluzione dei nuovi sistemi di sicurezza. Di contro, non può ascriversi a responsabilità del cliente il fatto di non essere stato al corrente di tali modalità di frode e, di conseguenza, di non essersi accorto che le e-mail ricevute fossero, in realtà, atti di pirateria informatica tesi a carpire i suoi codici di accesso al sistema.

A questo proposito, già la giurisprudenza di legittimità, con specifico riferimento ai servizi e strumenti che si avvalgono di mezzi meccanici o elettronici (compresi quelli con funzione di pagamento), aveva affermato che l'istituto bancario non può omettere l'adozione delle misure idonee a garantire la sicurezza del servizio stesso, dal momento che, in base ai canoni di condotta appena richiamati, la diligenza posta a suo carico ha natura tecnica e deve essere valutata tenendo conto dei rischi tipici della sfera professionale di riferimento (43). Detto inciso è stato poi raccolto e fatto proprio da una recente sentenza di merito, resa su caso simile a quello annotato, pubblicata su queste pagine (44).

Il passo in esame evoca il dibattito sorto intorno ai canoni di condotta esigibili dalle aziende di credito nell'erogazione dei loro servizi alla clientela, condensato nella locuzione nota come « diligenza del buon banchiere » (45), istituto che, nel tempo, ha assunto una fisionomia talmente caratterizzata da giustificare, da una parte della dottrina, l'interrogativo circa una responsabilità da *status*(46) in capo alla banca. Pur nella sinteticità data dal taglio del presente approfondimento, sembra quindi utile richiamare, anche in questa sede, alcuni dei passaggi salienti di questa tematica, già espressi su questa *Rivista*(47), che meglio sembrano attagliarsi al caso esaminato.

Nel premettere che, secondo un'autorevole definizione, « diligenza è qualificazione di un comportamento, il cui rovescio può dirsi rappresentato dalla colpa » (48), appare oggi consolidata l'opinione secondo la quale la diligenza cui la banca è tenuta è quella professionale (49) e non semplicemente quella media.

Non sono mancate, per il vero, alcune voci di segno contrario (50), sebbene più isolate. In particolare, a suo tempo, seguendo un percorso ermeneutico strettamente aderente alla lettera della norma, è stato evidenziato, al riguardo, che l'art. 1856 c.c. prescrive, nell'esecuzione degli incarichi bancari, di attenersi alle regole del mandato, richiamando quindi il concetto di diligenza del buon padre di famiglia di cui all'art. 1710 c.c.: quest'ultimo, che trova il suo referente nel comma 1 dell'art. 1176 c.c., costituirebbe tuttavia un canone di condotta diverso rispetto a quello — più severo — della diligenza professionale, contemplata al comma 2 della medesima norma (51).

Taluni, peraltro, hanno inteso cogliere una distinzione sotto un diverso profilo, affermando che la figura del « buon padre di famiglia » evocata dall'art. 1176, comma 1, c.c., non si identifica con l'uomo medio di comune intelligenza, ma guarda alla figura del modello di cittadino avveduto, la cui diligenza deve tendere verso livelli più elevati: in altre parole, secondo la riferita opinione, il criterio del buon padre di famiglia sarebbe più rigoroso di quello dell'uomo medio (52).

Tanto premesso, la tematica della diligenza del buon banchiere, formatasi prevalentemente intorno al problema della responsabilità per la negoziazione dei titoli di credito, si pone ora con rinnovata attenzione — e, probabilmente, con alcune sostanziali differenze — in ordine alla prestazione di servizi telematici di pagamento (53).

Come visto, gli orientamenti dell'Arbitro Bancario Finanziario sopra richiamati — che, fra l'altro, investono una casistica di gran lunga più estesa rispetto ai contenziosi devoluti alla giurisdizione ordinaria — tendono recentemente a ravvisare, nell'erogazione di detti servizi, una responsabilità « sbilanciata » in danno dell'intermediario, motivando detto assetto con il richiamo al principio del rischio d'impresa e soggiungendo, al riguardo, che solo la banca sarebbe in grado, attraverso la determinazione dei prezzi di vendita dei beni o di fornitura del servizio, di ripartire sulla massa dei consumatori e degli utenti il costo (dell'assicurazione) di detti rischi. Si tratterebbe, quindi, di una forma di socializzazione del rischio, atta ad evitare che quest'ultimo ricada esclusivamente e direttamente sul singolo utente (54).

La teoria del rischio di impresa (55) anche a carico della banca, per il vero, non costituisce una novità e ha registrato, da tempo, alcuni significativi riscontri (56). Da ciò è derivato il formarsi, in sede interpretativa, di alcuni orientamenti tesi a configurare una responsabilità oggettiva (57) dell'azienda bancaria, in primo luogo per quanto riguarda la negoziazione di titoli di credito (e, in special modo, assegni non trasferibili) (58), ma, più di recente, in tema di risarcimento dei danni derivanti dall'operato del promotore finanziario (59).

Il tratto in esame evoca il noto dibattito (che, per ovvi motivi, qui non è possibile ripercorrere) circa la possibilità di individuare, nel nostro sistema, ipotesi di responsabilità oggettiva, che ha visto da un lato le opinioni di chi sostiene doversi superare il principio della colpa e, sul lato opposto, quelle di chi ritiene inopportuno abbandonare detta configurazione (60).

Tornando al tema in esame, da quanto sopra esposto deriva, in sintesi, un quadro in cui la responsabilità per la violazione dei sistemi di pagamento telematici, in forza anche di alcuni recenti riferimenti normativi, tende sempre di più a gravare in capo all'intermediario, il quale viene onerato di una prova liberatoria (non sempre agevole) sull'idoneità dei presìdi adottati.

Peraltro, se si confrontano le motivazioni adottate dalla giurisprudenza e dall'Arbitro Bancario Finanziario, il percorso argomentativo adottato appare differente. La prima, infatti, tende a fondare l'eventuale condanna dell'azienda di credito sulla violazione di obblighi di diligenza, con ciò mostrando di muoversi — almeno nominalmente — nel solco di una responsabilità per colpa, sebbene l'imposizione di una soglia particolarmente elevata e rigorosa di diligenza professionale, in sostanza, lascia alla stessa banca margini esigui per liberarsi dalla responsabilità. Di contro, l'Arbitro Bancario Finanziario sembra propendere per una responsabilità oggettivamente ascritta in capo all'intermediario, sulla scorta di una asserita possibilità di migliore allocazione e ripartizione finale del rischio.

6. PROFILI DEL DANNO NON PATRIMONIALE

La sentenza annotata dedica un breve passo alla liquidazione di una somma a titolo di danno non patrimoniale in favore delle due vittime della frode, valorizzando, al riguardo, «l'inevitabile sofferenza e preoccupazione degli stessi, in esito alla truffa informatica subìta, nel constatare la perdita dell'intera provvista accreditata sul conto ».

La sinteticità dell'inciso e il taglio di questo contributo non consentono di trattenersi su questo aspetto, al quale pare tuttavia opportuno dedicare qualche breve cenno.

Al riguardo, va premesso che, in questi termini, la decisione offre un profilo di una certa novità, dal momento che sono rari i casi editi in cui si rinvengono espressi richiami ad una liquidazione di danno non patrimoniale per fattispecie analoghe. In altro precedente giurisprudenziale, oltre a tutto, era stato utilizzato un differente inquadramento, che aveva fondato la condanna della banca al risarcimento sulla normativa relativa al trattamento dei dati personali (61): ciò aveva reso in qualche modo più agevole un percorso interpretativo di questo tipo, dato lo specifico richiamo al pregiudizio non patrimoniale contemplato dell'art. 15 del d.lgs. n. 196/2003.

Di contro, il giudice di Milano ha individuato detta componente di danno argomentando nel solco di una responsabilità sostanzialmente negoziale dell'intermediario bancario, evocando così implicitamente la tematica del danno non patrimoniale da inadempimento (62) ed evidenziando, a tal fine, la gravità del turbamento derivante dall'aver perso tutte le disponibilità liquide sul conto.

La pronuncia, quindi, aggiunge un tassello ai possibili pregiudizi derivanti dal furto di credenziali bancarie meritevoli di risarcimento, che iniziano ad affermarsi sia in dottrina che in giurisprudenza (63). Tuttavia, essa non si spinge fino a configurare la ricorrenza di un danno esistenziale, categoria non di rado richiamata in caso di danni non patrimoniali contrattuali (64).

I materiali su questo aspetto risultano quindi rari e non consolidati. Al riguardo, parrebbe tuttavia auspicabile che eventuali futuri sviluppi in sede interpretativa tengano conto, ad esempio, della noto arresto secondo cui non sarebbero meritevoli dalla tutela risarcitoria, *sub specie* di danno esistenziale, i pregiudizi consistenti in meri disagi, fastidi, disappunti, ansie ed in ogni altro tipo di insoddisfazione concernente gli aspetti più disparati della vita quotidiana (65). Sarebbe interessante, ad esempio, verificare il trattamento, in sede giudiziale, di questa componente di danno in caso di solo marginale incidenza sul patrimonio della vittima (a differenza del caso annotato).

7. CONSIDERAZIONI CONCLUSIVE

L'esposizione che precede induce ad alcune osservazioni di sintesi.

In primo luogo, la rassegna esaminata fa emergere una pragmatica considerazione di fondo, vale a dire che, almeno allo stato attuale della tecnica, non paiono essere stati raggiunti *standard* di protezione dei sistemi di pagamento telematici tali da essere completamente inviolabili da parte di terzi abusivi utilizzatori. Detta conclusione vale, a maggior ragione, quando i presìdi adottati dall'azienda di credito risultino non evoluti dal punto di vista tecnologico. In prospettiva, ciò fa intravedere, tuttavia, una possibile proliferazione delle decisioni di condanna a carico degli intermediari, specie qualora si ritenga di fondare la relativa responsabilità su criteri oggettivi.

Al riguardo, le argomentazioni utilizzate dalla giurisprudenza e dall'Arbitro Bancario Finanziario mostrano tuttavia alcune divergenze. Il tratto si coglie, innanzitutto, sul fondamento della responsabilità, posto che, in sede giudiziale, si preferisce mantenere un riferimento all'obbligo di osservanza dei canoni di diligenza. Di contro, l'adozione, da parte del citato organo di composizione, di una responsabilità in chiave oggettiva, o quantomeno di inversione dell'onere della prova, rende un richiamo di questo tipo sostanzialmente desueto o quantomeno ne limita la portata a poco più che un elemento di stile. Non a caso, la norma più gravosa in tema di responsabilità del prestatore del servizio (d.lgs. n. 11/2010) stenta a trovare riscontri in giurisprudenza, dove invece l'Organismo di composizione citato vi fa ampio ricorso.

Per inciso, detta ultima configurazione si rivelerebbe, sul piano economico, non del tutto neutra per la generalità dell'utenza bancaria, sulla quale verrebbe poi a ripartirsi l'onere finale derivante dall'aumento delle tariffe del servizio (al fine di consentire la copertura, anche assicurativa, dei sinistri).

Quanto al tema del pregiudizio risarcibile, si è visto come, anche in questo tipo di controversie, inizi ad affermarsi la figura del danno non patrimoniale da inadempimento, tanto da non poter escludere che, in futuro, la stessa venga riproposta in chiave di danno esistenziale, profilo che già (ri)affiora in alcuni recenti materiali in tema di danno non patrimoniale contrattuale.

In prospettiva più ampia, si assiste, infine, al moltiplicarsi dei percorsi argomentativi che, nella materia in esame, ravvisano una forma di responsabilità quantomeno aggravata dell'intermediario. Già in precedenza, infatti, si è avuto modo di constatare come alcune decisioni abbiano sancito, per fattispecie analoghe, una condanna di quest'ultimo derivante dalla disciplina sul trattamento dei dati personali, che, giusto il combinato disposto dell'art. 15, d.lgs. n. 196/2003-art. 2050 c.c. condurrebbe, in ultima analisi, a considerare i servizi di pagamento telematici come attività pericolosa (opinione peraltro non condivisa da una parte della giurisprudenza e che necessiterebbe di una più ponderata riflessione, viste le implicazioni) e, non ultimo, ad agevolare, visto l'espresso referente normativo, la liquidazione della partizione non patrimoniale del danno.

Come già a suo tempo osservato su queste pagine, il consolidamento e la convergenza di tali orientamenti comporterebbero, oltre a tutto, ricadute pratiche significative, considerando che andrebbero progressivamente a restringersi le fattispecie riconducibili ad una responsabilità di tipo comune, in favore di una più marcata e generalizzata devoluzione verso i criteri di imputazione più severi.

Note:
(*) Contributo approvato dai Referee.
(1) Su cui si avrà modo di tornare più dettagliatamente nel seguito.
(2) Probabilmente per un refuso, in sentenza la mail esca viene richiamata con una datazione (21 settembre 2009) successiva ai prelevamenti fraudolenti (14 e 19 settembre 2009). È invece ragionevole presumere che si tratti di messaggio ricevuto in data anteriore.
(3) Secondo una prima definizione, per home banking potrebbe intendersi « lo svolgimento di operazioni bancarie dal proprio domicilio, normalmente mediante personal computer »: v. il nostro, Privacy e attività economica, in Ricciuto (a cura di), Nuovi Temi di diritto privato. Casi e materiali, Napoli, 1999, 189 ss., 217. Ma v. anche la definizione nei termini di « servizio bancario che consente al cliente, attraverso l'uso di videoterminali, di controllare il proprio conto o di effettuare pagamenti da casa o dall'ufficio »: cfr. Sabatini Coletti, (voce) Home banking, in

Dizionario della lingua italiana, http://dizionari.corriere.it.
(4) V. Trib. Verona, 2 ottobre 2012, in questa Rivista, 2103, 1284, con nostra nota Home banking, bonifici non autorizzati e responsabilità della banca; ma anche Trib. Palermo, 12 gennaio 2010, ivi, 2011, 1827 ss., con nostra nota, Sottrazione di credenziali informatiche, bonifici non autorizzati e responsabilità civile della banca da trattamento di dati personali, ivi, 1830 ss.
(5) Ma v. già Trib. Torino, Sez. IV, 28 marzo 2007, in Giur. merito, 2007, 2898, che motivava la responsabilità dell'intermediario bancario con argomentazioni similari. Più recentemente, Per un'analoga configurazione di responsabilità in tema di home banking, v. Trib. Siracusa, Sez. II civ., 15 marzo 2012, in www.dirittobancario.it, ma anche in www.altalex.com; nonché Giud. Pace Ottaviano, 30 settembre 2011, in www.dirittobancario.it. Sebbene implicitamente, segna un orientamento contrario Giud. Pace Milano, Sez. IV, 7 gennaio 2011, n. 41, in www.diritto24.ilsole24ore.com, la quale respinge l'ipotesi di una responsabilità da attività pericolose ex art. 2050 c.c. (cui la disciplina sul trattamento dei dati fa rinvio).
(6) Profilo espressamente evocato anche nelle conclusioni degli attori, ma poi non accolto dalla sentenza che si annota.
(7) Ma si ricorda che secondo Giud. Pace Milano, Sez. IV, 7 gennaio 2011, n. 41, cit., l'attività di home banking non riveste i caratteri di pericolosità ex art. 2050 c.c.
(8) Sul tema delle password di accesso al servizio di home banking come dati personali, attesa l'ampia definizione di legge, sia consentito richiamare il nostro, Le problematiche dell'attività bancaria, in Cuffaro-Ricciuto (a cura di), Il trattamento dei dati personali, II, Torino, 1999, 39 ss., 45; e Id., Privacy e attività economica, cit., 193 (già nella vigenza della l. n 675/1996). Sul fenomeno, in generale, della verifica elettronica della legittimazione v. Devescovi, Titolo di credito e informatica, Padova, 1991, 309 ss. Per un più ampio richiamo alla materia del trattamento dei dati nell'attività bancaria, si rinvia a Gaggero, Il trattamento dei dati personali nel settore bancario. Brevi note, in Contratto impr. Europa, 1998, 259 ss.; Bonzanini, Attività bancaria e tutela dei dati personali, in Banca borsa tit. cred., 1998, I, 213 ss.; Id., Privacy e banche: il nuovo regime di trattamento dei dati personali (d.lgs. 28 dicembre 2001, n. 467), ivi, 2003, 481 ss.; nonché il nostro, Le problematiche dell'attività bancaria, in Cuffaro-Ricciuto (a cura di), Il trattamento dei dati personali, cit., 39 ss.; e, più di recente, Attività bancaria e trattamento dei dati personali, in Cuffaro-D'Orazio-Ricciuto (a cura di), Il codice del trattamento dei dati personali, Torino, 2007, 519 ss. Per l'esperienza iberica su queste tematiche, si rinvia allo studio di Llacer Matacas, Comercializaciòn de servicios y tutela de datos personales: el sector bancario y asegurador, in Rev. esp. prot. de datos, 2007, 171 ss.
(9) Fra le altre, v. Cass. civ., 24 settembre 2009, n. 20543, in Guida dir., 2009, 48, 56 (s.m.); e in Il civilista, 2012, 1, 49 (s.m.), con nota di Pianezze. L'inciso più significativo della motivazione risulta il seguente: « È vero, infatti, che la diligenza del buon banchiere deve essere qualificata dal maggior grado di prudenza e attenzione che la connotazione professionale dell'agente consente e richiede. Tale diligenza (come già ritenuto da questa Corte in termini generali, con le sent. n. 1865 del 30 gennaio 2006, rv. 586699; n. 4571 del 15 aprile 1992, rv. 476801; n. 5267 del 12 ottobre 1982, rv. 423073) trova applicazione non solo con riguardo all'attività di esecuzione di contratti bancari in senso stretto, ma anche in relazione ad ogni tipo di atto od operazione che sia comunque oggettivamente esplicato presso una struttura bancaria e soggettivamente svolto da un funzionario bancario. Tale diligenza va valutata, non alla stregua di criteri rigidi e predeterminati, ma tenendo conto delle cautele e degli accorgimenti che le circostanze del caso concreto suggeriscono ». Va detto, peraltro, che, a fronte di tale assunto generale, nel caso concreto era stata negata la responsabilità della banca trattaria per aver riconosciuto l'incasso di un assegno poi rivelatosi contraffatto.
(10) Cass. civ., 12 giugno 2007, n. 13777, cit.
(11) Il citato provvedimento trae origine dalla Direttiva 2007/64/CE del Parlamento Europeo e del Consiglio del 13 novembre 2007.
(12) In caso, ovviamente, di coinvolgimento del cliente nella partecipazione all'illecito. Questa pare infatti l'interpretazione ragionevolmente da attribuire al passo: diversamente argomentando e sostenendo che qualsiasi sospetto di frode — anche quella subìta dal cliente — giustifichi il rifiuto del rimborso da parte della banca, si giungerebbe infatti a vanificare il senso della prescrizione.
(13) Intitolato « Attuazione del Titolo II del Decreto legislativo n. 11 del 27 gennaio 2010 relativo ai servizi di pagamento (Diritti ed obblighi delle parti) ».

(14) Sul primo profilo, si segnala, ad esempio, quanto previsto all'art. 2 dell'Allegato Tecnico, nota 28: « Le metodologie di autenticazione forte degli utenti si basano su una pluralità di “fattori”, tra i quali: i) qualcosa che l'utente conosce (es: password/PIN); ii) qualcosa che l'utente possiede (es. smart card, token, OTP, SIM cellulare, Firma Digitale); iii) qualcosa che l'utente è (es: caratteristiche biometriche). Fattori di diverso tipo possono essere combinati insieme per ottenere soluzioni di autenticazione “multifattore” in grado di elevare il livello complessivo di sicurezza ». Quanto al secondo aspetto richiamato (cautele dell'utilizzatore), l'art. 2.1 del provvedimento dispone che, quando uno strumento prevede l'accesso mediante dispositivi personalizzati di sicurezza (ad esempio PIN e password), l'utilizzatore è obbligato a mettere in atto gli accorgimenti idonei a preservarne la riservatezza, al fine di evitarne un uso non autorizzato. Tale esigenza — soggiunge la norma — rileva in modo specifico nel caso in cui il pagamento sia effettuato a distanza, ad esempio per mezzo di un dispositivo telefonico o di un sito internet. Essa prevede, pertanto, che l'utilizzatore debba ottenere l'autorizzazione del proprio prestatore di servizi di pagamento prima di fornire a terzi i codici personali: in tal modo è possibile, per quest'ultimo, individuare le richieste abusive di terzi celate sotto un'apparenza di legittimità, e, in genere, di limitare i rischi connessi con operatività di internet banking.Qualora, infine, il contratto sottostante vieti all'utilizzatore di comunicare a terzi i codici di sicurezza, la norma dell'Autorità di vigilanza prevede che la violazione di tale divieto integri una condotta negligente, non consentendo quindi all'utilizzatore stesso di avvalersi dell'esenzione di responsabilità di cui al successivo paragrafo della norma in esame.
(15) Deformazione, nel gergo degli hacker informatici, di fishing.
(16) Recentemente, v. Catalano, Lotta al phishing, in Internal Audit, 2011, 4, 25 ss. Sul tema v. Cajani-Costabile-Mazzaraco, Phishing e furto d'identità digitale, Padova, 2008; Perri, Analisi informatico-giuridica delle più recenti interpretazioni giurisprudenziali in tema di phishing, in Ciberspazio e diritto, 2008, 93 ss. Ulteriori contributi in Cajani, Profili penali del phishing, in Cass. pen., 2007, 2294; Flor, Phishing, identity theft e identity abuse: le prospettive applicative del diritto penale vigente, in Riv. it. dir. proc. pen., 2007, 899; nonché in Di Ronzo, Uso non autorizzato di carte di credito e concorso di reati nel phishing, in Dir. inf., 2009, 1, 83; Ferola, Il riciclaggio da phishing tra vecchie e nuove questioni interpretative, in Giur. merito, 2009, 2831. Ma v. anche Bartoli, La frode informatica tra “modellistica”, diritto vigente, diritto vivente e prospettive di riforma, in Dir. inf., 2011, 383 ed ivi ulteriori riferimenti in nota 28; Ciraolo, Prelievi fraudolenti e responsabilità della banca nell'erogazione del servizio Bancomat, in Banca borsa tit. cred., 2009, II, 21; Corasaniti, Prove digitali e interventi giudiziari sulla rete nel percorso della giurisprudenza di legittimità, in Dir. inf., 2011, 399 ss.; Pioletti, Possesso o utilizzo abusivo di carte di credito, in Giur. merito, 2012, 1937.
(17) Si veda la descrizione contenuta nel Decalogo ABI sul phishing, in www.abilab.it: « Il phishing consiste nella creazione e nell'uso di e-mail e siti web ideati per apparire come e-mail e siti web istituzionali di organizzazioni finanziarie o governative, con lo scopo di raggirare gli utenti internet di tali enti e carpire loro informazioni personali riguardanti il proprio account, quali le proprie password per accedere a servizi di home banking o il proprio numero di carta di credito. Tali informazioni vengono catturate dai “phishers” e vengono successivamente riutilizzate per scopi criminali, come frodi finanziarie o furti di identità. Le e-mail apparentemente provengono da una banca o da una società emittente carte di credito, e vengono composte utilizzando il logo, il nome e il layout tipico dell'azienda imitata. Tali e-mail invitano il destinatario a collegarsi tramite un link a un sito internet del tutto simile a quello della banca e a inserirvi, generalmente attraverso una finestra pop up che si apre dallo stesso link, le informazioni riservate ».
(18) Il c.d. malware: sul tema, ex multis, v. i riferimenti in Catalano, Lotta al phishing, cit., 25.
(19) Trib. Monza, 7 maggio 2009, in Riv. pen., 2010, 1301.
(20) In dottrina, v. Perri, Analisi informatico-giuridica dei reati di frode informatica e accesso abusivo a un sistema informatico o telematico con l'aggravante dell'abuso della qualità di operatore del sistema, in Giur. merito, 2008, 1651
(21) Uff. Ind. Prel. Milano, 10 dicembre 2007, in Foro ambrosiano, 2008, 280.
(22) Uff. Ind. Prel. Palermo, 21 aprile 2009, in Giur. merito, 2009, 2825 (s.m.), con nota di Ferola, Il riciclaggio da phishing fra vecchie e nuove questioni interpretative, cit. Nella fattispecie, il dolo del delitto di riciclaggio, nella forma del dolo eventuale, è stato ritenuto sussistente in considerazione della natura dell'operazione complessivamente effettuata dall'imputato principale e

dal compartecipe suo genitore, operazione originata dall'accettazione di una proposta di prestazione lavorativa inviata tramite e-mail, contenente la prospettazione di facili guadagni in relazione alla semplice attività, richiesta da una società straniera non meglio identificata, di porre all'incasso e successivamente trasferire verso l'estero somme di denaro. Più recentemente, si veda Trib. Milano, 7 ottobre 2011, in Guida dir., 2013, dossier 5, 60, la cui massima è riportata come segue: « Chi utilizza tecniche di "phishing" per ottenere, tramite artifici e raggiri e inducendo in errore l'utente, le credenziali di autenticazione necessarie ad accedere abusivamente a spazi informatici esclusivi del titolare (ad esempio relativi alla gestione dei conti correnti on line) e a svolgere, senza autorizzazione, operazioni bancarie o finanziarie, può rispondere dei delitti di cui agli art. 494 (sostituzione di persona), 615-ter (accesso abusivo a sistemi informatici o telematici) e 640 c.p. (truffa). Sono penalmente responsabili coloro che, senza essere concorsi nel reato presupposto, nella piena consapevolezza della provenienza illecita o, comunque, accettandone il rischio — purché non desunto da semplici motivi di sospetto, bensì da una situazione fattuale inequivoca — a seguito di proposte di collaborazione in internet, tramite e-mail, contatti in chat o messaggi allocati su pagine web, e la prospettazione di facili guadagni in relazione alla semplice attività richiesta ai cosiddetti "financial manager", pongono all'incasso e successivamente trasferiscono somme di denaro, tutte provenienti da delitti non colposi ».

(23) Cfr. Cass. pen., Sez. II, 17 giugno 2011, n. 25960, in Guida dir., 2011, 44, 76 (s.m.), con nota di Cisterna: secondo la relativa massima, sussiste il delitto di riciclaggio nel caso di ricezione sul proprio conto corrente, e di successivo trasferimento ad altro beneficiario all'estero con il sistema del money transfer, di somme di denaro prelevate fraudolentemente dal conto di un ignaro cliente di banca con il sistema del c.d. phishing. V. anche Uff. Ind. Prel. Milano, 29 ottobre 2008, in Foro ambrosiano, 2008, 406; e in Corr. merito, 2009, 285 ss.; con nota di Agnino. In dottrina, v. gli spunti in Barbieri, I difficili rapporti tra dolo e presupposti della condotta: l'accertamento del dolo nel delitto di riciclaggio, in Cass. pen., 2014, 2520.

(24) Sul punto, v. recentemente Cajani, La tutela penale dell'identità digitale alla luce delle novità introdotte dal d.l. 14 agosto 2013, n. 93 (convertito con modificazioni dalla l. 15 ottobre 2013, n. 119), in Cass. pen., 2014, 1094. Ivi la configurazione del phishing come ipotesi di furto di identità con danno patrimoniale. Ma già Resta, Identità personale e identità digitale, in Dir. inf., 2007, 511 ss.

(25) Trib. Torino, Sez. IV, 28 marzo 2007, cit.

(26) Cass. civ., 11 febbraio 2009, n. 3350, in Dir. giust., 2009.

(27) V. Cajani, ult. cit., spec. § 4 ed ivi ulteriori riferimenti.

(28) Per alcune analogie con la fattispecie concreta decisa nell'annotata sentenza, v. Trib. Palermo, 12 gennaio 2010, cit., sebbene, come visto, il percorso interpretativo utilizzato sia stato diverso, in quanto la responsabilità dell'intermediario veniva fondata sul d.lgs. n. 196/2003.

(29) Per una parziale attinenza con il tema accennato, si ricorda il provvedimento del Garante per la protezione dei dati personali relativo alla vicenda di un correntista di banca on line, il quale, nel consultare in via telematica la propria posizione contabile, aveva accidentalmente avuto la visibilità su informazioni riservate (numeri di conti correnti e carte di credito, operazioni bancarie, bonifici, emolumenti, assegni, titoli, polizze assicurative) di altri ignari correntisti. In tale occasione era emerso che la banca non aveva adottato le misure minime di sicurezza in grado di ridurre il rischio di accesso non autorizzato ai dati personali da parte di terzi: si veda, in tal senso, la Newsletter E-banking e privacy dei clienti N. 196 del 5-11 gennaio 2004, nel sito www.garanteprivacy.it e il relativo rinvio al provvedimento 19 novembre 2003, doc. web. n. 1083182, ibidem, nonché in Bollettino n. 44/novembre 2003. Peraltro, nel caso concreto, pur a fronte di una potenziale violazione della riservatezza, non vi era stato un utilizzo abusivo da parte del terzo, venendo quindi a mancare il profilo del danno economico.

(30) Organo di risoluzione stragiudiziale delle controversie istituito ai sensi dell'art. 128-bis della legge bancaria. Si vedano, al riguardo, Caradonna-Bossi, L'arbitro bancario finanziario quale strumento di gestione delle liti fra gli intermediari finanziari e la propria clientela, in Riv. dott. comm., 2010, 283; Ruperto, L'« Arbitro Bancario Finanziario », in Banca borsa tit. cred., 2010, 325. In giurisprudenza, alcuni incisi sulla natura di detta Autorità giungono da Corte cost., 21 luglio 2011, n. 218, in Guida dir., 2011, 36, 50 (s.m.), con nota di Finocchiaro; e in Foro it., 2011, I, 2906, dove si afferma che l'Arbitro Bancario Finanziario, in considerazione dei criteri e requisiti per la nomina, degli indici di riconoscibilità delle funzioni giurisdizionali, della natura ed efficacia

delle decisioni emesse, non è riconducibile alla nozione di « giudice » o « autorità giudiziaria » e non è pertanto legittimato a sollevare questioni di legittimità costituzionale. Si veda anche, più recentemente, Corti-Trevisan, La responsabilità della banca nelle decisioni dell'Arbitro Bancario Binanziario, in questa Rivista, 2014, 60.
(31) Decisione n. 46 del 15 febbraio 2010, Collegio di Milano, ibidem. Si veda, per un utile panoramica sul tema e sulle decisioni assunte, la Sintesi dell'attività svolta dal citato organismo per l'anno 2010, ibidem.
(32) Decisione n. 1241 del 9 novembre 2010, Collegio di Milano, in www.arbitrobancariofinanziario.it; analogamente la decisione n. 719 del 9 luglio 2010, stesso Collegio, ibidem, che ripartiva l'onere al 50%.
(33) Il Collegio di Coordinamento della citata Autorità ha sancito che anche l'utilizzo di un sistema di sicurezza rafforzato non consente di per sé di affermare la sussistenza di una colpa grave in capo all'utilizzatore: decisione n. 3498 del 26 ottobre 2012, ibidem. Sul piano pratico, ad es., la condanna dell'intermediario è stata sancita anche in caso di rilascio al cliente del sistema di credenziali elettroniche PCR (Personal Card Reader), con lettore e carta a microchip di autenticazione dell'utente, che comporta un accesso al sistema mediante la partecipazione di un essere umano, non sostituibile in via elettronica o informatica: Decisione n. 700 del 4 febbraio 2013, Collegio di Roma; ma v. anche Decisione n. 458 del 22 gennaio 2013, n. 709 del 5 febbraio 2013; Decisione n. 735 del 6 febbraio 2013, Collegio di Napoli. Fa riferimento ai sistemi avanzati definiti come « terzo livello di protezione » (serie numeriche casuali, generate da chiavette o token, digipass, ecc.) la decisione n. 211 del 14 gennaio 2013, Collegio di Roma
(34) Decisione n. 3498 del 26 ottobre 2012, Collegio di Coordinamento, cit., che richiama anche la decisione n. 1111/2010 del Collegio di Roma.
(35) Decisione n. 510 del 28 gennaio 2013, cit., 4-5 ed ivi ulteriori richiami alle pronunce n. 2027/2011 del Collegio di Milano, n. 2610/2011 del Collegio di Napoli e n. 1137/2012 del Collegio di Roma.
(36) Decisione n. 311 del 14 gennaio 2013, Collegio di Napoli, ibidem.
(37) Trib. Verona, 2 ottobre 2012, cit.
(38) Decisione n. 709 del 5 febbraio 2013, Collegio di Roma, in www.arbitrobancariofinanziario.it. Per completezza, va richiamata anche la tecnica di captazione c.d. man in the middle (richiamata per inciso anche nella sentenza del giudice di Milano): al riguardo, per una prima definizione, si veda http://it.wikipedia.org/wiki/Attacco_man_in_the_middle e, in particolare, il seguente passo: « La locuzione man in the middle (traducibile in italiano come “uomo nel mezzo”), in informatica indica un tipo di attacco crittografico, meglio conosciuto come man in the middle attack, MITM o MIM, nel quale l'attaccante è in grado di leggere, inserire o modificare a piacere, messaggi tra due parti comunicanti tra di loro. Caratteristica è il non permettere che nessuna delle due sia in grado di sapere se il collegamento che li unisce reciprocamente sia stato effettivamente compromesso da una terza parte, ovvero appunto un attaccante. L'attaccante così è in grado di osservare, intercettare e replicare verso la destinazione prestabilita il transito dei messaggi tra le due vittime ».
(39) Decisione n. 909 del 10 settembre 2010, Collegio di Milano, ibidem. Fa espresso richiamo agli artt. 33-36 cod. cons. di cui al d.lgs. n. 206/2005 la decisione n. 709 del 5 febbraio 2013, Collegio di Roma.
(40) Decisione n. 211/2013, Collegio di Roma, cit., ibidem.
(41) Decisione n. 4237 del 2 agosto 2013, Collegio di Roma, ibidem; decisione n. 4767 del 18 settembre 2013, Collegio di Milano, ibidem. Le decisioni in materia dell'Organismo citato, per la verità, sono numerosissime e, data l'estensione del presente contributo, ci si permette rinviare, per ulteriori approfondimenti, al sito del medesimo, in www.arbitrobancariofinanziario.it.
(42) Un recente riferimento in tal senso sta nella decisione del Collegio Nord n. 3815 del 18 giugno 2014, ibidem.
(43) Cass. civ., 12 giugno 2007 n. 13777, pure citata in motivazione, che si legge in Banca borsa tit. cred., 2009, II, 21 (s.m.), con nota di Ciraolo, op. cit.; e in Guida dir., 2007, 27, 30 (s.m.), con nota di Micali. Si veda anche Cass. civ., 24 settembre 2009, n. 20543, cit.
(44) Trib. Verona, 2 ottobre 2012, cit.
(45) Su tale figura, v. già Ferri, La diligenza del buon banchiere, in Banca borsa tit. cred., 1958, I, 1; Vitale, Fondamento e limiti della “libertà” del banchiere nel pagamento degli assegni bancari,

ivi, 1959, I, 513; Nigro, La responsabilità della banca per concessione “abusiva” di credito, in Portale (a cura di), Le operazioni bancarie, Milano, 1978, 301 ss., 309, 338; Comporti, Rischio professionale della banca e responsabilità extracontrattuale, in Maccarone-Nigro (a cura di), Funzione bancaria, rischio e responsabilità extracontrattuale, Milano, 1981, 21 ss., 53; Molle;La banca nell'ordinamento giuridico italiano, II ed., Milano, 1987, 33 ss. Ma anche Clarizia, Sulla responsabilità del banchiere, in Riv. dir. civ., 1976, II, 436 ss.
(46) Cfr. Scognamiglio, Sulla responsabilità dell'impresa bancaria per violazione di obblighi discendenti dal proprio status, in Giur. it., 1995, I, 1, 356; Id., Ancora sulla responsabilità della banca per violazione di obblighi discendenti dal proprio status, in Banca borsa tit. cred., 1997, II, 655; Marzona, Lo status (professionalità e responsabilità) della banca in una recente sentenza della Cassazione, ivi, 1994, II, 266. In giurisprudenza, v. Cass. civ., 13 gennaio 1993, n. 343, in Giur.it., 1993, I, 2129; Cass. civ., 8 gennaio 1997, n. 72, in Banca borsa tit. cred., 1997, II, 653.
(47) Se ne fa cenno nel nostro, Home banking, bonifici non autorizzati e responsabilità della banca, cit.
(48) Ferri, La diligenza del buon banchiere, cit., 1. Ma v. anche De Cupis, Il danno. Teoria generale della responsabilità civile, I, Milano, 1966, 124, dove si individua la colpa del debitore nel « non uso, da parte di questo, della diligenza che, a norma dell'art. 1176 c.c., è a suo carico ».
(49) V., fra le altre, Cass. civ., 24 settembre 2009, n. 20543, cit.; e Cass. civ., 12 giugno 2007 n. 13777, già richiamate in premessa, nonché Cass. civ., 28 luglio 2000, n. 9902, in Giust. civ., 2001, I, 1320. Ma v. anche, Cass. civ., 15 aprile 1992, n. 4571, in Giur. it., 1994, I, 1089, con nostra nota Sottrazione di titoli di credito al portatore e responsabilità della banca per incauta negoziazione.
(50) Da ultimo, v. Cass. civ., 18 marzo 2010, n. 6624, in Giust. civ. Mass., 2010, 3, 397, che preferisce richiamarsi a canoni di diligenza media.
(51) Cass. civ., 7 luglio 1982, n. 4043, in Foro it., 1982, I, 2843; Trib. Bologna, 25 febbraio 1980, in Banca borsa tit. cred., 1980, II, 244 ss.; Trib. Napoli, 22 dicembre 1969, ivi, 1970, II, 606 ss. Per una sintesi di questo dibattito, v. anche il nostro, Sottrazione di titoli di credito al portatore e responsabilità della banca per incauta negoziazione, cit. ed ivi ulteriori riferimenti alla posizione minoritaria nelle note 5-7.
(52) In tal senso, Cass. civ., 11 gennaio 1951, n. 49, in Rep. Foro it., voce Deposito, n. 6. Più recentemente, Trib. Milano, 3 ottobre 1988, in Banca borsa tit. cred., 1990, II, 645.
(53) Peculiare la prospettazione offerta da Trib. Siracusa, 15 marzo 2012, cit., in cui si cerca di coordinare il canone di diligenza professionale del banchiere, per le obbligazioni discendenti dal contratto di home banking, con una responsabilità di tipo aquiliano da trattamento dei dati, ai sensi del disposto combinato ex art. 15, d.lgs. n. 196/2003-art. 2050 c.c. Si ricorda anche Giud. Pace Milano, Sez. IV civ., 7 gennaio 2011, n. 41, cit., secondo cui il servizio di home banking non potrebbe costituire attività pericolosa nel senso inteso dall'art. 2050 c.c. in quanto i rischi cui sono esposti i clienti in relazione alle azioni di malviventi non derivano direttamente dall'attività propria della banca, ma quest'ultima costituisce soltanto l'occasione per tali evenienze.
(54) V. sopra, decisione n. 3498 del 26 ottobre 2012, Collegio di Coordinamento; e decisione n. 1111/2010, Collegio di Roma
(55) In termini generali, data la sede, sia consentito restringere la citazione a Betti, Teoria generale delle obbligazioni, Milano, 1953-1954, 150 ss.; Scognamiglio, Rischio e impresa, in Riv. dir. comm., 1967, I, 417 ss.; Trimarchi, Rischio e responsabilità oggettiva, Milano, 1961, 34 ss. Ma v. Rodotà, Il problema della responsabilità civile, Milano, 1964, passim, spec. 176 ss.
(56) Con specifico riguardo alla trattazione del rischio di impresa in ambito bancario v. già Vivante, Trattato di diritto commerciale, V ed., Milano, III, 1916, 145. Ma anche Ascarelli, Pagamento di assegni falsi e diligenza del traente, in Banca borsa. tit. cred., 1954, II, 170; De Semo, Diritto cambiario, Padova, 1963, 689; Di Lauro, Colpa, rischio e responsabilità obiettiva di impresa bancaria, in Banca borsa. tit. cred., 1968, II, 606; Graziani;Manuale di diritto commerciale, Napoli, 1955, 301; Gualtieri, Titoli di credito, Torino, 1953, 311; Lo Giudice, Responsabilità della banca nel pagamento di assegni con sottoscrizione falsa, in Aa.Vv., Responsabilità contrattuale ed extracontrattuale delle banche, Milano, 1986, 235; Molfese, Pagamento di assegno alterato - Responsabilità - Rischio professionale, in Foro pad., 1982, I, 278; Mossa, Lo chèque e l'assegno circolare, Milano, 1939, 227; Paolucci, Il pagamento dell'assegno con sottoscrizione falsa e i suoi effetti, in Aa.Vv., Responsabilità contrattuale ed extracontrattuale

delle banche, cit., 311. v. anche Benatti, Le clausole di esonero da responsabilità nella prassi bancaria, in Portale (a cura di), Le operazioni bancarie, Milano, 1978, 137; Nigro, Statuti delle banche e clausole limitatrici della responsabilità, in Maccarone-Nigro (a cura di), Funzione bancaria, rischio e responsabilità extracontrattuale, cit., 117; Vitale, Funzione bancaria e responsabilità contrattuale della banca, ivi, 3.

(57) In termini generali sulla responsabilità oggettiva e senza pretesa di completezza, si vedano, per tutti, Alpa, Responsabilità civile e danno, Bologna, 1991; Id., Responsabilità oggettiva, in Contr. impr., 2005, 959 ss.; Castronovo, Responsabilità oggettiva. II. Disciplina privatistica - dir. comp. e stran., in Enc. giur., XXVII, Roma, 1991, 2 ss.; Rodotà, Modelli e funzioni della responsabilità civile, in Riv. crit. dir. priv., 1984, 595 ss.; Scognamiglio, Responsabilità per colpa e responsabilità oggettiva, in Studi in Onore di Andrea Torrente, Milano, 1968, 1113 ss.; Trimarchi, Rischio e responsabilità oggettiva, cit. passim. Ma già Coviello, La Responsabilità senza colpa, in Riv. it. sc. giur., 1897, 188 ss. Più recentemente, Tramontano-Rossi-Bordon (a cura di), La nuova responsabilità civile. Causalità. Responsabilità oggettiva. Lavoro. Torino, 2010; ed iviRossi, Colpa presunta e responsabilità oggettiva. I due volti della responsabilità civile, 411 ss., 427; Ziviz, Responsabilità oggettiva, in Cendon (a cura di), La colpa nella responsabilità civile, Torino, III, 2006, 149 ss.

(58) V. già Cass. civ., 7 ottobre 1958, n. 3133, in Banca borsa tit. cred., 1959, II, 299, in tema di pagamento di assegni non trasferibili. Più recentemente, Cass. civ., 10 novembre 2010, n. 22816, in Giust. civ., 2011, 1782; Cass. civ., 31 marzo 2010, n. 7949, ivi, 2010, 1874. V. anche Sez. Un. civ., 26 giugno 2007, n. 14712, in Corr. giur., 2007, 1706, con nota di Di Majo, Contratto e torto: la responsabilità per il pagamento di assegni non trasferibili; in Giur. it., 2008, I, 1150, con nota di Cottino, Dalle Sezioni unite alle Sezioni semplici: precisazioni (e dubbi) in tema di responsabilità per il pagamento di assegno bancario (trasferibile e non) a soggetto non legittimato ad esigerlo; in Danno resp., 2008, 160, con nota di Benedetti, Assegno non trasferibile, banca girataria e contatto sociale: responsabilità contrattuale?; in Nuova giur. civ. comm., 2007, 1443, con nota di Leggieri, Natura della responsabilità della banca negoziatrice per il pagamento di assegni non trasferibili a persone diverse dal prenditore. Si esprime in senso contrario Trib. Napoli, 10 giugno 1997, in Banca borsa tit. cred., 1999, II, 238, secondo cui la responsabilità della banca per il pagamento di assegni alterati a soggetti non legittimati non può valicare i limiti della colpa e sconfinare sul terreno della responsabilità oggettiva. In dottrina, contro la prospettazione di una responsabilità oggettiva nella negoziazione di assegni, v., fra gli altri, Pellizzi, La responsabilità della banca, in Aa.Vv., Responsabilità contrattuale ed extracontrattuale delle banche, Milano, 1986, 11 ss., 24; e, in prospettiva più ampia, De Marinis, Rischio professionale e responsabilità extracontrattuale della banca, ivi, 147 ss., 151, in particolare sostenendo l'insussistenza, nei sistemi di civil law, del principio « cuius commoda eius et incommoda ».

(59) Cass. civ., 19 luglio 2012, n. 12448, in Giust. civ., 2012, 2297, la cui motivazione si esprime nei seguenti termini testuali: « A norma dell'art. 2049, la società di intermediazione è responsabile degli illeciti commessi dal promotore finanziario anche a titolo oggettivo, cioè indipendentemente da comportamenti negligenti o colposi suoi propri, in relazione ai danni che l'investitore possa avere subito per avere fatto affidamento sull'esistenza del rapporto di preposizione ». Recentemente, si veda anche quanto riportato in Cass. civ., 15 maggio 2014, n. 10645, in questa Rivista, 2015, 1917. Più cauta, sull'ipotesi di una responsabilità oggettiva nella fattispecie in esame, è invece Cass. civ., 25 gennaio 2011 n. 1741, in Giust. civ., 2011, I, 332; in Corr. giur., 2011, 1589, con nota di Guerinoni, Illecito del promotore e responsabilità dell'intermediario e concorso di colpa dell'investitore?; in Giur. it., 2011, 2575, con nota di D'Auria, Ancora sul nesso di occasionalità necessaria negli illeciti dei promotori finanziari: profili problematici; in Danno resp., 2011, 727, con nota di Bartolini, L'occasionalità necessaria non tramonta mai: una conferma sulla responsabilità della Sim per gli illeciti del promotore; in questa Rivista., 2011, 1770, con nota di Greco, Illecito del promotore e responsabilità della Sim: fine di un percorso ad ostacoli?). Sul tema, v. ampliusNardi, La responsabilità dell'intermediario per l'illecito del promotore finanziario, in questa Rivista, 2010, 371; Barcellona, Mercato mobiliare e tutela del risparmio, Milano, 2009; Lamorgese, Considerazioni sparse sulla responsabilità degli intermediari finanziari nella giurisprudenza, in Giust. civ., 2009, II, 17; Luminoso, Contratti di investimento, mala gestio dell'intermediario e rimedi esperibili dal risparmiatore, in questa Rivista, 2007, 1422 ss.

(60) Per una sintesi delle contrapposte visioni sul punto, si vedano Rodotà, Il problema della

responsabilità civile, cit., passim; e De Cupis, Il danno. Teoria generale della responsabilità civile, I, cit., spec. 119 ss. In particolare, Rodotà muove una critica al tradizionale condizionamento della responsabilità al principio della colpa, evidenziando come detto tratto paia affetto da eccessivo individualismo e da una concezione statica degli interessi patrimoniali (op. cit., 20). De Cupis, di contro, evidenzia come il far carico, in assenza di colpa, dell'obbligo risarcitorio si traduca nello « spostare la bilancia della giustizia a favore del danneggiato, senza che suffraghi riprovazione morale dell'autore del danno », ammonendo sul rischio di dilatazione oltre misura dell'istituto della responsabilità civile (op. cit., 144, 146).

(61) Al riguardo, si veda Trib. Siracusa, 15 marzo 2012, cit. Spunti anche in Catalano, Lotta al phishing,cit. Sul tema v. Cajani-Costabile-Mazzaraco, Phishing e furto d'identità digitale, cit.

(62) Il tema può essere qui solo accennato. In letteratura, fra i contributi più recenti e autorevoli, ci si limiterà qui a richiamare gli studi di Mazzamuto, Il danno non patrimoniale contrattuale, in Europa dir. priv., 2012, 437; Nivarra, La contrattualizzazione del danno non patrimoniale: un'incompiuta, ivi, 2012, 475; Messinetti, Considerazioni sul danno non patrimoniale da inadempimento contrattuale, in Riv. dir. civ., 2012, I, 333. Ma v. anche Ziviz, I danni non patrimoniali, Torino, 2012, 425 ss. In giurisprudenza, fra i riferimenti più recenti che ammettono il risarcimento del danno non patrimoniale in caso di inadempimento contrattuale, Cass. civ., 24 ottobre 2011, n. 21999, in Giust. civ. Mass., 2011, 10, 1502. Ma, in precedenza, v., fra le c.d. « sentenze gemelle » del 2008, Sez. Un. civ., 11 novembre 2008, n. 26972, in questa Rivista, 2009, 38 ss., con note di Monateri, Il pregiudizio esistenziale come voce del danno non patrimoniale (56 ss.); Navarretta, Il valore della persona nei diritti inviolabili e la complessità dei danni non patrimoniali (63 ss.); Poletti, La dualità del sistema risarcitorio e l'unicità della categoria dei danni non patrimoniali (76 ss.); Ziviz, Il danno non patrimoniale: istruzioni per l'uso (94 ss.)

(63) V., ad es., Carnesecchi, Quei ladri di bancomat e carte di credito furto e indebito utilizzo: questo il catalogo, in Dir. giust., 2006, 48, annotando (criticamente) Cass. pen., Sez. V, 8 giugno 2006, n. 25870, la quale aveva ravvisato nel furto del bancomat e dei relativi codici di accesso un fatto di particolare tenuità, tale da rendere applicabili le attenuanti generiche. In quest'ottica, la nota offre una rassegna di potenziali disagi (onere della denuncia, mancanza di mezzi finanziari, ecc.) in cui potrebbe venire a trovarsi la vittima della frode. Per un riferimento al possibile danno esistenziale da truffe on line, cfr. Sargenti, Giurisdizione e competenza territoriale in materia penale, in Giur. merito, 2012, 2641 ss.

(64) Per limitarci ad un recente studio pubblicato sulle pagine di questa Rivista, v. al riguardo Martini Barzolai, I presupposti per il risarcimento del danno esistenziale da inadempimento, ivi, 956 ss., annotando Trib. Tivoli, 14 marzo 2012, ibidem, 954 (ed ivi ulteriori riferimenti).

(65) Fra le altre, v. la stessa Sez. Un. civ., 11 novembre 2008, n. 26972, poc'anzi citata.