Quaderni di Diritto Mercato Tecnologia

Rivista Scientifica

ISSN (Online edition): 2239-7442

QUADERNI DI

diritto mercato tecnologia

Numero 2
Anno V
Aprile/Giugno 2015

CON CONTRIBUTI DI:

Fabrizio Calisai, Francesca Corrado, Claudio Ghidini,
Gaetano Marino, Giovanni Maria Nori, Rosaria Petti

Diritto Mercato Tecnologia
N.2-2015

Il Phishing: profili civilistici ed evoluzione delle forme di tutela alla luce delle decisioni dell'Arbitro Bancario Finanziario

di
Fabrizio Calisai

Abstract:
Il *Phishing* consiste in una frode informatica volta all'appropriazione di credenziali utilizzate per servizi di *home banking*. In certi casi, la banca è responsabile per le perdite subite dal cliente e deve restituire le somme perdute. Si analizzano le decisioni dell'Arbitro Bancario Finanziario inerenti alla diligenza della banca e alla colpa dei clienti. È interessante osservare come le forme di tutela per i clienti si evolvono insieme alle tecniche utilizzate per i *phishing attacks*.

Phishing consists in computer fraud intended to acquire references used in home banking services. In certain cases, the bank is liable for capital losses suffered by the clients and has to refund the lost sums. We analyse the determinations of ABF concerning about the diligence of the bank and the fault of the clients. It is interesting to observe how the forms of protection of the clients develop concurrently with tecniques used in phishing attacks.

1. Inquadramento del fenomeno Phishing.

In prima approssimazione, il *Phishing* [1] può essere definito come quel peculiare atteggiarsi della fattispecie frode informatica, volta all'acquisizione abusiva delle credenziali di utilizzo relative a *home banking* e carte prepagate. Si fa riferimento a tutti i comportamenti perpetrati attraverso il c.d. furto delle identità telematiche, consistente nell'appropriazione fraudolenta di codici (*user id* e *passwords*) identificativi di un dato soggetto, ovvero delle credenziali

che lo stesso soggetto utilizza in ambito internet, allo scopo di conseguirne determinate illecite utilità.
In sostanza, l'obiettivo dei *phishing attacks* è quello di indurre (ovviamente con l'inganno) l'utente a fornire dati o informazioni personali, riguardanti principalmente le credenziali di autenticazione valide per accedere ad aree informatiche esclusive o a servizi bancari e/o finanziari on-line, i numeri di carte di credito o di pagamento, di conto corrente, gli identificativi per l'abilitazione all'accesso a siti di vario genere, gli *user id* e le *passwords* di accesso alla gestione on-line dei conti correnti, il numero o gli estremi della carta di identità o della patente di guida.
Il *phisher* utilizza i dati in tal modo ottenuti per conseguire l'abilitazione all'accesso a determinati servizi on-line, assumendo virtualmente l'identità del legittimo titolare o utente vittima dell'attacco.
Tale attività viene per lo più posta in essere attraverso l'invio di e-mail, apparentemente provenienti da enti o istituzioni reali, (es. l'istituto di credito con cui il soggetto destinatario della mail fraudolenta intrattiene rapporti di conto corrente) contenenti messaggi diretti a indurre l'utente a connettersi a una pagina web non autentica, ma molto simile a quella delle suddette istituzioni, e a inserire nei *form* predisposti dal *phisher* i dati funzionali all'accesso ad aree informatiche riservate o a servizi on-line [2].
Il *Phishing*, in tutte le sue declinazioni, rappresenta chiaramente una fattispecie penalmente rilevante che può essere ricondotta nell'alveo della truffa, ma non solo [3].
Per questo, al fenomeno si sono interessate, in prevalenza, dottrina [4] e giurisprudenza [5] dell'ambito penalistico.
A ogni modo, oltre ai manifesti profili criminosi connessi alla fattispecie *Phishing* e in particolare alla individuazione (spesso assai difficoltosa se non impossibile) dei soggetti colpevoli, emerge una differente prospettiva di analisi, connessa all'aspetto forse più rilevante per la vittima dei *phishing attacks*, ovvero, alla possibilità di recuperare, in tutto o in parte, le somme di denaro eventualmente perdute ricevendo così una tutela più concreta.
In questo senso, il sistema di tutela stragiudiziale offerto dall'Arbitro Bancario Finanziario (di seguito ABF) appronta delle possibili soluzioni per dei precisi interrogativi: i) quali potrebbero essere le forme di tutela riservate al cliente dell'intermediario e fornitore del sistema di *home banking* che è stato vittima di *phishing attack* e che, in conseguenza di ciò, ha subito delle perdite e si è visto sottrarre in modo illegittimo delle somme di denaro dal proprio conto corrente? ii) Il cliente può recuperare le somme perdute? iii) Si possono individuare profili di responsabilità in capo all'intermediario in caso di *phishing attack* subito dal cliente?

Si cercherà, quindi, di offrire una panoramica esaustiva degli orientamenti dell'ABF in materia di *Phishing* e di analizzare il sistema di tutela approntato in favore del cliente che abbia "abboccato" all'amo dei *phishers*, alla luce delle più recenti e significative decisioni.

2. Il substrato normativo di riferimento per le decisioni ABF: dalla banca "irresponsabile" alla banca "potenzialmente responsabile".

In prima battuta, appare utile dedicare un cenno al panorama normativo di riferimento in materia di servizi di pagamento e *home banking* e, in generale, ricostruire la cornice all'interno della quale l'ABF orienta le proprie decisioni in materia di frodi informatiche.
Infatti, proprio la recente introduzione di importanti innovazioni normative, unita alla particolare interpretazione orientata di alcune specie di clausole inserite nei contratti tra intermediario e cliente, hanno consentito di aggirare alcuni limiti ontologici e di approntare una tutela più incisiva, arrivando a configurare, in determinati casi, una responsabilità dell'intermediario nei confronti del cliente vittima di *phishing attack*.
Il primo limite alla configurazione di un'efficace tutela per il cliente era di natura sistematica e scaturiva dall'assenza di una normativa *ad hoc* dedicata alla regolamentazione e alla disciplina dei sistemi di pagamento e, in particolare, delle operazioni di *home banking* effettuate tramite l'utilizzo di apposite credenziali fornite al cliente dall'intermediario.
In questo senso, la prima paralizzante eccezione che l'intermediario poteva sollevare di fronte alla denuncia di un cliente vittima di un *phishing attack* era quella basata sulla regolarità dell'utilizzo delle credenziali nelle operazioni on-line contestate: sostanzialmente, nel momento in cui le credenziali fornite (*user id e password*) venivano inserite correttamente nel sistema (non importa da chi), l'intermediario tendeva a considerarsi esente da responsabilità, responsabilità che ricadeva interamente sul cliente per omessa diligente custodia dei dati relativi all'*home banking*.
Questo limite è venuto meno a seguito del recepimento della dir. 200/64/CE del 13 novembre 2007, art. 59, c. 2, la quale ha introdotto degli importanti principi generali in materia di servizi di pagamento nel mercato interno, successivamente trasfusi nel corpo del d.lgs. n. 11/2010, art. 10, c. 1 e 2.
Sulla base delle disposizione citate, «*Qualora l'utilizzatore di servizi di pagamento neghi di avere autorizzato un'operazione di pagamento già eseguita (...) è onere del prestatore di servizi di pagamento provare che l'operazione di pagamento è stata autenticata, correttamente registrata e contabilizzata e che non ha subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o altri inconvenienti*».

Ancora: «*Quando l'utilizzatore di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento eseguita, l'utilizzo di uno strumento di pagamento registrato dal prestatore di servizi di pagamento non è di per sé necessariamente sufficiente a dimostrare che l'operazione sia stata autorizzata dall'utilizzatore medesimo, né che questi abbia agito in modo fraudolento o non abbia adempiuto con dolo o colpa grave a uno o più degli obblighi di cui all'articolo 7*» [6].
In forza delle disposizioni citate, è attualmente onere dell'intermediario dimostrare, da un lato, la legittimità dell'operazione on-line non autorizzata, dall'altro, la violazione, da parte del cliente, degli obblighi scaturenti dal contratto [7].
Il testo normativo in analisi contribuisce a creare una precisa cornice di obblighi in capo all'intermediario [8] e al cliente [9] in materia di strumenti di pagamento, e pone in capo al primo l'obbligo di rimborsare il cliente che abbia subito delle perdite in conseguenza di operazioni non autorizzate e/o fraudolente [10].
Profili di responsabilità in capo al cliente si configurano in modo pieno nell'ipotesi in cui lo stesso abbia agito con intenti fraudolenti, o abbia omesso, per dolo o colpa grave, di adempiere agli obblighi derivanti dal contratto sottoscritto con il prestatore dei servizi.
In tutti gli altri casi, comprese le omissioni derivanti da colpa lieve, il cliente va incontro a una responsabilità limitata e sopporta le perdite subite per un importo massimo di 150 Euro [11].
Con tutta evidenza, si assiste a un'alterazione normativa dei profili di responsabilità tra i soggetti coinvolti: si passa da una banca "irresponsabile" e "insensibile" di fronte alle pretese del cliente, a una banca "potenzialmente responsabile", tenuta, in determinate ipotesi, a rimborsare il cliente e a tenerlo indenne dalle perdite subite.
Come meglio si vedrà nel successivo punto 3, il fulcro della tutela giuridica approntata in favore del cliente è rappresentato, soprattutto in una prima fase, da questa traslazione del rischio in capo alla banca.
Il secondo limite ontologico alla tutela del cliente vittima di *Phishing* aveva natura contrattuale ed era basato sulla presenza di alcune clausole inserite nel contratto sottoscritto dal cliente stesso [12], volte a limitare la responsabilità dell'intermediario nell'ipotesi di profili patologici legati all'*home banking*.
Recentemente, però, tali clausole sono state ritenute inidonee a determinare l'irresponsabilità dell'intermediario: infatti, in considerazione del loro contenuto, tali previsioni negoziali sono state considerate alla stregua di clausole vessatorie, ai sensi dell'art. 33, c. 2, lett. b), d.lgs. n. 206/2005 (c.d. Codice del Consumo) [13].
In conseguenza di ciò, dette clausole, quand'anche fossero inserite all'interno

del regolamento contrattuale, sarebbero inopponibili al cliente-consumatore [14].
Infine, a completamento della ricostruzione del panorama normativo di riferimento, appare utile ricordare che la raccolta e la gestione dei dati forniti dai clienti dell'intermediario è regolamentata dalle disposizioni del d.lgs. n. 196/2003 (Codice Privacy) [15].
In forza di tali disposizioni, il gestore dei conti correnti on-line è tenuto a predisporre misure evolute per cautelarsi dal rischio di accessi non consentiti e non autorizzati.
In particolare, tale custodia e tale controllo devono essere commisurati alle conoscenze acquisite in base all'evoluzione del progresso tecnico, oltre che al tipo di trattamento effettuato, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.
La responsabilità del gestore che contravviene alle disposizioni del d.lgs. n. 196/2003 (in particolare artt. 15 e 31), è quella tratteggiata dall'art. 2050 c.c., che deriva dallo svolgimento di attività pericolose: una fattispecie di responsabilità oggettiva dal quale l'intermediario si libera solamente provando di avere adottato tutte le misure idonee a evitare il danno [16].
Il gestore dei dati ha quindi l'onere di provare di avere posto in essere tutte le necessarie precauzioni, valutate anche con riferimento all'attuale progresso tecnologico, per evitare la perdita dei dati informatici, nonché il loro fraudolento utilizzo da parte di terzi che illegittimamente hanno fatto irruzione nel sistema informatico.
Nel caso in cui l'intermediario non riuscisse ad adempiere all'onere probatorio di cui sopra, sarebbe responsabile per le perdite subite dal cliente in conseguenza del *phishing attack*.
Un eventuale comportamento contrassegnato da colpa grave ascrivibile al cliente, su cui grava l'obbligo di custodire con diligenza le chiavi di accesso al sistema di *home banking,* potrebbe mitigare la responsabilità dell'intermediario, fino a integrare un'ipotesi di concorso di colpa.

3. Architettura delle decisioni dell'ABF ed evoluzione delle forme di tutela per il cliente: diligenza della banca e sistemi di sicurezza statici.

Ricostruito il substrato normativo di riferimento, fondamenta su cui poggiano le decisioni dell'ABF, si possono analizzare le forme di tutela approntate per il cliente, nonché le *rationes* sottese alle stesse.
Aspetto peculiare di tali forme di tutela è rappresentato dalla loro evoluzione e adattamento ai sistemi di sicurezza offerti dall'intermediario al cliente che

opera tramite *home banking*, ma anche ai sempre nuovi sistemi adoperati dai *phishers* per perpetrare le frodi informatiche.
Come osservato in precedenza, l'introduzione della normativa citata (d.lgs. n. 11/2010) è stata determinante per la costruzione di un sistema di responsabilità in capo all'intermediario in relazione alle perdite subite dal cliente e derivanti da frodi informatiche e transazioni non autorizzate.
Tale sistema è strutturato sul criterio del c.d. «rischio di impresa»: si tende a traslare il rischio contrattuale [17] derivante dall'utilizzo fraudolento degli strumenti di pagamento sulla banca, in quanto soggetto più adatto a sopportarlo dal punto di vista giuridico, ma soprattutto economico [18].
Si crea così una sorta di squilibrio controllato in cui la posizione della banca appare deteriore rispetto a quella del cliente, che, esclusi i casi di colpa grave [19], dolo e intenti fraudolenti, non sopporta il peso delle perdite subite, o lo sopporta in minima parte [20].
L'individuazione di un profilo di responsabilità in capo alla banca nelle ipotesi di frode informatica all'attenzione dell'ABF nasce da una sorta di bilanciamento che coinvolge le condotte dei soggetti interessati: da un lato si indaga circa la sussistenza di colpa grave in capo al cliente, che deve comunque custodire con la dovuta diligenza le proprie credenziali, evitando di renderle facilmente accessibili a soggetti esterni; dall'altro, si punta la lente sul contegno dell'intermediario, al quale viene richiesta una diligenza specifica, professionale, [21] che rientra nell'alveo dell'art. 1176, c. 2 c.c. [22] [23].
Per esemplificare, in caso di rapporti di conto corrente la banca ha l'obbligo di «*conservare*» le somme depositate e di custodirle con la «*particolare correttezza e diligenza che grava sulla stessa nell'esecuzione dei contratti con i clienti*» [24], «*per poterle eventualmente restituire al depositante e/o utilizzarle per compiere le operazioni che egli eventualmente richieda, nel rispetto degli obblighi di correttezza e buona fede riconducibili alla figura del mandatario (art. 1856 c.c.)*». [25]. «*Il parametro di valutazione dell'«accorto banchiere» è destinato a valere anche con specifico riferimento ai servizi di home banking*» [26].
Sull'intermediario incombe altresì l'onere di dimostrare l'esistenza di un comportamento gravemente colposo in capo al cliente, al fine di liberarsi dalla responsabilità [27].
In prima battuta, si tende a considerare non diligente il comportamento dell'intermediario che abbia omesso di adottare tutti i migliori accorgimenti della tecnica volti a scongiurare il rischio di impiego fraudolento degli strumenti di pagamento.
Assume particolare rilievo, sul piano applicativo, «*l'individuazione degli adempimenti di protezione dovuti dall'intermediario al fine di garantire la sicurezza del sistema di pagamento e delle relative procedure*» [28].

In particolare, non è ritenuta sufficiente l'adozione, da parte dell'intermediario, di misure di sicurezza di primo livello, espressione di un sistema di protezione a un solo fattore che consiste nella fornitura di credenziali con *password* fissa (uno *user id* e una *password* che non cambia mai) [29].
Di fronte a tali sistemi di sicurezza insufficienti si tende a proteggere il cliente, nonostante le tecniche del *phishing*, per poter funzionare, richiedano evidentemente la collaborazione (seppure inconsapevole) del cliente stesso, che deve riscontrare la mail fraudolenta inserendo le proprie credenziali.
In determinate circostanze, il cliente che risponde alla mail fraudolenta può essere comunque considerato esente da colpa, come nel caso in cui la suddetta mail sia del tutto simile a un'altra, precedente e autentica, inviata poco tempo prima al cliente dall'intermediario [30].
Ancora, anche la poca notorietà o la non conoscenza, almeno in origine, del fenomeno *phishing,* può essere una circostanza attenuante, valida a escludere la colpa del cliente [31].
Ovviamente, la situazione appare differente in caso di cliente recidivo, più volte vittima dello stesso sistema fraudolento: in simili ipotesi, sarebbe difficile non considerare il comportamento del cliente come gravemente colposo [32].
Ancora, il contegno del cliente può assumere connotati colposi (o gravemente colposi) nei casi in cui lo stesso abbia dato riscontro alla mail fraudolenta, inserendo così le credenziali, pur avendo avuto il sospetto circa la falsità di tale e-mail [33].
A riguardo, è frequente nella casistica la frode perpetrata promettendo al cliente vantaggi economici o addirittura accrediti, invitandolo, con false e-mail spedite per conto dell'intermediario, a inserire i propri dati [34].
La colpa grave del cliente si manifesta in modo evidente nell'ipotesi in cui la e-mail ricevuta appaia manifestamente fraudolenta e pur «*rivestendo le caratteristiche formali riconducibili all'intermediario*», sia «*redatta in un italiano approssimativo, con errori lessicali e una terminologia che avrebbero dovuto mettere in guardia il cliente*» [35].
In ogni caso, anche nelle ipotesi di manifesta colpa del cliente per omessa diligente custodia delle credenziali, in alcuni casi, l'ABF non giunge a configurare una responsabilità piena in capo allo stesso, ma opta per una linea basata sul concorso di colpa [36] con l'intermediario, al quale si contesta in più occasioni una responsabilità concorrente [37], derivante dalla mancata adozione di strumenti tecnici di protezione evoluti, soprattutto se già disponibili e fruibili [38].

3.1. Diligenza della banca e sistemi di autenticazione "a due fattori".

Il sistema di bilanciamento di responsabilità nelle decisioni dell'ABF muta

leggermente a seguito dell'adozione, da parte dell'intermediario, di strumenti di sicurezza più evoluti e affidabili, definibili come sistemi a "due fattori".
Tali sistemi consentono di superare l'ormai obsoleto e poco sicuro metodo della *password* fissa e prevedono l'utilizzo di strumenti quali (ulteriori) *password* dispositive di accesso, firme digitali, chiavette elettroniche personalizzate che generano *password* dinamiche diverse ogni 30 secondi (es. sistema *Token* o *OTP – one time password*) e infine l'utilizzo del cellulare del cliente che viene associato alla carta di pagamento o al numero di conto: in questo modo l'utente inserisce le credenziali per accedere al sistema dell'*home banking*, ma per operare deve utilizzare una ulteriore *password* "usa e getta", valida per un breve lasso di tempo, che gli viene comunicata istantaneamente dall'intermediario via sms [39].
Se il cliente non compie l'operazione entro una determinata finestra temporale, deve richiedere e ottenere una nuova e diversa *password*.
Una volta che il nuovo e più evoluto sistema di sicurezza è stato messo a disposizione del cliente tramite un'offerta personalizzata e individuale e non tramite una generica promozione destinata a tutta la clientela, come accade per la prassi dei messaggi *inbox* [40], si configura una nuova ulteriore traslazione del rischio derivante dall'utilizzo fraudolento dei sistemi di pagamento informatici: la responsabilità si sposta in capo al cliente, su cui grava il rischio derivante dall'utilizzo, dalla conservazione e dalla protezione di credenziali ormai considerate sicure e difficilmente intercettabili da soggetti esterni [41].
Si configura una responsabilità in capo al cliente anche nelle ipotesi in cui lo stesso abbia volontariamente scelto di non avvalersi dei sistemi di sicurezza evoluti anche a fronte di una precisa e specifica offerta individuale a lui rivolta dall'intermediario [42].
In linea di massima, a seguito dell'introduzione dei sistemi di sicurezza "a due fattori", considerati, «*allo stato attuale dell'arte tecnologica*» [43], come il metodo più sicuro per la sicurezza dei sistemi informatici di pagamento, in caso di accesso illegittimo e di utilizzo fraudolento delle credenziali, la responsabilità non può che ricadere sul cliente.
In particolare, in alcune pronunce, l'invulnerabilità del sistema a due fattori si considera addirittura idonea a fondare una presunzione di colpa grave in capo al cliente, al quale automaticamente, in caso di violazione del sistema, viene contestata l'omessa diligente custodia delle credenziali di accesso [44].
Non mancano, comunque, decisioni dell'ABF che, pur considerando il sistema di sicurezza a due fattori come sicuro e affidabile, non arrivano ad accogliere la ricostruzione, forse eccessivamente rigida, della automatica presunzione di colpa grave in capo al cliente discendente dall'utilizzo dei sistemi di sicurezza evoluti adottata dal Collegio milanese [45].

In particolare, si afferma che, per quanto il sistema di sicurezza a due fattori sia senz'altro caratterizzato da una spiccata capacità protettiva (nella fattispecie sistema OTP), tale assunto non sia comunque valido a fondare una irreversibile presunzione di negligenza in capo al cliente in caso di violazioni e intrusioni in detto sistema, bensì (solamente) a indurre una valutazione più rigorosa del contegno del cliente stesso [46].
Ancora, in talune ipotesi, l'incidenza quantitativa e temporale di frodi informatiche perpetrate in danno di più clienti dello stesso intermediario è stata ritenuta circostanza valida a fondare una responsabilità in capo a quest'ultimo, nonostante l'adozione di sistemi di sicurezza evoluti [47].

3.2. Diligenza della banca e nuove tipologie di *Phishing attacks*.

La prospettiva muta ancora nel momento in cui si entra in quella che si può definire come "terza fase" dell'evoluzione della tutela approntata per il cliente vittima di *phishing attack*.
In questo caso si assiste a un «*progressivo spostamento del metro valutativo nella direzione di una più ampia ed efficace protezione del cliente*», giustificata «*alla luce della parallela evoluzione dei metodi di aggressione informatica*» [48].
Le forme di tutela devono quindi adattarsi al progresso tecnologico e non possono cristallizzarsi, al fine di proteggere il cliente da artifizi fraudolenti tali da trarre in inganno anche utenti – se si accetta il gioco di parole - più "navigati".
Un caso emblematico di *phishing attack* di nuova generazione è dato dall'utilizzo di *software* malevoli (*malware*), difficilmente individuabili e neutralizzabili anche dai più evoluti ed efficienti sistemi antivirus.
La tecnica, definita *man-in-the-browser* [49], rappresenta 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*» [50].
Tale sistema è capace di generare pagine web fraudolente, del tutto identiche a quelle in cui, normalmente, l'utente effettua l'accesso per il compimento delle operazioni di *home banking*.
Evidente, quindi, la differenza sostanziale rispetto alle tecniche di *Phishing* più note e ormai obsolete, a seguito delle quali il cliente cadeva vittima di una «*colpevole credulità*» [51].
Di fronte alle nuove tecniche di *phishing attack*, si assiste così a un'ulteriore traslazione del rischio, che torna in capo all'intermediario, su cui grava l'obbligo di predisporre opportuni accorgimenti volti a scongiurare violazioni

del sistema e operazioni fraudolente.
Il cliente non è tenuto a sopportare le conseguenze derivanti dal *phishing attack* perpetrato tramite la tecnica del *man-in-the-browser*, e perfino la presenza del *malware* nel sistema non vale a fondare una presunzione di colpa grave in capo allo stesso, posta la difficile identificabilità di tale *software* malevolo.
Ricompare il concetto di "rischio di impresa", fulcro teorico e dogmatico del sistema di tutela costruito nella prima fase e volto a porre la responsabilità derivante da frodi informatiche in capo all'intermediario, in quanto soggetto più adatto a sopportarla e ad assorbirne le conseguenze dannose [52].
Un'ulteriore fattispecie di frode informatica rilevante, riconducibile anch'essa alle tecniche di *Phishing* più evolute, è il c.d. *Farming:* tecnica che non si basa più sull'invio di messaggi-esca fraudolenti che l'utente deve riscontare, ma sulla creazione di siti *web* falsi, verso i quali l'utente viene reindirizzato nonostante abbia digitato correttamente l'indirizzo *web* della banca e/o del portale su cui compiere le operazioni.
«*Si tratta di una forma assai subdola di truffa on-line che implica una sorta di duplicazione della pagina web, la quale si presenta perciò identica all'ignaro utente on-line*» [53].
Nei casi di *phishing attacks* maggiormente evoluti, come sono le tecniche del *man-in-the-browser* e del *farming*, si tende in generale a escludere una responsabilità del cliente basata su colpa grave, con conseguente (ri)allocazione del rischio derivante da frodi e illecite intrusioni nel sistema in capo all'intermediario.
A dimostrazione di un'evoluzione delle tutele che corre in parallelo con quella delle tecniche di *phishing*, si evidenzia come, allo stato, si riscontri una maggiore severità dell'ABF nei casi di frodi perpetrate con tecniche di *phishing* di prima generazione e ormai note, in cui «*la credulità del cliente appare non scusabile*» [54].
Resta da dire circa un'ulteriore forma di tutela per il cliente, attuabile, si può dire, in via d'urgenza e cautelativa e che consiste nell'immediato blocco della carta [55] a opera dell'intermediario in ipotesi di transazioni non autorizzate.
La misura *de quo* ha posto svariati problemi applicativi, soprattutto legati alle ipotesi in cui non siano presenti nel contratto sottoscritto tra banca e cliente clausole che, di fatto, autorizzino l'intermediario a eseguire il blocco suddetto.
In realtà, come risulta dall'analisi di recenti decisioni, L'ABF opta per consentire all'intermediario di effettuare il blocco immediato della carta, anche in assenza di previsioni contrattuali *ad hoc* e ciò sul presupposto che una tale azione rientrerebbe tra i doveri dell'intermediario stesso, quale corollario del generale principio di buona fede [56]. Ci si troverebbe probabilmente di fronte a un obbligo di protezione posto in capo alla banca, obbligo accessorio che

promana, secondo l'accezione espansa [57] che spesso si accoglie [58], dal suddetto principio generale [59].
A ogni modo, si ritiene corretto da parte della banca che ponga in essere la misura in analisi, dare pronta comunicazione al cliente [60].

4. Un ulteriore corollario connesso alle fattispecie di Phishing – risarcimento dei danni non patrimoniali subiti dal cliente: un'ipotesi per ora negata.

In diverse occasioni, i clienti vittima di *phishing attacks* si sono visti negare il diritto a ottenere il ristoro dei danni non patrimoniali derivanti da ansia, turbamento, grave limitazione del diritto di autodeterminazione per aver dovuto soppesare ogni attività o interesse che comportasse una spesa di denaro e per aver dovuto operare sgradite rinunce.
Vi è da dire che l'apertura verso la risarcibilità dei danni non patrimoniali da inadempimento è piuttosto recente.
Il discorso sul danno non patrimoniale, derivante dalla lesione di interessi estranei alla sfera patrimoniale [61], nato in una prima fase nell'ambito di fattispecie di responsabilità aquiliana e contrassegnato da progressive aperture, si sposta successivamente verso il terreno dell'inadempimento contrattuale, trovando, a dispetto di una iniziale chiusura riconducibile agli studi più datati [62], un terreno fertile sia tra i contributi della dottrina [63], che tra le pronunce della giurisprudenza.
L'orientamento restrittivo scontava i limiti derivanti dall'applicazione, anche in ambito contrattuale, dell'art. 2059 c.c., norma generale situata nel corpo della disciplina relativa all'illecito aquiliano che ammette il risarcimento del danno non patrimoniale solamente in casi tipici, previsti dalla legge e nel caso in cui la condotta da cui il danno deriva integri un illecito penale [64].
Nonostante tale orientamento, nelle pronunce della giurisprudenza, si assiste alla nascita di specifiche ipotesi di danno volte a offrire una reintegrazione a vantaggio di un soggetto che non ha ottenuto una prestazione preordinata alla realizzazione di interessi non patrimoniali [65].
Il passo successivo e determinante in materia è dato dalle pronunce della Consulta [66] e della Suprema corte [67], che svincolano definitivamente il danno non patrimoniale dai limiti normativi dell'art. 2059 c.c., ritenendo il danno non patrimoniale risarcibile tutte le volte in cui consegua alla lesione di interessi costituzionalmente protetti.
Una conferma del principio sopra citato e della lettura costituzionalmente orientata delle disposizioni dell'art. 2059 c.c. si ritrova in una importante pronuncia a Sezioni Unite della Suprema Corte [68].

La Corte ribadisce che, anche in assenza di reato, pregiudizi di tipo esistenziale, e quindi danni non patrimoniali, sono risarcibili se conseguenti alla lesione di un diritto inviolabile della persona tutelato a livello costituzionale.
Conferma, inoltre, come un danno non patrimoniale possa derivare anche dall'inadempimento di un'obbligazione incardinata in un rapporto contrattuale.
Tale assunto risulta confermato anche alla luce di pronunce successive. [69]
Il diritto per il cliente vittima di *phishing attack* al risarcimento del danno non patrimoniale viene negato dall'ABF proprio sulla base degli assunti enucleati dalle Sezioni unite della Suprema Corte per la carenza delle tre necessarie condizioni, ovvero la rilevanza costituzionale dell'interesse leso; la gravità della lesione e la non futilità del danno lamentato , che non deve consistere in meri disagi o fastidi [70].
In numerose ipotesi, la tutela risarcitoria relativa al ristoro dei danni patrimoniali è stata negata in quanto «*sfornita di qualsiasi supporto probatorio*» [71] o perché il cliente non ha proceduto a evocare «*alcun preciso fattore di danno o di lesione nella sua sfera giuridica*» [72].

Note
[*] Il presente contributo è stato preventivamente sottoposto a referaggio anonimo affidato ad un componente del Comitato di Referee secondo il Regolamento adottato da questa Rivista.
[1] Il termine è di chiara derivazione anglosassone e rappresenta una deformazione lessicale del lemma *to fish* (pescare). La metafora "marina" appare particolarmente incisiva ed efficace se si pensa al *phishing* come a una sorta di pesca volta a far abboccare gli utenti del *web* che sono definiti, appunto, naviganti.
[2] È frequente l'utilizzo di codici malevoli, (c.d. *trojan banking*) in grado di carpire le credenziali di accesso a servizi on line. Tali "virus", in continua evoluzione e non sempre rilevati o rilevabili dai *software antivirus*, sono in grado di autoinstallarsi, autoriprodursi, diffondersi, di determinare alterazioni del corretto funzionamento del sistema e di esportare i dati presenti nel sistema stesso verso altri terminali. Si individuano principalmente quattro classi di codici malevoli: a) gli *Spyware* (programmi spia), in grado di raccogliere informazioni di qualunque genere sul computer infettato e di inviarle al destinatario fraudolento; b) *Key-logging*: programmi in grado di attivarsi nel momento in cui gli utenti si connettono al sito di una banca o instaurano una connessione protetta (https), predisposti in modo da registrare

i dati digitati dall'ignaro utente per poi indirizzare tali informazioni a un ignoto destinatario; c) *Redirector*: si tratta di un codice malevolo predisposto per reindirizzare il traffico internet del computer infettato verso indirizzi IP differenti da quelli che in realtà si intendevano raggiungere; d) *Screen grabbing*: simile per funzionamento ai *Key-logging.* Sono programmi in grado di "fotografare" la videata nel momento in cui l'ignaro utente accede al portale e inserisce le proprie credenziali, per poi inviare tale "istantanea" a un ignoto destinatario.

[3] Cfr. Trib. Milano, 7 ottobre 2011, in *Guida dir., 2013, p. 62*: «*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 artt. 494 (sostituzione dei persona), 615 ter (accesso abusivo a sistemi informatici o telematici) e 640 c.p. (truffa) [...]*»

[4] Cfr., senza pretesa di esaustività, F. 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, p. 1094; V. Lembo, *La disciplina del* "phishing", in *Riv. pen.*, 2013, p. 892; ID., *La frode informatica,* in *Riv. pen.*, 2013, p. 892; F. Agnino, *Computer crime e fattispecie penali tradizionali,* in *Corr. merito*, 2009, p. 288.

[5] Vedi Trib. Milano, 7 ottobre 2011, cit.; Trib. Monza, 7 maggio 2009, in *Riv. pen.*, 2010, p. 1301: «*La condotta cosiddetta di "phishing", consistente nel "pescare", mediante abusivo inserimento nel sistema informatico di un'istituzione finanziaria 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 "donare" 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 sparizione del denaro fraudolentemente sottratto, integra la fattispecie di truffa punita ex art. 640 c.p. e non il delitto di frode informatica di cui all'art. 640 ter c.p.*»; Ufficio GIP Milano, 10 dicembre 2007, in *Foro amb.*, 2008, p. 280: «*Il c.d. "phishing" consiste nell'illecita intrusione via internet da parte di soggetti su sistemi informatici concernenti servizi "home banking" per utenti titolari di conti correnti bancari, clienti degli istituti di credito e integra, di per sé, i reati di accesso abusivo informatico e falsificazione del contenuto di comunicazioni informatiche di cui agli art. 615 ter e 617 sexies c.p. Qualora detta attività venga svolta da parte di soggetti operanti in Paesi stranieri, in accordo con soggetti residenti nel territorio dello Stato al fine di realizzare truffe ai danni*

dei clienti utenti dei predetti sistemi informatici, carpendo le loro generalità ed i codici segreti (user i.d. e password) relativi e i detti servizi bancari su internet, mediante l'invio di false e-mails apparentemente spedite da detti istituti di credito, ma in realtà false, essa concreta i reati di associazione a delinquere, con l'aggravante di reato transnazionale, di accesso abusivo informatico e di falsificazione di comunicazioni informatiche».

[6] Il recepimento delle disposizioni di cui alla citata direttiva comunitaria ha posto un delicato problema di diritto transitorio, relativo alla analisi e decisione di fattispecie risalenti a un periodo antecedente al recepimento della direttiva stessa. A riguardo si richiama l'orientamento ABF, espresso dalla decisione del Collegio di Roma, 2 luglio 2010, n. 665, su https://www.arbitrobancariofinanziario.it/decisioni/categorie/Bancomat%2520e%2520carte%2520di%2520debito/Utilizzo%2520fraudolento/Dec-20100702-665.PDF e suffragato da importanti indici giurisprudenziali interni e comunitari: «[...] *Le disposizioni delle direttive non ancora attuate o non correttamente attuate negli ordinamenti nazionali, quando siano (come si reputano quelle sopra richiamate) incondizionate e sufficientemente precise (c.d. auto esecutive) e sia scaduto il termine per il loro recepimento, sono immediatamente applicabili nei rapporti tra Stato (o pubbliche amministrazioni in genere) e soggetti privati (c.d. efficacia verticale), non invece nei rapporti "orizzontali" tra privati; indirizzo che ha ricevuto in più occasioni l'avvallo sia della Corte di Giustizia Europea sia della nostra Corte Suprema (di recente cfr. Cass., sez. IV civile, n. 23937/2006). Questo Collegio ritiene tuttavia che la limitazione così introdotta all'operatività negli ordinamenti nazionali delle disposizioni, di contenuto puntuale ed incondizionato, contenute in direttive comunitarie che sono ancora inattuate (o non correttamente attuate) e delle quali sia scaduto il termine per l'attuazione, non sia del tutto soddisfacente; condivide pertanto l'orientamento interpretativo di maggiore apertura [...] secondo il quale dette disposizioni, quando abbiano un contenuto sufficientemente dettagliato, preciso e incondizionato, possono essere invocate, all'interno degli Stati membri, anche nelle controversie tra privati. Del resto, la Corte di Giustizia - pur riaffermando la propria adesione all'orientamento contrario alla diretta applicabilità delle direttive nei confronti dei soggetti privati - ha in più di un'occasione puntualizzato che "il giudice nazionale deve interpretare il diritto nazionale per quanto possibile alla luce del testo e dello scopo della direttiva [rimasta in tutto o in parte inattuata] onde conseguire il risultato [da essa] perseguito." Viene così a realizzarsi, come non si è mancato di rilevare, un effetto orizzontale "indiretto" delle direttive, mediante un'interpretazione "teleologicamente orientata alla realizzazione dei risultati prescritti dal legislatore comunitario", che non deve rimanere circoscritta alle norme interne*

eventualmente introdotte per recepire la direttiva, ma deve essere esteso "a tutto il diritto nazionale per valutare in quale misura possa essere applicato in modo tale da non addivenire a un risultato contrario a quello a cui mira la direttiva" (cfr. Corte di Giustizia Comunità Europee, 5 ottobre 2004, cause riunite da C-397/01 a C-403/01, Pfeiffer): infatti, "spetta ai giudici nazionali assicurare ai singoli la tutela giurisdizionale derivante dalle norme del diritto comunitario e assicurarne la piena efficacia." Invero, gli Stati membri, pur non essendo ancora tenuti (perché non è scaduto il termine di adempimento del relativo obbligo) a recepire i contenuti della direttiva all'interno del proprio ordinamento, debbono astenersi dall'adottare disposizioni che possano compromettere "gravemente" la realizzazione del risultato prescritto dal legislatore comunitario (Corte di Giustizia, 1997, in C-129/96). E, al tempo stesso, i giudici debbono evitare di fornire interpretazioni del diritto interno idonee a pregiudicare "gravemente" il risultato imposto dalla direttiva e il suo effetto utile (Corte di Giustizia, 4 luglio 2006, in C-221/04). Le Sezioni Unite della Corte di Cassazione si sono spinte, a quest'ultimo riguardo, ancora oltre, affermando che il giudice nazionale è tenuto a "prendere in considerazione tutto il diritto interno e a valutare, attraverso l'utilizzazione dei metodi interpretativi dallo stesso ordinamento riconosciuti, in quale misura esso possa essere applicato in modo da non addivenire ad un risultato contrario a quello cui mira la direttiva" (Cass., Sez. Un. 17 novembre 2008, n. 27310, 16 marzo 2009, n. 6316); affermando, in altri termini, l'esistenza di un obbligo di interpretazione "conforme" al diritto comunitario configurato in termini non dissimili da quelli individuati dalla Corte di Giustizia in relazione alle direttive il cui termine di attuazione sia già scaduto (Corte di Giustizia, 5 ottobre 2004)».

[7] Cfr. *ex plurimis* ABF, Coll. Roma, decisione n. 105 del 14 gennaio 2011, su https://www.arbitrobancariofinanziario.it/decisioni/categorie/Conto%2520corrente%2520bancario%2520e%2520postale/Banca%2520on%2520line/Dec-20110114-105.pdf: «*Dal nuovo quadro normativo sopra riportato discende che qualora il cliente contesti alla banca l'effettuazione di operazioni elettroniche di pagamento non autorizzate chiedendo il riaccredito delle somme addebitatigli in conto: a) grava sulla banca l'onere di provare che l'operazione è stata correttamente autorizzata, ovvero che il cliente si è reso inadempiente agli obblighi scaturenti dal contratto; b) l'utilizzo non autorizzato dei codici di accesso non costituisce, di per sé, necessariamente prova di un comportamento negligente da parte del cliente*».

[8] Cfr. art. 7, d.lgs. n. 11/2010: «*1. L'utilizzatore abilitato all'utilizzo di uno strumento di pagamento ha l'obbligo di: a) utilizzare lo strumento di pagamento in conformità con i termini, esplicitati nel contratto quadro, che ne regolano l'emissione e l'uso; b) comunicare senza indugio, secondo le modalità previste dal contratto quadro, al prestatore di servizi di pagamento o al*

soggetto da questo indicato lo smarrimento, il furto, l'appropriazione indebita e l'uso non autorizzato dello strumento non appena ne viene a conoscenza. 2. Ai fini di cui al comma 1, lettera a), l'utilizzatore, non appena riceve uno strumento di pagamento, adotta le misure idonee a garantire la sicurezza dei dispositivi personalizzati che ne consentono l'utilizzo».

[9] Cfr. art. 8, d.lgs. n. 11/2010: «*Il prestatore di servizi di pagamento che emette uno strumento di pagamento ha l'obbligo di: a) assicurare che i dispositivi personalizzati che consentono l'utilizzo di uno strumento di pagamento non siano accessibili a soggetti diversi dall'utilizzatore legittimato ad usare lo strumento medesimo, fatti salvi gli obblighi imposti a quest'ultimo ai sensi dell'art. 7; b) astenersi dall'inviare strumenti di pagamento non specificamente richiesti, a meno che lo strumento di pagamento già consegnato all'utilizzatore debba essere sostituito; c) assicurare che siano sempre disponibili strumenti adeguati affinché l'utilizzatore dei servizi di pagamento possa eseguire le comunicazione di cui all'art. 7, comma 1, lettera b), nonché, nel caso di cui all'art. 6, comma 4, di chiedere la riattivazione dello strumento di pagamento o l'emissione di uno nuovo ove il prestatore di servizi di pagamento non vi abbia già provveduto. Ove richiesto dall'utilizzatore, il prestatore di servizi di pagamento gli fornisce i mezzi per dimostrare di aver effettuato la comunicazione per i 18 mesi successivi la comunicazione medesima; d) impedire qualsiasi utilizzo dello strumento di pagamento successivo alla comunicazione dell'utilizzatore, di cui all'articolo 7, comma 1, lettera b). 2. I rischi derivanti dalla sparizione di uno strumento di pagamento e dei relativi dispositivi personalizzati che ne consentono l'utilizzo sono a carico del prestatore di servizi di pagamento*».

[10] Cfr. art. 11, d.lgs. n. 11/2010: «*1. Fatto salvo l'articolo 9, nel caso in cui un'operazione di pagamento non sia stata autorizzata, il prestatore di servizi di pagamento rimborsa immediatamente al pagatore l'importo dell'operazione medesima. 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. 2. In caso di motivato sospetto di frode, il prestatore di servizi di pagamento può sospendere il rimborso di cui al comma 1 dandone immediata comunicazione all'utilizzatore. 3. Il rimborso di cui al comma 1 non preclude la possibilità per il prestatore di servizi di pagamento di dimostrare anche in un momento successivo che l'operazione di pagamento era stata autorizzata; in tal caso il prestatore di servizi di pagamento ha il diritto di chiedere ed ottenere dall'utilizzatore la restituzione dell'importo rimborsato. 4. Il risarcimento di danni ulteriori subiti può essere previsto in conformità alla disciplina applicabile al contratto stipulato tra l'utilizzatore e il prestatore di servizi di pagamento*».

[11] Cfr. art. 12, d.lgs. n. 11/2010: «*1. Salvo il caso in cui abbia agito in modo fraudolento, l'utilizzatore non sopporta alcuna perdita derivante dall'utilizzo di uno strumento di pagamento smarrito, sottratto o utilizzato indebitamente intervenuto dopo la comunicazione eseguita ai sensi dell'articolo 7, comma 1, lettera b). 2. Salvo il caso in cui abbia agito in modo fraudolento, l'utilizzatore non è responsabile delle perdite derivanti dal'utilizzo dello strumento di pagamento smarrito, sottratto o utilizzato indebitamente, quando il prestatore di servizi di pagamento non ha adempiuto all'obbligo di cui all'articolo 8, comma 1, lettera c). 3. Salvo il caso in cui l'utilizzatore abbia agito con dolo o colpa grave ovvero non abbia adottato le misure idonee a garantire la sicurezza dei dispositivi personalizzati che consentono l'utilizzo dello strumento di pagamento, prima della comunicazione eseguita a i sensi dell'articolo 7, comma 1, lettera b), l'utilizzatore medesimo può sopportare per un importo comunque non superiore complessivamente a 150 euro la perdita derivante dall'utilizzo dello strumento di pagamento conseguente al suo furto o smarrimento. 4. Qualora abbia agito in modo fraudolento o non abbia adempiuto ad uno o più obblighi di cui all'articolo 7 con dolo o colpa grave, l'utilizzatore sopporta tutte le perdite derivanti da operazioni di pagamento non autorizzate e non si applica il limite di cui al comma 3. 5. La Banca d'Italia con proprio regolamento può ridurre le responsabilità massime di cui ai commi 3 e 4 nel caso di strumenti di pagamento aventi particolari caratteristiche di sicurezza; la Banca d'Italia assicura la generale conoscibilità degli strumenti di pagamento rispondenti a tali caratteristiche di sicurezza*».

[12] Era frequente l'inserimento di clausole del seguente tenore: «Il titolare è responsabile di ogni conseguenza dannosa che possa derivare dall'abuso o dall'uso illecito della Carta e del P.I.N.» Oppure: «in caso di smarrimento o sottrazione della carta o del P.I.N., il Titolare è responsabile per le perdite derivanti da eventuali prelievi fraudolenti [...]».

[13] «*Si presumono vessatorie fino a prova contraria le clausole che hanno per oggetto, o per effetto, di: a) escludere o limitare la responsabilità da un fatto o da un'omissione del professionista; b) escludere o limitare le azioni o i diritti del consumatore nei confronti del professionista o di un'altra parte in caso di inadempimento totale o parziale o di adempimento inesatto da parte del professionista*».

[14] Cfr. ABF, Coll. Roma, decisione n. 665/2010, cit. In materia di clausole vessatorie nei rapporti banca-cliente cfr. Trib. Roma, 21 gennaio 2000, in *Giur. rom.*, 2000, p. 430: «*Sono vessatorie, in quanto escludono o limitano la responsabilità del professionista nei confronti del consumatore, le clausole che attribuiscono alla banca facoltà di dare o meno esecuzione agli incarichi assunti nei confronti del cliente o di stabilire in modo discrezionale le modalità di esecuzione degli stessi, le clausole del contratto di servizio delle cassette di*

sicurezza che realizzano l'effetto di limitare la responsabilità della banca al massimale assicurativo dichiarato dal cliente, le clausole che autorizzano in maniera irrevocabile la banca al trattamento dei dati personali del cliente, le clausole sulla prestazione di servizi bancari e finanziari che escludono la responsabilità della banca per fatti non direttamente imputabili ad essa, le clausole che escludono la responsabilità della banca per gli incarichi delegati ad un proprio corrispondente, le clausole che escludono la responsabilità della banca per il pagamento di assegni falsi qualora il cliente non abbia dato immediata comunicazione dello smarrimento o del furto dei moduli».

[15] Cfr. artt. 32-35, d.lgs. n. 196/2003: «*Art. 32 (Particolari titolari): 1. Il fornitore di un servizio di comunicazione elettronica accessibile al pubblico adotta ai sensi dell'articolo 31 idonee misure tecniche e organizzative adeguate al rischio esistente, per salvaguardare la sicurezza dei suoi servizi, l'integrità dei dati relativi al traffico, dei dati relativi all'ubicazione e delle comunicazioni elettroniche rispetto ad ogni forma di utilizzazione o cognizione non consentita. 2. Quando la sicurezza del servizio o dei dati personali richiede anche l'adozione di misure che riguardano la rete, il fornitore del servizio di comunicazione elettronica accessibile al pubblico adotta tali misure congiuntamente con il fornitore della rete pubblica di comunicazioni. In caso di mancato accordo, su richiesta di uno dei fornitori, la controversia è definita dall'Autorità per le garanzie nelle comunicazioni secondo le modalità previste dalla normativa vigente. 3. Il fornitore di un servizio di comunicazione elettronica accessibile al pubblico informa gli abbonati e, ove possibile, gli utenti, se sussiste un particolare rischio di violazione della sicurezza della rete, indicando, quando il rischio è al di fuori dell'ambito di applicazione delle misure che il fornitore stesso è tenuto ad adottare ai sensi dei commi 1 e 2, tutti i possibili rimedi e i relativi costi presumibili. Analoga informativa è resa al Garante e all'Autorità per le garanzie nelle comunicazioni». «Art. 33 (Misure minime): 1. Nel quadro dei più generali obblighi di sicurezza di cui all'articolo 31, o previsti da speciali disposizioni, i titolari del trattamento sono comunque tenuti ad adottare le misure minime individuate nel presente capo o ai sensi dell'articolo 58, comma 3, volte ad assicurare un livello minimo di protezione dei dati personali». «Art. 34 (Trattamenti con strumenti elettronici): 1. Il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime: a) autenticazione informatica; b) adozione di procedure di gestione delle credenziali di autenticazione; c) utilizzazione di un sistema di autorizzazione; d) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici; e)*

protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici; f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi; g) tenuta di un aggiornato documento programmatico sulla sicurezza; h) adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitart». «Art. 35 (Trattamenti senza l'ausilio di strumenti elettronici): 1. Il trattamento di dati personali effettuato senza l'ausilio di strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime: a) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative; b) previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti; c) previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati».

[16] Cfr., da ultimo, Cass., 5 settembre 2014, n. 18812, in *Foro it.*, 2015, c. 119: «*I danni cagionati per effetto del trattamento dei dati personali in base all'art. 15 del d.lgs. 30 giugno 2003, n.196, sono assoggettati alla disciplina di cui all'art. 2050 cod. civ., con la conseguenza che il danneggiato è tenuto solo a provare il danno e il nesso di causalità con l'attività di trattamento dei dati, mentre spetta al convenuto la prova di aver adottato tutte le misure idonee ad evitare il danno*». In dottrina cfr. M. Cicoria, *Quale danno in materia di privacy?,* in *Giust. civ.*, 2007, p. 39; F. Azzarri, *Responsabilità presunta, responsabilità oggettiva e danno,* in *Resp. civ. prev.*, 2008, p. 1078; E. Pellecchia, *La responsabilità civile per trattamento dei dati personali,* in *Resp. civ. prev.*, 2006, p. 221; M.C. Polo, *La tutela della riservatezza nei pagamenti elettronici,* in *Contratto e impresa, 2004, p. 1376*; E. Giannantonio, *Responsabilità civile e trattamento dei dati personali,* in *Dir. informatica*, 1999, p. 1035; C.M. Bianca, *Diritto civile, vol. V,* Milano, 1994, p. 704 ss.

[17] Cfr. M. Bessone, *Adempimento e rischio contrattuale*, Milano, 1969; G. Alpa, voce *Rischio* (dir. vig.), in *Enc. dir.*, vol. XL, Milano, 1989, p. 1144; ID., voce *Rischio contrattuale,* in *Nov. Dig. it.*, app., vol. VI, Torino, 1986, p. 863; ID., M. Bessone, V. Roppo, *Rischio contrattuale e autonomia privata*, Milano, 1982; P. Gallo, *Sopravvenienza contrattuale e problemi di gestione del contratto*, Milano, 1992; E. Gabrielli, *Alea e Rischio nel contratto*, Napoli, 1997; F. Delfini, *Autonomia privata e rischio contrattuale*, Milano, 1999.

[18] Vedi ABF, Coll. Roma, decisione n. 665/2010, cit.: «*Si tratta di una disciplina 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, in funzione dell'obiettivo di incrementare la fiducia del pubblico riguardo ai suddetti strumenti e di incentivarne l'uso e la diffusione, in quanto strumenti atti a facilitare e perciò moltiplicare le transazioni commerciali, nell'interesse delle imprese, degli stessi utenti/consumatori, nonché, ovviamente, delle banche».

[19] Cfr. Cass., 19 novembre 2001 n. 14456, in *Dir. maritt.,* 2003, p. 1300: «*Ad integrare gli estremi della colpa grave del cliente è necessario che il suo comportamento sia connotato da straordinaria ed inescusabile imprudenza o negligenza, idonea a far ritenere che chi ha agito ha omesso di osservare, non soltanto la diligenza del buon padre di famiglia, ma anche quel grado minimo di elementare diligenza generalmente osservato da tutti*». Cfr. anche ABF, Coll. Milano, decisione n. 40 del 13 gennaio 2012, su https://www.arbitrobancariofinanziario.it/decisioni/categorie/Bancomat%2520e%2520carte%2520di%2520debito/Utilizzo%2520fraudolento/Dec-20120113-40.pdf e Coll. Roma, decisione n. 2157 del 14 ottobre 2011, su https://www.arbitrobancariofinanziario.it/decisioni/categorie/Bancomat%2520e%2520carte%2520di%2520debito/Utilizzo%2520fraudolento/Dec-20111014-2157.pdf.

[20] Cfr., ABF, Collegio di Coordinamento, decisione n. 3498 del 26 ottobre 2012, su https://www.arbitrobancariofinanziario.it/decisioni/categorie/Conto%2520corrente%2520bancario%2520e%2520postale/Banca%2520on%2520line/Dec-20121026-3498.pdf: «*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 [...] Naturalmente, la concreta traduzione del principio non può prescindere da una corretta applicazione del limite che le norme regolatrici vi appongono e che, al netto di ogni ulteriore considerazione, si riduce allo stabilire se l'intermediario abbia adottato tutti i migliori accorgimenti della tecnica nota per scongiurare questo genere di rischi e quando (esclusa ovviamente la condotta fraudolenta del cliente di per sé tale da precludere l'operatività di qualsivoglia presidio) l'eventuale negligenza del cliente possa ricadere o meno*

nella nozione di colpa grave al cui ricorrere il cit. art. 8 esclude ogni responsabilità dell'intermediario».

[21] Cfr. ABF, Coll. Roma, decisione n. 1440 del 6 dicembre 2010, su https://www.arbitrobancariofinanziario.it/decisioni/categorie/Conto%2520corrente%2520bancario%2520e%2520postale/Banca%2520on%2520line/Dec-20101206-1440%20.pdf: «*In ordine alla diligenza qualificata richiesta all'intermediario, un ausilio interpretativo può rinvenirsi nelle disposizioni che, con riferimento alle carte di pagamento e sebbene per finalità diverse, dettano criteri per l'individuazione di operazioni sospette. Il Regolamento di attuazione della l. 17 agosto 2005, n. 166, recante istituzione di un sistema di prevenzione delle frodi sulle carte di pagamento, detta specifici criteri con riferimento agli indicatori di rischio. Per quanto rileva al caso in esame, ai sensi dell'art. 8, si configura il rischio di frode quando vengono raggiunti determinati parametri, in particolare: - una ovvero più richieste che nelle 24 ore esauriscano l'importo totale del plafond della carta di pagamento; - due o più richieste di autorizzazione provenienti da Stati diversi, effettuate con la stessa carta, nell'arco di sessanta minuti*».

[22] Vedi Cass. 24 settembre 2009, n. 20543, in *Guida al dir., 2009,* p. 56: «*La diligenza del buon banchiere deve essere qualificata dal maggior grado di prudenza ed attenzione che la connotazione professionale richiede. Tale diligenza 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. In quest'ambito si osserva che generalmente gli schemi contrattuali per il servizio on-line non prevedono né direttamente massimali di utilizzo (giornalieri/mensili), né la possibilità (o l'obbligo) per il correntista di indicare egli stesso all'intermediario dei limiti massimi (ovvero modificarli se previsti) oltre i quali non sia possibile disporre on line del conto*».

[23] In materia di responsabilità contrattuale e adempimento diligente si rimanda alle opere di E. Betti, *Teoria generale delle obbligazioni. Prolegomeni: funzione economico-sociale dei rapporti d'obbligazione*, Milano, 1953; C.M. Bianca, Dell'*inadempimento delle obbligazioni, artt. 1218-1229,* in Scialoja, Branca (a cura di), *Comm. cod. civ.*, Bologna-Roma, 1979, XXVI ss.; ID., *Diritto civile, L'obbligazione*, vol. IV, Milano, 1990; ID., *Diritto civile, La responsabilità*, vol. V, Milano, 1994; M. Giorgianni, *L'inadempimento*, Milano, 1975; L. Mengoni, voce *Responsabilità contrattuale (dir.vig.),* in *Enc. dir.*, vol. XXXIX, Milano, 1988, p. 1072; G. Visintini, *Responsabilità del debitore, in* Rescigno (a cura di), *Tratt. dir. priv.*, vol. IX, Torino, 1999; ID., *Inadempimento e mora del*

debitore, artt. 1218-1222, in Schlesinger (a cura di), *Comm. cod. civ.*, Milano, 2006; V. Roppo, *Il contratto*, Milano, 2001; G. Villa, *Danno e risarcimento contrattuale,* in *Tratt. contr.*, Roppo, vol. V, Milano, 2006, p. 970; P. Trimarchi, *Il contratto: inadempimento e rimedi*, Milano, 2010; F. Galgano, *Trattato di diritto civile*, vol. II, Padova, 2010. Con particolare riferimento alla contrattazione on line Cfr. O. Troiano, *I servizi elettronici di pagamento*, Milano, 1996; A.M. Gambino, *L'accordo telematico*, Milano, 1997; C.M. Bianca, *I contratti digitali*, in *Studium iuris*, 1998, 1035; A. Gentili, *Documento informatico e tutela dell'affidamento,* in *Riv. dir. civ.*, 1998, ID., *L'inefficacia del contratto telematico,* in *Riv. dir. civ.*, 2000, 747; G. Oppo, *Disumanizzazione del contratto*, in *Riv. dir. civ.*, 1998, 525; V. Ricciuto; N. Zorzi, *Il contratto telematico*, Padova, 2002; F. Di Ciommo, *La responsabilità civile in internet: prove di governo dell'anarchia tecnocratica,* in *Resp. civ.*, 2006, 548; P. Gallo, *Il contratto telematico*, in Gallo (a cura di), *Tratt. del contr.*, Vol. 1, Torino, 2010, p. 841 ss. Con riferimento alla responsabilità contrattuale ed extracontrattuale on line si rimanda a S. Sica; N. Brutti, *La responsabilità in internet e nel commercio elettronico*, in Alpa (a cura di), *Tratt. resp. contr.*, vol. 2, Padova, 2009, 503 ss.; C. Iurilli, *Conto corrente on line e furto di identità. La controversa applicazione dell'art. 2050 c.c.,* in *Resp. civ.*, 2011, 54; S. Marino, *Nuovi sviluppi in materia di illecito extracontrattuale "on line"*, in *Riv. dir. internaz. priv.*, 2012, 879;

[24] Cfr. Cass., 23 giugno 2008, n. 17039, in *Giust. civ., 2008,* p.1012.

[25] Cfr. Cass., 31 marzo 2010, n. 7956, in *Foro it.,* 2010, c. 3092.

[26] Cfr., *ex plurimis,* ABF, Coll. Milano, decisione n. 1241 del 9 novembre 2010, su https://www.arbitrobancariofinanziario.it/decisioni/categorie/Conto%2520corrente%2520bancario%2520e%2520postale/Operazioni%2520sul%2520conto/Dec-20101109-1241.pdf e n. 1030 del 4 ottobre 2010, su https://www.arbitrobancariofinanziario.it/decisioni/categorie/Conto%2520corrente%2520bancario%2520e%2520postale/Banca%2520on%2520line/Dec-20101004-1030.pdf .

[27] Cfr. *ex plurimis* ABF, Coll. Napoli, decisione n. 6797 del 15 ottobre 2014, su https://www.arbitrobancariofinanziario.it/decisioni/categorie/Conto%2520corrente%2520bancario%2520e%2520postale/Banca%2520on%2520line/Dec-20141015-6797.PDF: «*In tali casi, al pari della presente controversia, appare decisiva l'indagine circa la sussistenza di elementi soggettivi integranti l'ipotesi di colpa grave, il cui onere della prova incombe, secondo la dottrina, sull'intermediario in base ai principi che regolano la responsabilità contrattuale (art. 1218 c.c.) [...]*». Cfr. in particolare ABF, Coll. Milano, decisione n. 6786 del 15 ottobre 2014, su

https://www.arbitrobancariofinanziario.it/decisioni/categorie/Conto%2520corrente%2520bancario%2520e%2520postale/Banca%2520on%2520line/Dec-20141015-6786.PDF: «*Sulla materia l'ABF si è pronunciato più volte e la questione della ripartizione delle responsabilità per frodi perpetrate attraverso l'home banking è stata portata anche all'attenzione del Collegio di Coordinamento, che nella Decisione n. 3498/2012 ha operato un accurato censimento delle fattispecie di frode più diffuse ed ha puntualizzato i termini di valutazione delle questioni connesse. In particolare, ha sottolineato il regime di particolare favore che il d.lgs. 11/2010 predispone per l'utilizzatore del servizio, cui consegue una ripartizione dei rischi collegati all'utilizzo di strumenti di pagamento in ambiente informatico sfavorevole all'intermediario, sul presupposto che questi sia la parte più attrezzata a gestire detti rischi e, in ultima analisi, il percettore dei vantaggi e delle efficienze legate all'utilizzo di sistemi informatici di pagamento. Tale opzione giustificherebbe la speciale distribuzione dell'onere della prova di cui al citato decreto, che pone a carico dell'intermediario l'onere di dimostrare che l'operazione disconosciuta dal cliente sia stata correttamente autenticata, registrata e contabilizzata e che non vi siano state disfunzioni del sistema e delle procedure che abbiano potuto dare causa all'illecita intrusione di terzi. Giustificherebbe altresì la limitazione della responsabilità dell'utilizzatore ai casi di dolo o colpa grave laddove le comunicazioni dovute in tali casi all'intermediario siano state tempestivamente e correttamente effettuate*».

[28] Cfr. ABF, Coll. Milano, decisione n. 6786 del 15 ottobre 2014, cit.

[29] Cfr. *ex plurimis* ABF, Coll. Milano, decisione n. 111 del 13 gennaio 2012, su https://www.arbitrobancariofinanziario.it/decisioni/categorie/Conto%2520corrente%2520bancario%2520e%2520postale/Banca%2520on%2520line/Dec-20120113-111.pdf e n. 113 del 13 gennaio 2012, su https://www.arbitrobancariofinanziario.it/decisioni/categorie/Carte%2520di%2520credito/Tipologia/Dec-20120113-113.pdf: «*È chiaro a questo Collegio che, al tempo del fatto all'origine della presente vertenza, esistevano già mezzi più efficienti per fronteggiare il fenomeno della pirateria informatica e questo costituisce ragione sufficiente per indurre a concludere che un sistema di protezione a un solo fattore – sebbene composto da user-id e password del titolare, numero della carta e data di scadenza della stessa, codice di sicurezza CVV2, non variabili di volta in volta – per permettere effettuazione di pagamenti o altre operazioni non può essere considerato misura idonea a proteggere adeguatamente il cliente*».”

[30] Cfr. ABF, Coll. Roma, decisione n. 491 dell'11 marzo 2011, su https://www.arbitrobancariofinanziario.it/decisioni/categorie/Conto%2520co

rrente%2520bancario%2520e%2520postale/Banca%2520on%2520line/Dec-20110311-491.pdf

[31] Cfr. ABF, Coll. Roma, decisione n. 1426 del 6 dicembre 2010, su https://www.arbitrobancariofinanziario.it/decisioni/categorie/Conto%2520corrente%2520bancario%2520e%2520postale/Banca%2520on%2520line/Dec-20101206-1426%20.pdf: «*L'aver dato seguito al messaggio di posta elettronica apparentemente proveniente dalla banca è comportamento certamente affetto da colpa e da imprudenza; tuttavia, sebbene la banca avesse pubblicato nel proprio sito un documento contenente una serie di suggerimenti idonei a prevenire i danni del phishing, la conoscenza da parte del pubblico di tale fenomeno non era (all'epoca dei fatti di causa) ancora così elevata e la percezione sociale della diffusione e pericolosità dello stesso così intensa da poter qualificare quel comportamento in termini di leggerezza e di imprudenza straordinarie ed assolutamente inescusabili*».

[32] Cfr. ABF, Coll. Roma, decisione n. 1426 del 6 dicembre 2010, cit.

[33] Cfr. ABF, Coll. Milano, decisione n. 20 del 7 gennaio 2011, su https://www.arbitrobancariofinanziario.it/decisioni/categorie/Conto%2520corrente%2520bancario%2520e%2520postale/Banca%2520on%2520line/Dec-20110107-20.pdf: «*In concreto, la colpa grave prevalente del ricorrente è emersa dall'ammissione che lo stesso fece nella denunzia ai carabinieri, allorché, asserendo di aver ricevuto una mail sospetta, aderì alla richiesta di inserire i codici di accesso del proprio conto corrente. Né va, peraltro, sottovalutato che il cliente nella denuncia dichiarò di ritenere che ignoti avessero acquisito i codici di accesso e movimentazione del conto corrente e che con detti codici avessero effettuato le movimentazioni contestate*».

[34] Cfr. ABF, Coll., Milano, decisione n. 1241 del 9 novembre 2010, su https://www.arbitrobancariofinanziario.it/decisioni/categorie/Conto%2520corrente%2520bancario%2520e%2520postale/Operazioni%2520sul%2520conto/Dec-20101109-1241.pdf: «*La questione che questo Collegio deve affrontare per la soluzione del caso attiene ai doveri di custodia dei codici di accesso da parte del cliente che utilizzi il servizio di home banking da un lato e del grado di diligenza che si può richiedere all'intermediario in relazione all'erogazione di detto servizio dall'altro lato. In relazione al caso in questione giova notare che risulta assolutamente pacifico che il ricorrente abbia risposto a una e-mail di phishing [...]. La circostanza è stata dichiarata dall'interessato anche nella denuncia alla Pubblica Autorità. Al riguardo il ricorrente ha precisato di avere fornito il proprio codice per ottenere un accredito collegato ad un'operazione a premi nell'assoluta certezza che a richiederlo fosse l'intermediario*».

[35] Cfr. ABF, Coll. Roma, decisione n. 237 del 15 aprile 2010, su https://www.arbitrobancariofinanziario.it/decisioni/categorie/Conto%2520corrente%2520bancario%2520e%2520postale/Banca%2520on%2520line/Dec-

20100415-237.pdf. Cfr. anche ABF, Coll. Milano, decisione n. 7435 del 7 novembre 2014, su https://www.arbitrobancariofinanziario.it/decisioni/categorie/Bonifico/Transfrontaliero/Dec-20141107-7435.PDF: «*È stato proprio il ricorrente, infatti, che ha risposto ad una e-mail di phishing (pratica tanto ormai diffusa quanto ormai certamente nota alla clientela bancaria), inserendo il codice necessario all'incasso della somma in corso di trasferimento e permettendo in tal modo che la truffa ai suoi danni potesse effettivamente essere posta in essere. Tale condotta – valutata anche alla luce del fatto che la e-mai di phishing appare scritta in una lingua che, pur assomigliando all'italiano, risulta difficilmente classificabile - integra pienamente gli elementi in fatto per poter integrare una condotta gravemente colpevole del ricorrente e tale da interrompere qualsiasi nesso di causalità tra un'eventuale inadempienza dell'intermediario resistente ed il danno lamentato dal ricorrente medesimo, con conseguente esclusione di qualsiasi responsabilità del primo per i fatti all'origine della presente vertenza*». Cfr. anche ABF, Coll. Milano, decisione n. 6651 dell'8 ottobre 2014, su https://www.arbitrobancariofinanziario.it/decisioni/categorie/Conto%2520corrente%2520bancario%2520e%2520postale/Banca%2520on%2520line/Dec-20141008-6651.PDF, in cui si afferma una responsabilità in capo al cliente il quale «*utilizzando un minimo di diligenza non avrebbe, infatti, potuto non accorgersi di avere ricevuto un messaggio di phishing, considerando innanzitutto che le banche non dialogano per posta elettronica con i clienti, se non per l'invio di estratti conto, e tenuto conto della genericità delle informazioni, degli errori di punteggiatura e del tono confidenziale utilizzato al di fuori del "tu generico". L'esistenza di simili comunicazioni, che spesso riescono a sfuggire anche ai sistemi antispam, costituisce peraltro ormai fatto notorio*». Dello stesso tenore ABF, Coll. Milano, decisione n. 6413 del 1 ottobre 2014, su https://www.arbitrobancariofinanziario.it/decisioni/categorie/Conto%2520corrente%2520bancario%2520e%2520postale/Banca%2520on%2520line/Dec-20141001-6413.PDF.

[36] Cfr., ABF, Coll. Roma, decisione n. 237 del 25 aprile 2010, cit.

[37] Cfr., *ex plurimis* ABF, Coll. Milano, decisione n. 719 del 9 luglio 2010, su https://www.arbitrobancariofinanziario.it/decisioni/categorie/Conto%2520corrente%2520bancario%2520e%2520postale/Banca%2520on%2520line/Dec-20100709-719.pdf : «*In sintesi dunque, nel caso all'origine del presente ricorso, da un lato si può verosimilmente ravvisare una responsabilità del cliente in relazione alla mancata diligente custodia dei codici di accesso per il servizio di home banking, dall'altro lato, non si può negare una concorrente responsabilità dell'intermediario che non ha predisposto adeguati sistemi per*

proteggere più efficacemente i propri clienti con riferimento al rischio di truffe perpetrate in via telematica. Questo Collegio, valutata la gravità delle rispettive colpe in relazione ai fatti illustrati e documentati, ritiene, dunque, di doverle ripartire nella misura del 50% in capo al cliente e del 50% in capo al resistente».

[38] Cfr. ABF, Coll. Roma, decisione n. 33 del 10 febbraio 2010, su https://www.arbitrobancariofinanziario.it/decisioni/categorie/Conto%2520corrente%2520bancario%2520e%2520postale/Banca%2520on%2520line/Dec-20100210-33.pdf : «*Alla stregua di detti principi va affermata la responsabilità della Banca, perché, se non è controvertibile che questa avesse adottato determinati accorgimenti tecnici allo scopo di proteggere la sicurezza nell'uso della rete per l'esecuzione da parte dei clienti di operazioni sui propri conti correnti (c.d. internet banking o home banking), è altrettanto incontrovertibile che, all'epoca dei fatti per cui è controversia, la tecnologia aveva già messo a disposizione dispositivi più raffinati, sicuri ed affidabili di quelli in concreto adottati, e perciò maggiormente adeguati rispetto all'obiettivo suddetto in quanto capaci di offrire al cliente un terzo livello di protezione, come le serie numeriche casuali e random, generate da dispositivi automatici quali chiavette o token, digipass e similia*»"

[39] Cfr., *ex plurimis,* ABF, Coll. Napoli, decisione n. 696 del 7 marzo 2012, su https://www.arbitrobancariofinanziario.it/decisioni/categorie/Carte%2520di%2520credito/Tipologia/Dec-20120307-696.PDF. Cfr. inoltre ABF Collegio di Coordinamento, decisione n. 3498 del 26 ottobre 2012, cit: «*[...] Lo strumentario avanzato di sicurezza è stato individuato, almeno per quanto specificamente attiene al caso che ci occupa (pagamenti disposti mediante sistemi di internet banking) nella messa a disposizione dei cc.dd. token o OTP (one time password), vale a dire congegni in grado di generare mutevoli password monouso, che, aggiungendosi alla password fissa nota solo all'utente, concorrono a formare un sistema di autenticazione a due fattori, (altri dice a tre fattori, includendovi anche lo user id per quanto più visibile e catturabile): sistema come tali di difficilissima, (quasi) impossibile forzatura e dunque ritenuto coerente alle indicazioni promananti dal provvedimento della Banca d'Italia adottato il 5 luglio 2011 ove si prevede che gli intermediari si attrezzino adeguatamente per identificare, valutare, monitorare e mitigare le minacce di natura tecnologica, individuando un insieme di misure di sicurezza e di controlli appropriati in grado di assicurare gli obiettivi di confidenzialità, integrità, disponibilità dei sistemi informativi e dei dati a essi associati*».

[40] Cfr. ABF, Coll. Napoli, decisione n. 6888 del 21 ottobre 2014, su https://www.arbitrobancariofinanziario.it/decisioni/categorie/Conto%2520corrente%2520bancario%2520e%2520postale/Banca%2520on%2520line/Dec-20141021-6888.PDF.

[41] Cfr. ABF, Coll. Coordinamento, decisione, n. 3498 del 26 ottobre 2012, cit.
[42] Cfr. ABF, Coll. Milano, decisione n. 528 del 17 febbraio 2012, su https://www.arbitrobancariofinanziario.it/decisioni/categorie/Conto%2520corrente%2520bancario%2520e%2520postale/Banca%2520on%2520line/Dec-20120217-528.pdf: «*Il fatto che il ricorrente, tempestivamente informato, abbia deciso di non usufruire di un dispositivo idoneo a innalzare il grado di sicurezza del servizio integra una condotta negligente, concorrente in termini rilevanti alla produzione del danno, pertanto responsabile ex art. 1218 c.c*».
[43] Così, ABF, Coll. Coordinamento, decisione n. 3498 del 26 ottobre 2012, cit.
[44] Vedi ABF, Coll. Milano, decisione n. 2103 del 20 giugno 2012, su https://www.arbitrobancariofinanziario.it/decisioni/categorie/Bonifico/Transfrontaliero/Dec-20120620-2103.pdf: «*Dalle informazioni rese dalla ricorrente e dalle precisazioni fornite dalla resistente, che non sono state contestate, è emerso, infatti, che per il compimento di un'operazione via internet il cliente è tenuto ad utilizzare uno strumento materiale in suo possesso, ossia il lettore, all'interno del quale va introdotta la carta di pagamento a microchip, pure in suo possesso. Egli deve inoltre digitare diversi codici, ora sul lettore, ora nell'apposito spazio sulla schermata che compare sul computer accedendo al servizio per il compimento di operazioni on line. Due di detti codici sono generati (si ha ragione di ritenere, casualmente e con modalità "usa e getta") uno dal sistema e uno dal lettore. Dal tipo di sistema adottato discende la presunzione, certamente grave e rilevante, che il cliente non avesse viceversa compiutamente custodito i dispositivi personali necessari per l'utilizzo del sistema di pagamento, con negligenza che si presenta rilevante*». Cfr. anche, ABF, Coll. Roma, decisione n. 2568 del 25 novembre 2011, su https://www.arbitrobancariofinanziario.it/decisioni/categorie/Centrale%2520rischi%2520finanziari%2520private/Segnalazioni%2520illegittime/Dec-20111125-2568%20.pdf e Coll. Milano, decisione n. 1462 del 9 ottobre 2012, su
https://www.arbitrobancariofinanziario.it/decisioni/categorie/Conto%2520corrente%2520bancario%2520e%2520postale/Banca%2520on%2520line/Dec-20120509-1462.pdf.
[45] Cfr. ABF, Coll. Roma, decisione n. 2264 del 28 giugno 2012, su https://www.arbitrobancariofinanziario.it/decisioni/categorie/Conto%2520corrente%2520bancario%2520e%2520postale/Banca%2520on%2520line/Dec-20120628-2264.pdf: «*Ora, se è indubitabile che il prelievo abusivo di fondi sul conto del cliente sia avvenuto per effetto di un atto di pirateria informatica, questo Collegio non può non osservare che la messa a disposizione dell'innovativo strumento di generazione della password non può essere*

considerata di per sé prova (presuntiva) della violazione degli obblighi di custodia in senso lato gravanti sul cliente; d'altro canto, resterebbe da provare che la ricorrente, per il solo fatto di aver subìto un attacco informatico, abbia tenuto una condotta gravemente negligente; in altri termini, è da dimostrare che l'attacco informatico ai danni della postazione del cliente sia riconducibile ad una sua condotta gravemente omissiva e negligente». Cfr. anche, ABF, Coll. Roma, decisione n. 2660 del 30 luglio 2012, su https://www.arbitrobancariofinanziario.it/decisioni/categorie/Conto%2520corrente%2520bancario%2520e%2520postale/Banca%2520on%2520line/Dec-20120730-2660.pdf e decisione n. 1910 del 6 giugno 2012, su https://www.arbitrobancariofinanziario.it/decisioni/categorie/Conto%2520corrente%2520bancario%2520e%2520postale/Banca%2520on%2520line/Dec-20120606-1910.pdf.

[46] Cfr. ABF, Coll. Napoli, decisione n. 3192 dell'8 ottobre 2012, su https://www.arbitrobancariofinanziario.it/decisioni/categorie/Conto%2520corrente%2520bancario%2520e%2520postale/Banca%2520on%2520line/Dec-20121008-0003192.pdf.

[47] Cfr. ABF, Coll. Roma, decisione n. 1910 del 6 giugno 2012, cit.: «*Ed infatti, da un punto di vista fattuale, va rilevato che l'intrusione non autorizzata del malware nel sistema di home banking, lungi dall'essere causata dal comportamento del cliente ed a lui addebitabile, potrebbe derivare da un insufficiente grado di protezione del sistema informatico e del servizio offerto dall'intermediario, come nella specie lamentato dal correntista. Peraltro, costituisce ormai un dato di comune esperienza che i codici personali di accesso ai sistemi di home banking possono essere catturati da terzi non autorizzati anche in assenza di comportamenti negligenti da parte del cliente che quei codici è tenuto diligentemente a custodire. Nel caso di specie, merita rilievo la circostanza - pacifica tra le parti – che fossero state rilevate diverse operazioni di truffa informatica a carico dei clienti della Banca e che la stessa non appare avere approntato alcun immediato rimedio volto a garantire la sicurezza dei clienti*».

[48] Cfr. ABF, Coll. Coordinamento, decisione n. 3498 del 26 ottobre 2012, cit.

[49] Cfr. ABF, Coll. Coordinamento, decisione n. 3498 del 26 ottobre 2012, cit.: «*Il principio operativo di tale meccanismo di intrusione viene definito man-in-the-browser a significare l'interposizione che questo genere di malware è in grado di operare fra il sistema centrale dell'intermediario e il singolo utente. Nella sua massima espressione di efficienza aggressiva, il programma malevolo, una volta annidatosi in un certo numero di computer, genera quella che in gergo suole definirsi una botnet, ossia per l'appunto una rete di macchine ugualmente infettate dallo stesso virus. Il malware – riconducibile alla più ampia categoria dei cc.dd. trojan ("cavalli di Troia") e dotato di*

sofisticate capacità di elusione dei migliori antivirus, si annida in modo silenzioso nel computer della vittima, senza creare alcun malfunzionamento o alterazione del sistema tali da attrarre l'attenzione dell'utente. Il malware resta perfettamente "in sonno" attivandosi solo nel momento in cui l'utente si colleghi ad un sito finanziario compreso tra quelli che il programma abbia posto nel mirino (targeted banks). In quel preciso istante il malware si risveglia ed entra in azione captando il collegamento dell'utente e propinandogli una pagina-video esattamente identica a quella che l'utente è abituato a riconoscere in sede di accesso regolare al sito del proprio intermediario. L'unica differenza, obiettivamente impercettibile ad un pur scrupoloso utente, è la stringa di descrizione della pagina che, a differenza di quella originale, reca un prefisso di accesso, (c.d. protocollo di trasferimento ipertestuale Hyper Textual Transfer Protocol) "http" e non già "https" (dove la "s" finale sta per secured, protetto). Ignaro dell'intervenuta sostituzione della pagina, l'utente è indotto a ritenere di trovarsi nel normale ambiente sicuro in cui normalmente egli opera. A quel punto il malware attiva una finestra a modulo, che pare sempre provenire dal sito dell'intermediario, in cui si trova (crede di trovarsi) l'utente, ove è richiesta una conferma di sicurezza con l'invito a compilare i campi del modulo con i propri dati e il codice generato dal dispositivo OTP: procedura che gli intermediari stessi talora attivano per controlli di sicurezza (specie come quando, nel caso in esame, l'accesso abbia luogo da una macchina diversa da quella abitualmente utilizzata dall'utente e come tale segnalata al server della banca da un differente indirizzo di provenienza: c.d. IP, Internet Protocol), il che rafforza nell'utente il convincimento della piena regolarità della situazione e della normalità del controllo automaticamente disposto dal sistema. L'utente, con ciò doppiamente ingannato, compila quindi i campi del modulo che il malware prontamente trasmette all'intruso. Questi, così callidamente interpostosi nell'operazione, ha modo di captare tutti i fattori di autenticazione e utilizzarli in tempo reale, nel mentre l'utente viene ulteriormente ingannato da un messaggio di attesa, che, qualche minuto dopo, si conclude con la segnalazione dell'impossibilità di procedere all'operazione e con l'invito a ritentare in un secondo momento».

[50] Cfr. ABF, Coll. Coordinamento, decisione n. 3498 del 26 ottobre 2012, cit: «*[...] L'unica differenza consta, come di è detto, nell'acronimo del protocollo di trasferimento, individuato come un normale "http" e non già come un "https" protetto. Ma va da sé che una simile variazione, che compare solo nella stringa di intestazione della video schermata mischiata ad almeno cinquanta o sessanta ulteriori caratteri, barre e altri segni di punteggiatura informatica, sfugge normalmente all'attenzione di chiunque si accosti alla pagina di un sito bancario per compiere un'operazione, dunque in un momento in cui l'attenzione dell'utente è concentrata sul contenuto della schermata e non*

certo sugli incomprensibili codici che la circondano e che fanno parte del normale apparato di contorno anche delle innocue consultazioni in rete».
[51] Cfr. ABF, Coll. Coordinamento, decisione n. 3498 del 26 ottobre 2012, cit.: «*[...] Colpevole in quanto egli è portato a comunicare le proprie credenziali di autenticazione al di fuori del circuito operativo dell'intermediario, e tanto più colpevole si rivela quell'atto di ingenuità quanto più si consideri che tali forme di "accalappiamento" possono dirsi ormai note al pur non espertissimo navigatore di internet*».
[52] In questo senso è chiarissima la decisione del Collegio di Coordinamento più volte citata, la quale è utile nel tracciare il discrimine anche tra nuove e vecchie tecniche di *Phishing*.
[53] Cfr. ABF, Coll. Milano, decisione n. 8364 del'11 dicembre 2014, su https://www.arbitrobancariofinanziario.it/decisioni/categorie/Carte%2520di%2520credito/Utilizzo%2520fraudolento/Dec-20141211-8364.PDF.
[54] Cfr. ABF, Coll. Roma, decisione n. 3262 del 16 maggio 2014, su https://www.arbitrobancariofinanziario.it/decisioni/categorie/Conto%2520corrente%2520bancario%2520e%2520postale/Banca%2520on%2520line/Dec-20140516-3262.PDF: «*[...] Il phishing operato tramite semplice mail deve ritenersi fenomeno ormai del tutto noto, tanto che qualunque utente dotato di quella normale avvedutezza e prudenza che si richiede a chi utilizzi servizi di home banking dovrebbe essere in grado di sottrarsi all'inganno*».
[55] Tale misura cautelativa è adottabile in forza del dettato dell'art. 6, d.lgs. n. 11/2010.
[56] In materia di buona fede cfr. A. D'Angelo, *La buona fede,* in Bessone (a cura di), *Tratt. dir. priv.,* vol. XIII, Torino, 2004, p. XIV. Cfr. anche ID., *Il contratto in generale. La Buona fede*, Torino, 2004; P.G. Monateri, *Ripensare il contratto: verso una visione antagonista del contratto, in Riv. dir. civ.*, 2003, I, p. 408; G. Sicchiero, *Buona fede e rischio contrattuale,* in *Contratto e impresa*, 2006, p. 919; M. Bessone, *Adempimento e rischio contrattuale*, cit.
[57] Sulle criticità derivanti dall'espansività del principio di buona fede si veda M. Bessone, *Adempimento e rischio contrattuale*, cit.; G. Sicchiero, *Buona fede e rischio contrattuale*, cit.
[58] Cfr. Cass., 10 novembre 2010, n. 22819, in *Vita not.*, 2011, p. 357; Cass., 22 gennaio 2009, n. 1618, cit.: «*Il principio di correttezza e buona fede nell'esecuzione del contratto, espressione del dovere di solidarietà fondato sull'art. 2 Cost., impone a ciascuna delle parti del rapporto obbligatorio di agire in modo da preservare gli interessi dell'altra e costituisce un dovere giuridico autonomo a carico di entrambe, a prescindere dall'esistenza di specifici obblighi contrattuali o di quanto espressamente stabilito da norme di legge, ne consegue che la sua violazione costituisce di per sé inadempimento e può comportare l'obbligo di risarcire il danno che ne sia derivato*». Cass., 27

settembre 2001, n. 12093, in *Vita not.*, 2001, p. 1309; Cass., 16 novembre 2000, n. 14865, in *Corr. giur.*, 2001, p. 762.

[59] Cfr. in particolare ABF, Coll. Roma, decisone n. 1341 del 12 marzo 2013, su https://www.arbitrobancariofinanziario.it/decisioni/categorie/Bancomat%2520e%2520carte%2520di%2520debito/Blocco/Dec-20130312-1341.pdf. Inoltre, secondo una recente ricostruzione dottrinale, la misura "cautelare" del blocco della carta può essere letta alla luce del principio generale di autotutela del contraente, con precipuo riferimento alla sospensione dell'esecuzione, regolata dall'art. 1461 c.c., che consente al creditore di far fronte al rischio di insolvenza della controparte, con riferimento a prestazioni che dovranno essere adempiute in un secondo momento (gli obblighi di pagamento a carico dell'utente.). Per questa ricostruzione cfr. Aa.Vv., *La nuova disciplina dei servizi di pagamento,* Torino, 2011.

[60] Vedi ABF, Coll. Roma, decisione n. 1312 del 10 novembre 2010, su https://www.arbitrobancariofinanziario.it/decisioni/categorie/Assegno%2520bancario%2520e%2520postale/Protesto/Dec-20101110-1312.pdf: «*Allorché la misura non sia stata comunicata tempestivamente alla ricorrente, con indicazione dei motivi giustificatici e dei contenuti della misura deve ritenersi che il comportamento della banca non risponda ai canoni della trasparenza e della buona fede che è tenuta ad osservare e che si concretano in un dovere giuridico espressione di un generale principio di solidarietà sociale, che, nell'ambito contrattuale, implica un obbligo di reciproca lealtà di condotta che deve presiedere sia all'esecuzione del contratto che alla sua formazione ed interpretazione, accompagnandolo in definitiva in ogni sua fase*».

[61] Cfr. G. Villa, *Danno e risarcimento contrattuale*, cit.

[62] Cfr. R. Scognamiglio, *Il danno morale (Contributo alla teoria del danno extracontrattuale),* in *Riv. dir. civ.*, 1937, p. 313.

[63] Cfr., M. Costanza, *Danno non patrimoniale e responsabilità contrattuale,* in *Riv. crit. dir. priv.*, 1987, p. 127; C. Scognamiglio, *Il danno non patrimoniale contrattuale*, in Mazzamuto (a cura di), *Il contratto e le tutele*, Torino, 2002. Per un approfondito studio del problema cfr. inoltre V. Zeno Zencovich, *Danni non patrimoniali e inadempimento,* in Visintini (a cura di), *Risarcimento del danno contrattuale ed extracontrattuale*, Milano, 1984; ID., *Interesse del creditore e danno contrattuale non patrimoniale,* in *Riv. dir. comm.*, 1987, I, p. 77.

[64] Parte della dottrina arrivava addirittura a escludere *in toto* la risarcibilità del danno non patrimoniale da inadempimento, sulla base della non applicabilità di tale norma in ambito contrattuale. Cfr., R. Scognamiglio, *Il danno morale (Contributo alla teoria del danno extracontrattuale),* cit.

[65] Cfr. G. P. Roma, 11 luglio 2003, in *Dir. fam.,* 2004, p. 106 per una ipotesi di danno esistenziale derivante da interruzione di una linea telefonica; G. P. Bari, 7 novembre 2003, in *Danno e resp*., 2004, p. 626 per danni derivanti dal ritardo di un volo aereo e G. P. Capaccio, 20 ottobre 2004, citata da G. Villa, *Danno e risarcimento contrattuale*, cit., p. 976, sub nota 138.

[66] Cfr. C. Cost., 11 luglio 2003, n. 233, in *Giur. it.* 2004, p. 1129: «*Può dirsi oramai superata la tradizionale affermazione secondo la quale il danno non patrimoniale riguardato dall'art. 2059 c.c. si identificherebbe con il cosiddetto danno morale soggettivo, dovendosi adottare un'interpretazione costituzionalmente orientata dell'art. 2059 c.c., tesa a ricomprendere nell'astratta previsione della norma ogni danno di natura non patrimoniale derivante da lesione di valori inerenti alla persona: e, dunque, sia il danno morale soggettivo, inteso come transeunte turbamento dello stato d'animo della vittima; sia il danno biologico in senso stretto, inteso come lesione dell'interesse, costituzionalmente garantito, all'integrità psichica e fisica della persona, conseguente ad un accertamento medico (art. 32 cost.); sia, infine, il danno (spesso definito in dottrina ed in giurisprudenza come esistenziale) derivante dalla lesione di (altri) interessi di rango costituzionale inerenti alla persona*».

[67] Cfr. Cass., 12 maggio 2003, n. 7281, in *Foro amm., CDS,* 2003, p.*1531.*

[68] Cfr. Cass., Sez. un., 11 novembre 2008, n. 26973, in *Foro it*., 2009, c. 120.

[69] Cfr. Trib. Salerno, 11 febbraio 2014, n. 464, *inedita*: «*Il danno non patrimoniale è risarcibile anche in presenza di un rapporto di natura contrattuale tra le parti, ove la prestazione promessa risulti finalizzata parimenti alla tutela di un interesse pertinente o connaturato ad un diritto inviolabile della persona, con l'avviso che se l'inadempimento dell'obbligazione determina, oltre alla violazione degli obblighi di rilevanza economica assunti con il contratto, anche la lesione di un diritto inviolabile della persona del creditore, la tutela risarcitoria del danno non patrimoniale potrà essere versata nell'azione di responsabilità contrattuale, senza ricorrere all'espediente del cumulo di azioni*»."

[70] Cfr. ABF, Coll. Milano, decisione n. 169 del 26 marzo 2010, su https://www.arbitrobancariofinanziario.it/decisioni/categorie/Bancomat%2520e%2520carte%2520di%2520debito/Utilizzo%2520fraudolento/Dec-20100326-169.pdf: «*Non sono meritevoli di tutela risarcitoria, invocata a titolo di danno esistenziale, i pregiudizi consistenti in disagi, fastidi, disappunti, ansie ed ogni altro tipo di insoddisfazione concernente gli aspetti più disparati della vita quotidiana che ciascuno conduce nel contesto sociale Al di fuori dei casi determinati dalla legge ordinaria, solo il diritto inviolabile della persona concretamente individuato è fonte di responsabilità risarcitoria non*

patrimoniale».
[71] Cfr. ABF, Coll. Milano, decisione n. 3147 del 7 giugno 2013, su https://www.arbitrobancariofinanziario.it/decisioni/categorie/Carte%2520di%2520credito/Tipologia/Dec-20130607-3147.pdf. Cfr. anche ABF, Coll. Roma, decisione n. 1879 dell'8 aprile 2013, su https://www.arbitrobancariofinanziario.it/decisioni/categorie/Conto%2520corrente%2520bancario%2520e%2520postale/Banca%2520on%2520line/Dec-20130408-1879.pdf.
[72] Cfr., ABF, Coll. Milano, decisione n. 6390 del 9 dicembre 2013, su https://www.arbitrobancariofinanziario.it/decisioni/categorie/Carte%2520di%2520credito/Blocco/Dec-20131209-6390.PDF.

Consiglio di Stato, Sez. III, 5 febbraio 2015, n. 582.

Comunicazioni elettroniche – Sanzioni amministrative e depenalizzazione – Obblighi informativi – Richiesta di informazioni – Informativa Economica di Sistema (IES) – Sistema Integrato delle Comunicazioni (SIC).

Non appare dubitabile l'ascrivibilità dei dati relativi al complesso dei ricavi da abbonamenti pay tv - ivi compresi quelli attinenti alla diffusione a pagamento di contenuti non editi direttamente dalla società interessata - entro il perimetro delle informazioni che l'Autorità per le garanzie nelle comunicazioni è legittimata a richiedere agli operatori televisivi che risultano, pertanto, obbligati alla trasmissione. (Massima redazionale)

REPUBBLICA ITALIANA
IN NOME DEL POPOLO ITALIANO
Il Consiglio di Stato
in sede giurisdizionale (Sezione Terza)
ha pronunciato la presente
SENTENZA

sul ricorso numero di registro generale 8475 del 2014, proposto da:
Autorita' per le garanzie nelle comunicazioni, rappresentata e difesa per legge dall'Avvocatura Generale dello Stato, domiciliata in Roma, Via dei Portoghesi, 12;

contro

Sky Italia Srl, rappresentata e difesa dall'avv. Ottavio Grandinetti, con domicilio eletto presso Ottavio Grandinetti in Roma, Via Caroncini N. 2;

per la riforma

della sentenza del T.A.R. LAZIO - ROMA: SEZIONE I n. 05863/2014, resa tra le parti, concernente informativa sui dati economici annuali che i soggetti operanti nel settore dei media sono tenuti ad inviare - irrogazione sanzione amministrativa pecuniaria;
Visti il ricorso in appello e i relativi allegati;
Visto l'atto di costituzione in giudizio di Sky Italia Srl;
Viste le memorie difensive;
Visti tutti gli atti della causa;
Relatore nell'udienza pubblica del giorno 15 gennaio 2015 il Cons. Carlo Deodato e uditi per le parti gli avvocati Grandinetti e dello Stato Varrone F.;

Svolgimento del processo

Con la sentenza impugnata il Tribunale amministrativo regionale per il Lazio ha annullato, in accoglimento del ricorso e dei motivi aggiunti proposti da Sky Italia s.r.l., le delibere con cui l'Autorità per le Garanzie nelle Comunicazioni (d'ora innanzi AGCom) aveva richiesto alla società ricorrente i dati economici relativi alla c.d. "Informativa Economica di Sistema" (d'ora innanzi IES), per gli anni 2010, 2011 e 2012, ed aveva, poi, irrogato alla stessa la sanzione pecuniaria di Euro 10.320,00, per aver comunicato solo il valore degli introiti strettamente riferibili ai contenuti editi direttamente da Sky, omettendo, in violazione della richiesta della stessa Autorità, di trasmettere l'importo complessivo dei ricavi relativi agli abbonamenti *pay tv*.
Avverso la predetta decisione proponeva appello l'AGCom, contestandone la correttezza, insistendo nel sostenere la riconducibilità alla IES di tutti i ricavi riferibili agli abbonamenti *pay tv* della piattaforma Sky, a prescindere dalla responsabilità editoriale dei programmi ivi contenuti, e concludendo per la riforma della statuizione gravata e per il conseguente rigetto del ricorso proposto in primo grado da Sky Italia s.r.l.
Resisteva quest'ultima, eccependo l'inammissibilità dell'appello dell'Autorità, contestandone, comunque, la fondatezza, proponendo appello incidentale avverso l'omessa pronuncia sul terzo atto per motivi aggiunti (con cui era stata impugnata la delibera AGCom n.665/13/CONS del 28 novembre 2013) e sulla domanda di restituzione della somma pagata in ottemperanza alla delibera con cui era stata irrogata la sanzione pecuniaria (annullata dal T.A.R.), riproponendo alcune censure non esaminate o assorbite dalla decisione di primo grado e concludendo per il rigetto dell'appello principale, per l'accoglimento di quello incidentale e per la coerente riforma parziale della statuizione gravata.
Il ricorso veniva trattenuto in decisione alla pubblica udienza del 15 gennaio 2015.

Motivi della decisione

1.- E' controversa l'ascrivibilità dell'intero volume dei ricavi da abbonamenti pay tv della piattaforma Sky entro il perimetro della IES (come preteso da AGCom e contestato da Sky Italia s.r.l.).
I giudici di prima istanza hanno negato la fondatezza della pretesa conoscitiva dell'Autorità e hanno giudicato dovuti i soli dati pertinenti ai ricavi riconducibili alla commercializzazione dei programmi editi da Sky Italia s.r.l. e nei confronti dei quali è, dunque, configurabile una responsabilità editoriale diretta della stessa società.
L'AGCom critica tale convincimento ed insiste nel sostenere che la normativa che regola la materia affida ad essa il potere di richiedere agli operatori

televisivi tutti i dati economici necessari alla conoscenza del mercato delle televisioni, ivi compresi quelli attinenti alla diffusione a pagamento di contenuti non editi direttamente dalla società interessata.
Sky Italia s.r.l. contesta tale tesi e ribadisce l'assunto per cui quest'ultima tipologia di ricavi esula da quelli acquisibili con la procedura controversa.
2.- Una compiuta disamina della questione appena sintetizzata postula una preliminare ricognizione della disciplina positiva che regola l'attività conoscitiva dell'AGCom nella specie dibattuta.
L'art.1, commi 28 e 29, del D.L. 23 ottobre 1996 , n.545 (convertito nella L. 23 dicembre 1996, n. 650) ha affidato al Garante per la radiodiffusione e l'editoria il compito di determinare e di acquisire, dagli operatori del settore di mercato affidato al suo monitoraggio, i dati contabili ed extracontabili ritenuti rilevanti ai fini dell'espletamento delle sue funzioni istituzionali.
Con decreto dell'11 febbraio 1997 il Garante per la radiodiffusione e l'editoria ha regolato le modalità e i contenuti delle suddette comunicazioni di sistema.
L'art.2, comma 20, lett.a), L.14 novembre 1995, n. 481 (che detta norme generali per le Autorità di regolazione dei servizi di pubblica utilità) ha attribuito alle Autorità il potere di chiedere "ai soggetti esercenti il servizio, informazioni e documenti sulle loro attività".
L'art.1, comma 6, lett. c), n.7, della L. 31 luglio 1997, n. 249 (istitutiva dell'Autorità per le garanzie nelle comunicazioni) ha stabilito che l'Autorità "verifica i bilanci ed i dati relativi alle attività ed alla proprietà dei soggetti autorizzati o concessionari del servizio radiotelevisivo", mentre i commi 29 e 30 della medesima disposizione prevedono le sanzioni applicabili agli operatori che non adempiono correttamente alle richieste informative dell'Autorità.
La stessa legge ha trasferito all'Autorità per le garanzie nelle comunicazioni le funzioni precedentemente assegnate al Garante per la radiodiffusione e l'editoria.
L'AGCom ha regolato, in via astratta, l'informativa economica di sistema con le delibere n.129/02/CONS, n.116/10/CONS e n.303/11/CONS, mediante la determinazione dei soggetti tenuti alle relative comunicazioni, dell'oggetto delle stesse e delle modalità della loro trasmissione all'Autorità.
L'art.43 D.Lgs. 31 luglio 2005 , n.177, testo unico dei servizi di media audiovisivi e radiofonici (d'ora innanzi TUSMAR), ha affidato all'AGCom il compito di verificare l'esistenza di posizioni dominanti nel sistema integrato delle comunicazioni e di adottare le determinazioni necessarie ad eliminarle o ad impedirne la formazione.
3.- Così riassunto il sistema di regole alla cui stregua dev'essere giudicata la legittimità delle delibere impugnate in primo grado, occorre procedere

all'esame degli appelli, principiando dallo scrutinio dell'eccezione di inammissibilità di quello principale, formulata da Sky Italia s.r.l.
Sostiene, in sintesi, la società resistente che l'Autorità appellante avrebbe violato il divieto codificato all'art. 104 c.p.a., là dove ha fondato l'appello su argomentazioni difensive del tutto nuove (rispetto alle procedure amministrative contestate e al giudizio di primo grado) o, addirittura, configgenti con le tesi difensive sostenute dinanzi al T.A.R.
L'eccezione è infondata e va disattesa.
Il divieto di ius novorum in appello, infatti, se rettamente inteso, implica il divieto di ampliare l'oggetto della domanda giudiziale proposta in prima istanza (Cons. St., sez. VI, 4 luglio 2012, n.3897), sia quanto alla causa petendi (mediante la formulazione di censure nuove in appello) che al petitum (mediante la proposizione di richieste ulteriori rispetto a quelle cristallizzate nel gravame originario).
Il principio in questione deve intendersi riferito all'atto amministrativo impugnato in primo grado e non alla decisione appellata, con l'ulteriore conseguenza che il divieto di proporre nuove domande ed eccezioni non riguarda le difese non articolate in prime cure dall'Amministrazione resistente (Cons. St., sez. VI, 24 gennaio 2011, n.479), che, quindi, possono trovare ingesso, senza alcuna preclusione, nel giudizio di secondo grado.
4.- Passando all'esame del merito dell'appello principale, si deve dichiarare inammissibile, per carenza di interesse, il primo motivo di impugnazione, con cui si assume l'utilizzo, nella motivazione della decisione gravata, di argomentazioni tra loro contraddittorie (in particolare tra quella che valorizza l'esegesi finalistica della normativa di riferimento e quella che si fonda sulla lettera delle disposizioni che regolano la materia), atteso che, quand'anche si ravvisasse tale conflitto logico (ma non è cosi, trattandosi di argomentazioni tra loro compatibili e non antinomiche), la decisione non potrebbe, per ciò solo, essere riformata o annullata, ma il predetto rilievo comporterebbe un nuovo esame della legittimità degli atti impugnati nel presente grado di giudizio, in virtù dell'effetto devolutivo dell'appello.
5.- Con il secondo motivo di appello, l'AGCom critica il convincimento, assunto a sostegno della decisione impugnata, secondo cui una corretta esegesi della normativa di riferimento impediva all'Autorità di richiedere dati economici relativi alla commercializzazione di contenuti non riferibili alla responsabilità editoriale diretta di Sky Italia s.r.l.
L'Autorità appellante assume, a sostegno della censura, che, al contrario, il complesso delle disposizioni che regolano le sue funzioni la autorizzava a richiedere a Sky Italia s.r.l. tutti i dati relativi ai ricavi degli abbonamenti pay tv, a prescindere dalla riferibilità editoriale alla medesima società dei programmi trasmessi nella relativa piattaforma.

5.1- La tesi è fondata.
L'esegesi della normativa di riferimento, preferita dal T.A.R., che limita l'oggetto della IES ai soli contenuti editi direttamente da Sky Italia s.r.l. si rivela, infatti, del tutto inaccettabile, siccome chiaramente configgente con le disposizioni attributive del potere nella specie esercitato dall'Autorità, sia quanto all'ambito applicativo soggettivo sia in ordine a quello oggettivo.
5.2- In merito al novero dei soggetti tenuti all'informativa in questione, si rileva che la semplice lettura dell'art.1, comma 28, del D.L. n. 545 del 1996 (da valersi quale la fonte attributiva del potere nella specie scrutinato, e, quindi, quale paradigma della sua legittimità) e dei coerenti regolamenti con cui l'Autorità ha disciplinato in via generale la IES (e, segnatamente, l'art.1 delle Delib. n.129 del 2002, Delib. n.116/ del 200 e Delib. n.303 del 2011) rivela l'univoca volontà di assoggettare agli obblighi di comunicazione in questione tutte le imprese che operano nel settore dei media.
Il catalogo degli operatori ivi contenuto, infatti, risulta comprensivo di tutte le tipologie di soggetti legittimate ad operare, a qualsiasi titolo, nel mercato, per quanto qui interessa, delle produzioni e delle trasmissioni radiotelevisive.
Che la volontà del legislatore fosse quella di costruire un meccanismo informativo idoneo a consegnare all'Autorità i dati economici riferibili a tutti gli operatori, senza alcuna esclusione, risulta, poi, confermato dal medesimo art.1, comma 28, D.L. n. 545 del 1996 cit. là dove, dopo aver catalogato tutte le tipologie di imprese soggette agli obblighi in questione, aggiunge "o che, comunque, esercitano in qualsiasi forma e con qualsiasi tecnologia, attività di radiodiffusione sonora o televisiva", con ciò manifestando chiaramente l'intenzione (peraltro coerente con le finalità della disposizione, agevolmente identificabili nell'esigenza di consentire all'Autorità di regolazione una conoscenza completa delle dinamiche economiche del mercato) di comprendere, nel proprio ambito applicativo soggettivo, ogni impresa autorizzata ad operare nel settore (per quanto qui interessa) delle televisioni.
In particolare, la dizione "in qualsiasi forma e con qualsiasi tecnologia" manifesta l'univoca volontà del legislatore di estendere gli obblighi informativi alla totalità degli operatori televisivi e di precludere all'interprete qualsivoglia opzione ermeneutica riduttiva della sua latitudine precettiva.
Non vale, quindi, dibattere sulla qualificazione di Sky Italia s.r.l. come "fornitore di servizi media audiovisivi", posto che la normativa di riferimento (ivi compresi i regolamenti emanati dall'AGCom e non impugnati da Sky Italia s.r.l.) non limita gli obblighi informativi in questione ai soli "fornitori di media", ma vi comprende tutte le imprese che, a qualsiasi titolo e con qualsiasi modalità, operano nel settore delle televisioni (anche mediante la trasmissione e la commercializzazione, con il sistema degli abbonamenti pay tv, di contenuti editi da altri soggetti).

Né può attribuirsi un significato dirimente, in favore della tesi sostenuta da Sky Italia s.r.l. (e avvalorata dai primi giudici), all'omessa inclusione nel catalogo dei soggetti obbligati alla IES, per come cristallizzato all'art.1, comma 28, del D.L. n. 545 del 1996 , della figura dei "fornitori di servizi interattivi o di servizi di accesso condizionato", atteso che quest'ultima tipologia di operatori (che non aveva ancora assunto rilievo nel mercato dei media nel 1996) va, comunque, ricompresa nella clausola generale e aperta, sopra ricordata e contenuta nella medesima disposizione sopra citata, e risulta, in ogni caso, correttamente inclusa nelle delibere dell'Autorità che hanno disciplinato, in via generale, le modalità applicative della IES (oltre che nelle coerenti istruzioni alla compilazione dei relativi moduli), perimetrandone, altresì, l'ambito applicativo soggettivo (proprio in attuazione della norma in esame).
Non può, in conclusione, dubitarsi dell'ascrivibilità di Sky Italia s.r.l. al catalogo delle imprese soggettivamente obbligate a trasmettere la IES all'AGCom.
5.3- Quanto alla latitudine oggettiva dei dati economici acquisibili dall'Autorità, invece, basti rilevare, anche qui, che la formulazione in termini generali ("i dati contabili ed extracontabili, nonché le notizie") e senza alcuna eccezione testuale dell'oggetto degli obblighi di comunicazione in questione (per come definito nella disposizione attributiva del potere) impedisce qualsivoglia esegesi limitativa dei contenuti della IES.
Non solo, ma anche le citate disposizioni contenute nelle leggi che regolano l'attività (in via generale) delle Autorità di regolazione dei servizi di pubblica utilità e (in particolare) dell'AGCom confortano la suddetta lettura, nella misura in cui assegnano alle stesse il potere di acquisire, dagli operatori, tutte le informazioni (anche economiche) necessarie all'espletamento delle funzioni di regolazione e di vigilanza (che presuppongono una compiuta conoscenza del mercato di riferimento) e di sanzionare le imprese inadempimenti.
Ragionando come vorrebbe Sky Italia s.r.l. (e come ritenuto dai primi giudici), e, cioè, escludendo dalla IES i ricavi riferibili alla diffusione di programmi non riconducibili alla responsabilità diretta di Sky Italia s.r.l., si perverrebbe all'inaccettabile conseguenza di precludere la conoscenza di un segmento rilevante del mercato, che resterebbe, quindi, sconosciuto alla stessa, con un'evidente e inaccettabile menomazione delle possibilità conoscitive che, invece, la normativa di riferimento ha voluto assicurare, in misura integrale, alle Autorità di regolazione.
Né vale, ancora, contestare la qualificazione dei ricavi relativi agli abbonamenti pay tv, per la parte relativa a contenuti non riferibili alla responsabilità editoriale diretta di Sky Italia s.r.l., come "servizi di media audiovisivi", secondo la definizione del TUSMAR, posto che, in coerenza con la lettura della normativa di riferimento sopra indicata come corretta, l'oggetto della IES va

esteso a tutti i dati economici astrattamente e genericamente riconducibili all'attività televisiva.
E non può attribuirsi un'efficacia limitativa dei dati dovuti alla menzione, nella rubrica dei modelli IES diramati dall'Autorità, della sola voce "servizi di media audiovisivi", posto che tale indicazione serviva solo alla perimetrazione (in senso atecnico) dell'ambito dell'informativa e che alla stessa non può, in alcun modo, assegnarsi una portata riduttiva dei contenuti della comunicazione, anche in considerazione che nella declinazione della relativa voce del modello risultano compresi proprio i ricavi da abbonamenti a pagamento sulla piattaforma satellitare.
Ne consegue che non appare dubitabile l'ascrivibilità dei dati relativi al complesso dei ricavi da abbonamenti pay tv entro il perimetro delle informazioni che l'Autorità era legittimata a richiedere a Sky Italia s.r.l. e che quest'ultima era obbligata a trasmettere.
5.4- Così verificata la coerenza delle delibere gravate in prima istanza con i paradigmi legali di riferimento, occorre esaminare le censure dedotte contro di esse in primo grado, non esaminate dal T.A.R. e ritualmente riproposte da Sky Italia s.r.l. ai sensi dell'art.101, comma 2, c.p.a.
5.4.1- Vanno, innanzitutto, disattese le censure (rubricate sub B1 e B2 nell'appello incidentale) con cui l'appellante incidentale insiste nel contestare, con una molteplicità di prospettazioni censorie, la propria qualificazione come "fornitore di servizi media audiovisivi" e la catalogazione dei dati economici richiesti nell'ambito della IES come "servizi di media audiovisivi" (anche ai fini della configurazione della violazione colpita con la sanzione pecuniaria), atteso che le pertinenti argomentazioni difensive sono già state esaminate e giudicate infondate nella parte della motivazione riferita all'accoglimento dell'appello principale (là dove si è chiarito che l'Autorità ha legittimamente richiesto a Sky Italia s.r.l. i dati pertinenti alla totalità dei ricavi percepiti per effetto degli abbonamenti alla piattaforma a pagamento).
5.4.2- Le censure rubricate sub B3 vanno, invece, dichiarate inammissibili, in quanto, dalla mera lettura della censura, non appare chiara la consistenza dei motivi riproposti contro la delibera n.303/11/CONS, non potendosi giudicare sufficiente, ai fini della valida riproposizione degli stessi, un richiamo alla sintetica, ma carente, rubrica dell'atto.
5.4.3- In ordine ai motivi rubricati sub B4, con cui si contesta l'attribuzione a Sky Italia s.r.l. dei ricavi riferiti a fornitori di "servizi media audiovisivi" terzi, è sufficiente rilevare che, ferma restando la correttezza dell'acquisizione dei relativi dati economici nell'ambito della IES, competerà poi all'Autorità imputare correttamente i pertinenti introiti ai diversi operatori coinvolti nell'attività di produzione e vendita di quei programmi, nell'abito dell'analisi delle dimensioni economiche del mercato, sicchè, nella fase procedurale in

questione, non appare ravvisabile alcuna violazione della sfera giuridica dell'appellante incidentale.
5.4.4- In merito, da ultimo, alle censure intese a contestare la legittimità della sanzione pecuniaria, si osserva, per un verso, che la misura della stessa (Euro 10.320,00, rispetto agli estremi, previsti dall'art.1, comma 30, L. n. 249 del 1997 , di Euro 516,00, minimo, e Euro 103.300,00, massimo) appare del tutto proporzionata alla gravità dell'inadempimento (nella misura in cui ha sottratto all'Autorità la conoscenza di una parte rilevante del mercato) e, per un altro, che la pretesa erroneità dell'individuazione della disposizione di riferimento (art.1, comma 30, L. n. 249 del 1997 , anziché art.51 del TUSMAR) si rivela del tutto irrilevante, con la conseguenza del difetto di interesse alla sua denuncia (e, quindi, della declaratoria dell'inammissibilità del relativo motivo), nella misura in cui la norma che avrebbe dovuto essere applicata (secondo l'appellante incidentale) contempla un minimo (Euro 5.165,00) sensibilmente più alto di quello (Euro 516,00) previsto dalla disposizione erroneamente applicata.
5.4.5- I motivi riproposti in appello da Sky Italia s.r.l. vanno, in definitiva, dichiarati inammissibili o respinti.
6.- L'accoglimento dell'appello principale implica, inoltre, l'improcedibilità dell'appello incidentale, atteso che Sky Italia s.r.l. ha perso interesse a contestare l'omessa pronuncia sia sul terzo atto di motivi aggiunti (nella misura in cui si rivolge a una delibera dal contenuto precettivo e dal fondamento identici a quelli delle delibere già giudicate immuni dai vizi ascritti a loro carico) sia sulla domanda di restituzione della somma versata in esecuzione della sanzione pecuniaria (nella misura in cui la medesima postula logicamente l'annullamento di quest'ultima).
Va dichiarato improcedibile anche il terzo motivo dell'appello incidentale, con cui si contesta l'asserita implicita reiezione del motivo con cui si sosteneva la differente fonte normativa del potere attinente alla IES, rispetto a quello su cui si fonda l'accertamento del SIC, atteso che le disposizioni legislative invocate come corrette da Sky Italia s.r.l. (e, cioè, quelle contenute nel D.L. n. 545 del 1996 , convertito nella L. n. 650 del 1996) sono proprio quelle in relazione alle quali è stata sopra giudicata la conformità delle delibere adottate dall'AGCom.
7- Alle considerazioni che precedono conseguono, in definitiva, l'accoglimento dell'appello principale, la declaratoria dell'improcedibilità di quello incidentale e, in riforma della decisione impugnata, il rigetto del ricorso e dei motivi aggiunti proposti in primo grado da Sky Italia s.r.l.
8.- Le spese del doppio grado di giudizio seguono la soccombenza e vengono liquidate come in dispositivo.

P.Q.M.

Il Consiglio di Stato in sede giurisdizionale (Sezione Terza), definitivamente pronunciando sull'appello, come in epigrafe proposto, lo accoglie e, per l'effetto, in riforma della decisione appellata, respinge il ricorso di primo grado e dichiara improcedibile l'appello incidentale.
Compensa le spese del doppio grado di giudizio.
Ordina che la presente sentenza sia eseguita dall'autorità amministrativa.
Così deciso in Roma nella camera di consiglio del giorno 15 gennaio 2015 con l'intervento dei magistrati:
Gianpiero Paolo Cirillo,Presidente
Carlo Deodato,Consigliere, Estensore
Vittorio Stelo,Consigliere
Angelica Dell'Utri,Consigliere
Roberto Capuzzi, Consigliere