Sentenza, Tribunale di Reggio Emilia, Giudice Francesca Malgoni, n. 821, del 05/07/2023

REPUBBLICA ITALIANA
IN NOME DEL POPOLO ITALIANO
TRIBUNALE ORDINARIO DI REGGIO EMILIA
SEZIONE SECONDA CIVILE

Il Tribunale, in composizione monocratica, nella persona del Giudice Francesca Malgoni, ha pronunciato ex art. 281 sexies c.p.c. la seguente

SENTENZA

nella causa civile di I Grado iscritta al n. R.G. xxxx/2020
promossa da:

BANCA S.P.A.;

ATTRICE

contro

(omissis);

CONVENUTA

*

Conclusioni delle parti
All'udienza odierna le parti hanno concluso come da verbale.
Concisa esposizione delle ragioni di fatto e di diritto della decisione
BANCA ha convenuto in giudizio (omissis) esponendo:
- che la convenuta è titolare del conto corrente n. (omissis), acceso presso la filiale di Reggio Emilia, al quale è collegato il servizio di home banking denominato "smart web";
- che sul conto corrente risultano effettuati, tramite home banking, in data 12.12.2019, n. 2 bonifici dell'importo rispettivamente di € 10.000,00 ed € 1.530,00 con la seguente causale "a favore di (omissis) – all'avvocato";
- che in data 13.12.2019, (omissis), figlio della (omissis), si è recato presso la filiale e ha disconosciuto le operazioni in quanto non autorizzate;
- di avere quindi immediatamente rimborsato alla correntista la somma di € 11.532,80, oltre spese e commissioni, salvo buon fine, in ottemperanza all'art. 10 D.Lgs. 11/10, che in tali casi prevede l'obbligo per l'istituto di rifondere la somma al cliente con diritto di richiederne la restituzione qualora, all'esito di eventuali accertamenti, il rimborso risultasse non dovuto;
- di avere successivamente svolto le necessarie verifiche e accertato che la sottrazione delle somme non era in alcun modo ascrivibile alla banca, in quanto le operazioni erano state disposte a seguito di corretta autenticazione tramite i codici inseriti dalla (omissis) nel sito dell'home banking;
- che il proprio sistema di autenticazione presenta un elevato livello di sicurezza, conforme alla normativa europea e a quella interna, poiché prevede sia l'accesso al sito attraverso USER ID e PASSWORD, sia l'inserimento, per ogni operazione, di un codice usa e getta (OTP) inviato tramite SMS al numero cellulare dell'utente;
- che nel caso di specie non vi sono stati malfunzionamenti nei sistemi informatici dell'istituto;
- che quindi l'unica persona ad essere stata in possesso del codice OTP poteva essere la convenuta;
- di avere reiteratamente invitato la (omissis) alla restituzione dell'importo rimborsato, ma senza esito.
Tanto premesso, **BANCA** ha chiesto la condanna della convenuta alla restituzione delle somme accreditate, deducendo, in subordine, un concorso di colpa di quest'ultima nella misura del 90%.
Si è costituita (omissis) eccependo in via preliminare l'improcedibilità della domanda per mancato esperimento della negoziazione assistita ai sensi della L. 162/14.
Ha poi contestato l'azione proposta in fatto e in diritto deducendo:
- che il servizio smart web sul proprio conto corrente è collegato all'utenza telefonica n. (omissis)intestata al proprio figlio (omissis), da ella delegato alle operazioni sia allo sportello in filiale sia tramite, appunto, home banking;
- di non avere autorizzato le transazioni delle somme in questione;
- che infatti nella cronologia sms della predetta utenza telefonica non vi è traccia dell'invio dell'sms recante il codice OTP;

Rivista di informazione giuridica, registrata al Tribunale di Napoli al numero 12 del 05/03/2012
Registro affari amministrativi numero 8231/11
Direttore Responsabile Avv. Antonio De Simone – Direttore Scientifico Avv. Walter Giacomo Caturano

- che, dunque, si è verificata una ipotesi di frode informatica ai propri danni, di cui è tenuta a rispondere in via esclusiva la banca in base alla disciplina di cui al D.Lgs. 11/10.

Il giudice precedentemente titolare del fascicolo, verificato il mancato esperimento della mediazione obbligatoria, ne ha disposto l'instaurazione assegnando il termine di legge.

Verificato l'esito negativo del procedimento, ha concesso i termini di cui all'art. 183, comma VI c.p.c. Una volta assegnata al sottoscritto magistrato, la causa è stata istruita attraverso l'escussione del testimone (omissis) ed è stata rinviata all'udienza odierna per precisazione delle conclusioni e discussione orale ex art. 281 sexies c.p.c.

L'eccezione di improcedibilità della domanda è superata dall'instaurazione in corso di causa del procedimento di mediazione obbligatoria, conclusosi, come detto, negativamente.

Venendo al merito, in punto di diritto si premette quanto segue:
- la disciplina di riferimento è posta dagli artt. 10 e 11 D.Lgs. 10/11 - "Attuazione della direttiva 2007/64/CE, relativa ai servizi di pagamento nel mercato interno" – (come modificato dal D.Lgs. 217/18);
- l'art. 10 prevede: "1. Qualora l'utente di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento già eseguita o sostenga che questa non sia stata correttamente 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 di altri inconvenienti.
1-bis. Se l'operazione di pagamento e' disposta mediante un prestatore di servizi di disposizione di ordine di pagamento, questi ha l'onere di provare che, nell'ambito delle proprie competenze, l'operazione di pagamento e' stata autenticata, correttamente registrata e non ha subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti connessi al servizio di disposizione di ordine di pagamento prestato.
2. Quando l'utente 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, compreso, se del caso, il prestatore di servizi di disposizione di ordine di pagamento, non e' di per se' necessariamente sufficiente a dimostrare che l'operazione sia stata autorizzata dall'utente medesimo, ne' che questi abbia agito in modo fraudolento o non abbia adempiuto con dolo o colpa grave a uno o piu' degli obblighi di cui all'articolo 7. E' onere del prestatore di servizi di pagamento, compreso, se del caso, il prestatore di servizi di disposizione di ordine di pagamento, fornire la prova della frode, del dolo o della colpa grave dell'utente";

- l'art. 11 prevede: "1. Fatto salvo l'articolo 9, nel caso in cui sia stata eseguita un'operazione di pagamento non autorizzata, il prestatore di servizi di pagamento rimborsa al pagatore l'importo dell'operazione medesima immediatamente e in ogni caso al piu' tardi entro la fine della giornata operativa successiva a quella in cui prende atto dell'operazione o riceve una comunicazione in merito. Ove per l'esecuzione dell'operazione sia stato addebitato un conto di pagamento, il prestatore di servizi di pagamento riporta il conto nello stato in cui si sarebbe trovato se l'operazione di pagamento non avesse avuto luogo, assicurando che la data valuta dell'accredito non sia successiva a quella dell'addebito dell'importo.
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 per iscritto alla Banca d'Italia.
2-bis. Se l'operazione di pagamento e' disposta mediante un prestatore di servizi di disposizione di ordine di pagamento, il prestatore di servizi di pagamento di radicamento del conto rimborsa al pagatore immediatamente e, in ogni caso, entro la fine della giornata operativa successiva, l'importo dell'operazione non autorizzata, riportando il conto di pagamento addebitato nello stato in cui si sarebbe trovato se l'operazione di pagamento non avesse avuto luogo. In caso di operazione di pagamento non autorizzata, se il relativo ordine di pagamento e' disposto mediante un prestatore di servizi di disposizione di ordine di pagamento, quest'ultimo e' tenuto a rimborsare immediatamente e, in ogni caso, entro la fine della giornata operativa successiva, senza che sia necessaria la costituzione in mora, al

prestatore di servizi di pagamento di radicamento del conto su richiesta di quest'ultimo, gli importi rimborsati al pagatore. Se il prestatore di servizi di disposizione di ordine di pagamento e' responsabile dell'operazione di pagamento non autorizzata, risarcisce immediatamente e, in ogni caso, entro la fine della giornata operativa successiva senza che sia necessaria la costituzione in mora il prestatore di servizi di pagamento di radicamento del conto, su richiesta di quest'ultimo, anche per le perdite subite. In entrambi i casi e' fatta salva la facolta' del prestatore di servizi di disposizione di ordine di pagamento di dimostrare, in conformita' a quanto disposto dall'articolo 10, comma 1-bis, che, nell'ambito delle sue competenze, l'operazione di pagamento e' stata autenticata, correttamente registrata e non ha subito le conseguenze di guasti tecnici o altri inconvenienti relativi al servizio di pagamento da questo prestato, con conseguente diritto in questi casi alla restituzione delle somme da quest'ultimo versate al prestatore di servizi di pagamento di radicamento del conto ai sensi del presente comma.
3. Il rimborso di cui ai commi precedenti non preclude la possibilita' 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 direttamente all'utente e ottenere da quest'ultimo la restituzione dell'importo rimborsato ai sensi dei commi 1 e 2-bis.

4. Il risarcimento di danni ulteriori subiti può essere previsto in conformità alla disciplina applicabile al contratto stipulato tra l'utente e il prestatore di servizi di pagamento compreso, se del caso, il prestatore di servizi di disposizione di ordine di pagamento";
- in estrema sintesi, la normativa riportata stabilisce come regola generale, per il caso di operazione non autorizzata dal cliente, la responsabilità dell'istituto di credito, che è dunque tenuto a rimborsare immediatamente la somma "sottratta", salva la possibilità di ottenerne la restituzione in un momento successivo laddove la banca stessa dimostri che l'operazione era stata in realtà autorizzata, oppure che essa è dipesa da dolo o dalla colpa grave del cliente stesso;
- la giurisprudenza sul punto ha precisato "La responsabilità della banca per operazioni effettuate a mezzo di strumenti elettronici, con particolare riguardo alla verifica della loro riconducibilità alla volontà del cliente mediante il controllo dell'utilizzazione illecita dei relativi codici da parte di terzi, ha natura contrattuale e, quindi, va esclusa solo se ricorre una situazione di colpa grave dell'utente" (C. 26916/20; C. 18045/19; C. 2950/17).

Ciò premesso, e venendo al caso di specie, si osserva:
- è incontroverso che in data 12.12.2019 sul conto corrente n. **OMISSIS** presso **BANCA** intestato a (omissis), su cui era delegato a operare il figlio (omissis), siano state effettuate n. 2 operazioni di bonifico tramite home banking degli importi di € 10.000,00 ed € 1.530,00 con la seguente causale "a favore di (omissis) – all'avvocato";
- è parimenti incontroverso che, il giorno dopo, il (omissis) si sia recato presso la filiale **BANCA di Reggio Emilia** per disconoscere dette operazioni e abbia sporto presso la Questura di Reggio Emilia denuncia querela contro ignoti;
- nella querela costui ha dichiarato di avere tentato il 12.12.2019 l'accesso al sito home banking di **BANCA** tramite il computer di casa, di avere inserito le proprie credenziali, di avere riscontrato difficoltà nel ricevere via sms il codice OTP e di avere poi desistito senza avere mai ottenuto detto codice; di avere successivamente ricevuto due sms recanti l'indicazione dei bonifici istantanei in favore di (omissis) soggetto a lui sconosciuto; di avere immediatamente contattato il numero verde per l'assistenza clienti della banca allo scopo di bloccare i bonifici; che l'operatore ha dichiarato di non poter provvedere in tal senso, limitandosi a bloccare la funzionalità home banking e invitando il (omissis) a recarsi in filiale il giorno dopo, come poi effettivamente avvenuto;
- è, ancora, pacifico che la Banca, a seguito del disconoscimento dei bonifici, abbia provveduto immediatamente al rimborso delle somme in favore della (omissis);
- essendo questi i fatti incontroversi e/o documentati del giudizio, è invece oggetto di controversia la sussistenza in capo **a BANCA** di una responsabilità per la sottrazione di tali somme;
- va in primo luogo evidenziato che la funzionalità home banking di **BANCA** è supportata da un sistema di sicurezza articolato su due fattori, ossia: 1) un codice utente e una password di accesso statica, conosciuti dal solo correntista; 2) una password temporanea (OTP), che viene generata dai sistemi della banca in occasione dell'operazione dispositiva e specificamente per la stessa, e inviata tramite messaggio sull'utenza telefonica certificata collegata al conto corrente;

- in sostanza, al fine di eludere il sistema di sicurezza è necessario non solo disporre dell'utenza telefonica del correntista, in modo da poter ricevere il codice OTP, ma ancora prima occorre conoscere le credenziali statiche, in quanto solo attraverso di esse è possibile accedere al conto online;
- il sistema di autenticazione apprestato da **BANCA** per l'utilizzo dell'home banking è considerato dalla costante giurisprudenza come un sistema "forte" e deve dunque ritenersi adeguato; né la convenuta, a fronte di ciò, ha allegato specifici elementi in senso contrario, limitandosi a dedurre solamente una generica "lacunosità";
- deve poi ritenersi accertato che il 12.12.2019 - data in cui ha avuto luogo il fatto oggetto di causa - non si sono verificati malfunzionamenti o attacchi informatici, come risulta peraltro dalla circostanza che non sono state rilevate frodi massive in danno della clientela abilitata all'uso dell'home banking;
- sul punto **BANCA** ha prodotto il report relativo all'istruttoria interna espletata successivamente al rimborso eseguito in favore della (omissis), che attesta il corretto funzionamento dei propri sistemi informatici nel periodo in questione, nonché la documentazione riportante il log relativo all'invio dell'OTP sul numero di cellulare collegato al servizio di home banking per operare sul conto corrente della convenuta;
- tale relazione, nel suo contenuto, non è stata contestata neppure genericamente da parte convenuta, essendosi quest'ultima limitata a rilevare la necessità di disporre una Consulenza Tecnica d'Ufficio (incombente al quale non è stato dato corso in quanto l'istanza, a fronte di contestazioni del tutto generiche, è risultata esplorativa);
- a questo punto, occorre verificare si vi sia stato dolo o colpa grave da parte dell'utente;
- ora, tralasciato nel caso di specie il profilo soggettivo del dolo, mai prospettato dalle parti, la Banca con l'atto di citazione ha prodotto una comunicazione datata 17.01.2020, indirizzata alla (omissis) e al (omissis), nella quale viene contestato ai clienti che le operazioni fraudolente sarebbero state determinate da un fenomeno di phishing;
- in particolare, nella predetta missiva l'attrice deduce che il (omissis) avrebbe ricevuto una comunicazione e-mail apparentemente proveniente da **BANCA** con l'invito ad accedere ad un link per visionare della documentazione di suo interesse, il (omissis) avrebbe seguito la procedura, sarebbe stato reindirizzato a un sito clone ove avrebbe inserito le informazioni richieste e in quell'occasione si sarebbe verificato il furto delle sue credenziali ad opera di ignoti malfattori, che avrebbero quindi posto in essere le operazioni contestate;
- la circostanza è stata poi compiutamente allegata nella memoria ex art. 183, comma VI n. 1) c.p.c. dell'attrice;
- la convenuta, dal canto suo, non ha preso posizione in merito, nulla avendo dedotto né nella comparsa costitutiva né nelle successive memorie;
- deve ritenersi che il prestare fede a una mail di phishing già di per sé sufficiente a integrare l'elemento soggettivo della colpa grave;
- al riguardo, infatti, costituiscono fatto ben notorio le campagne informative e gli avvisi sistematicamente diffusi dai vari istituti di credito e dai media che mettono in guardia i correntisti dall'inserire le proprie credenziali bancarie in siti internet o dal rispondere a mail apparentemente provenienti dalle banche (c.d. phishing), che invece non utilizzano questo meccanismo per contattare la clientela (anche questo fatto notorio);
- l'ampia diffusione di tali campagne e la conoscenza generalizzata dei fenomeni frodatori e della loro frequenza fanno sì che, oggi come oggi, il seguire le istruzioni contenute in una comunicazione e-mail che invita all'immissione delle proprie password e dei propri dati non possa non ascriversi a una condotta oggettivamente negligente, a meno che non si provi che il raggiro è stato attuato con modalità particolarmente persuasive, tali da indurre una persona di normale avvedutezza in errore sulla provenienza della richiesta e sulla plausibilità della stessa;
- pertanto, se da un lato è onere della banca, come sopra chiarito, dimostrare che l'operazione contestata sia stata effettuata da un soggetto non legittimato grazie alla condotta dolosa o gravemente colposa del cliente, una volta che tale elemento soggettivo sia stato prospettato (per il fatto che l'operazione risulti essere stata resa possibile per avere il cliente messo a disposizione le credenziali in risposta a una mail di phishing), sarà onere di quest'ultimo provare che in realtà l'inganno perpetrato con il messaggio era tale che, per le particolari sua modalità o caratteristiche, avrebbe potuto trarre in errore una persona di normale avvedutezza;

- nel caso in esame, ricostruita nei termini esposti la truffa di cui è rimasto vittima il (omissis), e di conseguenza la (omissis), sarebbe stato onere di quest'ultima in primo luogo svolgere delle specifiche contestazioni sul punto e in secondo luogo produrre la mail di phishing, al fine di dimostrare come la stessa, in considerazione delle sue particolarità specifiche, avrebbe tratto in inganno una persona di normale diligenza;
- in difetto sia di specifiche contestazioni sia di tale produzione e, quindi, della prova dell'elemento costitutivo della sua ipotetica contro eccezione, deve ritenersi sussistente la condotta gravemente colposa del cliente, con conseguente effetto liberatorio per la banca;
- la convenuta con la memoria ex art. 183, comma VI n. 2) c.p.c. ha prodotto alcuni atti (richiesta di rinvio a giudizio e avviso di fissazione udienza preliminare; perizia informatica effettuata su incarico del Pubblico Ministero) relativi al processo penale pendente innanzi al Tribunale di Brescia, a carico di tale (omissis), accusato di frodi informatiche ai danni del (omissis) e della (omissis) e di altri 3 clienti di **BANCA**;
- in particolare, per quanto qui interessa, costui è accusato – fra gli altri - dei seguenti reati:
"Capo di imputazione 3 A) : "per il reato previsto e punito dagli artt. 81 cpv, 61 n. 2, 110 e 615 quater c.p. perché, con più azioni esecutive di un medesimo disegno criminoso e in concorso con altri allo stato rimasti non identificati, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, utilizzando il software denominato Tor Browser, che permette una navigazione in internet anonima, abusivamente si procurava codici o parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, ed in specie si procurava i codici personali segreti univocamente identificativi del servizio di gestione on line della BANCA dei conti correnti nr. 1(omissis) e nr. (omissis) entrambi intestati a (omissis) e del conto corrente nr. (omissis) intestato a (omissis) e gestito dal figlio (omissis). Con l'aggravante di aver commesso il reato per eseguire od occultare un altro, ovvero per conseguire o assicurare a se il profitto. Commesso in **OMISSIS**) in data **OMISSIS**".
Capo di imputazione 3 B): "per il reato previsto e punito dagli artt. 81 cpv, 61 n. 2, 110 e 615 ter comma 1 c.p. perché, con più azioni esecutive di un medesimo disegno criminoso e in concorso con altri allo stato rimasti non identificati, utilizzando il software denominato Tor Browser, che permette una navigazione in internet anonima, violava il sistema informatico e telematico protetto, di accesso ai servizi via web **BANCA** dei conti correnti nr. **OMISSIS**, nr. **OMISSIS** e nr. **OMISSIS** indicati al capo A) che precede, accedendo al sistema di amministrazione e gestione, introducendosi abusivamente nello spazio dispositivo attribuito a (omissis) e (omissis), quale soggetto titolare abilitato in via esclusiva a disporre dei conti correnti nr. (omissis), nr. (omissis) e nr. (omissis). Con l'aggravante di aver commesso il reato per eseguire od occultare un altro, ovvero per conseguire o assicurare a se il profitto. Commesso in **OMISSIS** in data 12 dicembre 2019";
- Capo di imputazione 3 C): "per il reato previsto e punito dagli artt. 81 cpv, 110 e 640 tre comma 3 c.p. perché, con più azioni esecutive di un medesimo disegno criminoso e in concorso con altri allo stato rimasti
non identificati, utilizzando il software denominato Tor Browser, che permette una navigazione in internet anonima, si procuravano l'ingiusto profitto consistito nella somma di € 12.290,00 (con pari altrui danno), che accreditava effettuando cinque bonifici fraudolenti sulla carta superflash **Banca 1** n. (omissis) associata all'iban (omissis) intestata a se stesso; essendo intervenuti senza diritto nel sistema informatico e telematico protetto da password indicato ai capi che precedono, assumendo falsamente l'identità digitale della P.O., utilizzando i codici personali segreti univocamente identificativi dello stesso. Commesso in **OMISSIS** (BS) in data **OMISSIS**";
- secondo l'ipotesi accusatoria formulata dal Pubblico Ministero (sulla base di una perizia informatica prodotta in atti), sembrerebbe che (omissis), attraverso un particolare software che permette la navigazione in anonimato, si sia impossessato delle credenziali home banking della (omissis) e del (omissis) ("abusivamente si procurava codici o parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, ed in specie si procurava i codici personali segreti univocamente identificativi del servizio di gestione on line della BANCA dei conti correnti nr. (omissis) e nr. (omissis) entrambi intestati a P(omissis) e del conto corrente nr. (omissis) intestato a (omissis) e gestito dal figlio (omissis)");
- ciò, tuttavia, non riveste alcuna rilevanza al fine di dimostrare l'assenza dell'elemento soggettivo della colpa grave in capo all'odierna convenuta e, anzi, lungi dall'avvalorare la tesi difensiva di quest'ultima

Rivista di informazione giuridica, registrata al Tribunale di Napoli al numero 12 del 05/03/2012
Registro affari amministrativi numero 8231/11
Direttore Responsabile Avv. Antonio De Simone – Direttore Scientifico Avv. Walter Giacomo Caturano

– secondo la quale il sistema di sicurezza della banca sarebbe lacunoso – depone invece proprio in senso contrario, perché conforta la conclusione per cui il (omissis) abbia inconsapevolmente (e incautamente) messo i propri codici di accesso a disposizione dell'hacker;
- il ché, conseguentemente, rende irrilevante la circostanza, dedotta dalla convenuta (e confermata in sede testimoniale dallo stesso (omissis)), che costui non abbia mai ricevuto il codice OTP né perciò autorizzato "personalmente" le due operazioni, che invece sono state disposte e autorizzate da un terzo soggetto venuto in possesso delle credenziali.
Quanto sopra, dunque, esclude la responsabilità della banca e conduce all'accoglimento della domanda restitutoria proposta da quest'ultima.
In conclusione, la convenuta va condannata a restituire in favore dell'attrice la somma di € 11.532,80, oltre interessi legali dal 20.03.2020 (data della messa in mora) al saldo.

Le spese di lite seguono la soccombenza e vengono liquidate come da dispositivo in base ai parametri di cui al D.M. 55/14 (come modificati dal D.M. 147/22, applicabile ratione temporis), tenendo conto del valore della domanda e dell'attività svolta.

P.Q.M.

Il Tribunale, definitivamente decidendo nella causa in epigrafe, ogni diversa domanda, istanza eccezione disattesa,
CONDANNA la convenuta a restituire all'attrice la somma di € 11.532,80, oltre interessi legali dal 20.03.2020 (data della messa in mora) al saldo;
CONDANNA la convenuta a pagare all'attrice le spese di lite che liquida in € 3.200,00 per compensi, oltre 15% per spese generali, CPA e IVA se dovute per legge.

Così deciso a Reggio Emilia il 05/07/2023

Sentenza resa ex art. 281 sexies c.p.c., pubblicata mediante lettura e allegata al verbale.

Il Giudice
Francesca Malgoni

Rivista di informazione giuridica, registrata al Tribunale di Napoli al numero 12 del 05/03/2012
Registro affari amministrativi numero 8231/11
Direttore Responsabile Avv. Antonio De Simone – Direttore Scientifico Avv. Walter Giacomo Caturano