

## IL COLLEGIO DI ROMA

composto dai signori:

(RM) DE CAROLIS	Presidente
(RM) GEMMA	Membro designato dalla Banca d'Italia
(RM) LEPROUX	Membro designato dalla Banca d'Italia
(RM) NERVI	Membro designato da Associazione rappresentativa degli intermediari
(RM) ROSSI CARLEO	Membro designato da Associazione rappresentativa dei clienti

Relatore NERVI ANDREA

Nella seduta del 10/10/2014 dopo aver esaminato:

- il ricorso e la documentazione allegata
- le controdeduzioni dell'intermediario e la relativa documentazione
- la relazione della Segreteria tecnica

## FATTO

La ricorrente lamenta l'effettuazione di operazioni fraudolente attraverso il sito internet dell'intermediario e chiede che quest'ultimo provveda al rimborso dell'importo frodato, pari ad euro 1.875,00.

In particolare, la ricorrente espone di aver eseguito l'accesso al sito dell'intermediario allo scopo di provvedere al pagamento dell'IMU. Durante l'accesso si apriva una finestra che la avvertiva di tentativi di infiltrazione illecita, invitandola ad inserire il codice dispositivo associato al bancomat per completare la scansione del sistema ed eliminare le minacce, cosa che la ricorrente faceva. L'operazione (accesso, comparsa della finestra ed inserimento del codice dispositivo) si è ripetuta poco dopo, allorché la ricorrente ha inteso effettuare il pagamento dell'IMU anche per conto del coniuge. All'esito di quanto precede la ricorrente ha poi appreso dell'avvenuta effettuazione di due bonifici (rispettivamente di euro 933/00 ed euro 942/00) da essa mai autorizzati.

Parte resistente chiede che il ricorso sia rigettato, non essendosi verificata alcuna responsabilità in capo ad esso. In particolare, l'intermediario rappresenta che il sistema di sicurezza da esso adottato è un sistema a due fattori, e che non si è verificata alcuna

infrazione dei propri sistemi informatici. Ne deduce che sia stata attaccata la macchina della ricorrente, non adeguatamente protetta dai malware.

L'intermediario osserva quindi che la ricorrente ha inserito le proprie credenziali su un sito clone dell'originale, cosa che accade quanto la macchina dell'utente non è protetta adeguatamente da programmi antivirus. Peraltro, la ricorrente era solita utilizzare il sito dell'intermediario resistente, onde avrebbe dovuto accorgersi dell'anomalia nella richiesta dei codici dispositivi, posto che il sito "ufficiale" richiede tale dato solo dopo che l'utente ha effettuato la scelta circa l'operazione da compiere. L'intermediario, ricordato che sul proprio sito è stato predisposto un portale della sicurezza, in cui vengono spiegate le tecniche per evitare le frodi, conclude quindi ritenendo che, nel caso di specie, sussiste la colpa grave della ricorrente.

## DIRITTO

Il ricorso è fondato.

La presente controversia è riconducibile alla fattispecie del c.d. "man-in-the-browser", ossia un programma malevolo (malware) che genera una interposizione fra il sistema centrale dell'intermediario e quello del singolo utente. Il malware 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 completamente "in sonno" attivandosi solo nel momento in cui l'utente si colleghi ad un sito finanziario compreso fra 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.

Su questo genere di fattispecie si è già pronunciato il Collegio di coordinamento nella sua decisione n. 3498 del 26 ottobre 2012, cui ha poi fatto seguito quella resa dal Collegio di Roma n. 1363 del 7 marzo 2014.

In base agli orientamenti ivi emersi, cui questo Collegio ritiene di uniformarsi, nella fattispecie in discorso non è stata ravvisata la colpa grave dell'utente, il quale viene invece considerato vittima di un raggirato perpetrato con strumenti particolarmente sofisticati.

Per altro verso, si ritiene coerente con il quadro normativo vigente addossare all'intermediario i rischi connessi all'impiego di queste tecnologie informatiche, per quanto perverse, in ragione sia della sua maggiore idoneità a sopportarne le conseguenze, sia dei vantaggi che questi – nella sua veste di operatore professionale – ritrae dall'impiego generalizzato sul mercato dei propri servizi telematici.

Ne deriva la conclusione secondo la quale la condotta dell'utente non è stata connotata dal requisito essenziale della colpa grave e che, conseguentemente, debba essergli riconosciuto il diritto di essere tenuto indenne dal pregiudizio subito, salva l'imputazione a suo carico dell'importo di cui all'art. 12, 3° comma, D.Lgs. n. 11/2010, che il Collegio quantifica nella misura di € 150 (centocinquanta).

Pertanto, in accoglimento del ricorso, deve statuirsi che l'intermediario sia tenuto a risarcire al ricorrente la complessiva somma di € 1.725,00 (millesettecentoventicinque), pari alle somme richieste dal ricorrente, detratto l'importo a carico di quest'ultimo di € 150 ex art. 12, 3° comma, D.Lgs. n. 11/2010.

**P.Q.M.**

**Il Collegio dispone che l'intermediario corrisponda alla ricorrente la somma di euro 1.725,00 oltre interessi legali dalla data del reclamo al saldo.**

**Dispone, inoltre, ai sensi della vigente normativa, che l'intermediario corrisponda alla Banca d'Italia la somma di Euro 200,00 (duecento/00) quale contributo alle spese della procedura e al ricorrente quella di Euro 20,00 (venti/00) quale rimborso della somma versata alla presentazione del ricorso.**

IL PRESIDENTE

Firmato digitalmente da  
BRUNO DE CAROLIS