Senato della Repubblica

XVIII LEGISLATURA

N. 2295

DISEGNO DI LEGGE

d'iniziativa dei senatori LANNUTTI, BUCCARELLA, ROMAGNOLI e ORTIS

COMUNICATO ALLA PRESIDENZA IL 22 GIUGNO 2021

Disposizioni in materia di furti commessi mediante servizi bancari a distanza e di compravendita di strumenti finanziari tramite *internet* (*trading on line*)

TIPOGRAFIA DEL SENATO

ONOREVOLI SENATORI. – Le truffe digitali colpiscono migliaia di persone, svuotando e troppo spesso azzerando il loro conto corrente, i risparmi di una vita. Gli *hacker* informatici si impossessano, illegittimamente, dei dati personali del cittadino custoditi presso gli istituti bancari (credenziali di accesso, codici segreti, codici dispositivi, numeri del conto, della carta di credito) e, troppo facilmente, aggirano i presidi di sicurezza degli intermediari finanziari, ottenendo tutti i dati conservati dalle banche senza le dovute precauzioni.

Ciò che più emerge, dal dibattito anche giurisprudenziale tutt'ora in corso, è la capacità dei sempre più sofisticati attacchi informatici di aggirare i presidi di *strong customer authentication* senza la violazione dei canali (almeno non direttamente). Ciò comporta la necessità di un urgente ripensamento degli obblighi organizzativi e dei presidi di sicurezza imposti agli intermediari dall'articolo 8 decreto legislativo n. 11 del 2010.

Una grande criticità è l'invio dei codici dispositivi sul nostro cellulare, divenuto ormai un vero e proprio terminale bancario. Gli istituti bancari hanno adottato e imposto ai loro correntisti un nuovo modo di operare sul conto, in cui è lo *smartphone* ad avere un ruolo fondamentale, sostituendo il generatore di codici numerici, il cosiddetto « *token* », che permetteva una comunicazione esclusiva tra correntista e banca, utilizzato con l'unico scopo di autorizzare un'operazione bancaria sul proprio conto. Evidente come il « *token* » sia uno strumento di maggiore sicurezza, poiché riposto all'interno della propria casa, a differenza del telefonino, portato invece sempre con sé, utilizzato per infinite finalità e quindi esposto a infiniti pericoli.

La direttiva 2015/2366 del Parlamento europeo e del Consiglio, del 25 novembre 2015, cosiddetta *Payment Services Directive 2* o PSD2*,* ha reso necessario un doppio fattore di autenticazione, oltre alla *username* e *password* dell'*internet banking*. Gli istituti bancari hanno scelto e, di conseguenza, imposto ai loro correntisti un'applicazione (App) da scaricare sui propri *smartphone*, utilizzati per infiniti altri scopi e quindi soggetti ed esposti a infiniti rischi diversi.

Il sistema di utilizzo del proprio denaro, imposto dagli istituti bancari ai propri correntisti, si è in questi anni rivelato troppo labile esponendo i nostri dati personali ad attacchi sempre più frequenti, danneggiando la sicurezza di moltissime famiglie italiane in un periodo storico difficilissimo come quello che stiamo attraversando: si tratta ormai di una vera e propria emergenza nazionale, che richiede l'adozione di una legge che tuteli i risparmi degli italiani dai frequentissimi attacchi informatici.

Nell'etere non viaggiano solo i furti dai conti bancari, ma anche le truffe finanziarie, attraverso il mezzo della compravendita di strumenti finanziari tramite *internet*, il cosiddetto *trading on line.* Pubblicizzato come un modo facile per fare velocemente tanti soldi, è l'arena in cui attrarre risparmiatori ignari dei rischi a cui si espongono. Ormai, basta aprire un qualsiasi *social network* per essere inondati di annunci di pseudo « guru » di borsa che spiegano come diventare ricchi in poco tempo, senza fatica, aumentando anche il tempo libero e, soprattutto, senza perdere.

Viceversa, nella migliore delle ipotesi (anche se non si trattasse di truffa) il *trading*

on line, per gli inesperti, è una trappola mangiasoldi e anche vorace. Guadagnare è difficile, mentre perdere tutti i propri soldi in poche ore è un'esperienza traumatica subita da tante persone.

Da tempo le organizzazioni criminali hanno fiutato il *business* e lo stanno sfruttando per sottrarre soldi a ignari cittadini che, in buona fede, si lasciano coinvolgere in questa attività. Il termometro di questo fenomeno arriva dalle denunce presentate alla polizia postale: in tema di *trading on line* sono aumentate del 30 per cento da quando è iniziata la pandemia.

Il meccanismo è semplice: organizzazioni straniere contattano pensionati e li invitano ad aprire un conto, promettendo facili guadagni. I soldi vengono dirottati su conti stranieri per lo più nell'Europa dell'Est o in alcuni paradisi fiscali. Si inizia con piccole cifre, nell'ordine dei 100 o 200 euro, e poi di fronte anche a false vincite pilotate, per creare maggiore fiducia nel risparmiatore, si arriva anche a decine di migliaia di euro versati. A quel punto i conti vengono prosciugati. Le organizzazioni criminali fanno una serie di triangolazioni per far sparire il prima possibile questi soldi.

Il presente disegno di legge, come principale misura di argine al fenomeno, mira a introdurre l'assoluto divieto di pubblicità con qualsiasi strumento di comunicazione a distanza, ivi compreso quello telematico, delle attività di *trading on line*: a titolo di esempio, non deve essere possibile la pubblicizzazione di tali strumenti di investimento, né con telefonate, né con messaggi, né con metodiche porta a porta, né a mezzo *internet*.

Il presente disegno di legge è anche finalizzato a introdurre nel nostro ordinamento una norma che imponga agli istituti bancari l'adozione di misure precise impedendo ai truffatori di portare concretamente a termine la truffa ai danni dei consumatori (sim *swap*, *phishing* avanzato, *man in the middle*, *man in the browser*, *Vishing* con *smishing*, sms *spoofing*).

Il disegno di legge mira a obbligare gli istituti bancari a bloccare, congelare e non processare alcuna operazione bancaria in presenza di almeno una serie di condizioni, che rendono quell'operazione sospetta.

Il presente disegno di legge è finalizzato a imporre l'obbligo in capo agli istituti bancari di conservare e fornire al proprio cliente la documentazione richiesta. Inoltre, esso è volto a rendere non più automatica la possibilità per i correntisti di poter disporre bonifici istantanei, preferiti dai truffatori per la loro speditezza e impossibilità di essere efficacemente richiamati: il correntista che vorrà usufruire della facoltà di poter disporre bonifici istantanei, dovrà farne espressa richiesta, che dovrà essere esibita dall'istituto bancario.

Ciò elide il favore della direttiva PSD2 verso l'utilizzatore di servizi di pagamento permettendo alla banca di non rimborsare effettivamente al cliente l'operazione disconosciuta senza procedere a formale richiesta, con gli oneri probatori collegati a tale azione di recupero.

In relazione all'articolo 24 del decreto legislativo n. 11 del 10, che disciplina « Identificativi unici inesatti », occorre rilevare come il prestatore di servizi non sia responsabile se l'identificativo IBAN indicato risulti errato o non corrispondente al beneficiario indicato nell'ordine di pagamento.

La circostanza, infatti, risulta evidente in molti casi di truffa digitale che passa attraverso la modifica di beneficiario o codice IBAN. A rettifica di tale incongruenza, si ritiene opportuna l'introduzione dell'obbligo di controllo di corrispondenza tra IBAN e soggetto beneficiario, sia per la banca disponente, sia per la banca ricevente.

Portando tutto alla normalità il presente disegno di legge prevede (riformando *in toto* il suddetto articolo 24) che la banca dovrà verificare anche in automatico che le cre-

denziali indicate corrispondano a quel beneficiario e a quella determinata banca o istituto di credito, pena la responsabilità della banca che, in presenza di anomalie, dovrà bloccare l'operazione.

Non ultima, in tema d'importanza, è la possibilità di richiamo e blocco successivo dell'operazione in presenza di denuncia penale. In tali casi, sarà onere della banca richiamare immediatamente il pagamento con conseguente obbligo dell'istituto beneficiario di bloccare le somme ricevute e restituirle al legittimo proprietario.

Sul tema della necessità di un controllo di corrispondenza tra IBAN e beneficiario è intervenuta anche la Corte di giustizia europea, che sul tema ha articolato l'enunciazione del principio contenuto nella decisione C-245/18 del 21 marzo 2019.

L'articolo 74, paragrafo 2, della direttiva 2007/64/CE del Parlamento europeo e del Consiglio, del 13 novembre 2007, relativa ai servizi di pagamento nel mercato interno, recante modifica delle direttive 9717/CE, 2002/65/CE, 2005/60/CE e 2006/48/CE, che abroga la direttiva 97/5/CE, deve essere interpretato nel senso che, ove un ordine di pagamento sia eseguito conformemente all'identificativo unico fornito dall'utente di servizi di pagamento, che non corrisponde al nome del beneficiario specificato dall'utente stesso, la limitazione della responsabilità del prestatore di servizi di pagamento, prevista dalla disposizione in parola, si applica sia al prestatore di servizi di pagamento del pagatore, sia al prestatore di servizi di pagamento del beneficiario.

Invero, il dibattito sul tema si era già formato anche nella giurisprudenza dell'arbitro bancario finanziario, dove si fronteggiavano due opposti orientamenti, il primo formatosi nel collegio romano e il secondo in quello milanese, poi superato con l'enunciazione del principio formulato dal collegio di coordinamento (decisione 162 del 17) secondo il quale: « l'art. 24 d.lgs. 27 gennaio 2010, n. 11, va interpretato nel senso che, nell'esecuzione di un bonifico bancario, il prestatore di servizi di pagamento dell'ordinante ed il prestatore di servizi di pagamento del beneficiario sono autorizzati a realizzare l'operazione in conformità esclusivamente all'identificativo unico, anche qualora l'utilizzatore abbia fornito al suo prestatore di servizi di pagamento informazioni ulteriori rispetto all'IBAN. In particolare, il prestatore di servizi di pagamento di destinazione del bonifico non è tenuto a verificare la corrispondenza fra il nominativo del beneficiario ed il titolare del conto di accredito identificato tramite l'IBAN.

Se l'identificativo unico fornito dall'utilizzatore è inesatto, i prestatori di servizi di pagamento coinvolti nella realizzazione del bonifico non sono responsabili, ai sensi dell'articolo 25, della mancata o inesatta esecuzione dell'operazione di pagamento.

Nel caso in cui l'utilizzatore abbia fornito un codice identificativo inesatto, i prestatori di servizi di pagamento dell'ordinante e del ricevente si adoperano per il recupero dei fondi oggetto dell'operazione di pagamento sulla base degli obblighi di diligenza professionale che loro competono ».

Pertanto, con il presente disegno di legge si propone di modificare la norma recata dagli articoli 5 e 17 decreto legislativo n. 11 del 2010, inserendo l'obbligo che il bonifico debba essere sempre revocato e la somma restituita, anche se decorse le ventiquattro ore dalla sua esecuzione, ogni volta sia stata presentata una denuncia per truffa informatica o, comunque, per esigenze di giustizia.

Sul punto, preme ricordare come gli obblighi di consegna della documentazione non siano solo afferenti alle disposizioni di cui al testo unico delle leggi in materia bancaria e creditizia (TUB), di cui al decreto legislativo n. 385 del 1993, (articoli 119 e successivi) ma anche e soprattutto al regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, co-

siddetto GDPR, in quanto trattamento di dati personali riservati. Autenticarsi o accedere a un *account* significa, infatti, dimostrare la propria identità fisica a livello digitale e informatico con i conseguenti obblighi di gestione e conservazione del dato e conseguenti diritti dell'interessato (articoli 15 e successivi del GDPR).

Il presente disegno di legge mira, inoltre, a imporre agli istituti bancari di fornire, entro quindici giorni dalla richiesta, prova di aver adottato le procedure di RECALL della disposizione, esibendo tutta la relativa documentazione completa di date ed orari delle singole operazioni di RECALL.

In ogni caso, l'istituto di credito che fornisce tali servizi, dovrà provvedere a rafforzare la tutela con un'autenticazione ulteriore in aggiunta a quelle previste, con l'invio di un codice OTS dedicato sul dispositivo di recupero comunicato dal cliente per le emergenze, in sede di registrazione.

Infine, un obiettivo che la norma deve raggiungere, consiste nella finalmente corretta applicazione dell'articolo 11 decreto legislativo n. 11 del 2010. Si è affermata, nella prassi bancaria, la modalità di rimborso dell'operazione disconosciuta dal cliente con modalità salvo buon fine: ma è una modalità errata rispetto al dato letterale della norma e una sua interpretazione non solo esegetica ma anche e soprattutto teleologica. Tale cattiva prassi viene, inoltre, accompagnata da una successiva lettera della banca che dichiara di aver terminato l'istruttoria sulla frode informatica, senza dame alcuna evidenza (che emerge poi compiutamente nel corso dei giudizi) e di procedere al riaddebito degli importi accreditati in un primo momento s.b.f. (salvo buon fine).

In ogni caso, la comunicazione del riaddebito deve pervenire al cliente entro un termine minimo di quindici giorni, onde evitare possibili scoperti di conto, pena la risarcibilità del danno in caso di omesso tempestivo avviso.

DISEGNO DI LEGGE

Art. 1.

(Condizioni di blocco delle operazioni bancarie)

1. Gli istituti di credito hanno l'obbligo di bloccare e non processare alcuna operazione bancaria in presenza di una delle seguenti condizioni:

a) la scheda anagrafica del cliente è stata modificata, apportando modifiche al numero di telefono del cliente sul quale l'istituto bancario deve inviare le comunicazioni;

b) l'applicazione informatica dell'istituto di credito risulta essere stata disinstallata dal telefono cellulare o altro dispositivo in uso al correntista e successivamente installata su un dispositivo con un diverso codice *international mobile equipment identity* (IMEI), con una diversa carta SIM o con un diverso indirizzo *internet protocol* (IP), in particolare qualora all'istituto di credito risulti che il nuovo dispositivo si trovi in una città o regione diversa da quella comunicata dal correntista e dalla quale egli ha frequentemente utilizzato l'applicazione informatica per le sue operazioni abituali;

c) è richiesta l'autenticazione di una nuova applicazione informatica che permette di effettuare operazioni bancarie su un nuovo dispositivo che obblighi il cliente a inserire ogni volta che accede le sue credenziali e la *password*;

d) sono state richieste operazioni per un ammontare pari o superiore al 60 per cento delle somme disponibili sul conto;

e) sono state richieste tre o più operazioni ravvicinate nel tempo con una velocità incompatibile con l'attività di un'unica persona fisica e possibile solo se fatte da uno strumento elettronico;

f) la singola operazione è stata preceduta da un controllo sulla scheda anagrafica e sui massimali dispositivi di conto prima di essere eseguita, in un arco temporale complessivo di pochi minuti, con chiari indici di esecuzione dell'intera operazione da parte di un *software*;

g) attivazione automatica del servizio di avviso tramite SMS (« sms *alert* ») con invio di notifica sia su un'applicazione informatica o un numero di telefono collegato sia su un canale « *out of band* » non indicati nella scheda anagrafica del cliente e tenuti riservati, al fine di evitare che l'attacco informatico blocchi la possibilità di effettivo avviso al cliente di frode a seguito della captazione e deviazione su altro numero del messaggio.

2. È fatto obbligo all'istituto bancario che processa operazioni in presenza di una o più delle condizioni di cui al comma 1 di risarcire integralmente il correntista delle somme a lui sottratte, salvo il risarcimento del maggior danno. La comunicazione del risarcimento deve pervenire al cliente entro quindici giorni, onde evitare possibili scoperti di conto, pena la risarcibilità del danno in caso di omesso tempestivo avviso.

Art. 2.

(Bonifici istantanei)

1. I correntisti degli istituti di credito possono disporre bonifici istantanei qualora ne facciano esplicita richiesta, che deve essere conservata dall'istituto di credito e da questo esibita in caso di verifica. L'istituto di credito che fornisce il servizio di bonifico

istantaneo deve prevedere un'autenticazione aggiuntiva rispetto a quelle già previste, con l'invio di un codice via SMS (OTS) dedicato sul dispositivo di recupero comunicato dal cliente per le emergenze in sede di registrazione.

Art. 3.

(Documentazione da fornire ai correntisti da parte delle banche)

1. Gli istituti di credito hanno l'obbligo di conservare e fornire al proprio cliente entro quindici giorni dalla relativa richiesta scritta la seguente documentazione:

a) il completo elenco storico degli accessi, delle autorizzazioni e delle pre-autorizzazioni, anche se non andati a buon fine, relativi a tutti i movimenti sul conto corrente o sulla carta di credito o di debito del correntista nei quarantacinque giorni precedenti e susseguenti l'operazione o le operazioni oggetto di disconoscimento;

b) i *file* di *log* completi e integrali delle allerte e degli altri avvisi inviati dall'istituto di credito mediante applicazioni informatiche, sms o posta elettronica, con i dettagli relativi alla data, all'ora, al numero del destinatario e all'indirizzo IP;

c) l'elenco delle richieste di modifica della scheda anagrafica del profilo del correntista, specificando con quali modalità ciascuna richiesta è avvenuta, chi l'ha validata e in base a quali elementi, nonché la registrazione dei *file* relativi alla modifica e ogni comunicazione ad essa relativa, in qualsiasi modo sia avvenuta;

d) tutti i dettagli informatici dell'autenticazione delle disposizioni bancarie contestate, con tutti i dati relativi all'operazione, specificandone la provenienza;

e) i dettagli concernenti l'operatore che ha visualizzato il profilo del correntista, la

data di accesso e la postazione dalla quale sia stato visualizzato il medesimo profilo, in relazione ai prodotti bancari e finanziari del correntista stesso;

f) i « *record* di accesso » al numero direzione generale (NDG) identificativo del correntista.

2. All'istituto di credito che viola le disposizioni di cui al comma 1 si applica una sanzione amministrativa pari a 100.000 euro.

Art. 4.

(Verifica delle credenziali bancarie)

1. Quando esegue un ordine di pagamento, l'istituto di credito verifica in modo automatico che l'identificativo unico di cui all'articolo 1, comma 1, lettera *r)*, del decreto legislativo 27 gennaio 2010, n. 11, indicato dal cliente corrisponda al beneficiario e alla banca indicate. Tale obbligo di controllo è in carico sia all'istituto di credito disponente che all'istituto di credito ricevente. In presenza di anomalie l'istituto di credito procede al blocco dell'operazione.

2. In caso di denuncia penale relativa all'ordine di pagamento, spetta all'istituto di credito richiamare immediatamente il pagamento, con conseguente obbligo dell'istituto beneficiario di bloccare le somme ricevute e restituirle al legittimo proprietario.

3. Se l'istituto di credito non ottempera agli obblighi di cui ai commi 1 e 2, esso è soggetto alla multa di 100.000 euro.

Art. 5.

(Divieti per le aziende che praticano la compravendita di strumenti finanziari tramite internet*)*

1. Le aziende che praticano la compravendita di strumenti finanziari tramite *internet* (*trading on line*) hanno il divieto:

a) di fare pubblicità con qualsiasi strumento di comunicazione a distanza, ivi com-

preso quello telematico, per le attività di compravendita di strumenti finanziari tramite *internet* e in particolare di pubblicizzare tali attività né con telefonate, né con messaggi, né con metodiche porta a porta, né a mezzo *internet*;

b) di commercializzare i contratti per differenza (CFD) a clienti al dettaglio e di sollecitare in qualsiasi forma il cliente affinché chieda di diventare cliente professionale per poter acquistare prodotti ad alto rischio, con conseguente previsione di sanzioni di natura anche penale;

c) di utilizzare nell'ambito della compravendita di strumenti finanziari tramite *internet* pratiche scorrette e in particolare: pratiche commerciali aggressive, attraverso anche l'offerta di *bonus* o altri incentivi similari; mancata informativa sugli effettivi rischi degli investimenti effettuati; mancata profilatura della clientela; pressioni e consigli da parte di addetti dell'impresa (cosiddetto « *account manager* ») che possano causare perdite, talora fino all'intero capitale investito; anomalie nella gestione dei rimborsi richiesti dalla clientela; malfunzionamenti della piattaforma di compravendita di strumenti finanziari tramite *internet*; effettuazione di operazioni non autorizzate dai clienti.

2. La violazione degli obblighi di cui al comma 1 rende nulle le operazioni eseguite con tali modalità, con conseguente obbligo di restituzione delle somme investite.

Art. 6.

(Obblighi delle società di compravendita di strumenti finanziari tramite internet*)*

1. Tutte le società, anche estere, che praticano la compravendita di strumenti finanziari tramite *internet*, che entrano in contatto con clienti italiani, hanno l'obbligo di comu-

nicare le proprie sedi effettive, fornire i riferimenti reali dei propri promotori finanziari, indicare esattamente la qualifica dei soggetti che entrano in contatto con clienti italiani e (se si tratta di semplici venditori o di soggetti qualificati) fornire la propria iscrizione al relativo albo.

2. Le società di cui al comma 1 sono tenute a fornire idonee garanzie in merito alla restituzione delle somme investite, con indicazione dei tempi massimi a ciò necessari.

Art. 7.

(Poteri della Consob)

1. Alla Commissione nazionale per le società e la borsa (Consob) sono attribuiti, nel caso in cui siano presentate denunce penali o segnalazioni dettagliate, poteri ispettivi su tutte le società italiane ed estere che praticano la compravendita di strumenti finanziari tramite *internet*, le quali offrono servizi a clienti italiani.

Art. 8.

(Clausola di invarianza finanziaria)

1. Dalla presente legge non devono derivare nuovi o maggiori oneri a carico della finanza pubblica.

Art. 9.

(Entrata in vigore)

1. La presente legge entra in vigore il giorno successivo a quello della sua pubblicazione nella *Gazzetta Ufficiale.*

€ 1,00