ATTENZIONE ALLE TRUFFE LEGATE ALLE COORDINATE BANCARIE (CODICE IBAN)

AVV. MASSIMO CAMPANELLA Del. Di Roma

Tra le truffe che si sono sviluppate in questi ultimi anni, relative alle transazioni commerciali , una particolare attenzione meritano quelle che vengono perpetrate da hacker professionisti sui bonifici bancari.

Tali truffatori possono intercettare email con allegate fatture di pagamento, e cambiare il codice iban, le fatture che verranno ricevute dal destinatario della email, a causa della modifica del codice, verranno pagate a soggetti diversi rispetto agli effettivi creditori.

Su tali fattispecie si è già più volte pronunciato l'A.B.F.(Arbitro bancario e Finanziario), l'organismo stragiudiziale che si occupa del contenzioso bancario. In particolare alcune pronunce del Collegio di Roma sono state favorevole ai correntisti, sanzionando a volte la banca del soggetto emittente ed altre quella del beneficiario del bonifico.

Con provvedimento del 12 gennaio 2017 n. 162, il Collegio di Coordinamento dell'ABF, interveniva a sanare il conflitto creatosi tra collegi, infatti in merito alla non corrispondenza tra intestatario del conto e codice Iban, alcuni collegi si erano pronunciati pro consumatore ed altri pro banca.

A seguito dell'istruttoria Il Collegio di coordinamento, enunciava il seguente principio di diritto: " *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'art. 25, della mancata o inesatta esecuzione dell'operatore di pagamento*".

In sostanza le banche non sono responsabili per non aver verificato la corrispondenza tra codice identificativo Iban ed intestatario del conto corrente .

Tale impostazione non è condivisibile ed è criticabile sotto diversi profili.

1) ***LE CONDOTTE REITERATE E L'OBBLIGO DELLE BANCHE DI PREDISPORRE MISURE IDONEE PER TUTELARE I CLIENTI***

Innanzitutto va rilevato come si tratti di condotte reiterate nel tempo, non si tratta di episodi sporadici, per cui possa essere invocato dagli Istituti bancari il caso fortuito o l'evento eccezionale o situazioni imprevedibili, tali problematiche sono sicuramente conosciute dagli Istituti bancari, a causa dei reclami inoltrati ormai da anni. Infatti il Collegio di Roma si pronunciava su tali fattispecie già nel 2014 con la pronuncia del 3/7/2014 n.4172, e successivamente con la n. 7845 del 8/10/2015 e di nuovo con la 405 del 19/1/2016. Di recente altri due casi sono stati posti alla mia attenzione, da parte di associati Adusbef.

Aprendo una breve parentesi vorrei ricordare come in materia di Phishing, decideva il Tribunale di Palermo in una sentenza del 2011. Il Giudice nell'occasione ha ritenuto applicabile al caso di specie la normativa del Codice della Privacy (D.Lgs. 196/2003), affermando che:"..la colpa di eventuali intromissioni fraudolente nel sistema ricade *sulla società che offre il servizio la quale è tenuta a predisporre tutte le misure necessarie per tutelare i clienti ed i loro dati personali, non potendo ricadere su questi ultimi il rischio del verificarsi di detti fenomeni.* A tal proposito veniva richiamato l'art. 15 del Codice, che avendo portata generale prevede che chiunque cagiona danno ad altri per effetto del trattamento dei dati personali è tenuto al risarcimento ai sensi dell'art. 2050 c.c. (Si veda sul punto su Diritto 24 Edizione novembre 2011, l'articolo: "Phishing, la banca deve adottare i migliori sistemi di sicurezza tecnologici Tribunale di Palermo, Sez. II, Sentenza 11 giugno 2011, n. 2904 - Giudice Dott.ssa Spiaggia ").

Se la sentenza citata, può considerarsi limitata ai soli casi di ingerenza nei conti correnti da parte di phisher, certo non si può negare, che le attività malavitose, che modificano le coordinate bancarie dei correntisti, incidano sulla sicurezza delle transazioni commerciali e di conseguenza sugli obblighi delle banche di adottare tutte le misure idonee per tutelare i propri clienti.

Si rende pertanto indispensabile sotto tale profilo un controllo automatico da parte delle stesse, quantomeno sulla corrispondenza tra codice Iban e soggetto intestatario del conto di riferimento, poiché appare assurdo che a causa della mancanza di semplici controlli(che possono benissimo essere automatici), gli Istituti di credito

possano pagare a soggetti non legittimati, costringendo poi i correntisti a presentare denunce anche in sede penale per riottenere le somme così erroneamente pagate.

2) *LA SICUREZZA NEGLI STRUMENTI DI PAGAMENTO ED I RELATIVI CONTROLLI SONO DISCIPLINATI DA LEGGI NAZIONALI, COMUNITARIE E DALLA BANCA D'ITALIA*

Che gli Istituti di credito debbano adoperarsi affinchè gli strumenti di pagamento siano sicuri, discende anche dalla legge, sia nazionale, sia comunitaria nonché dalle disposizioni della stessa Banca D'Italia.

In materia di privacy con l'entrata in vigore del nuovo Regolamento Ue, infatti dal *25 maggio 2018 il regolamento (Ue) 2016/679 del 27 aprile 2016, relativo alla "protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/Ce (regolamento generale sulla protezione dei dati)", sarà applicabile in tutti gli Stati membri e, nello stesso giorno, la direttiva 95/46/Ce del 24 ottobre 1995, relativa "alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati", alla base di tutte le legislazioni nazionali vigenti nell'Unione europea, verrà abrogata.*

Ciò comporta che dal punto di vista organizzativo, le banche dovranno adempiere a tutta una serie di obblighi quali:

- rivedere la propria governance, inserendo all'interno della loro compagine un ufficio dedicato alla protezione dei Dati (Dpo);- sviluppare e, laddove esistente, implementare un modello operativo di governance improntato alla protezione dei Dati personali (bisogna rivedere le figure privacy).

Con riferimento alla gestione dei Trattamenti, le banche dovranno:

- implementare dei processi di sviluppo e pianificazione dei Trattamenti che siano basati sulla corretta identificazione dei Dati personali (Dati necessari v. Dati non necessari);- definire la base giuridica del Trattamento e, nel caso in cui questa sia il Consenso del cliente, gestire opportunamente l'acquisizione del Consenso, comunicare al cliente la Finalità del Trattamento, il tempo di conservazione dei Dati, assicurare l'esercizio del diritto alla portabilità dei Dati e quello alla cancellazione;- rivedere tutta la documentazione privacy (dalle nomine alla tenuta del Registro dei Trattamenti);- formare il proprio personale in materia privacy.

MA SOPRATTUTTO DAL PUNTO DI VISTA DELLA SICUREZZA LE BANCHE DOVRANNO :

- aggiornare e cambiare l'infrastruttura e architettura IT;

- espandere la gestione dei metadata;

- fare l'"inventario" dei Dati personali trattati in banca.

Tutti obblighi che depongono per una maggior sicurezza nelle transazioni commerciali.

Nello stesso senso deve essere letto il documento stilato da Banca D'Italia, già nel 2017,e che va sotto il nome di "Piano Strategico 2017-2019".Con tale documento vengono definiti gli *OBIETTIVI STRATEGICI E I PIANI D'AZIONE*, voglio ricordare solo alcuni dei temi trattati:

al Capitolo 1 *"Promuovere in Italia e in Europa servizi di pagamento innovativi efficienti e sicuri"; al Capitolo 2 Rafforzare l'azione di vigilanza e la tutela dei clienti dei servizi bancari finanziari e di pagamento*";al Capitolo 4 "Essere più innovativi ed efficienti, ed al paragrafo 4.4. *"Rafforzare la cyber security della Banca in relazione a nuovi scenari di rischio"*:

e questo proprio perché , si scrive nello stesso paragrafo *".. La Banca d'Italia offre importanti servizi a banche, imprese, istituzioni e cittadini e gestisce infrastrutture critiche, tra cui quelle del sistema dei pagamenti; diviene, dunque, vitale la difesa da minacce informatiche che sono in continua e rapida evoluzione".*

Appare chiaro che tutti questi buoni propositi non possono prescindere da una sicurezza nella esecuzioni dei bonifici, da sempre utilizzati nei pagamenti e nelle transazioni commerciali, laddove ne risulti incerta e rischiosa l'utilizzazione a causa della mancanza di controlli anche automatici, sulla corrispondenza: tra *Iban /soggetto beneficiario/ nome dell'Istituto di credito verso cui debba essere eseguito/Agenzia ed ubicazione della stessa sul territorio.*

Diversamente, gli Istituti di credito si vedranno esposti ad azioni di responsabilità contrattuale ed extracontrattuale da parte di molti correntisti.