# Il PHISHING BANCARIO: NORMATIVA ED ORIENTAMENTI GIURISPRUDENZIALI

***Abstract:*** Lo sviluppo delle tecnologie trasforma sempre più rapidamente le modalità delle transazioni commerciali e dei sistemi di pagamento, ma accresce anche la sofisticazione ed i rischi delle truffe telematiche, effettuate mediante appropriazione indebita ed accesso illegale alle banche-dati che custodiscono gli elementi identificativi ed i conti degli operatori economici. In particolare, è assai diffuso il fenomeno del *phishing* bancario. Le normative europee e la legislazione nazionale di recepimento si preoccupano di garantire la sicurezza dei dati personali e delle operazioni di pagamento, imponendo specifici obblighi di protezione a carico degli istituti di credito. Il presente articolo analizza la vigente disciplina europea, con riferimento a quella generale in tema di tutela della *Privacy* e di quella specifica in tema di operazioni di pagamento, individuando in particolare gli obblighi di protezione e le connesse responsabilità degli istituti di credito, anche alla luce degli orientamenti giurisprudenziali della S. Corte di Cassazione e dell'Arbitro Bancario Finanziario.

## 1. LA DIFFUSIONE DEL *PHISHING* NELLE OPERAZIONI DI PAGAMENTO ELETTRONICO A DISTANZA

Il proliferare di fenomeni di truffe informatiche sofisticate costituisce la logica conseguenza dell'utilizzo sempre più diffuso di sistemi tecnologici da parte degli istituti bancari per l'erogazione dei servizi di credito. Tra questi, indubbia rilevanza ha assunto nel corso degli ultimi anni il cosiddetto *"phishing*". Con tale espressione vengono individuati tutti quei comportamenti illeciti diretti all'intrusione illeciti di terzi nelle piattaforme di *home banking* al fine di sottrarre liquidità dai conti correnti degli utenti delle banche.

Il *phishing* è una truffa digitale realizzata attraverso l'acquisizione fraudolenta dei dati sensibili degli utenti. Avviene principalmente tramite l'invio di *e-mail* o sms ingannevoli da parte di un *hacker* alla vittima designata, con utilizzo del nome o del logo di istituti bancari, attraverso un sito molto simile a quello loro proprio, con invito ad accedere al proprio *account* bancario e con richiesta di inserimento di *username*, *password*, codici fiscali o addirittura codici di accesso ai conti bancari, in modo da carpire i dati personali dell'utente. Ove si assecondano queste richieste, i dati inseriti entreranno in possesso dei terzi che tenteranno di utilizzarli per furti d'identità o pagamenti non autorizzati.

Il cliente, convinto di essere stato contattato dall'istituto bancario, cede, in modo inconsapevole e incolpevolmente, le credenziali per l'accesso al proprio conto corrente, rischiando in tal modo di subire la sottrazione di somme di denaro anche molto consistenti.

Dai dati dei ricercatori dell'Avast, una delle più grandi aziende competenti per contrastare gli attacchi informatici, è emerso un quadro problematico per il comparto bancario italiano rispetto alle ripetute truffe informatiche. Infatti, più di 100 banche italiane sono state prese di mira dal *malware* "*Ursnif",* un *software* capace di entrare in possesso delle credenziali per accedere, attraverso l'*home banking*, ai conti correnti degli utenti che inconsapevolmente lo installano sul loro *personal computer*.
Questa situazione offre lo spunto per riflettere sulla vigente normativa, europea e nazionale, finalizzata ad assicurare la sicurezza delle transazioni *on line* ed a prevenire queste forme di frodi. Ciò consentirà di individuare la ripartizione delle responsabilità e dei rischi tra gestori dei servizi di pagamento ed utenti, nonché gli strumenti più adeguati al fine di tutelare gli interessi di questi ultimi. In particolare, giova analizzare la disciplina contenuta nel Regolamento UE 2016/679, del Parlamento Europeo e del Consiglio, del 27 aprile 2016, applicabile a decorrere dal 25 maggio 2018 e noto anche come GDPR (*General Data ProtectionRegulation*), relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali; nella Direttiva 2015/2366/UE, del Parlamento europeo e del Consiglio, del 25 novembre 2015, relativa ai servizi di pagamento nel mercato interno [nota anche come PSD2 – *Payment Services Directive*, che ha sostituito con effetto dal 13 gennaio 2018 la 2007/64/CE (cd. PSD), recepita nell'ordinamento interno per mezzo del decreto legislativo del 27 gennaio 2010 n. 11, poi modificato con il d.lgs. n. 218 del 15 dicembre 2017], e nel Regolamento delegato (UE) 2018/389, entrato in vigore il 14 settembre 2019, che integra la Direttiva 2015/2366/UE per quanto riguarda le norme tecniche di regolamentazione per l'autenticazione forte del cliente e gli *standard* aperti di comunicazione comuni e sicuri.

## 2. GLI STRUMENTI DI TUTELA DEI DATI PERSONALI DELL'UTENTE: DAL CODICE DELLA *PRIVACY* AL REGOLAMENTO UE 2016/679.

La normativa in tema di protezione dei dati personali fornisce il quadro generale al quale devono ispirarsi i fornitori di servizi di pagamento per impedire l'accesso abusivo di terzi alle banche dati che custodiscono gli elementi identificativi dei propri clienti, in modo da scongiurare il possibile compimento di operazioni illecite e la conseguente sottrazione di denaro dai propri conti. Ad essa si ispirano le sentenze fino ad ora emanate dalla Suprema Corte di Cassazione per affermare la responsabilità delle banche per l'inadeguata protezione dei dati personali dei clienti, che abbia concorso al compimento di frodi informatiche ai loro danni.

Nell'ordinamento interno l'originaria disciplina della materia era contenuta nella legge 31 dicembre 1996, n. 675, adottata in attuazione della direttiva 95/46/CE ed abrogata, a decorrere dal 1° gennaio 2004, a seguito dell'entrata in vigore del Codice sulla *Privacy*, introdotto con il d.lgs. 30 giugno 2003, n. 196 [1]. Il Codice è stato poi integralmente riformato con il d.lgs. 10 agosto 2018, n. 101, che ha adeguato l'ordinamento nazionale al regolamento (UE) n. 2016/679, entrato in vigore il 25

maggio 2018, che ha abrogato la direttiva 95/46/CE. Pertanto, la materia è attualmente disciplinata sia dal Regolamento UE (GDPR), sia dal Codice *Privacy,* così come modificato ed adeguato alla normativa europea dal d.lgs. 101/2018 [2].
La normativa originaria ancorava il trattamento dei dati personali a previsioni minime di sicurezza, definite in modo puntuale nel disciplinare tecnico contenuto nell'allegato B del Codice della *Privacy*. L'art. 15 del Codice ricollegava il trattamento illecito dei dati personali alla responsabilità civile prevista dall'art. 2050 c.c. per i casi di esercizio di attività pericolosa, e sanciva inoltre la risarcibilità del danno non patrimoniale (art. 2059 c.c.). Ciò comportava che il titolare del trattamento era tenuto al risarcimento per i danni eventualmente prodotti, se non avesse provato di avere adottato tutte le misure idonee a evitarli.
La normativa introdotta dal Regolamento europeo si concentra sul principio dell' *accountability*, che si sostanzia nell'obbligo posto in capo ai titolari del trattamento dei dati personali di valutare le informazioni in loro possesso ed il loro conseguente valore, al fine di approntare le misure tecniche ed organizzative adeguate a mettere al sicuro tali dati. Il principio di *accountability* impone una gestione responsabile che tenga conto dei rischi connessi all'attività svolta e che sia idonea a garantire la piena conformità del trattamento dei dati personali ai principi sanciti dal Regolamento e dalla legislazione nazionale [3].
A questo principio si associa quello di "proporzionalità": il trattamento dei dati deve essere proporzionato rispetto allo scopo legittimo perseguito e riflettere in tutte le fasi un giusto equilibrio tra tutti gli interessi coinvolti e i diritti e le libertà in gioco. La concretizzazione del principio di *accountability* impone dunque al titolare di disporre le misure tecniche e organizzative adeguate per garantire che siano trattati solo i dati personali necessari per ogni specifica finalità del trattamento. Affinché una misura rispetti il principio di proporzionalità, i vantaggi derivanti dalla misura non dovrebbero essere compensati dagli svantaggi che la stessa comporta rispetto all'esercizio dei diritti fondamentali. Per adottare le misure di sicurezza adeguate in base al tipo di trattamento svolto, il titolare del trattamento deve effettuare un'analisi del rischio, vale a dire valutare tutti i possibili rischi che possono verificarsi in ordine ai dati trattati (articolo 24 del Reg. (UE) 2016/679 GDPR) [4].
Dalla normativa europea emerge chiaramente la volontà del legislatore di instaurare un apparato di tutela in relazione ai trattamenti effettuati con strumenti elettronici, individuando i necessari oneri che il titolare del trattamento deve porre in essere per assicurare il necessario *standard* di sicurezza, legislativamente previsto. Rispetto al Codice *Privacy* del 2003, si abbandona l'intento di ancorare i titolari del trattamento a previsioni minime di sicurezza, diversamente preferendo la loro responsabilizzazione, affidando ad essi l'incarico di comprendere l'importanza dei dati in proprio possesso; di decidere autonomamente le misure tecniche ed organizzative che si ritengono necessarie per assicurare la effettiva tutela dei dati personali, in considerazione della realtà produttiva in cui si opera; di dimostrare di aver adottato i necessari

adempimenti con l'osservanza delle adeguate misure, per soddisfare gli *standard* di tutela richiesti.

A tal fine, l'art. 5 del GDPR prevede espressamente i principi generali applicabili al trattamento dei dati personali. In particolare, esso richiama i principi della liceità e correttezza, riprendendo altri concetti quali la trasparenza, la minimizzazione, l'esattezza, la limitazione di conservazione, l'integrità e la riservatezza.

In sintesi, il passaggio dall'Allegato B del Codice della Privacy ad un sistema fondato sulla responsabilizzazione del titolare si fonda sia sugli effetti derivanti dal progresso tecnologico, sia – e soprattutto – sulla comprensione della diversità dei contesti in cui i dati sono trattati, prescrivendo ai titolari del trattamento un onere di rendicontare e dimostrare di aver predisposto tutti gli adempimenti necessari [6]. Il titolare è quindi tenuto ad adottare tutti quegli strumenti che siano inerenti al contesto di riferimento e che mettano al sicuro i dati in loro possesso, tenendo conto che alcune misure di sicurezza che risultano adeguate ad un contesto potrebbero non esserlo in altri.

In applicazione di questi principi, l'art. 24 del GDPR prescrive che il titolare del trattamento è tenuto ad adottare tutte le misure di sicurezza adeguate, prime tra tutte quelle atte a verificare l'identità di chi chiede l'accesso, con particolare attenzione ai casi in cui ciò avvenga direttamente *on line*. In questo contesto, egli è responsabile in via generale per qualsiasi trattamento di dati personali che abbia effettuato direttamente o che altri abbiano effettuato per suo conto, nonché del pregiudizio per i diritti e le libertà delle persone fisiche. Sotto quest'ultimo profilo, si rileva che i rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale [7]. Il rischio dovrebbe essere considerato in base a una valutazione oggettiva, mediante cui si stabilisce se i trattamenti di dati comportano un rischio ordinario o elevato.
Nella nuova normativa, il sistema della responsabilità civile per l'illecito trattamento dei dati personali, trova cardine nell'art. 82 del GDPR; di conseguenza, il d.lgs. 101/2018, che costituisce la legge di raccordo con il regolamento europeo, ha abrogato espressamente l'art. 15 del Codice *Privacy*. L'articolo 82 del Regolamento europeo sancisce al primo paragrafo che chiunque subisca un danno *"materiale o immateriale"* (ossia, patrimoniale o non patrimoniale), causato da una violazione del GDPR, ha diritto ad ottenere il risarcimento del danno dal titolare o dal responsabile del trattamento dei dati personali. Viene così riconosciuta espressamente l'ammissibilità anche del danno non patrimoniale e vengono identificati gli elementi necessari per la nascita dell'obbligazione risarcitoria: la condotta attiva o quella omissiva contraria al regolamento; il danno; il rapporto causa-effetto tra questi. Il legislatore pone al centro della fattispecie il soggetto debole del rapporto, costruendo la disposizione attorno al danneggiato ed al suo diritto al risarcimento [8].

La disposizione normativa dell'art. 82, comma 3, del GDPR, chiarisce le condizioni di esonero dalla responsabilità; in particolare, stabilisce che il titolare e il responsabile del trattamento sono esenti da responsabilità solo nel caso in cui dimostrano che l'evento dannoso non è in alcun modo a loro imputabile.

La ragione dell'inversione dell'onere della prova risiede nel fatto che il trattamento dei dati è attività considerata pericolosa. Infatti, essa è consentita dall'ordinamento giuridico perché utile, con conseguente compensazione del rischio di violazione dei dati personali tramite l'obbligo a carico delle organizzazioni di garantirne la sicurezza dei trattamenti.

Soprattutto al fine di proteggere il soggetto debole del rapporto è il titolare, ovvero il contitolare e il responsabile del trattamento a dover dimostrare che l'evento dannoso non è a loro imputabile. In altri termini, seguendo la logica dell'inversione dell'onere della prova, i suddetti soggetti, per poter essere esonerati da responsabilità, dovranno provare che l'evento dannoso non è loro ascrivibile in quanto dipendente da una fonte estranea alla loro sfera di competenza o di controllo, oppure che sono state da loro predisposte ed attuate, in seguito alla valutazione dei rischi (*Data Protection Impact Assessment*: art. 35 GDPR), tutte le prevedibili misure adeguate (art. 32 GDPR) al fine di evitare che si verificasse il danno. Diversamente, nel chiedere il risarcimento del danno, l'interessato dovrà provare l'esistenza del danno e la sua quantificazione, la sussistenza di una condotta in violazione della normativa a tutela dei dati personali e la relazione causale tra i primi due elementi.
Nel definire le misure di sicurezza da adottare, il paragrafo 1 dell'articolo 32 prevede alla lettera b) "*la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento*" e alla lettera c) "*la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico*". Infine, la lettera d) prevede il ricorso ad una procedura che ha l'obiettivo di *"testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento"*. Il secondo paragrafo dell'articolo richiede inoltre che si valuti *"l'adeguato livello di sicurezza"* e che si tenga conto dei rischi presentati dal trattamento che derivano *"dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati"*.

Pertanto, la norma individua una serie di misure tecniche e di condotte che misurano il grado di diligenza che il responsabile del trattamento dei dati personali ha l'obbligo di adottare, dal punto di vista tecnico e organizzativo [9]; nel contempo, essa pone in evidenza i rischi che potrebbero emergere dalla distruzione, dalla perdita o dalla modifica dei dati, e fa emergere la tipologia dei danni che potrebbero derivare dalla violazione dei necessari obblighi di protezione [10].

Secondo il Regolamento, le azioni legali per l'esercizio del diritto al risarcimento del danno devono essere promosse dinanzi alle Autorità giurisdizionali dello Stato membro in cui l'interessato risiede abitualmente, salvo che il titolare, il contitolare o il responsabile del trattamento sia un'Autorità pubblica di uno Stato membro nell'esercizio dei pubblici poteri (art. 79, par. 2); nel qual caso, prevale la giurisdizione che comprende l'Autorità pubblica.
In Italia, la competenza spetta in via ordinaria al Giudice civile, fatto sempre salvo, in sintonia con quanto stabilito dal Regolamento, il criterio del riparto di giurisdizione tra giustizia ordinaria ed amministrativa di cui all'art. 103 Cost. e art. 7 Codice del processo amministrativo (d.lgs. 104/2010). Un ruolo importante è riconosciuto all'Arbitro Bancario Finanziario (ABF), il quale costituisce un sistema di risoluzione alternativa delle controversie (*ADR-Alternative Dispute Resolution*) che possono sorgere tra i clienti e le banche e gli altri intermediari in materia di operazioni e servizi bancari e finanziari.

Nella logica della protezione dei dati personali la presenza di un obbligo risarcitorio civile, unitamente alla presenza di sanzioni penali e amministrative, costituisce un incentivo per il titolare e il responsabile a mantenere maggiore attenzione e diligenza, così da predisporre, verificare e aggiornare le misure di sicurezza idonee ad impedire la violazione dei dati personali. Nel caso in cui vi fossero più responsabili, al fine di garantire l'effettivo e tempestivo risarcimento all'interessato, il soggetto o i soggetti lesi potranno domandare anche ad uno solo dei danneggianti l'intero ammontare del danno, e questi sarà tenuto a corrisponderlo, salva poi la possibilità di rivalersi nei confronti dei coobbligati in solido per la quota ad essi imputabile [11].

In altri termini, ove siano coinvolti più soggetti nella stessa qualità [due o più titolari (contitolari) o due o più responsabili] oppure in qualità diverse (un titolare ed un responsabile), tutti risponderanno in solido del danno cagionato. Dal combinato disposto delle norme di cui agli artt. 28 e 82 GDPR emerge che la richiesta di risarcimento potrà essere proposta non solo nei confronti del titolare del trattamento, ma anche verso il responsabile del trattamento designato, limitatamente all'inadempimento degli obblighi a lui imposti dal GDPR o se abbia agito in modo difforme o in contrasto con le istruzioni ricevute dal titolare. Questa limitazione si giustifica in virtù dell'incarico conferito al titolare e della strumentalità della cornice complessiva che deve essere definita da parte del titolare [12].

In ogni caso sia il titolare, sia il responsabile hanno obblighi generali di prevenire i danni derivanti da un trattamento di dati. L'imputabilità del titolare e del responsabile dovrà essere necessariamente interpretata alla luce del principio di responsabilizzazione o *accountability* che incentra il GDPR. Tuttavia, tale principio configura una responsabilità civile quando si concretizzerà un danno e sarà quindi necessario accertare l'imputabilità dell'evento dannoso al titolare e al responsabile, i quali dovranno provare non di aver predisposto tutte le misure idonee a prevenire il

danno, ma che tale danno si è verificato per un fatto che non poteva essere prevenuto (e quindi previsto), poiché esulava dal loro controllo (caso fortuito o forza maggiore).

Sul punto, possono esserci molteplici elementi idonei a dimostrare che il fatto non potesse essere ricondotto al controllo del titolare e del responsabile, quali, ad esempio, l'adesione a codici di condotta approvati, la tenuta di un registro delle attività di trattamenti, il ricorso a responsabili del trattamento con comprovata conoscenza specialistica per approntare le misure tecniche ed organizzative richieste dal GDPR. Tali elementi però non saranno sufficienti, in quanto occorrerà dimostrare che le misure di azzeramento o diminuzione del rischio di violazione dei dati fossero proporzionali al grado di rischio che il trattamento presentava originariamente.

Per quanto concerne le tipologie di danni risarcibili, l'art. 82 GDPR afferma che l'interessato può richiedere il risarcimento dei danni materiali e immateriali. In pratica dovrà essere risarcito ogni tipo di danno che l'interessato possa subire dalla violazione dei suoi dati personali, quali: la perdita del controllo dei dati personali; la limitazione dei loro diritti; il furto o l'usurpazione d'identità; perdite finanziarie; perdita di riservatezza dei dati personali protetti da segreto professionale; o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata.

Il senso è ovviamente quello di attribuire all'interessato il diritto ad essere risarcito per ogni tipo di danno che quest'ultimo possa subire dalla lesione dalla violazione dei suoi dati personali, anche se le definizioni di danni materiali e immateriali non sono letteralmente identiche a quelle del codice civile italiano, ove il riferimento è ai danni patrimoniali e non patrimoniali. Inoltre, il concetto di danno dovrebbe essere interpretato alla luce della giurisprudenza della Corte di Giustizia ai fini di ripristino del pregiudizio subito dall'interessato. Ciò apre la possibilità di estendere al campo della protezione dei dati personali (quale diritto fondamentale dell'UE) numerose tipologie di danni enucleate negli anni dalla Corte in questione.

Pertanto, vista l'importanza e la delicatezza della materia e soprattutto dei dati degli utenti che vengono trattati, è doveroso affidarsi a soggetti competenti in materia, tenuti ad effettuare una valutazione del rischio legato al trattamento stesso ed a mettere quindi in campo adeguate contromisure per limitare gli eventuali rischi. Si tratta di misure che hanno come fine la garanzia di un livello di sicurezza adeguato, e quindi anche della riservatezza.

## 3. LE NORMATIVE EUROPEE SUI SERVIZI DI PAGAMENTO.

Con riguardo agli istituti di credito, la normativa generale sulla tutela dei dati personali deve essere integrata con quella che disciplina la tutela dell'utente per i servizi di pagamento. La prima direttiva europea in materia – identificabile con la Direttiva 2007/64/CE, anche nota come PSD – *Payment Services Directive* – ha definito un quadro giuridico comunitario moderno per i servizi di pagamento elettronici. Più in dettaglio, la PSD si è proposta i seguenti obiettivi: regolamentare l'accesso al mercato

per favorire la concorrenza nella prestazione dei servizi; garantire maggiore tutela degli utenti e maggiore trasparenza; standardizzare i diritti e gli obblighi nella prestazione e nell'utilizzo dei servizi di pagamento per porre le basi giuridiche per la realizzazione dell'Area unica dei pagamenti in euro (Sepa); stimolare l'utilizzo di strumenti elettronici e innovativi di pagamento per ridurre il costo di inefficienti strumenti, quali quelli cartacei ed il contante. La PSD è stata recepita nell'ordinamento nazionale con il d.lgs. 27 gennaio 2010, n. 11.
La Direttiva 2007/64/CE è stata sostituita dal 13 gennaio 2018 dalla Direttiva 2015/2366/UE (cosiddetta PSD2), la quale si inserisce nell'ambito degli interventi di modernizzazione del quadro legislativo del mercato europeo dei pagamenti al dettaglio, volti a sviluppare sistemi di pagamento elettronico sicuri, efficienti ed innovativi per consumatori, imprese ed esercenti. Le maggiori novità della PSD2 rispetto alla prima direttiva sui servizi di pagamento riguardano le nuove procedure di sicurezza per l'accesso al conto *online* ed i pagamenti elettronici e ai nuovi servizi di pagamento offerti dalle banche e dai nuovi operatori di mercato nell'area dell'*e-commerce* e dello *shopping online*. Essa tiene conto dell'evoluzione, anche culturale, che si è registrata nel settore dei pagamenti digitali, che registrano una crescita elevata anche in Italia [13].

La PSD2 è stata recepita nell'ordinamento nazionale con il d.lgs. del 15 dicembre 2017, n. 218, che ha modificato con effetto dal 13 gennaio 2018 il d.lgs. 11/2010. Essa è integrata dalle disposizioni del Regolamento delegato (UE) 2018/389, entrato in vigore il 14 settembre 2019, che disciplina le nuove misure di sicurezza e la comunicazione sicura tra i soggetti coinvolti nella prestazione dei servizi di pagamento.

In particolare, la nuova direttiva PSD2 ridefinisce il mercato europeo dei pagamenti, tracciando una linea di rottura con il passato e favorendo lo sviluppo di un nuovo inquadramento. Essa si propone soprattutto di creare un mercato unico dei pagamenti elettronici e di fronteggiare l'aumento dei rischi per la sicurezza dovuto sia alla previsione di nuovi strumenti di pagamento, tecnologicamente più avanzati, sia allo sviluppo del volume dell'*e-commerce* [14].
Aspetto centrale della direttiva PSD2 è la maggior tutela per l'utente, in risposta al bisogno di regolamentare le transazioni digitali, che negli ultimi anni stanno subendo un forte sviluppo, con conseguente evoluzione del settore dei pagamenti, attribuendo un ruolo centrale alla *digital transformation* del mondo bancario, soprattutto con riferimento all'operato sia delle banche, sia dei soggetti considerati fornitori di "*servizi di tipo bancario*". La PSD2 prevede un modo di operare delle banche più semplice ed una gestione dei pagamenti più sicura e conveniente. Dal punto di vista della semplicità i nuovi sistemi di pagamento *online* consentono di evitare il ricorso alle carte di credito ed ai *bancomat*; dal punto di vista della sicurezza dei pagamenti *online*, la direttiva in esame prevede che tutte le piattaforme di *e-*

*commerce* devono prevedere, nelle proprie procedure di pagamento, sistemi di autenticazione innovativi, in grado di ottimizzare la sicurezza nelle transazioni (quali la 3DS 2.0 e la SCA – *Strong Customer Authentication*) [15].

Specificamente, al fine di assicurare un'adeguata tutela dell'utente, l'articolo 64 della PSD2 prevede che ciascuna operazione di pagamento deve essere da lui autorizzata mediante appositi strumenti di pagamento e credenziali di sicurezza personalizzate. Nel contempo, la disposizione in esame pone specifici obblighi di diligenza a carico dell'utente: infatti, egli è tenuto a notificare al prestatore del servizio lo smarrimento, il furto, l'appropriazione indebita o l'utilizzo non autorizzato dello strumento di pagamento e ad adottare le misure necessarie per proteggere le credenziali di sicurezza personalizzate dello strumento di pagamento.

Tuttavia, la normativa europea prevede obblighi più rigorosi e pregnanti nei confronti del prestatore dei servizi in relazione agli strumenti di pagamento, ex artt. 70, 72 e 73 PSD2. Infatti, il favor per la tutela dell'utente trova riscontro nelle disposizioni che disciplinano le sue responsabilità [16].

In particolare, il prestatore dei servizi di pagamento sostiene il rischio dell'invio all'utente di uno strumento di pagamento o delle eventuali credenziali di sicurezza personalizzate necessarie. Inoltre, egli deve assicurare che le credenziali di sicurezza personalizzate siano accessibili solo all'utente autorizzato ad usufruire dello strumento e la disponibilità di mezzi adeguati affinché egli possa provvedere alla notifica in caso di furto o uso indebito.

L'articolo 73 della PSD2 prevede poi espressamente che il prestatore di servizi di pagamento è responsabile per le operazioni di pagamento non autorizzate e deve rimborsare al pagatore l'importo dell'operazione di pagamento non autorizzata, immediatamente e in ogni caso al più tardi entro la fine della giornata operativa successiva a quella in cui prende atto dell'operazione o riceve una notifica in merito, salvo il caso di sospetto di frode.

Reciprocamente, l'articolo 74 prevede che l'utente può essere obbligato a sopportare fino alla concorrenza massima di 50 EUR la perdita relativa ad operazioni di pagamento non autorizzate, derivante dall'uso di uno strumento di pagamento smarrito o rubato o dall'appropriazione indebita di uno strumento di pagamento [17]. Tuttavia, tale franchigia non si applica se lo smarrimento, il furto o l'appropriazione indebita di uno strumento di pagamento non potevano essere notati dal pagatore prima di un pagamento, ad eccezione dei casi in cui il pagatore ha agito in modo fraudolento, ovvero se la perdita è stata causata da atti o omissioni di dipendenti o agenti del fornitore di servizi o di un'entità a cui sono state esternalizzate le attività.

Il pagatore sarà tenuto a sostenere tutte le perdite relative ad operazioni di pagamento non autorizzate soltanto nel caso in cui ha agito in modo fraudolento o non

adempiendo a uno o più obblighi di prescritti con dolo o con negligenza grave. In tali casi, il massimale non si applica.

Quanto agli oneri probatori, qualora siano disposte ed eseguite operazioni non autorizzate dall'utente, spetta al prestatore di servizi di pagamento dimostrare che l'operazione di pagamento è stata autenticata, correttamente registrata e contabilizzata, e che non ha subito le conseguenze di guasti tecnici o altri inconvenienti del servizio fornito dal prestatore di servizi di pagamento. Inoltre, l'utilizzo di uno strumento di pagamento registrato dal prestatore di servizi di pagamento non è di per sé sufficiente a dimostrare che l'operazione di pagamento sia stata autorizzata dal pagatore, né che questi abbia agito in modo fraudolento o non abbia adempiuto, dolosamente o con negligenza grave, ai suoi obblighi. Il prestatore di servizi di pagamento è tenuto altresì a fornire gli elementi di prova che dimostrano la frode o la negligenza grave da parte dell'utente di servizi di pagamento.

La ragione giustificativa delle responsabilità del fornitore dei servizi di pagamento nel caso di pagamenti non autorizzati, deve essere rinvenuta negli obblighi di protezione su di lui gravanti. Egli è infatti tenuto a garantire la sicurezza delle transazioni effettuate con l'uso di strumenti di pagamento, con particolare riguardo a quelli elettronici a distanza.

L'elemento centrale di questa disciplina è costituito dall'obbligo di procedere all' "autenticazione forte" dell'utente che disponga il pagamento, ai sensi degli articoli 97 e 98 PSD2**,** integrata dal Regolamento Delegato UE 218/389 della Commissione, che contiene le norme tecniche per assicurare *standard* aperti di comunicazione comuni e sicuri.
L' "autenticazione forte" dell'utente (c.d. *strong customer authentication*) costituisce una delle principali novità apportate al regime della responsabilità del fornitore dei servizi per le operazioni di pagamento non autorizzate. L**'** art. 4, n. 30, PSD2 la definisce come *"un'autenticazione basata sull'uso di due o più elementi, classificati nelle categorie della conoscenza (qualcosa che solo l'utente conosce), del possesso (qualcosa che solo l'utente possiede) e dell'inerenza (qualcosa che caratterizza l'utente), che sono indipendenti, in quanto la violazione di uno non compromette l'affidabilità degli altri, e che è concepita in modo tale da tutelare la riservatezza dei dati di autenticazione"*. Essa deve comprendere elementi che colleghino in maniera dinamica l'operazione a uno specifico importo e ad un beneficiario specifico, nonché la predisposizione di misure di sicurezza adeguate per tutelare la riservatezza e l'integrità delle credenziali di sicurezza personalizzate degli utenti di servizi di pagamento [18]**.**
L' "autenticazione forte" costituisce un irrigidimento degli *standard* di autenticazione, e cioé della procedura che consente al prestatore di verificare l'identità di un utente o di verificare la validità dell'uso di uno strumento di pagamento, compreso l'uso delle credenziali di sicurezza personalizzate dell'utente. In altri termini, perché

l'autenticazione possa dirsi "forte", l'utente che voglia disporre un'operazione di trasferimento di fondi deve superare almeno due ostacoli.
Per quanto disposto dagli articoli 6, 7 ed 8 del Regolamento delegato (UE) 2018/389, gli elementi di autenticazione possono afferire: a) alla categoria della "conoscenza" (così da rientrare tra i dati trattenuti nella memoria dell'utente e prudentemente da non divulgare, come la *username*, la *password*, i dati relativi alle ultime transazioni effettuate, i dati relativi alla residenza e alla nascita dell'utente, ecc.); alla categoria del "possesso" (rientrando così tra i dati che possano essere reperiti attraverso un oggetto materiale e siano preferibilmente generati *ad hoc*, con utilizzabilità molto limitata nel tempo, come avviene per il codice generato da un *token* o per un codice inviato al numero di telefono dell'utente); alla categoria dell' "inerenza" (come avviene per tutti i dati biometrici utilizzabili dall'utente per autenticarsi, quali la voce, lo *scan* dell'occhio, il riconoscimento facciale, la lettura dell'impronta digitale, ecc.). Trattasi di tecnologie sicure, già considerevolmente diffuse da diversi anni nelle prassi dei fornitori di servizi di pagamento, che il fornitore di servizi di pagamento può liberamente adottare nell'ambito della sua autonomia organizzativa, nel rispetto del principio di "neutralità tecnologica".

Nella procedura di autenticazione "forte" assume particolare importanza il requisito della "indipendenza" degli elementi che la compongono [19]. Ciò implica che ciascuno degli elementi classificati nelle categorie della conoscenza, del possesso e dell'inerenza, attraverso i quali si compie la procedura di autenticazione, non deve condizionare e non deve essere condizionato dagli altri. In questo modo, la violazione di un elemento non deve compromette l'affidabilità degli altri, che dovrebbero risultare da soli sufficienti a proteggere la riservatezza dei dati di autenticazione [20].

Con l'attuazione della PSD2, l'impiego di tecnologie adeguate alla *strong authentication*, costituisce un vero e proprio obbligo per il prestatore di servizi di pagamento. L'art. 74, paragrafo 2, PSD2 dispone infatti che se il prestatore di servizi di pagamento del pagatore non esige un'autenticazione forte del cliente, il pagatore non sopporta alcuna conseguenza finanziaria, salvo qualora abbia agito in modo fraudolento [21]. Parimenti, il mancato impiego dell'autenticazione forte, ai sensi dell'art. 92, par. 1, PSD2, comporta una più sfavorevole modulazione della ripartizione di responsabilità per le operazioni non autorizzate, ai fini dell'eventuale esercizio del diritto di regresso fra più prestatori.
Interessa infine evidenziare che l'autenticazione forte del cliente è richiesta per tutte le attività e le operazioni che possono comportare rischi per la tutela della sua *privacy* e per la sicurezza delle sue operazioni e del suo patrimonio. In particolare, l'art. 97, comma 1, PSD2, e l'art. 4, comma 1, secondo periodo, del Regolamento delegato (UE) 2018/389, prescrivono che i prestatori di servizi di pagamento devono applicare l'autenticazione forte del cliente tutte le volte che egli accede al suo conto di pagamento *on line* o dispone un'operazione di pagamento elettronico, nonché tutte le

volte che *"effettua qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi"*.
Ai sensi dell'art. 98, comma 1, lett. b), della PSD2 e degli artt. 2 e 18 del Regolamento delegato (UE) 2018/389, i prestatori di servizi di pagamento sono autorizzati a non applicare l'autenticazione forte solo se abbiano determinato che l'operazione di pagamento elettronico a distanza, disposta dal pagatore, presenta un basso livello di rischio; da ciò si desume, con ragionamento *a contrario*, che questo obbligo assume particolare cogenza per le operazioni che presentino fattori di rischio maggiori o che si presentino particolarmente sospette.
L'opzione per l'effettuazione o meno dell' "autenticazione forte" deve essere effettuata sulla base di meccanismi di monitoraggio delle operazioni che i fornitori dei servizi sono obbligati ad adottare per poter rilevare le operazioni di pagamento non autorizzate o fraudolente, tenendo conto di una serie di fattori di rischio, tra cui – in particolare – l'importo di ciascuna operazione di pagamento; gli scenari di frode noti nella prestazione dei servizi di pagamento; i segnali della presenza di *malware* in una qualsiasi delle sessioni della procedura di autenticazione. Come affermato dal primo considerando del Regolamento delegato (UE) 2018/389, infatti, occorre assicurare che i servizi di pagamento offerti elettronicamente siano prestati in maniera sicura, *"ricorrendo a tecnologie in grado di garantire l'autenticazione sicura dell'utente e di ridurre il più possibile il rischio di frode. La procedura di autenticazione dovrebbe includere, in generale, meccanismi di monitoraggio delle operazioni al fine di rilevare i tentativi di utilizzo delle credenziali di sicurezza personalizzate di un utente dei servizi di pagamento che sono state perse, rubate o oggetto di appropriazione indebita e dovrebbe altresì garantire che l'utente dei servizi di pagamento sia l'utente legittimo, che pertanto acconsente al trasferimento di fondi e all'accesso alle informazioni sul suo conto attraverso un utilizzo normale delle credenziali di sicurezza personalizzate"*.
In applicazione di queste regole, occorre ritenere che sia richiesta l'autenticazione forte in tutti i casi in cui l'utente, modificando i dati del suo profilo personale, richieda la variazione del dispositivo associato alle operazioni di pagamento (e, quindi, la variazione del numero di cellulare a cui inviare i messaggi per l'identificazione dell'utente); e ciò per l'evidente ragione che una simile variazione comporta il grave rischio che gli elementi di autenticazione di una successiva operazione di pagamento, che rientrino nella categoria dell' "inerenza" (come una *One Time Password*), siano dirottati dal dispositivo dell'utente (al quale dovrebbero essere inviati per assicurare la sua corretta individuazione, secondo le prescrizioni dell'art. 24 del Reg. 2018/389), verso quello di un altro soggetto, che abbia richiesto abusivamente la variazione per finalità fraudolente. In altri termini, occorre evitare che la sola acquisizione delle credenziali di accesso ad un conto da parte di un terzo sia sufficiente a modificare i dati identificativi dell'utente e l'associazione del suo dispositivo, in modo da vanificare la sua protezione in caso di successive operazioni di pagamento; è dunque necessario assicurare che l'acquisizione abusiva delle credenziali di un utente da parte di un terzo

non sia sufficiente a disporre un pagamento abusivo sul suo conto, per l'esistenza di ulteriori sistemi che permettano di rilevare l'utilizzo abusivo dei dati di identificazione dell'utente legittimo.
Qualora sia compromessa l'integrità dei dati personali dell'utente (come nel caso di abusiva variazione degli elementi di associazione al dispositivo da lui utilizzato per le operazioni a distanza), risulterà conseguentemente compromessa la procedura di autenticazione nelle successive operazioni di pagamento elettronico a distanza, che prevedano elementi di autenticazione classificati come inerenza. Infatti, gli elementi di autenticazione (come la *One Time Password*) saranno inviati, letti ed utilizzati da altro soggetto, che potrà autenticarsi abusivamente ed effettuare l'operazione di pagamento a nome dell'utente effettivo, in violazione dell'art. 8 del Reg. 2018/389. La violazione di queste regole potrà apparire di gravità ancor maggiore in caso di operazioni di pagamento anomale, che dovrebbero essere rilevate e prevenute dai meccanismi di monitoraggio poste in essere dai fornitori dei servizi di pagamento (come nel caso di emissione di un bonifico immediato di rilevante importo, che segua di pochi minuti l'avvenuta variazione del numero di telefono cellulare dell'utente, a cui inviare la OTP richiesta per l'autenticazione).

## 4. LA RESPONSABILITÀ DEI FORNITORI DI SERVIZI DI PAGAMENTO PER LE OPERAZIONI NON AUTORIZZATE NELLA GIURISPRUDENZA ORDINARIA ED ARBITRALE

Alla luce delle normative esposte, assume particolare rilevanza la questione della responsabilità degli istituti bancari, quali fornitori di servizi di pagamento elettronici a distanza, per la mancata adozione delle necessarie misure di sicurezza avverso i tentativi di frode effettuati sui conti del cliente da parte di terzi, mediante l'utilizzo abusivo delle sue credenziali personalizzate, che siano state perse o rubate o abbiano costituito oggetto di appropriazione indebita. Occorre verificare se ed in quali termini sia possibile ricondurre nell'area del rischio professionale dei fornitori dei servizi di pagamento l'abusiva utilizzazione dei codici di accesso al sistema da parte dei terzi, che non sia attribuibile al dolo o alla colpa grave dello stesso utente e che non potesse essere fronteggiata in anticipo.

Sul tema occorre analizzare gli interventi giurisprudenziali adottati dalla Corte di Cassazione e dall'Arbitro Bancario Finanziario (ABF) [22], nell'intento di assicurare la sicurezza nei pagamenti elettronici a distanza e di tutelare i soggetti danneggiati.

A tal riguardo, si registra una comune tendenza a valorizzare la tutela del cliente e ad evidenziare gli obblighi di protezione delle banche, sulla base di un duplice indirizzo:

a) la giurisprudenza della S. Corte, che – intervenendo in sede legittimità su giudizi instaurati alcuni anni fa, sulla base della disciplina vigente all'epoca – riflette normalmente i principi civilistici e le disposizioni generali in tema di protezione dei dati personali contenuta nel Codice *Privacy*, nel periodo antecedente alle modifiche

apportate dal Regolamento UE 2016/679 (e perciò, come si è già visto, sulle disposizioni dell'art. 15 del d.lgs. 196/2003, che ricollegava la responsabilità del titolare del trattamento dei dati personali alla disciplina dell'esercizio di attività pericolose contenuta nell'art. 2050 c.c.);

b) la giurisprudenza arbitrale, che – quale giurisdizione di primo grado – riguarda fatti e situazioni più recenti, disciplinati dall'ultima normativa europea sui pagamenti con mezzi elettronici a distanza.

La giurisprudenza della Suprema Corte di Cassazione tende a riconoscere la responsabilità civile dell'intermediario per le fraudolente sottrazioni di denaro subite dal correntista, superando così l'indirizzo precedente, ritenuto eccessivamente gravoso per il cliente, in forza del quale la responsabilità per l'intercettazione dei dati informatici ricadeva unicamente in capo al cliente, colpevole di aver adottato un comportamento incauto o negligente nell'esecuzione delle operazioni bancarie o nella custodia delle chiavi di accesso. A tal proposito, viene valorizzato il fatto che la banca fornisce i suoi servizi nell'esercizio di un'attività professionale e deve impiegare una diligenza qualificata nell'adempimento del contratto, che impone l'adozione di tutte le misure di sicurezza più adeguate al fine di prevenire insorgenza di danni in capo ai correntisti.

In particolare, in tema di ripartizione dell'onere della prova ed alla stregua dell'art. 15 del Codice della *Privacy* e dell'art. 2050 c.c., al correntista abilitato ad eseguire operazioni *online* spetta soltanto la prova del danno, in quanto riferibile al trattamento dei suoi dati personali, mentre l'istituto creditizio risponde, quale titolare del trattamento dei dati, dei danni conseguenti al fatto di non avere impedito a terzi l'intrusione illegittima mediante la captazione dei codici di accesso del correntista, ove non dimostri che l'evento dannoso non gli sia imputabile, perché discendente da errore o frode del correntista o da forza maggiore [23]. Quindi, non solo la banca, qualora ne ricorrano i requisiti, deve essere chiamata a rispondere del danno patito dal suo utente, che non sia incorso in colpa grave, ma la sua responsabilità è gravata dell'onere di provare il corretto funzionamento del sistema adottato e la sua adeguatezza a fronteggiare ogni possibile attacco informatico [24].

Questa impostazione ha trovato condivisione nelle decisioni di molteplici Tribunali ed ha poi ricevuto l'avvallo della giurisprudenza di legittimità (cfr. Cass. Civ., n. 18045/2019; Cass. Civ., ord. n. 9158 del 2018; Cass. Civ., n. 31199/2017; Cass. Civ. n. 2950/2017; Cass Civ. n. 10638/2016. Nella giurisprudenza di merito, cfr. Tribunale di Palermo, 20 Dicembre 2009; Tribunale di Nocera, 15 settembre 2011; Tribunale di Parma, 23 luglio 2013; Giudice di pace di Lecce, 4 dicembre 2013; Tribunale di Milano, 4 dicembre 2014; Tribunale di Roma, 31 agosto 2016).

Questo indirizzo è stato recentemente confermato dalla ordinanza resa dalla S. Corte in data 26 novembre 2020 con il n. 26916, che dà seguito alla pregressa

giurisprudenza, secondo cui: *"in tema di responsabilità della banca, ovvero dell'erogatore del corrispondente servizio, in caso di operazioni effettuate a mezzo di strumenti elettronici, anche al fine di garantire la fiducia degli utenti nella sicurezza del sistema (il che rappresenta interesse degli stessi operatori), è del tutto ragionevole ricondurre nell'area del rischio professionale del prestatore dei servizi di pagamento – prevedibile ed evitabile con appropriate misure destinate a verificare la riconducibilità delle operazioni alla volontà del cliente – la possibilità di un'utilizzazione dei codici di accesso al sistema da parte dei terzi, non attribuibile al dolo del titolare o a comportamenti talmente incauti da non poter essere fronteggiati in anticipo"*. Da ciò consegue che, *"anche prima dell'entrata in vigore del d.lgs. n. 11 del 2010, attuativo della direttiva n. 2007/64/CE relativa ai servizi di pagamento nel mercato interno, l'erogatore di servizi, cui è richiesta una diligenza di natura tecnica, da valutarsi con il parametro dell'accorto banchiere, è tenuto a fornire la prova della riconducibilità dell'operazione al cliente (Cass., 03/02/2017, n. 2950; cfr. altresì Cass., 05/07/2019, n. 18045, secondo cui 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, configurabile, ad esempio, nel caso di protratta attesa prima di comunicare l'uso non autorizzato dello strumento di pagamento, posto che la sollecita consultazione degli estratti gli avrebbe consentito di conoscere quell'uso in tempo più utile)"*.

Per tali motivi, occorre affermare che la possibilità di un'utilizzazione dei codici di accesso al sistema da parte dei terzi, non attribuibile al dolo del titolare o ai comportamenti incauti da non potere essere fronteggiati in anticipo, rientra nell'area del rischio professionale del prestatore dei servizi di pagamento, prevedibile ed evitabile con appropriate misure volte a verificare la riconducibilità delle operazioni alla volontà del cliente. Tale conclusione è funzionale a garantire la fiducia degli utenti nella sicurezza del sistema bancario, tutelando così lo stesso interesse degli operatori economici, e nella legislazione attuale trova oggigiorno più puntuale e solido fondamento nella PSD2 in materia di servizi di pagamento nel mercato interno e nella normativa nazionale di recepimento (in virtù della quale è onere del prestatore di servizi fornire la prova della frode, del dolo o della colpa grave dell'utente che intenda disconoscere le operazioni di pagamento, la quale integra l'unica possibilità per la Banca di essere esente da responsabilità).

La suddetta diligenza presuppone che l'istituto di credito sia munito di un adeguato sistema di sicurezza, tale da impedire l'accesso ai dati personali del correntista da parte di terzi, con un obbligo contrattuale di garantire e tutelare i clienti dalle frodi informatiche. Pertanto, l'erogatore dei servizi è tenuto a fornire la prova della riconducibilità delle operazioni effettuate a mezzo di strumenti elettronici alla volontà

del cliente, mediante il controllo dell'utilizzazione illecita dei relativi codici da parte di terzi. Questa responsabilità trova tuttavia un limite, nel caso di colpa grave o dolo del cliente.

**4.2.** Gli orientamenti dell'ABF si incentrano su aspetti tecnici sottesi alle truffe informatiche attuate attraverso il *phishing* bancario, e su elementi relativi agli obblighi di protezione degli istituti di credito, alla ripartizione dei rischi, all'onere della prova e alla configurazione di dolo o colpa grave a carico dell'utilizzatore dei servizi.
Per quanto riguarda gli obblighi di protezione degli istituti di credito, la giurisprudenza arbitrale evidenzia che il sistema di autenticazione forte, introdotto dalla normativa europea, deve essere tale da impedire i tentativi fraudolenti di accesso alla *home banking* del cliente, attraverso l'uso di due o più elementi indipendenti, laddove la violazione di uno non deve compromettere l'affidabilità degli altri. A tal riguardo, le pronunce dell'ABF sottolineano che non deve sussistere una relazione funzionale tra le singole misure di sicurezza, perché in tal caso si finirebbe per eludere l'obbligo di doppia autenticazione, rendendo così il sistema debole. Invero, quando la violazione di una misura di sicurezza è in grado di compromettere anche l'affidabilità dell'altra, non si registra il requisito dell'"autenticazione forte", per il quale – al contrario – la piena operatività dell'organizzazione fondata sul multi-fattore deve incentrarsi sul concetto di indipendenza tra le singole misure di sicurezza (Cfr. Collegio Roma n. 14550/2019 e Collegio Milano n. 10666/2019).

Inoltre, l'Autorità bancaria europea individua un ulteriore profilo di responsabilità dell'intermediario, prevedendo l'obbligo di monitoraggio delle operazioni sospette prima che il prestatore dei servizi di pagamento autorizzi le operazioni o i mandati elettronici. Nello specifico, tutte le operazioni che sono sospette, ovvero ad alto rischio, devono essere sottoposte ad una dettagliata analisi e procedura di valutazione (Cfr. Collegio Roma n. 14550/2019).

In riferimento al profilo dell'onere della prova, è stato precisato in primo luogo che grava sull'istituto di credito provare l'insussistenza di malfunzionamenti dei propri apparati, la regolare autenticazione dell'utente per le operazioni compiute per il loro tramite, e la correttezza della registrazione e contabilizzazione delle operazioni medesime. Infatti, la banca è tenuta a fornire la prova della riconducibilità dell'operazione al cliente. L'inadempimento dell'obbligo di assicurarsi che le credenziali che consentono l'accesso al servizio di *internet banking* non fossero fruibili da soggetti diversi dall'utente, a norma dell'art. 8 d.lgs. 11/2010 e dell'art. 73 PSD2, determina una responsabilità dell'istituto bancario.
In secondo luogo, la prova di un corretto sistema di sicurezza, ove fornita, non si ritiene di per sé sufficiente a dimostrare il dolo o la colpa grave dell'utilizzatore. Conseguentemente grava sull'intermediario l'onere di dimostrare anche tutti i fatti idonei ad integrare la colpa grave o il dolo dell'utilizzatore, che integrano le sole fattispecie nelle quali questi è chiamato a subire le conseguenze dell'utilizzo

fraudolento dello strumento di pagamento. Per poter riconoscere una colpa grave nella condotta del cliente, è necessario che questa sia caratterizzata da una "*straordinaria e inescusabile*" imprudenza, negligenza o imperizia, determinata dalla violazione della diligenza ordinaria del buon padre di famiglia di cui all'art. 1176, co.1 c.c., ma anche da quel grado minimo ed elementare di diligenza generalmente osservato da tutti (cfr. Cass. n. 913/2011 e Cass. n. 14456/2011). In questa prospettiva, si riconosce una responsabilità, totale o parziale, dell'utente se, pur debitamente informato della esistenza ed adozione delle misure di sicurezza, ometta tuttavia di avvalersene (Cfr. Collegio dec. 528/2012).

Con riferimento ai più diffusi profili pratici, si è rilevato che l'operazione di variazione del numero di telefono abbinato alla carta di credito, mediante il quale effettuare la procedura di identificazione con invio di una *One Temporary Password* (OTP), deve esse garantita e disposta "solo" accedendo all'area riservata del portale con la digitazione delle credenziali personali del cliente, e che detta variazione deve essere completata solo inserendo una OTP che l'intermediario invia all'indirizzo di posta elettronica rilasciato dall'utente al momento dell'iscrizione allo stesso portale. Pertanto, costituisce fonte di responsabilità il cambiamento delle utenze telefoniche associate allo strumento di pagamento senza richiedere un'autenticazione forte del cliente (cfr., fra le molte, Collegio Roma, dec. n. 14550/2019; Collegio Milano, dec. n. 18393/2019, dec. n. 10666/2019, dec. n. 13624/2018; Collegio Bologna, dec. n. 7666/2017; Collegio Palermo, dec. 13217/2017; Collegio Bari, n. 14190/2017).

Invero, in applicazione dell'art. 12, comma 2, e dell'art. 8, comma 1, lett. a), d.lgs. 11/2010, il cliente deve essere avvertito con apposito *sms-alert* della modifica dell'utenza telefonica associata alla carta, "prima" di rendere effettive e irrevocabili le operazioni bancarie delle quali l'istituto di credito non ha la sicurezza della riconducibilità e dell'autorizzazione dell'utente, anche rispetto alla complessità del rischio delle disposizioni economiche impartite. Pertanto, la condotta dell'intermediario non è esente da colpa quando la modifica del recapito telefonico per il servizio di *sms-alert,* presenta un livello di sicurezza inidoneo alla diligenza richiesta dalla legge.

Sul tema, recenti decisioni adottate dell'ABF hanno riconosciuto una colpa grave della banca per la mancata adozione di un sistema adeguatamente protetto, con la doppia autenticazione, anche nel caso in cui il cliente comunichi i dati ovvero l'intero codice OTP al truffatore. Infatti, il solo codice OTP non è ritenuto sufficiente a garantire la sicurezza dei pagamenti *online*, in quanto la banca è tenuta ad aggiornare regolarmente i propri meccanismi di sicurezza per costituire un'autenticazione più sicura possibile. L'orientamento dei Collegi ABF è costante nel ritenere che la mancata attivazione di un sistema di *alert* delle operazioni compiute tramite carte di pagamento o dispositivi mobili costituisca una disfunzione organizzativa imputabile all'intermediario, restando, pertanto, ferma la responsabilità civile dell'intermediario (Cfr. Collegio Bologna, dec. n. 6551/2021, e dec. n. 6232/2021).

Giova ribadire che la nozione di autenticazione forte del cliente è definita con l'individuazione di specifici requisiti, prevendendo che sia tale un'autenticazione basata sull'uso di due o più elementi, classificati nelle categorie della conoscenza, del possesso e dell'inerenza, che sono indipendenti, in quanto la violazione di uno non compromette l'affidabilità degli altri, e che è concepita in modo tale da tutelare la riservatezza dei dati di autenticazione. Costituisce, infatti, principio costantemente affermato dai Collegi dell'ABF quello per il quale un sistema di protezione ad un solo fattore (cui può essere assimilato sostanzialmente il sistema statico, adottato nel caso di specie con l'invio del terzo codice OTP solo per le operazioni e non per il rinnovo di credenziali) non può essere considerato misura sufficiente a proteggere adeguatamente il cliente [25].

Come già esposto, la formula, fondata sui requisiti della conoscenza, del possesso e dell'inerenza, è chiarita dal Regolamento delegato (UE) 2018/389, il quale precisa che i prestatori di servizi di pagamento devono adottare misure volte ad attenuare il rischio che gli elementi dell'autenticazione forte del cliente siano acquisiti da terzi. Pertanto, dall'interpretazione della normativa europea e degli orientamenti decisionali e giurisprudenziali emerge chiaramente come l'autenticazione forte del cliente deve intendersi in senso sostanziale, e non meramente formale, dovendo garantire determinati requisiti che costituiscono elementi imprescindibili della stessa, tutti correlati alla necessità che sia tutelata la riservatezza dei dati di autenticazione.

La diligenza e gli obblighi che gravano sull'istituto bancario determinati dalla normativa europea, al fine di tutelare la sicurezza dei pagamenti elettronici e dell'utente, impongono l'utilizzo dell'autenticazione forte, a due fattori, anche per l'associazione dell'identità dell'utente alle credenziali personali, dispositivi e *software*, soprattutto in caso di associazione attuata per mezzo di canali a distanza e nel caso di rinnovo dei suddetti elementi. L'utilizzo di un dispositivo multifunzione (vale a dire un dispositivo come un *tablet* o un telefono cellulare) che può essere impiegato sia per disporre l'esecuzione del pagamento sia nel processo di autenticazione, impone che, ai sensi dell'art. 9 del Regolamento delegato (UE) 2018/389 siano adottate da parte del prestatore di servizi di pagamento misure di sicurezza al fine di attenuare il rischio che deriverebbe dalla compromissione di tale dispositivo multifunzione.
In mancanza di ulteriori misure di sicurezza, un sistema che consenta di modificare le credenziali personali e/o le modalità di ricezione delle credenziali dinamiche (necessarie per effettuare un'operazione di pagamento elettronico) attraverso canali per loro natura inidonei ad escludere il rischio di intromissione da parte di soggetti non possiede le caratteristiche proprie dell'autenticazione forte per garantire un elevato standard di tutela dell'utente. L'invio tramite *sms* della notifica di variazione dell'utenza cellulare collegata al sistema di autenticazione delle operazioni di pagamento risulta non inidoneo a tutelare efficacemente gli utenti, in quanto integra

un sistema di mera notifica *ex post* dell'avvenuta modifica. Da ciò deriva che, in tali ipotesi, sarà configurabile la responsabilità del prestatore dei servizi.

In altri termini, pur in presenza di un sistema di sicurezza basato sull'inserimento di un codice OTP, inviato ad un numero di cellulare associato all'utenza del titolare per poter effettuare le operazioni di pagamento, anche il controllo sull'associazione del dispositivo al cliente e il rinnovo delle credenziali dovrebbe essere ugualmente protetto da un sistema a due fattori: in caso contrario, i truffatori, accedendo all'area riservata del titolare, possono modificare il numero su cui la banca invia SMS e OTP, neutralizzando di fatto la protezione della chiave dinamica mediante OTP da utilizzare per la fase dispositiva. Si rende perciò evidente la necessità di inserimento del codice OTP anche per le operazioni di modifica dei dati anagrafici, che costituisce un doveroso presidio di sicurezza a tutela del cliente, idoneo a impedire il compimento delle operazioni di acquisto da parte di terzi.

## CONCLUSIONI

Alla luce della nuova cornice normativa, risulta centrale, allo stato attuale, la necessità di misure di sicurezza adeguate da parte degli Istituti bancari a tutela dei propri clienti ed a prevenzione dei fenomeni di truffa informatica. Dalla violazione degli obblighi di protezione derivano profili di responsabilità, da valutare sulla base dell'effettivo danno economico degli interessati, della gravità delle carenze rilevate nei sistemi bancari e della disponibilità del titolare del trattamento dei dati a porre un immediato rimedio al pregiudizio. Infatti, l'istituto di credito è tenuto all'immediato rimborso dell'importo dell'operazione di pagamento che non sia stata autorizzata, come previsto dall'art. 11, comma 1, d.lgs. 11/2010 e dall'art. 73 PSD2.

In ogni caso, le carenze individuate in tema di sicurezza per i pagamenti *online*, hanno reso non scusabili le violazioni al fine di responsabilizzare gli istituti di credito. Infatti, lo sviluppo delle tecnologie digitali e la diffusione del sistema telematico rendono inescusabili errori che comportano danni, economici e no, per l'utente.
Da questa prospettiva la sicurezza informatica costituisce l'evoluzione della protezione dei dati personali. Nei casi di specie sopra esposti, come il *phishing* bancario, le carenze di misure minime di sicurezza e di gestione della riservatezza dei dati integrano inevitabilmente gli estremi della responsabilità degli istituti bancari, a tutela della sicurezza e della fiducia dell'utente.
È evidente la necessità di programmare strumenti sempre più evoluti (diretti a proteggere i *file* e le informazioni raccolte nelle banche dati) e maggiore diligenza nell'operato degli istituti bancari. Da qui anche la necessità di costruire progressivamente una metodologia nella quale oltre agli aspetti tecnologici, oggi prevalenti, coesistono elementi di carattere giuridico (definizione e interpretazione delle regole legislative, comunitarie, amministrative, di autodisciplina volontaria delle categorie, di carattere contrattuale specifico), di carattere tecnico-scientifico

(definizione chiara di *standard* e sistemi telematici) e di carattere organizzativo ed economico.
Posto che la normativa europea ha introdotto un'autenticazione forte per la tutela degli utenti, si ritiene necessaria l'applicazione della suddetta *Strong Authentication* soprattutto in relazione al diffuso utilizzo di bonifici bancari istantanei (introdotti nel novembre 2017), che nel complesso del sistema determinano un maggior rischio di truffe *online*. Infatti, attraverso il bonifico istantaneo, che non è revocabile, si dispone il trasferimento del denaro da un conto corrente all'altro in pochi secondi e con disponibilità immediata da parte del beneficiario, senza possibilità di porre rimedio ad eventuali condotte abusive intercorse nella fase di autenticazione del disponente.

Avv. Carlotta Scotti

---

[1] Per ciò che riguarda la responsabilità penale viene in considerazione, innanzitutto, l'art. 167 del Codice sulla *Privacy*. Tale norma, infatti, punisce chiunque, al fine di trarre per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione della normativa di riferimento e arrecando un nocumento all'interessato. Sempre dal punto di vista penale, la condotta del cd. *phisher* potrebbe configurare gli estremi del reato di truffa ex art. 640, co.1 c.p. Il phishing integra, inoltre, una serie di fattispecie delittuose, tra cui: il reato di frode informatica di cui all'640-ter c.p., che presuppone l'alterazione di un sistema informatico o l'introduzione illecita sullo stesso o sui dati in esso contenuti, al fine di determinare un ingiusto profitto per il soggetto attivo e un danno per il soggetto passivo; il reato di cui all'art. 615-*ter*, comma 1, c.p., costituito dall'accesso abusivo ad un sistema informatico o telematico; il delitto di utilizzo indebito di carte di credito e di pagamento, previsto dall'art. 12 del d.l. n. 143/1991. Sul piano della responsabilità civile, come di seguito esposta, la questione si incentra sulla responsabilità da attività pericolosa e sul risarcimento del danno.
[2] L'*accountability* pre-GDPR del sistema bancario e le misure minime di adeguatezza della vecchia disciplina (Allegato B) non si differenziano totalmente dalle misure adeguate del nuovo paradigma del GDPR, anzi in quanto alcune sono in esse ricomprese. Nonostante sia stato abrogato il Disciplinare Tecnico costituito dall'Allegato B e tutte le norme di riferimento del vecchio Codice della *Privacy* richiamate per l'adozione del provvedimento ovvero i pre-vigenti artt. 162, comma 2-*bis*, 162, comma 2-*ter*, e 164-*bis*, comma 2, in relazione agli artt. 33 e 154, comma 1, lett. c), del medesimo Codice, tranne l'art. 154 comunque interamente emendato dal d.lgs. 101/2018, di modifica del Codice italiano per armonizzazione la normativa con il Regolamento Europeo. La mancata conservazione dei sistemi di tracciamento delle operazioni di accesso che avrebbe consentito l'individuazione di eventuali abusi delle credenziali dell'utente a causa di un errore di programmazione,

così come la mancata generazione di alert per l'individuazione di accessi abusivi, sono certamente argomenti ancora attuali in costanza di nuovo Regolamento. Le disposizioni normative previgenti si occupavano di buone prassi emerse dall'operato di chi doveva fornire protezione ai dati personali tramite sistemi informatizzati. I suddetti principi, nonostante l'abrogazione del Codice della *Privacy*, sono tenuti in considerazione in quanto validi avendo dato sostanza alla disciplina del settore. Tuttavia, si ritiene necessaria un'integrazione, anche considerando gli *upgrade* di tecnologia proposti dalle soluzioni del mercato. Concetti come il sistema di autenticazione informatica, le credenziali di autenticazione, il codice per l'identificazione dell'incaricato associato a una parola chiave conosciuta solamente dal medesimo, il dispositivo di autenticazione in possesso e l'uso esclusivo dell'incaricato, la segretezza delle credenziali, la diligente custodia dei dispositivi, la modifica periodica di parole chiave, sono conformi al nuovo sistema di "pseudonimizzazione e cifratura dei dati personali" (art. 32, paragrafo 1, lett. a), GDPR) il quale prevede modalità tecniche di validazione segreta atte a garantire sicurezza e blindatura dei dati e la capacità di garantire su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento (art. 32, paragrafo 1, lett. b), GDPR). La vecchia e la nuova normativa sono quindi conformi e spesso non confliggenti, soprattutto nel caso in cui sono volte a statuire in continuità il sistema di protezione dei dati personali e l'adeguamento dell'organizzazione a tutela dei dati personali. Ne consegue che l'istituto di credito non può trascurare l'adozione di soluzioni tecniche che siano alla portata di tutti, quali la registrazione di log, i controlli periodici, gli sms-alert per movimenti di terminali relativi ad accessi anomali.

[3] Il suddetto approccio è in totale contrapposizione a quanto predisponeva il Codice della *Privacy*, d.lgs. 196/2003 che, accanto al concetto di diritto alla riservatezza, introduceva un autonomo diritto alla protezione dei dati personali, con diverse modalità tra cui, le più significative, si risolvevano nell'attuare un back up a scadenza ad esempio settimanale, l'installazione e l'aggiornamento di un antivirus, l'utilizzo di password.

[4] Articolo 24 Reg. (UE) 2016/679 – Responsabilità del titolare del trattamento: *"1. Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario. 2. Se ciò è proporzionato rispetto alle attività di trattamento, le misure di cui al paragrafo 1 includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento. 3. L'adesione ai codici di condotta di cui all'articolo 40 o a un meccanismo di certificazione di cui all'articolo 42 può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento"*.

[5] L'articolo 5, par. 1 Reg. (UE) 2016/679 prescrive le misure tecniche e organizzative adeguate per la tutela dei dati personali: *"Principi applicabili al trattamento di dati personali: 1. I dati personali sono: a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»); b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»); c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»); d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»); e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»); f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»). 2. Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («responsabilizzazione»)"*.

[6] Ai sensi dell'art. 25 del GDPR, i titolari devono eseguire la valutazione di conformità *"tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento"*. Il paragrafo 2 del medesimo articolo prevede il concetto di responsabilizzazione, per cui *"il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo"*. Il principio di auto responsabilizzazione è integrato con i nuovi principi di protezione dei dati dalla progettazione *"privacy by design"* e con il concetto della *"privacy by default"*, introdotti dal suddetto art. 25 e diretti a garantire i dati dalla fase di ideazione e progettazione di un sistema e, quindi, di adottare comportamenti che consentano di prevenire possibili problematiche.

[7] In particolare: se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, o qualsiasi altro danno

economico o sociale significativo; se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano; se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose nonché dati genetici, dati relativi alla salute o a condanne penali; in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica; se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori. La probabilità e la gravità del rischio per i diritti e le libertà dell'interessato devono essere determinate rispetto alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento. Per prevenire le violazioni del regolamento, il titolare del trattamento dovrebbe valutare i rischi inerenti al trattamento e attuare misure per garantire un adeguato livello di sicurezza, inclusa la riservatezza, in base allo stato dell'arte e dei costi di attuazione rispetto ai rischi che presentano i trattamenti e alla natura dei dati personali da proteggere. È necessario tenere in considerazione i rischi presentati dal trattamento dei dati personali, quali la distruzione accidentale o illegale, la modifica, l'accesso non autorizzati a dati personali trasmessi, che potrebbero produrre un danno fisico, materiale o immateriale.

[8] Art. 82 Reg. (UE) 2016/679: *"1. Chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento. 2. Un titolare del trattamento coinvolto nel trattamento risponde per il danno cagionato dal suo trattamento che violi il presente regolamento. Un responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del presente regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento. 3. Il titolare del trattamento o il responsabile del trattamento è esonerato dalla responsabilità, a norma del paragrafo 2 se dimostra che l'evento dannoso non gli è in alcun modo imputabile. 4. Qualora più titolari del trattamento o responsabili del trattamento oppure entrambi il titolare del trattamento e il responsabile del trattamento siano coinvolti nello stesso trattamento e siano, ai sensi dei paragrafi 2 e 3, responsabili dell'eventuale danno causato dal trattamento, ogni titolare del trattamento o responsabile del trattamento è responsabile in solido per l'intero ammontare del danno, al fine di garantire il risarcimento effettivo dell'interessato. 5. Qualora un titolare del trattamento o un responsabile del trattamento abbia pagato, conformemente al paragrafo 4, l'intero risarcimento del danno, tale titolare del trattamento o responsabile del trattamento ha il diritto di reclamare dagli altri titolari del trattamento o responsabili del trattamento coinvolti nello stesso trattamento la parte del risarcimento corrispondente alla loro parte di responsabilità per il danno conformemente alle condizioni di cui al paragrafo 2. 4.5.2016 L 119/81 Gazzetta ufficiale dell'Unione europea IT 6. Le azioni legali per l'esercizio del diritto di ottenere il risarcimento del danno sono promosse dinanzi*

*alle autorità giurisdizionali competenti a norma del diritto dello Stato membro di cui all'articolo 79, paragrafo 2"*.

[9] Invero, dall'articolo 32 si desume che i soggetti attivi del trattamento debbano ricorrere a misure di sicurezza organizzative, oltre che a misure tecniche, al fine di garantire e tutelare i dati durante il trattamento. Infatti, il GDPR prevede una divisione della responsabilità tra il titolare del trattamento e il responsabile, oltre alla necessità di disporre di soggetti abilitati al trattamento dei dati personali. Il titolare del trattamento è un soggetto sottoposto ad obblighi che esulano dalla semplice azione di custodia dei dati, perché l'espletamento delle sue funzioni riguarda anche la protezione dei dati per evitare che essi possano andare persi o distrutti o violati, richiamando così il disposto dell'articolo 5 GDPR, che espressamente prevede che *"i dati personali sono trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita o distruzione o dal danno accidentali (integrità e riservatezza)"*.

[10] Nel caso in cui si sia di fronte ad una violazione e questa non venga affrontata con tutti gli strumenti a disposizione, le persone fisiche potrebbero subire danni sia materiali che immateriali come la perdita del controllo dei dati personali oppure potrebbero subire una limitazione dei loro diritti o ancora i loro dati potrebbero essere decifrati da chi non ne ha l'autorizzazione (cifratura dei dati). Per questo motivo è stato previsto il termine di 72 ore entro le quali devono essere comunicate eventuali violazioni (*data breaches*), a meno che il titolare del trattamento non dimostri che questa violazione non comporti un rischio.

[11] L'art. 82, paragrafo 1, del GDPR, chiarisce l'ambito soggettivo attivo e passivo del diritto al risarcimento, stabilendo che: *"Chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento"*.

[12] Con riferimento ai soggetti che gestiscono il trattamento dei dati personali, occorre ricordare che il titolare del trattamento è il soggetto che determina la finalità e i mezzi del trattamento dei dati, mentre il responsabile è il soggetto che tratta i dati personali per conto del titolare o dei contitolari (artt. 4, 24 e 28 GDPR). Il titolare del trattamento risponde quando è coinvolto nel trattamento che, violando il regolamento, ha cagionato il danno; diversamente il responsabile del trattamento risponderà per il danno causato dal trattamento soltanto nel caso in cui non abbia correttamente adempiuto agli obblighi stabiliti specificamente dal Regolamento a carico dei responsabili del trattamento, oppure qualora abbia agito in modo difforme o contrario rispetto alle legittime istruzioni dategli dal titolare in merito al trattamento dei dati di sua competenza. Questa disposizione sembrerebbe delineare una fattispecie di responsabilità, in capo al titolare e al responsabile del trattamento dei dati personali, apparentemente molto restrittiva.

[13] Il quadro generale dei sistemi di pagamenti deve essere considerato tenendo conto dei cambiamenti nei traffici economici verificatisi negli ultimi anni. Infatti, il cammino verso la globalizzazione, lo sviluppo sempre maggiore della rete internet e la crescita del commercio elettronico e dei mercati virtuali hanno alimentato la diffusione dei nuovi sistemi di pagamento elettronici, utilizzabili sia dai consumatori che dalle imprese, così denominati per il fatto che, a differenza dei sistemi di pagamento tradizionali, utilizzano tecniche, programmi e strumenti innovativi. Pertanto, accanto alla moneta con corso legale, ai titoli di credito bancari e alle carte di credito, che rappresentano la c.d. moneta scritturale, si è entrati nella c.d. quarta generazione dei sistemi di pagamenti, rappresentati dalla moneta elettronica o *e-money*. Tra i sistemi di pagamento elettronici che non costituiscono moneta elettronica rientrano i bancomat (comprese le carte PagoBancomat o BancomatPos) e le carte di credito. Appaiono molto più diffusi, tra i sistemi di pagamento *online*, sia il *PayPal* che le carte prepagate. Il sistema PayPal consente a chiunque possegga un indirizzo *e-mail* di inviare o ricevere pagamenti *online* in modo sicuro. Esso funziona come un normale conto corrente che consente di effettuare varie transazioni, associando una carta di credito, una carta prepagata o un conto bancario. Al momento del pagamento, l'utente è collegato ad una pagina sicura nella quale vengono richiesti *e-mail* e *password*. Ciò consente di effettuare il pagamento detraendo l'importo dovuto dal proprio conto in modo del tutto sicuro, essendo anche previste procedure per eventuali rimborsi e contestazioni. Negli ultimi anni, poi, si registra una percentuale sempre più alta di pagamenti elettronici che avvengono per mezzo di *smartphone* o *tablet*. Infatti, si stanno sempre più diffondendo altre due modalità di pagamento, rappresentate dai mobile *payment* e dalla moneta virtuale: i primi sono applicazioni progettate per effettuare pagamenti da *smartphone*, che attraverso l'utilizzo di nuovi sistemi consentono di fare uso di portafogli elettronici, utilizzati come sostituti dei veri e propri portafogli e delle carte fisiche. Sia pure nella loro eterogeneità, i sistemi di digitale *mobile payment* vengono ricondotti alle operazioni di pagamento a distanza, eseguite in seguito alla disposizione di un ordine di pagamento. Ciò significa che l'operazione di pagamento digitale deriva dalla disposizione di pagamento di un consumatore ad un prestatore di servizi che opera su internet il quale, a sua volta, dovrà ordinare ad un altro istituto (presso il quale il cliente risulti titolare di un conto di pagamento) di eseguire il trasferimento dei fondi monetari. L'ordine di pagamento, in tali casi, è impartito mediante un *mobile device*, per mezzo di internet. Gli strumenti di pagamento utilizzabili devono essere in grado di rispondere a numerosi bisogni dei consumatori, in particolare di quelli che decidono di effettuare acquisti *online*. Il consumatore deve poter sempre controllare il proprio saldo, via web o via cellulare, e deve poter fare affidamento su operazioni di pagamento veloci e sicure. I sistemi di *e-payment* e di *mobile payment* si presentano piuttosto sicuri e semplici da utilizzare, in quanto consentono di effettuare i pagamenti *online* da un conto ad un altro, soltanto inviando un sms o una *e-mail*, confermando i propri dati e l'ordine di pagamento tramite il telefono cellulare o un

altro dispositivo mobile, sia per gli acquisti *online* che per quelli tradizionali, riguardanti servizi, prodotti e beni. Questi strumenti di pagamento hanno fatto crescere lo sviluppo del commercio elettronico, in quanto semplificano gli acquisti; dall'altro lato essi impongono di soddisfare in modo sempre più adeguato le esigenze e le aspettative dei consumatori, ampliando le garanzie di sicurezza. Invero, la riflessione sugli strumenti di pagamento elettronici non può prescindere dall'analisi di colui che ne è l'utilizzatore: il consumatore. Rispetto ai profili che impattano su quest'ultimo, si riscontrano aspetti rilevanti per la *privacy*, la sicurezza, la facilità di utilizzo di un mezzo di pagamento, i costi e i tempi di accredito e di addebito di un pagamento. Infatti, uno dei rischi negli acquisti *online* investe quello dell'intercettazione dei dati personali (Cfr. I. D'AMBROSIO, *"La tutela del consumatore nei pagamenti elettronici e la nuova direttiva europea PSD2"*, in *Notariato*, 2019, 6, 676).

[14] La diffusione dei pagamenti online con l'utilizzo di smartphone ha comportato un aumento dei rischi di violazione della *privacy*, date le numerose informazioni e i dati che i consumatori fanno transitare dai propri *smartphone*. La nuova criminalità organizzata, infatti, si concretizza attraverso frodi sui pagamenti elettronici, l'uso della carta di credito e per mezzo di internet, insieme ai furti d'identità. Pertanto, al fine di evitare l'intercettazione dei dati personali occorre aumentare i livelli di sicurezza, informando il consumatore, fornendogli eventuali *alert*, per impedire tutte le possibili frodi. Proprio il timore di una violazione della *privacy* induce molti consumatori a non utilizzare i sistemi di pagamento elettronici, in particolare, quelli del c.d. *mobile payment*.

[15] La PSD2 e il GDPR presentano contrasti applicativi sotto diversi profili. La PSD2 si occupa dei nuovi sistemi che consentono agli utenti dei servizi bancari e di pagamento di rivolgersi a operatori di derivazione non bancaria, definiti "terze parti" (o *Third Parties Provider* – TPP), per chiedere l'esecuzione di operazioni di pagamento e altre attività connesse ai servizi di pagamento. I TPP operano come "intermediari virtuali", frapponendosi tra il cliente e i servizi di pagamento disposti dagli operatori bancari veri e propri. I TPP si distinguono, a seconda della tipologia di servizio erogato, in particolare in: PISP – *Payment Initiation Service Provider* [termine con il quale sono indicati i servizi di pagamento (PSP) che si pongono come intermediari tra il consumatore, che deve avviare un pagamento dando impulso allo stesso, e il suo conto *online*, c.d. *merchant*, come, ad esempio, Amazon]; gli AISP – *Account Information Service Provide* [termine con il quale si fa riferimento a servizi di pagamento mediante i quali il consumatore-utente può mettere insieme più informazioni da diversi conti di pagamento a lui intestati, per renderle gestibili attraverso un'unica interfaccia, così da avere sotto controllo la propria situazione finanziaria, seppure gestita da diversi PSP] e i CISP – *Card Issuer Credit Provider [che sono prestatori di servizi di pagamento basati su carta, che emettono carte di pagamento, regolate su un conto di pagamento, accessibile online, di un istituto di credito diverso da quello che ha emesso la carta].*

I dati derivanti da tutte le operazioni di pagamento vengono trasmessi dagli operatori bancari tradizionali ai TPP, i quali si frappongono tra cliente e operatore bancario, acquistando tutte le informazioni relative ad una transazione (ad esempio il bene/servizio acquistato ovvero l'identità del "professionista" che vende il bene o il servizio *online*). Ne consegue che alcuni aspetti dell'attività di profilazione potranno essere eseguiti dai nuovi fornitori di servizi di pagamento. Occorre precisare che la PSD2 e il GDPR presentano due finalità diverse: la PSD2 spinge il sistema bancario verso la cosiddetta *open banking,* assicurando quindi maggiore flessibilità all'ingresso per i nuovi operatori e maggiore facilità di accesso ai dati dei clienti; il GDPR è diretto a rafforzare, in tutti i settori, compreso quello bancario, la tutela dei dati personali e le garanzie volte a consentire la condivisione e il trasferimento di tali dati solo a certe condizioni. Tuttavia, è l'utente stesso a dover autorizzare l'accesso al fine di utilizzare i servizi prestati dai *Third Party Providers*. Il segnale di autorizzazione viene così inviato alla Banca del cliente mediante meccanismi rinforzati di sicurezza. Infatti, a tale scopo, l'*European Banking Authority (EBA)* prevede l'obbligo di registrazione di tutti i TTP, in un apposito registro elettronico pubblico, autorizzati ad operare servizi di pagamento nell'Unione Europea in ambito PSD2. Questo sistema consente ad ogni consumatore di verificare se il *Player* Finanziario da autorizzare è presente nel registro, al fine di garantire la sicurezza di consentire l'accesso ai propri dati bancari e alle operazioni di pagamento solo ad enti certificati ed effettivamente approvati a livello normativo.
Grazie alla PSD2, *l' Open Banking* e gli AISP consentono ai clienti di disporre di nuove funzionalità con lo scopo di ottimizzare i propri finanziamenti e migliorare la gestione dei conti *online*.
Lo *shopping online* costituisce un altro cambiamento importante su cui il legislatore è intervenuto attraverso la PSD2. La nuova normativa ha consentito a società *FinTech* e dell'*e-commerce*, come Apple o Amazon, di gestire in modo completo i processi di pagamento dei propri utenti-consumatori. In ultimo la PSD2 permette di ridurre notevolmente i costi dei pagamenti, cosicché i consumatori europei potranno ricavare vantaggi economici dalla nuova normativa e ridurre le proprie responsabilità in caso di pagamenti non autorizzati.
[16] Articolo 70 – Obblighi a carico del prestatore di servizi di pagamento in relazione agli strumenti di pagamento*: "Il prestatore di servizi di pagamento che emette lo strumento di pagamento: assicura che le credenziali di sicurezza personalizzate siano accessibili solo all'utente di servizi di pagamento autorizzato ad utilizzare lo strumento stesso, fatti salvi gli obblighi imposti all'utente di servizi di pagamento di cui all'articolo 69; si astiene dall'inviare uno strumento di pagamento non richiesto, salvo qualora uno strumento di pagamento già detenuto dall'utente debba essere sostituito; assicura che siano sempre disponibili mezzi adeguati affinché l'utente dei servizi di pagamento possa provvedere alla notifica di cui all'articolo 69, paragrafo 1, lettera b), o richiedere lo sblocco dello strumento di pagamento ai sensi dell'articolo 68, paragrafo 4; su richiesta il*

*prestatore di servizi di pagamento fornisce all'utente dei servizi di pagamento mezzi per provare l'avvenuta notifica nei 18 mesi successivi alla stessa; fornisce all'utente dei servizi di pagamento la possibilità di procedere alla notifica a norma dell'articolo 69, paragrafo 1, lettera b), a titolo gratuito e imputa, eventualmente, solo i costi di sostituzione direttamente attribuiti allo strumento di pagamento; impedisce qualsiasi utilizzo dello strumento di pagamento una volta effettuata la notifica ai sensi dell'articolo 69, paragrafo 1, lettera b). 2. Il prestatore di servizi di pagamento sostiene il rischio dell'invio all'utente dei servizi di pagamento di uno strumento di pagamento o delle eventuali relative credenziali di sicurezza personalizzate.*

Articolo 72 – Prova di autenticazione ed esecuzione delle operazioni di pagamento*: "1. Gli Stati membri dispongono che, qualora l'utente di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento già eseguita o sostenga che l'operazione di pagamento non è stata correttamente eseguita, spetti al prestatore di servizi di pagamento fornire la prova del fatto che l'operazione di pagamento è stata autenticata, correttamente registrata e contabilizzata, e che non ha subito le conseguenze di guasti tecnici o altri inconvenienti del servizio fornito dal prestatore di servizi di pagamento. Se l'operazione di pagamento è disposta mediante un prestatore di servizi di disposizione di ordine di pagamento spetta a quest'ultimo dimostrare che, nell'ambito delle sue competenze, l'operazione di pagamento è stata autenticata, corretta mente registrata che non ha subito le conseguenze di guasti tecnici o altri inconvenienti legati al servizio di pagamento del quale è incaricato. 2. Se l'utente di servizi di pagamento nega 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 è di per sé necessariamente sufficiente a dimostrare che l'operazione di pagamento sia stata autorizzata dal pagatore né che questi abbia agito in modo fraudolento o non abbia adempiuto, dolosamente o con negligenza grave, a uno o più degli obblighi di cui all'articolo 69. Il prestatore di servizi di pagamento, compreso, se del caso, il prestatore di servizi di disposizione di ordine di pagamento, fornisce gli elementi di prova che dimostrano la frode o la negligenza grave da parte dell'utente di servizi di pagamento".*

Articolo 73 – Responsabilità del prestatore di servizi di pagamento per le operazioni di pagamento non autorizzate: *"1. Gli Stati membri provvedono affinchè, fatto salvo l'articolo 71, nel caso di un'operazione di pagamento non autorizzata il prestatore di servizi di pagamento del pagatore rimborsi al pagatore l'importo dell'operazione di pagamento non autorizzata, immediatamente e in ogni caso al più tardi entro la fine della giornata operativa successiva a quella in cui prende atto dell'operazione o riceve una notifica in merito, a meno che il prestatore di servizi di pagamento del pagatore abbia ragionevoli motivi per sospettare una frode e comunichi tali motivi per iscritto alla pertinente autorità nazionale competente. Se del caso, il prestatore di servizi di pagamento del pagatore riporta*

*il conto di pagamento addebitato nello stato in cui si sarebbe trovato se l'operazione di pagamento non autorizzata non avesse avuto luogo. Sarà inoltre assicurato che la data valuta dell'accredito sul conto di pagamento del pagatore non sia successiva alla data di addebito dell'importo. 2. Se l'operazione di pagamento è disposta mediante un prestatore di servizi di disposizione di ordine di pagamento, il prestatore di servizi di pagamento di radicamento del conto rimborsa immediatamente, e in ogni caso entro la fine della giornata operativa successiva, l'importo dell'operazione di pagamento non autorizzata e, se del caso, riporta il conto di pagamento addebitato nello stato in cui si sarebbe trovato se l'operazione di pagamento non autorizzata non avesse avuto luogo. Se il prestatore di servizi di disposizione di ordine di pagamento è responsabile dell'operazione di pagamento non autorizzata, risarcisce immediatamente il prestatore di servizi di pagamento di radicamento del conto su richiesta di quest'ultimo per le perdite subite o gli importi pagati in conseguenza del rimborso al pagatore, compreso l'importo dell'operazione di pagamento non autorizzata. Conformemente all'articolo 72, paragrafo 1, spetta al prestatore di servizi di disposizione di ordine di pagamento dimostrare che, nell'ambito delle sue competenze, l'operazione di pagamento è stata autenticata, correttamente registrata e non ha subito le conseguenze di guasti tecnici o altri inconvenienti riguardanti il servizio di pagamento del quale è incaricato.3. Un'ulteriore compensazione finanziaria può essere stabilita conformemente alla normativa applicabile al contratto stipulato fra il pagatore e il prestatore di servizi di pagamento o, se del caso, al contratto stipulato fra il pagatore e il prestatore di servizi di disposizione di ordine di pagamento".*

[17] Articolo 74 – Responsabilità del pagatore per le operazioni di pagamento non autorizzate: *"1. In deroga all'articolo 73 il pagatore può essere obbligato a sopportare, a concorrenza massima di 50 EUR, la perdita relativa ad operazioni di pagamento non autorizzate derivante dall'uso di uno strumento di pagamento smarrito o rubato o dall'appropriazione indebita di uno strumento di pagamento. Il primo comma non si applica se: a) lo smarrimento, il furto o l'appropriazione indebita di uno strumento di pagamento non potevano essere notati dal pagatore prima di un pagamento, ad eccezione dei casi in cui il pagatore ha agito in modo fraudolento; o b) la perdita è stata causata da atti o omissioni di dipendenti, agenti o succursali di un fornitore di servizi di pagamento o di un'entità a cui sono state esternalizzate le attività. Il pagatore sostiene tutte le perdite relative ad operazioni di pagamento non autorizzate se è incorso in esse agendo in modo fraudolento o non adempiendo a uno o più degli obblighi di cui all'articolo 69 dolosamente o con negligenza grave. In tali casi, il massimale di cui al primo comma non si applica. Nei casi in cui il pagatore non ha agito in modo fraudolento o non è intenzionalmente inadempiente ai propri obblighi di cui all'articolo 69, gli Stati membri possono ridurre la responsabilità di cui al presente paragrafo tenendo conto, in particolare, della natura delle credenziali di sicurezza personalizzate e delle specifiche circostanze dello smarrimento, del furto o*

*dell'appropriazione indebita. 2. Se il prestatore di servizi di pagamento del pagatore non esige un'autenticazione forte del cliente, il pagatore non sopporta alcuna conseguenza finanziaria salvo qualora abbia agito in modo fraudolento. Qualora non accettino un'autenticazione forte del cliente, il beneficiario o il suo prestatore di servizi di pagamento rimborsano il danno finanziario causato al prestatore di servizi di pagamento del pagatore. 3. Salvo qualora abbia agito in modo fraudolento, il pagatore non sopporta alcuna conseguenza finanziaria derivante dall'uso di uno strumento di pagamento smarrito, rubato o oggetto di appropriazione indebita, intervenuto dopo la notifica ai sensi dell'articolo 69, paragrafo 1, lettera b). Se il prestatore di servizi di pagamento non fornisce strumenti adeguati per la notifica, in qualsiasi momento, dello smarrimento, del furto o dell'appropriazione indebita di uno strumento di pagamento, secondo quanto disposto dall'articolo 70, paragrafo 1, lettera c), il pagatore non è responsabile delle conseguenze finanziarie derivanti dall'uso dello strumento di pagamento, salvo qualora abbia agito in modo fraudolento"*.

[18] A tal proposito, l'ABE (Autorità Bancaria Europea) emana, a norma dell'articolo 10 del regolamento (UE) n. 1093/2010, progetti di norme tecniche di regolamentazione indirizzati ai prestatori di servizi di pagamento, in cui sono specificati i requisiti dell'autenticazione forte del cliente, le esenzioni dall'applicazione. In particolare, i requisiti che le misure di sicurezza devono soddisfare per tutelare la riservatezza e l'integrità delle credenziali di sicurezza personalizzate degli utenti di servizi di pagamento e i requisiti per standard aperti di comunicazione comuni e sicure ai fini dell'identificazione, dell'autenticazione, della notifica e della trasmissione di informazioni, nonché dell'attuazione delle misure di sicurezza, tra i soggetti coinvolti.

[19] Articolo 9 – Indipendenza degli elementi: *"1. I prestatori di servizi di pagamento assicurano che l'utilizzo degli elementi di autenticazione forte del cliente di cui agli articoli 6, 7 e 8 sia soggetto a misure volte a garantire che, in termini di tecnologia, algoritmi e parametri, la violazione di uno degli elementi non comprometta l'affidabilità degli altri elementi"*.

[20] A titolo esemplificativo, il "*Digipass"* genera una *one-time password* ("OTP") dopo che il consumatore ha inserito una *password* statica (fattore di conoscenza, ossia "qualcosa che l'utente conosce") in uno speciale dispositivo *hardware* o associato in via esclusiva allo stesso consumatore (fattore di possesso, ossia "qualcosa che l'utente possiede"). Questi due fattori di autenticazione sono reciprocamente indipendenti. Esempi analoghi possono essere fatti nel caso di un dispositivo cellulare utilizzato per verificare caratteristiche biometriche oppure *password* statiche/PIN.

[21] Art. 74 PSD2: *"2. Se il prestatore di servizi di pagamento del pagatore non esige un'autenticazione forte del cliente, il pagatore non sopporta alcuna conseguenza finanziaria salvo qualora abbia agito in modo fraudolento. Qualora non accettino un'autenticazione forte del cliente, il beneficiario o il suo prestatore*

*di servizi di pagamento rimborsano il danno finanziario causato al prestatore di servizi di pagamento del pagatore"*.

[22] L'Arbitrato Bancario Finanziario (ABF) è un sistema di risoluzione alternativa delle controversie (in inglese ADR – *Alternative Dispute Resolution*) che possono sorgere tra i clienti e le banche e gli altri intermediari in materia di operazioni e servizi, bancari e finanziari.

[23] Viene così a configurarsi un sistema di responsabilità di tipo "semi-oggettivo", in forza del rinvio all'art. 2050 c.c. contenuto nell'art. 15 del Codice della *Privacy*, nel presupposto che tale modello di responsabilità è coerente con quello delineato anche a livello comunitario dal considerando n. 55 e dall'art. 23 e della Direttiva 95/46/CE, relativamente alla tutela delle persone fisiche con riguardo al trattamento dei dati personali. Quindi, il mero disconoscimento delle operazioni bancarie determina un'inversione dell'onere della prova, ponendo a carico della Banca il compito di provare l'adeguatezza nel suo sistema informatico.

[24] Secondo i principi generali del nostro ordinamento in tema di responsabilità civile contrattuale, contenuti nell' art. 1218 c.c., il creditore che agisce per il risarcimento del danno, per la risoluzione del contratto o per l'adempimento, deve provare la fonte del suo diritto e il relativo termine di scadenza, allegando puramente e semplicemente l'inadempimento della controparte; al contrario, sul debitore convenuto grava l'onere di provare che il fatto lamentato dall'attore sia dovuto a una circostanza a lui non imputabile.

[25] Pur in presenza di un sistema di sicurezza basato sull'inserimento di un codice OTP, inviato ad un numero di cellulare associato all'utenza del titolare per le operazioni di pagamento, anche l'accesso al Portale titolare dovrebbe essere ugualmente protetto da un sistema a due fattori. L'inserimento dell'OTP anche per la modifica di dati anagrafici, costituisce un doveroso strumento di sicurezza a tutela del cliente, diretto ad evitare le operazioni fraudolente.