UNIVERSITA' DEGLI STUDI DI ROMA TOR VERGATA

European Digital Law of the Person, of the Contract

***and of the Technological Marketplace* - EUDILA**

Cattedra Jean Monnet del Progetto ERASMUS +

MONETA ELETTRONICA, BANCHE ONLINE E PAGAMENTI DIGITALI:

funzionamento e criticità nel diritto digitale

Alessia Cherici

0359000

Anno accademico 2023/2024

INDICE

Abstract

La moneta elettronica, le banche online e i sistemi di pagamento digitali hanno trasformato il settore finanziario, portando innovazione e accessibilità, ma anche nuove sfide in termini di sicurezza e regolamentazione. Questa tesina esplora le tipologie di moneta elettronica, le principali tipologie di pagamenti digitali e i modelli operativi delle banche online, evidenziandone i vantaggi e gli svantaggi rispetto al sistema bancario tradizionale. Un focus è dedicato poi ai rischi legati alle frodi nei pagamenti digitali, con un'analisi dettagliata delle diverse tecniche di attacco, tra cui phishing, smishing, vishing e altre pratiche fraudolente.

Vengono inoltre esaminate le normative europee e internazionali che regolano il settore, tra cui la Direttiva sulla Moneta Elettronica (EMD2), la PSD2, il GDPR e le normative antiriciclaggio (AML), esplorando il loro impatto sulla protezione dei consumatori e sulla sicurezza dei dati finanziari. Particolare attenzione è riservata alle tecnologie avanzate di protezione, come l'autenticazione forte del cliente (SCA), la crittografia e la tokenizzazione, che garantiscono maggiore sicurezza nelle transazioni.

Infine, attraverso una serie di casi studio pratici, come le sanzioni a N26 e UniCredit, gli interventi dell'AGCM su ApplePay e la regolamentazione di PayPal, la tesina offre un'analisi critica delle dinamiche di conformità normativa e dei rischi emergenti in un settore in rapida evoluzione. Questi casi studio evidenziano l'importanza di un quadro normativo solido e dell'uso di tecnologie di sicurezza per mitigare i rischi legati alla digitalizzazione del settore finanziario.

1 Moneta elettronica

1.1 Definizione

La moneta elettronica è una rappresentazione digitale di valore, emessa su supporti elettronici o memorizzata in sistemi di pagamento elettronico, utilizzabile per effettuare transazioni finanziarie senza l'uso di denaro contante.

Secondo la Direttiva 2009/110/CE dell'Unione Europea, la moneta elettronica rappresenta un credito nei confronti di un emittente, convertibile in denaro contante su richiesta e accettato da soggetti diversi dall'emittente stesso per il pagamento di beni o servizi.

Essa è una forma moderna di denaro che si differenzia dalle valute fisiche (come le monete e le banconote) perché esiste solo in formato digitale. Viene trasferita attraverso sistemi di pagamento elettronici, tra cui carte prepagate, applicazioni di pagamento mobili e portafogli digitali. La moneta elettronica include sia i fondi immagazzinati su supporti hardware (come le carte prepagate) che quelli memorizzati nei conti online o in piattaforme di pagamento.

La principale differenza tra la moneta elettronica e la valuta tradizionale risiede nella modalità di gestione e trasferimento del valore. Mentre la valuta tradizionale richiede il trasferimento fisico di denaro, la moneta elettronica consente trasferimenti istantanei attraverso reti elettroniche, spesso più veloci e sicuri. Inoltre, mentre le banche centrali controllano l'emissione di valuta tradizionale, gli emittenti di moneta elettronica includono soggetti privati come banche e piattaforme fintech.

1.2 Tipologie

Esistono diverse tipologie di moneta elettronica, ciascuna con caratteristiche, modalità d'uso, vantaggi e sfide distintive. Le principali categorie includono:

- Le carte prepagate, che sono uno degli esempi più comuni di moneta elettronica. Queste carte, ricaricabili o usa e getta, permettono ai consumatori di caricare una somma di denaro che può essere utilizzata per effettuare acquisti online e nei negozi fisici.
  Un esempio sono le PostePay e le carte prepagate offerte da banche e istituti di pagamento. Queste carte non sono collegate a un conto bancario e offrono spesso un maggiore controllo sulla spesa, poiché l'utente può spendere solo quanto caricato sulla carta;

- I portafogli elettronici, o e-wallet, che sono piattaforme digitali che memorizzano moneta elettronica e le informazioni di pagamento degli utenti e permettono di effettuare pagamenti online o tramite dispositivi mobili. Esempi popolari di portafogli elettronici che consentono agli utenti di effettuare pagamenti sicuri senza bisogno di inserire ogni volta i dettagli della carta o del conto bancario sono: PayPal, uno dei sistemi di pagamento digitale più utilizzati al mondo, permette transazioni tra individui e aziende, integrato in milioni di piattaforme di e-commerce; Apple Pay e Google Pay, piattaforme di pagamento mobile che permettono agli utenti di collegare le proprie carte di credito e debito ai dispositivi mobili, consentendo pagamenti rapidi tramite smartphone e smartwatch; Satispay, un sistema italiano di pagamento mobile, basato sull'associazione di un IBAN bancario all'app, che permette trasferimenti di denaro istantanei e senza commissioni. I portafogli elettronici offrono quindi praticità, ampie opzioni di utilizzo e sono comunemente utilizzati per transazioni sia online che offline, ma possono sollevare questioni di sicurezza dei dati;
- Le criptovalute, che rappresentano una forma innovativa di moneta elettronica. Si tratta di valute digitali basate su tecnologie crittografiche e distribuite, come la blockchain, che consentono transazioni sicure e decentralizzate senza l'intervento di intermediari. Le criptovalute più conosciute includono il Bitcoin, Ethereum e Litecoin. Sebbene siano utilizzate per pagamenti e investimenti, le criptovalute non sono emesse da un'autorità centrale e il loro status giuridico varia in base alla giurisdizione.
  Le criptovalute, pur offrendo anonimato e decentralizzazione, presentano sfide regolatorie e rischi di volatilità;
- Le stablecoin, che sono un tipo particolare di criptovaluta progettata per mantenere un valore stabile nel tempo, solitamente ancorato a una valuta tradizionale come il dollaro o l'euro. Esempi di stablecoin includono Tether (USDT) e USD Coin (USDC). Queste valute sono progettate per offrire i vantaggi della tecnologia blockchain (come la sicurezza e la velocità delle transazioni) senza la volatilità tipica delle criptovalute non ancorate;
- La moneta mobile, la quale si riferisce all'uso di dispositivi mobili per effettuare transazioni finanziarie, particolarmente comune in molte regioni in via di sviluppo dove le infrastrutture bancarie tradizionali possono essere limitate. Questa categoria include pagamenti tramite NFC (Near Field Communication), in cui gli utenti avvicinano il proprio dispositivo a un

terminale di pagamento, e QR code payments, in cui un codice QR viene scansionato per completare la transazione. Servizi come M-Pesa in Kenya hanno rivoluzionato l'accesso ai servizi finanziari, consentendo agli utenti di inviare e ricevere denaro utilizzando il loro telefono cellulare senza necessità di un conto bancario. Sistemi come WeChat Pay e Alipay in Cina sono altri esempi di piattaforme di pagamento mobile di successo;

- Piattaforme di Pagamento Digitali con Conti Aggregati, come ad esempio Revolut, N26 o Hype, che offrono conti correnti digitali che possono essere ricaricati e utilizzati come moneta elettronica per pagamenti online e offline;

2 Banche online: modello e funzionamento

2.1 Definizione e principali attori

Le banche online, anche conosciute come banche digitali o neobanche, sono istituti finanziari che offrono servizi bancari tramite canali digitali, senza necessità di filiali fisiche. L'evoluzione della tecnologia, unita alla crescente richiesta di soluzioni finanziarie rapide e flessibili, ha favorito l'espansione di questa tipologia di banche.

Il modello di business delle banche online è incentrato sull'uso di piattaforme digitali per la gestione di conti correnti, risparmi, investimenti e finanziamenti. Grazie all'infrastruttura digitale, esse possono ridurre i costi operativi rispetto alle banche tradizionali, consentendo spesso condizioni più vantaggiose per i clienti, come tassi di interesse competitivi o l'assenza di commissioni.

Le banche online possono essere suddivise in due categorie principali:

- Neobanche: queste sono banche completamente digitali, che non hanno filiali fisiche e offrono servizi bancari principalmente attraverso app e piattaforme web. Esempi di neobanche includono N26, Revolut, Monzo e Hype. Si concentrano su un'esperienza utente fluida e servizi semplificati, spesso rivolti a un pubblico giovane e tecnologicamente esperto;
- Banche tradizionali con servizi online: molte banche tradizionali hanno adattato i propri servizi per includere opzioni completamente digitali. Alcuni esempi includono Intesa Sanpaolo con la piattaforma XME, o UniCredit, che offrono agli utenti la possibilità di gestire i propri conti, effettuare pagamenti e accedere ad altri servizi finanziari tramite app o siti web.

Entrambi i modelli mirano a migliorare l'accessibilità e l'efficienza dei servizi bancari, eliminando la necessità di interazioni fisiche e garantendo operazioni finanziarie disponibili 24/7.

2.2 Vantaggi e svantaggi

I principali vantaggi delle banche online sono:

- **Accessibilità e praticità**

  Le banche online consentono agli utenti di accedere ai servizi bancari in qualsiasi momento e da qualsiasi luogo, attraverso dispositivi connessi a Internet. L'eliminazione delle filiali

fisiche riduce le limitazioni geografiche, facilitando la gestione finanziaria per individui che si trovano in aree remote o che viaggiano frequentemente. Questa disponibilità 24/7 permette un'estrema flessibilità nella gestione delle operazioni bancarie;

- **Costi ridotti**

  L'assenza di filiali fisiche e la riduzione dei costi operativi consentono alle banche online di offrire servizi a condizioni più vantaggiose rispetto alle banche tradizionali. Spesso, i conti correnti sono senza commissioni, le transazioni sono gratuite o a costi molto bassi, e i tassi d'interesse sui prestiti e sui risparmi sono più competitivi;

- **Innovazione tecnologica**

  Le banche online investono molto in tecnologie innovative, come l'intelligenza artificiale e l'analisi dei big data, per personalizzare l'esperienza utente e migliorare la sicurezza delle transazioni. Inoltre, molte piattaforme di banche digitali offrono funzionalità avanzate, come l'analisi delle spese, il budgeting automatico e l'accesso a investimenti a basso costo direttamente dall'app;

- **Integrazione con sistemi di pagamento digitali**

  Le banche online sono strettamente integrate con i principali sistemi di pagamento digitali, come Apple Pay, Google Pay e Samsung Pay, permettendo pagamenti contactless e trasferimenti di denaro peer-to-peer istantanei. Questa connessione con le piattaforme fintech amplia l'accesso a servizi aggiuntivi e facilita le transazioni internazionali a costi inferiori rispetto ai tradizionali bonifici bancari.

I principali svantaggi delle banche online sono:

- **Assenza di filiali fisiche**

  Uno dei principali svantaggi delle banche online è l'assenza di filiali fisiche, il che può rappresentare un problema per i clienti meno abituati alla tecnologia o che preferiscono l'interazione faccia a faccia con un consulente bancario. Inoltre, per alcune operazioni più complesse, come la richiesta di mutui o la gestione di controversie, i clienti possono sentirsi limitati dalla mancanza di un contatto personale;

- **Sicurezza e frodi**

  Anche se le banche digitali investono molto in sicurezza informatica, esiste sempre il rischio di attacchi hacker o frodi online. Le transazioni completamente digitali sono soggette a

vulnerabilità, come il phishing o la compromissione delle credenziali di accesso. Tuttavia, la regolamentazione europea, in particolare la Direttiva PSD2, ha introdotto misure di sicurezza avanzate, come l'autenticazione forte del cliente (Strong Customer Authentication, SCA), per ridurre questi rischi;

- **Problemi di assistenza clienti**

  L'assistenza clienti delle banche online è generalmente fornita tramite chat, e-mail o assistenza telefonica. Tuttavia, per alcuni utenti, la mancanza di supporto diretto o la lentezza delle risposte possono rappresentare un limite. La complessità di alcune operazioni o la risoluzione di controversie può richiedere più tempo rispetto a una banca tradizionale;

- **Limitata offerta di servizi**

  Anche se molte banche online offrono una gamma completa di servizi bancari, alcune potrebbero non disporre di prodotti più complessi, come prestiti ipotecari o strumenti di gestione patrimoniale avanzati. Ciò è dovuto in parte alla natura semplificata del loro modello di business e all'obiettivo di mantenere costi operativi ridotti.

3 Sistemi di pagamento digitale e frodi

3.1 Tipologie di sistemi di pagamento

I sistemi di pagamento digitale rappresentano l'infrastruttura tecnologica attraverso cui avvengono le transazioni finanziarie in formato elettronico. Essi comprendono vari strumenti e tecnologie che consentono agli utenti di effettuare pagamenti senza l'uso di denaro contante, facilitando l'interconnessione tra consumatori, aziende e istituzioni finanziarie in tutto il mondo.

Le forme più tradizionali di pagamento digitale includono:

- Bonifici bancari e addebiti diretti: Questi strumenti, operanti principalmente tra istituzioni bancarie, rappresentano le modalità più consolidate e regolamentate per il trasferimento di denaro. I bonifici sono generalmente utilizzati per pagamenti più consistenti, mentre gli addebiti diretti consentono pagamenti ricorrenti. Inoltre mentre i bonifici istantanei sono irrevocabili, sugli altri si ha un diritto di revoca, ma la procedura deve essere eseguita prima che la cifra venga accreditata sul conto del beneficiario;

- Carte di pagamento: Le carte emesse da circuiti come Visa, Mastercard e American Express rimangono strumenti centrali nel panorama dei pagamenti digitali, sia per gli acquisti online che fisici. Secondo un rapporto della Banca d'Italia, circa il 60% delle transazioni digitali in Italia avviene tramite carte di credito o debito, con una progressiva crescita dell'uso contactless. Queste carte possono essere fisiche o virtuali, quelle fisiche sono tradizionalmente delle tessere plastificate, con un microchip e/o una banda magnetica e riportano solitamente sul fronte nome e cognome del titolare della carta, numero della carta, il circuito al quale la carta aderisce (infrastruttura tecnologica che permette di far circolare questo denaro elettronico, ad esempio Pagobancomat, Visa, MasterCard, American Express), l'intermediario finanziario che l'ha emessa e la data di scadenza, mentre sul retro si può trovare un codice di sicurezza, composto da 3 o 4 cifre detto CVV, richiesto ad esempio nei pagamenti online. Queste carte consentono di pagare presso esercizi commerciali (tramite POS o tramite CVV per pagamenti online) o di prelevare/inserire contante tramite sportelli automatici ATM. Per effettuare operazioni, viene fornito inoltre un codice PIN, che il titolare deve inserire nel POS o sulla tastiera dell'ATM. È fondamentale mantenere il PIN segreto, evitando che altre persone lo conoscano o lo condividano. Durante il prelievo di

denaro da un ATM, potrebbe essere applicata una commissione, che viene indicata prima di completare l'operazione. Tra le carte di pagamento distinguiamo:

- Carte di credito, le quali consentono di effettuare pagamenti a credito, con l'importo pagato successivamente, ovvero l'importo speso o prelevato viene addebitato al titolare della carta in un momento successivo rispetto a quello dell'utilizzo e può avvenire in un'unica soluzione (carte di credito a saldo) o a rate (carte di credito revolving);
- Le carte di debito (Bancomat), che consentono di detrarre il denaro direttamente dal conto corrente dell'utente al momento dell'acquisto/prelievo, gli importi vengono dunque addebitati con effetto immediato sul conto del titolare, possono essere quindi spese solo le somme già disponibili. Esistono limiti mensili per gli acquisti e limiti sia giornalieri che mensili per i prelievi di contante.;
- Le carte prepagate sono invece ricaricabili con un importo limitato, usate per spese controllate e con rischi ridotti;
- Le carte contactless sono carte di credito o di debito che permettono di pagare semplicemente avvicinando la carta al POS, grazie a specifiche tecnologie.

Negli ultimi anni, l'avvento di nuove tecnologie ha favorito l'ascesa di sistemi di pagamento digitali innovativi tra cui i portafogli elettronici (PayPal, Google Pay, Apple Pay), le criptovalute e i pagamenti mobili, che sono forme di moneta elettronica già analizzate nel capitolo 1.

3.2 Obblighi

La legge impone ai commercianti (inclusi artigiani) di dotarsi di un POS per accettare pagamenti elettronici, ma non prevede sanzioni per il mancato rispetto di tale obbligo. L'obbligo di accettare pagamenti con carta si applica per importi superiori a 5 euro.

Per l'esercente, l'accettazione di pagamenti con carta comporta dei costi, come il noleggio del POS e le commissioni su ogni transazione. Tuttavia, per favorire la diffusione dei pagamenti elettronici, dal 2021 non vengono applicate commissioni agli esercenti per pagamenti inferiori a 5 euro. Per il consumatore, invece, non ci sono costi aggiuntivi; è infatti vietato addebitare commissioni per pagamenti con bancomat o carta di credito (divieto di surcharge).

Dal 1° gennaio 2021 è stato inoltre aumentato l'importo massimo sopra il quale è necessario inserire il pin: 50 euro. Dunque, per pagamenti sotto questa cifra, se la propria banca si è adeguata, è possibile pagare senza dover digitare il pin, consentendo delle operazioni più fluide e rapide. In particolare, questa esigenza è nata con il Covid, avendo la necessità di massimizzare l'igiene e il distanziamento sociale.

3.3 Frodi e sicurezza informatica

Nonostante gli avanzamenti nella sicurezza, le frodi nei pagamenti digitali sono in continua evoluzione. Le banche e le piattaforme di pagamento sono costantemente impegnate nell'implementazione di tecnologie di rilevamento delle frodi, come l'intelligenza artificiale e l'analisi comportamentale, per identificare e prevenire attività sospette in tempo reale.

Le principali tecniche di frode includono: phishing, smishing, vishing, carding, man-in-the-middle, skimming, SIM-Swap.

3.3.1 Phishing e smishing

Il phishing è una delle tecniche di frode più comuni e consiste nell'ingannare una vittima inducendola a fornire informazioni sensibili come credenziali di accesso, numeri di carte di credito o altri dati personali, facendole credere di interagire con un'entità legittima (ad esempio, una banca o un servizio di pagamento online). I truffatori inviano e-mail (phishing) o SMS (smishing) falsi che imitano quelli di istituzioni affidabili, chiedendo all'utente di cliccare su un link che porta a un sito web identico a quello originale dell'istituto di credito o del servizio, ma in realtà contraffatto. Qui, le vittime vengono indotte a inserire i loro dati riservati di accesso al servizio, che vengono poi sottratti poiché saranno disponibili ai criminali.

Alcuni esempi possono essere falsi messaggi e-mail che chiedono di aggiornare la password del conto bancario o di confermare una transazione sospetta.

Tra le possibili tecniche difensive abbiamo: Autenticazione multifattore (MFA), software anti-phishing, attenzione posta ai dettagli del mittente delle e-mail e ai link dei siti a cui rimandano.

Vi è poi un altro tipo di phishing che avviene attraverso i motori di ricerca, chiamato anche avvelenamento SEO (Search Engine Optimization) o trojan SEO, che consiste in una tecnica usata dagli hacker per far apparire i loro siti web tra i primi risultati di una ricerca su Google o altri

motori di ricerca. Se l'utente clicca su questi link, viene reindirizzato a un sito controllato dall'hacker. Una volta lì, se l'utente inserisce dati sensibili, come credenziali o informazioni personali, l'hacker può appropriarsene. Questi siti fraudolenti spesso imitano portali legati a banche, PayPal, social media o piattaforme di e-commerce, rendendoli particolarmente ingannevoli.

3.3.2 Vishing

Il vishing (voice phishing) è una tecnica di truffa in cui i criminali utilizzano chiamate telefoniche per ingannare le vittime e convincerle a fornire informazioni personali, finanziarie o sensibili. Spesso si fingono operatori di enti affidabili, come banche, società di carte di credito o istituzioni governative. Durante la chiamata, il truffatore cerca di ottenere dati come numeri di conto, codici PIN o altre credenziali. A differenza del phishing tradizionale, che avviene tramite e-mail o siti web falsi, il vishing sfrutta il contatto diretto e la pressione psicologica per convincere la vittima a collaborare.

3.3.3 Carding

Il carding è una forma di frode in cui i criminali utilizzano informazioni rubate relative a carte di credito o debito per effettuare acquisti non autorizzati. I dati delle carte possono essere ottenuti tramite hacking di database aziendali, phishing o tramite mercati illegali sul dark web. Una volta in possesso delle informazioni, i truffatori testano la validità delle carte effettuando piccoli acquisti, e se la transazione va a buon fine, utilizzano la carta per acquisti di valore più elevato.

Un esempio può essere l'uso di numeri di carte di credito rubate per effettuare acquisti su piattaforme di e-commerce.

Tra le possibili tecniche difensive abbiamo: monitoraggio delle transazioni da parte dei fornitori di servizi di pagamento, blocco automatico delle carte sospette, utilizzo di soluzioni di tokenizzazione nei pagamenti.

3.3.4 Man-in-the-middle

Un attacco Man-in-the-Middle si verifica quando un truffatore intercetta la comunicazione tra due parti (ad esempio, tra un utente e una piattaforma bancaria) e si inserisce nel flusso di dati per rubare informazioni sensibili, alterare i dati o reindirizzare le transazioni. Questo attacco può avvenire tramite reti Wi-Fi non protette o sfruttando vulnerabilità nei protocolli di comunicazione.

Tra le tecniche difensive da utilizzare abbiamo: uso di connessioni sicure con crittografia (TLS/SSL), VPN, certificati digitali e autenticazione multi-fattore.

3.3.5 Skimming

Lo skimming è una tecnica in cui i truffatori installano dispositivi sui terminali POS (Point of Sale) o sugli sportelli bancomat per clonare i dati delle carte di credito o debito. I dispositivi skimmer catturano i dettagli della carta e possono essere utilizzati per creare copie della carta fisica o per condurre transazioni online fraudolente.

Tra le tecniche difensive vi sono: controllo regolare dei terminali POS, utilizzo di carte con chip EMV, avvisi di frode da parte delle banche.

3.3.6 SIM-Swap

La SIM swap è una frode in cui i truffatori riescono a trasferire il numero di telefono di una vittima su una nuova SIM card in loro possesso. Per farlo, i criminali raccolgono informazioni personali della vittima, come nome, data di nascita e dati finanziari, tramite tecniche di phishing o altre forme di inganno. Successivamente, contattano il provider telefonico fingendosi il proprietario del numero, convincendolo a trasferire il servizio sulla nuova SIM. Una volta effettuato il cambio, i truffatori ottengono accesso a messaggi e chiamate della vittima, che spesso includono codici di autenticazione a due fattori (2FA), permettendo loro di accedere a conti bancari o profili online per rubare fondi o informazioni sensibili.

4 Sicurezza e protezione della privacy: aspetti normativi e regolamentari

4.1 Introduzione

Con l'evoluzione delle tecnologie digitali, la crescente adozione della moneta elettronica, dei sistemi di pagamento online e delle banche digitali ha portato alla necessità di una regolamentazione solida che possa garantire la sicurezza, la privacy e l'integrità delle transazioni finanziarie. Questo capitolo si concentrerà sugli aspetti normativi e regolamentari che disciplinano i pagamenti elettronici e la moneta elettronica, le normative riguardanti la protezione dei dati personali degli utenti e le misure adottate per prevenire le frodi.

4.2 Regolamentazione, privacy e protezione dei dati

Uno degli aspetti più critici dell'adozione della moneta elettronica e dei sistemi di pagamento digitali è la gestione e la protezione dei dati personali degli utenti. La privacy dei dati è tutelata da regolamentazioni specifiche a livello europeo, come il Regolamento Generale sulla Protezione dei Dati (GDPR), l'EMD2, la PSD2 e le normative antiriciclaggio. Le violazioni della privacy, come l'uso improprio dei dati finanziari, sono severamente punite, come dimostrano le sanzioni imposte a piattaforme bancarie e di pagamento da parte delle autorità di regolamentazione, di cui saranno riportati alcuni esempi nel seguito di questo studio (Capitolo 5).

4.2.1 Direttiva sulla Moneta Elettronica (EMD2)

La Direttiva EMD2 (2009/110/CE) è un'importante normativa dell'Unione Europea che regolamenta l'emissione di moneta elettronica. Essa rappresenta un aggiornamento della prima direttiva del 2000, mirato a creare un quadro normativo più chiaro e coerente per le istituzioni finanziarie e le aziende che operano nel settore dei pagamenti digitali.

Questa direttiva ha ampliato la gamma di soggetti autorizzati a emettere moneta elettronica, includendo non solo le banche tradizionali ma anche le istituzioni di pagamento non bancarie, facilitando così la concorrenza e l'innovazione nel mercato.

Un obiettivo chiave di EMD2 è garantire un elevato livello di protezione per i consumatori. La direttiva impone requisiti rigorosi in termini di sicurezza e gestione dei fondi, richiedendo alle istituzioni emittenti di mantenere i fondi dei clienti separati dai propri. Inoltre, EMD2 promuove la

trasparenza nelle informazioni fornite ai consumatori riguardo ai costi e alle condizioni dei servizi di moneta elettronica. Questo non solo protegge gli utenti finali, ma contribuisce anche a rafforzare la fiducia nei pagamenti digitali, elemento fondamentale per l'adozione crescente di tali strumenti nell'era della digitalizzazione.

La vigilanza delle autorità regolatorie nazionali, come la Banca d'Italia, è centrale nel monitoraggio degli emittenti, per prevenire illeciti e pratiche rischiose.

Uno degli aspetti più importanti della EMD2 è il principio di rimborsabilità. Questo principio garantisce agli utenti che il valore della moneta elettronica detenuta presso un emittente possa essere sempre convertito in denaro reale su richiesta. La rimborsabilità è uno strumento di tutela per i consumatori, che possono richiedere il rimborso del loro saldo elettronico in qualsiasi momento, limitando i rischi di perdite finanziarie. La direttiva prevede anche requisiti stringenti sulle riserve di capitale che gli emittenti devono mantenere. Gli emittenti sono obbligati a conservare riserve sufficienti per coprire l'ammontare di moneta elettronica in circolazione, a garanzia dei fondi dei clienti in caso di insolvenza o fallimento. Questa disposizione contribuisce a proteggere i consumatori, riducendo il rischio che il valore detenuto in forma elettronica venga perso in caso di problemi finanziari dell'emittente.

4.2.2 PSD2 e PSD3

La PSD2 (2015/2366/UE), o Payment Services Directive 2, è una direttiva europea introdotta nel 2018, che rappresenta un aggiornamento cruciale della precedente direttiva sui servizi di pagamento (PSD1) ed è stata concepita per affrontare le sfide moderne nel settore dei pagamenti digitali. In particolare, è stata introdotta per promuovere la concorrenza, aumentare la trasparenza e migliorare la sicurezza nei pagamenti elettronici.

I punti principali di questa direttiva sono:

- Apertura del mercato: la PSD2 ha introdotto il concetto di open banking, che richiede alle banche di consentire a terze parti autorizzate di accedere alle informazioni dei conti dei clienti, previa autorizzazione. Questo permette a nuove aziende fintech (innovazione nei servizi finanziari) di sviluppare servizi innovativi, come app di gestione delle finanze personali e servizi di pagamento più efficienti (fornitori di servizi di pagamento terzi, TPP), aumentando così la scelta per i consumatori. L'open banking funziona grazie all'API

(Application Programming Interface), che consente alle banche di condividere i dati in modo sicuro con queste terze parti. I TPP possono così accedere a informazioni come saldo del conto, transazioni e pagamenti, senza dover avere accesso diretto al conto corrente dell'utente;

- Accesso ai dati: Le banche sono obbligate a fornire accesso ai dati dei conti correnti dei clienti ai TPP (Third Party Providers), previa autorizzazione del cliente. Questo facilita l'innovazione e la concorrenza nel settore dei pagamenti;
- Sicurezza: La direttiva introduce requisiti di Strong Customer Authentication (SCA), che richiedono l'uso di almeno due fattori di autenticazione per autorizzare i pagamenti. Questo approccio mira a ridurre il rischio di frodi e garantire che solo gli utenti legittimi possano accedere ai propri conti;
- Trasparenza: La PSD2 impone obblighi di trasparenza sui costi e sulle condizioni dei servizi di pagamento, migliorando la protezione dei consumatori;
- Soluzione controversie: La direttiva garantisce che i consumatori possano richiedere il rimborso di pagamenti non autorizzati o errati, aumentando la fiducia nei servizi di pagamento digitali. In particolare, se il consumatore subisce un danno a causa di un'operazione di pagamento non autorizzata, l'intermediario è obbligato a rimborsarlo entro il giorno lavorativo successivo alla segnalazione. Il consumatore ha 13 mesi dall'addebito per richiedere il rimborso. Se la carta è stata rubata o smarrita e sono state effettuate operazioni non autorizzate, il cliente ha diritto al rimborso, con una franchigia di 50 euro per operazioni avvenute prima del blocco (eccetto per le carte contactless). L'emittente non deve rimborsare se il consumatore ha agito con frode, dolo o colpa grave, ad esempio non seguendo le regole di sicurezza. Il rimborso può essere negato se è dimostrata la frode o la colpa grave del cliente, soprattutto se è stata applicata l'autenticazione forte del cliente (SCA). Se il cliente ha agito in modo fraudolento, non ha mai diritto al rimborso. Spetta al prestatore dei servizi di pagamento (ad esempio, alla Banca) e, se del caso, al prestatore dei servizi di disposizione di ordine di pagamento, fornire la prova della frode, del dolo o della colpa grave dell'utente.

La PSD3 (Payment Services Directive 3) rappresenta un nuovo aggiornamento delle normative europee sui servizi di pagamento, proposto dalla Commissione Europea a giugno 2023 e attualmente in fase di revisione, per poi essere successivamente discussa e approvata dal Parlamento Europeo e dal Consiglio dell'Unione Europea. Questa direttiva mira a modernizzare e rendere più sicuro il panorama dei pagamenti digitali nell'Unione Europea. I punti salienti della PSD3 sono:

- Maggiore protezione dei consumatori: la PSD3 introduce misure più rigide per migliorare l'autenticazione dei clienti e la prevenzione delle frodi. Viene rafforzata la Strong Customer Authentication (SCA), con nuove norme che obbligano i fornitori di servizi a condividere ulteriori dati sulle transazioni (come la localizzazione dell'utente) per identificare meglio possibili tentativi di frode. Inoltre, saranno previsti regimi di responsabilità più rigorosi per i fornitori che non implementano correttamente le procedure di sicurezza;
- Trasparenza e protezione dei consumatori: miglioramenti nella trasparenza delle informazioni fornite ai clienti, soprattutto riguardo ai costi dei servizi di pagamento. I consumatori riceveranno dettagli più chiari sulle tariffe applicate e sulle modalità di gestione delle transazioni;
- Apertura al mercato e promozione della concorrenza: la PSD3 prevede di facilitare l'ingresso di nuovi attori nel mercato finanziario, come fintech e altre aziende innovative, per stimolare la concorrenza e favorire l'innovazione nei servizi di pagamento, consentendo loro di competere con le banche tradizionali. La direttiva propone inoltre di unificare i regimi normativi per gli istituti di pagamento e quelli di moneta elettronica, semplificando il quadro giuridico per le aziende che operano in entrambi i settori;
- Nuove regole per l'open banking: regolamentazione più chiara delle attività legate all'open banking, facilitando l'accesso ai conti bancari per i fornitori di servizi di pagamento terzi in modo sicuro e standardizzato. Queste nuove regole rendono il sistema di open banking più sicuro e regolamentato, definendo chiaramente il ruolo e le responsabilità di chi accede a questi dati, e facilitando l'accesso a un maggior numero di servizi finanziari.;
- Aumento della supervisione delle autorità: rafforzamento dei poteri di supervisione delle autorità competenti (come le banche centrali e le autorità di regolamentazione nazionali) sui fornitori di servizi di pagamento. Questo dovrebbe garantire una migliore vigilanza e protezione contro comportamenti scorretti;
- Maggiore armonizzazione con il GDPR: rafforzamento del legame tra la PSD3 e il Regolamento Generale sulla Protezione dei Dati (GDPR), assicurando una protezione più efficace dei dati personali dei clienti durante le transazioni.

4.2.3 GDPR e la Protezione dei Dati

Il Regolamento Generale sulla Protezione dei Dati (GDPR), entrato in vigore nel 2018, è il principale quadro normativo che ha rafforzato i diritti degli utenti in materia di privacy e protezione dei dati personali e regola il loro trattamento all'interno dell'Unione Europea. Anche i sistemi di pagamento digitali e le banche online devono conformarsi a questa normativa, poiché gestiscono enormi quantità di dati sensibili, come informazioni finanziarie e personali.

Il GDPR stabilisce, infatti, che qualsiasi piattaforma di pagamento o istituzione bancaria deve adottare misure tecniche e organizzative adeguate, per proteggere i dati personali e garantire la loro riservatezza. Queste misure includono i seguenti obblighi:

- La raccolta e il trattamento dei dati personali solo con il consenso esplicito dell'utente.
- La protezione dei dati sensibili con tecnologie adeguate (come la crittografia) durante la trasmissione e l'archiviazione.
- L'obbligo di notificare alle autorità di controllo (come il Garante per la protezione dei dati in Italia) e agli utenti eventuali violazioni dei dati (data breach) entro 72 ore.
- Valutazione d'impatto sulla protezione dei dati (DPIA) per identificare e mitigare i rischi.

4.2.4 Normative antiriciclaggio (AML) e il contrasto alle frodi nei pagamenti digitali

Le normative antiriciclaggio nell'Unione Europea (AMLD - Anti-Money Laundering Directives) sono volte a prevenire l'uso dei sistemi finanziari per fini illeciti, come il riciclaggio di denaro e il finanziamento del terrorismo. La 5ª direttiva antiriciclaggio (AMLD5), entrata in vigore nel 2020 e implementata a livello europeo, ha rafforzato il quadro normativo per rispondere meglio alle minacce derivanti dalle nuove tecnologie, come le criptovalute. In particolare, ha introdotto ha introdotto alcuni obblighi:

- Eseguire procedure di verifica dell'identità (KYC) approfondite.
- Monitorare in tempo reale le transazioni sospette.
- Segnalare qualsiasi attività sospetta alle autorità competenti.
- Obbligo per gli Stati membri di creare registri pubblici sui beneficiari effettivi delle società e di includere i fornitori di servizi legati a valute virtuali (criptovalute) e portafogli digitali tra i soggetti obbligati (L'obiettivo è rendere più difficile per i criminali nascondere il loro denaro usando società fittizie).

La normativa mira a garantire una maggiore trasparenza, cooperazione tra gli Stati membri e un rafforzamento dei meccanismi di controllo e supervisione per combattere il riciclaggio di denaro su scala internazionale.

4.2.5 L'Impatto delle Violazioni di Dati

Le violazioni di dati nel settore finanziario possono avere conseguenze gravi, non solo in termini di perdita economica per i consumatori, ma anche in termini di reputazione per gli operatori del settore. I recenti casi di attacchi informatici hanno dimostrato quanto sia cruciale la protezione

delle informazioni personali e finanziarie. Le autorità regolatorie hanno quindi imposto multe severe per le aziende che non rispettano le normative sulla protezione dei dati, con sanzioni che possono arrivare fino al 4% del fatturato globale dell'azienda.

4.3 Tecnologie per la sicurezza dei pagamenti digitali

I pagamenti digitali richiedono elevati standard di sicurezza per proteggere i dati sensibili degli utenti e ridurre i rischi di frode. Diverse tecnologie e misure di sicurezza, come l'Autenticazione Forte del Cliente (SCA), la crittografia end-to-end e la tokenizzazione, sono state implementate per garantire la sicurezza delle transazioni e la protezione delle informazioni finanziarie degli utenti.

4.3.1 Strong Customer Authentication

Un buon livello di sicurezza nelle transazioni digitali è garantito dall'autenticazione multifattore (MFA). Oltre a username e password, la MFA richiede all'utente di fornire ulteriori fattori di verifica, come un codice inviato via SMS, una notifica push su uno smartphone o dati biometrici (impronta digitale o riconoscimento facciale). L'obiettivo è rendere più difficile per un malintenzionato completare una transazione anche se riesce ad ottenere le credenziali di accesso.

La Direttiva PSD2 (Payment Services Directive 2), emanata dalla Commissione Europea nel 2018, ha introdotto la Strong Customer Authentication (SCA) come misura obbligatoria per ridurre le frodi nei pagamenti digitali. Questa misura rappresenta una forma avanzata di MFA, che impone l'utilizzo di almeno due dei tre seguenti fattori di autenticazione, per completare le transazioni online:

- Conoscenza: qualcosa che solo l'utente conosce (ad esempio, una password o un PIN).
- Possesso: qualcosa che l'utente possiede (come uno smartphone o un token di sicurezza).
- Inerenza: qualcosa che è legato all'utente (biometria, come impronte digitali o riconoscimento facciale).

La procedura di autenticazione deve essere sviluppata in modo da garantire la protezione delle informazioni inserite; per questa ragione i fattori scelti devono essere indipendenti l'uno dall'altro, in modo che la compromissione di uno non influisca sugli altri. Inoltre, almeno uno dei fattori dovrebbe essere non riutilizzabile, non replicabile e non trasferibile attraverso Internet.

L'autenticazione forte del cliente (SCA) è necessaria nei seguenti casi: quando si accede al conto online; al momento dell'invio di un ordine di pagamento elettronico; per qualsiasi attività eseguita a distanza che potrebbe comportare rischi di frode o altri tipi di abusi nei pagamenti.

Il Rapporto 2023 della Banca d'Italia evidenzia come l'introduzione della SCA abbia ridotto il tasso di frodi nei pagamenti online di circa il 60% rispetto agli anni precedenti l'implementazione della PSD2.

4.3.2 Crittografia e tokenizzazione

La sicurezza è cruciale per garantire che i pagamenti digitali siano protetti da frodi e attacchi informatici. Per questa ragione, oltre alla SCA, l'uso di tecnologie avanzate come la crittografia end-to-end e la tokenizzazione garantiscono che i dati sensibili degli utenti non vengano mai trasmessi direttamente.

La crittografia end-to-end (E2EE) è una tecnica che garantisce che i dati scambiati tra due parti (ad esempio, tra un cliente e una piattaforma di pagamento) siano protetti da terzi. Questa tecnologia utilizza un sistema di chiavi crittografiche, una pubblica e una privata, per cifrare i dati prima che vengano trasmessi e per decifrarli solo all'arrivo.

Nel contesto dei pagamenti digitali, la crittografia end-to-end è utilizzata per proteggere le informazioni sensibili, come numeri di carte di credito, PIN e credenziali bancarie. Una volta che un utente inserisce i suoi dati su una piattaforma di pagamento, questi vengono immediatamente cifrati, in modo che, se un hacker dovesse intercettarli durante il trasferimento, i dati risulterebbero illeggibili.

Un esempio concreto è l'uso della crittografia TLS (Transport Layer Security) nelle connessioni tra i browser web e i server delle piattaforme di pagamento, la quale assicura che le informazioni scambiate siano protette durante l'intero processo di transazione. Il protocollo TLS è considerato lo standard di sicurezza per il trasferimento sicuro di dati su internet, ed è utilizzato da piattaforme come PayPal, Amazon, e servizi bancari online.

La European Central Bank (ECB), nel suo rapporto annuale del 2022, ha evidenziato che l'uso di crittografia avanzata come TLS debba essere un requisito obbligatorio per tutte le istituzioni finanziarie e le piattaforme che trattano dati sensibili. Questo standard si applica non solo alle transazioni finanziarie, ma anche alla comunicazione interna tra server e data center delle banche.

La tokenizzazione è un'altra tecnologia fondamentale per la sicurezza nei pagamenti digitali. Invece di trasmettere direttamente i dati della carta di credito o del conto bancario, permette di sostituire queste informazioni con un "token" unico, ovvero una stringa casuale di numeri e lettere che non ha alcun valore intrinseco per chi dovesse intercettarla. Questo token viene utilizzato per completare la transazione, mentre i dati originali restano memorizzati in un server sicuro e non vengono mai trasmessi durante la transazione stessa. Se un hacker dovesse ottenere il token, non potrebbe utilizzarlo per eseguire transazioni, in quanto è legato a quella singola operazione o a quel determinato dispositivo.

Apple Pay e Google Pay sono esempi di piattaforme che utilizzano la tokenizzazione per garantire la sicurezza delle transazioni. Quando un utente effettua un pagamento con uno di questi servizi, il numero della carta di credito non viene mai inviato al commerciante; invece, viene utilizzato un token associato alla transazione.

Secondo il Rapporto PCI DSS (Payment Card Industry Data Security Standard) 2022, l'adozione della tokenizzazione ha contribuito a ridurre significativamente le frodi nei pagamenti online, specialmente nel settore e-commerce.

5 Casi di studio e analisi pratica

5.1 Il caso delle frodi nelle banche digitali: sanzioni a N26

N26, una delle principali banche digitali europee, è stata al centro di diverse indagini e sanzioni da parte delle autorità di regolamentazione, in particolare della BaFin (Bundesanstalt für Finanzdienstleistungsaufsicht), l'autorità di vigilanza finanziaria tedesca, a causa di inadeguatezze nel rispettare le normative antiriciclaggio (AML).

Nel caso di N26, la BaFin ha imposto una multa di 4,25 milioni di euro nel 2021 per non aver rispettato gli obblighi relativi al monitoraggio delle transazioni e alla verifica dell'identità dei clienti. La banca è stata accusata di non aver implementato controlli adeguati a rilevare e prevenire attività di riciclaggio di denaro e frodi, e di non aver risposto tempestivamente alle segnalazioni di transazioni sospette. La crescita rapida di N26 ha portato infatti a carenze nei suoi sistemi di conformità, poiché la banca non è riuscita a potenziare i suoi meccanismi di controllo al passo con l'aumento del numero di clienti.

Per queste ragioni, il 28 marzo 2022, la Banca d'Italia ha ordinato alla Succursale Italiana di N26 di sospendere temporaneamente l'apertura di nuovi conti per i clienti, indicando aree da migliorare riguardo alle procedure antiriciclaggio. Di conseguenza, N26 non ha potuto temporaneamente offrire nuovi prodotti o servizi ai clienti della Succursale Italiana fino a quando le problematiche segnalate non fossero state risolte.

5.2 Il caso UniCredit e la sicurezza dei pagamenti online: Intervento del Garante per la Privacy

Nel 2018, UniCredit ha subito un attacco informatico che ha compromesso i dati di circa 780.000 clienti. A seguito di questo attacco, nel 2024 il Garante per la Protezione dei Dati Personali (Garante Privacy) ha multato UniCredit per 2,8 milioni di euro, evidenziando le carenze nei sistemi di protezione dei dati personali, dunque la violazione delle normative del GDPR.

La violazione ha riguardato informazioni sensibili come nome, cognome, codice fiscale e, per circa 6.800 clienti, anche il PIN di accesso al portale di mobile banking. La banca non aveva implementato misure sufficienti per contrastare attacchi informatici e per prevenire l'uso di PIN deboli.

Il Garante ha tenuto conto della gravità della violazione e dell'alto numero di persone coinvolte, ma ha anche riconosciuto le misure correttive adottate tempestivamente dalla banca e il fatto che i dati bancari non erano stati compromessi.

Parallelamente, è stata inflitta una multa di 800.000 euro alla società NTT Data Italia, incaricata da UniCredit per i test di sicurezza. La società è stata sanzionata per aver comunicato in ritardo la violazione dei dati e per aver subappaltato parte dei test senza autorizzazione.

5.3 Intervento dell'AGCM su ApplePay e pratiche anticoncorrenziali (European commission)

Nel 2021, l'Autorità Garante della Concorrenza e del Mercato (AGCM) ha avviato un'indagine su Apple riguardo alle pratiche anticoncorrenziali relative all'utilizzo del chip NFC (Near Field Communication) sugli iPhone, essenziale per i pagamenti contactless tramite ApplePay. L'indagine è nata in seguito a una denuncia presentata da vari operatori di servizi di pagamento, tra cui PayPal, i quali sostenevano che Apple limitasse l'accesso al chip NFC a servizi di pagamento terzi, impedendo così loro di competere in modo equo nel mercato.

Secondo l'AGCM, Apple ha effettivamente garantito l'accesso al chip NFC esclusivamente per il proprio servizio ApplePay, obbligando i consumatori ad utilizzare il suo sistema di pagamento se utilizzano un iPhone. Questa pratica è stata considerata una violazione delle normative europee in materia di concorrenza, in particolare degli articoli 101 e 102 del Trattato sul funzionamento dell'Unione Europea, che vietano comportamenti anticoncorrenziali da parte delle imprese dominanti nel mercato.

L'indagine dell'AGCM è stata supportata dalla Commissione Europea, che ha ribadito la necessità di mantenere un mercato aperto e competitivo per tutti i fornitori di servizi di pagamento. Questo caso rappresenta un esempio importante di come le autorità regolatorie stiano intervenendo per garantire che le innovazioni tecnologiche non diventino barriere all'accesso al mercato per nuovi attori.

5.4 Il caso Intesa Sanpaolo e il trattamento dei dati biometrici: Sanzione del Garante per la Privacy

Il caso di Intesa Sanpaolo riguardante il trattamento dei dati biometrici ha attirato l'attenzione del Garante per la protezione dei dati personali, che ha imposto una sanzione significativa.

L'Autorità ha riscontrato che l'istituto bancario ha trattato i dati biometrici di 288 dipendenti senza rispettare le normative vigenti, violando i principi di liceità, correttezza e trasparenza previsti dal Regolamento generale sulla protezione dei dati (GDPR). In partcolare, secondo l'articolo 9 del GDPR, il trattamento di dati biometrici è generalmente vietato, salvo in alcune circostanze molto specifiche.

Intesa Sanpaolo ha infatti installato sistemi di riconoscimento biometrico per la rilevazione delle presenze dei dipendenti e il Garante ha sanzionato la banca per non aver fornito le garanzie appropriate per i diritti degli interessati e per non aver rispettato i requisiti di minimizzazione e integrità dei dati, portando a considerare il trattamento come illecito. La violazione delle misure di garanzia può comportare responsabilità penale e amministrativa, oltre a sanzioni pecuniarie.

Questa decisione è un chiaro avviso per le aziende che intendono implementare tecnologie biometriche, poiché le autorità di protezione dei dati stanno intensificando i controlli su questi sistemi, richiedendo un rigoroso rispetto delle normative esistenti.

5.5 Il caso PayPal e la regolamentazione europea

Nel 2023, la Commissione Europea e le autorità nazionali per la tutela dei consumatori hanno avviato un dialogo con PayPal per affrontare questioni relative ai termini e condizioni del servizio, ritenuti eccessivamente difficili da comprendere e sleali nei confronti dei consumatori.

La Commissione Europea e le autorità nazionali per la tutela dei consumatori hanno riscontrato che le clausole contrattuali di PayPal non rispettavano la direttiva sulle clausole abusive nei contratti, che mira a proteggere i consumatori da termini contrattuali ingiusti e sbilanciati.

PayPal si è allora impegnata a modificare i propri termini e condizioni per renderli più trasparenti e comprensibili, allineandosi meglio alle prescrizioni del diritto dell'UE in materia di tutela dei consumatori. Questo intervento è stato coordinato dalla rete di cooperazione per la tutela dei consumatori (rete CPC), guidata dall'autorità tedesca Umweltbundesamt.

Conclusioni

Questo lavoro ha descritto l'utilizzo della moneta elettronica, delle banche online e dei pagamenti digitali, evidenziando sia i vantaggi che le criticità di questo settore in continua espansione.

La digitalizzazione dei servizi finanziari ha infatti offerto notevoli benefici, tra cui una maggiore accessibilità, velocità e convenienza nelle transazioni. Tuttavia, essa ha mostrato anche diversi punti di vulnerabilità, specialmente sul fronte della sicurezza e della protezione dei dati personali, su cui i vari capitoli si sono concentrati.

L'implementazione di misure come l'autenticazione forte del cliente (SCA) e l'uso di tecnologie avanzate come la crittografia e la tokenizzazione, essenziali per prevenire frodi e violazioni dei dati, è stata presentata come possibile soluzione alle tante frodi esistenti oggi in questo ambiente, di cui sono stati riportati alcuni esempi.

Attraverso l'analisi delle principali normative, come la PSD2, la EMD2 e il GDPR, è emerso chiaramente che l'Unione Europea ha compiuto passi significativi per regolamentare il settore e garantire la sicurezza dei consumatori. Questo è stato testimoniato dai casi studio presentati, i quali hanno dimostrato come le normative e le tecnologie di sicurezza vengano applicate in scenari reali, offrendo una panoramica pratica delle sfide e delle soluzioni adottate dalle aziende del settore finanziario. Le sanzioni inflitte a N26 e UniCredit, nonché gli interventi dell'AGCM su ApplePay e del Garante per la Privacy su Intesa SanPaolo, sottolineano l'importanza di conformarsi a un quadro normativo stringente per tutelare i diritti degli utenti.

In conclusione, mentre la digitalizzazione dei pagamenti continua a crescere, sarà fondamentale mantenere un equilibrio tra innovazione, sicurezza e protezione dei dati. Le istituzioni finanziarie devono quindi adattarsi rapidamente alle nuove minacce informatiche e alle esigenze normative, adottando soluzioni tecnologiche avanzate che garantiscano un livello elevato di fiducia e sicurezza del cliente. Solo così sarà possibile promuovere un ecosistema finanziario digitale sicuro, innovativo e inclusivo, in grado di sostenere la fiducia dei consumatori e contribuire alla crescita economica.

Bibliografia

1. Banca d'Italia. (2022). *Moneta elettronica e sistemi di pagamento in Italia: Evoluzione e prospettive*. (https://www.bancaditalia.it)
2. European Central Bank (ECB). (2021). *Electronic money, payment instruments, and cryptocurrencies: An overview*. (https://www.ecb.europa.eu)
3. OECD. (2022). Digital Banking: Trends, Regulation, and Innovation. (https://www.oecd.org)
4. Garante per la protezione dei dati personali. (2021). Rapporto sulla protezione dei dati personali nelle banche online. (https://www.garanteprivacy.it)
5. Banca d'Italia. (2023). *Rapporto annuale sulla sicurezza dei pagamenti digitali e l'implementazione della Strong Customer Authentication (SCA)*. (https://www.bancaditalia.it)
6. European Central Bank (ECB). (2022). Payments security and encryption standards: Guidelines for secure transactions. (https://www.ecb.europa.eu)
7. M. D. Meyer, "The EMD2 Directive: Balancing Innovation and Consumer Protection." *Journal of Banking Regulation*, vol. 19, no. 2, 2018, pp. 123-145.
8. European Commission. (2018). *Revised Payment Services Directive (PSD2) – Impact on Payment Systems and Fintech*. (https://ec.europa.eu)
9. European Banking Authority (EBA). (2020). *Strong Customer Authentication (SCA) and Secure Payment Systems under PSD2*. (https://www.eba.europa.eu)
10. M. A. A. M. H. H. El-Sheikh, "The Role of GDPR in Protecting Consumers' Data." International Journal of Law and Information Technology, vol. 27, no. 3, 2019, pp. 287-303.
11. Z. Chikova, "Understanding Anti-Money Laundering Directives in the Context of Digital Finance." Journal of Financial Regulation and Compliance, vol. 29, no. 2, 2021, pp. 146-162.
12. K. R. Smith, "Cryptography and Tokenization in Payment Systems: A Comparative Analysis." Journal of Information Security and Applications, vol. 53, 2020, pp. 102-118.
13. BaFin (BaFin - Pubblicazione di misure - N26 Bank GmbH: BaFin ordina misure per limitare la crescita e nomina un ...)
14. GarantePrivacy (Newsletter del 7/03/2024 - Data breach: il Garante sanziona UniCredit... - Garante Privacy)
15. GarantePrivacy (Ordinanza ingiunzione nei confronti di Intesa Sanpaolo S.p.a.. - 20... - Garante Privacy)
16. UE prepara le accuse antitrust contro Apple Pay e il chip NFC degli iPhone (iphoneitalia.com)
17. AGCM - Autorita' Garante della Concorrenza e del Mercato
18. PayPal si impegna a modificare termini e condizioni per rispettare pienamente le norme dell'UE in materia di tutela dei consumatori - Commissione europea (europa.eu)