LUISS

Corso di laurea in Economia e Management

Cattedra Diritto Privato

Cybersecurity ed evoluzione del sistema dei pagamenti tra direttive PSD2 e DORA

Prof. Francesco Di Ciommo

RELATORE

Chiara Molendini - 256561

CANDIDATO

Anno Accademico 2022/2023

Indice

Introduzione

Nel corso della storia, l'evoluzione dei pagamenti subisce una grandiosa trasformazione, trasportandoci da un'era in cui le transazioni avvenivano attraverso il baratto e lo scambio diretto, fino a raggiungere un mondo digitale in cui è possibile pagare istantaneamente con un semplice tocco dello smartphone. È come se l'antico sistema di scambio di merci fosse stato catapultato nel futuro, consentendoci di superare i confini fisici e di condurre transazioni a velocità supersonica. I pagamenti hanno attraversato secoli di progresso, trasformando monete d'oro in carte di credito, passando da banconote e assegni a transazioni senza contanti e pagamenti online. Grazie all'incalzante avanzamento tecnologico che sembra non avere mai sosta tra AI e valute digitali come le cripto e all'evoluzione che ha portato la comodità e l'efficienza a livelli incredibili, l'esperienza di acquisto si è integralmente trasformata aprendo le porte ad un'infinità di possibilità finanziarie.

Al passo dello stesso progresso tecnologico ha dovuto (e deve) in continuazione adeguarsi anche la branca del diritto assieme a quella dell'economia, l'uno inevitabilmente dipendente dall'altra: da un lato il mercato economico deve necessariamente essere normato da direttive e regolamenti affinché non viga il totale liberalismo economico e, per sua parte, la giurisdizione si ritrova di volta in volta obbligata a legiferare conformemente ai repentini cambiamenti del mercato, incessantemente: due macrocategorie della società necessariamente complementari.

Il seguente elaborato si propone di focalizzare l'attenzione sull'attuale tema dell'innovazione tecnologica, come si è già fatto riferimento sopra, e, nello specifico di discutere ed esplorare un ramo molto importante della suddetta nonché quello della cybersicurezza e come il sistema dei pagamenti sia progredito fino ad oggi principalmente per merito delle leggi che sono state emanate nel corso del tempo.

Ad oggi il sistema dei pagamenti, in cui distinguiamo due essenziali tipologie di attori quali players (operativi) e le istituzioni (cui compito fondamentale è garantire l'osservanza delle norme e vigilanza)[1], rasenta il completo inutilizzo del contante, le banche tradizionali arrancano nel momento in cui non si dimostrano aperte ad adottare strategie per adeguarsi al cambiamento, in particolar modo successivamente alla nascita degli IMEL, nonché istituti di moneta elettronica, i quali costituiscono imprese, diverse dalle banche, che emettono moneta elettronica.

E ancora, l'invenzione di carte come Revolut ed N26, le quali presentano diverse innovazioni nel settore bancario e delle carte di pagamento. Entrambi offrono numerosi ed innovativi vantaggi, fra cui gestione delle proprie finanze tramite app e accessibilità in qualsiasi istante e posto, cambio valuta in tempo reale a tariffe di cambio convenienti e tanto altro. Diritto ed economia si ritrovano

[1] Bruni, M. (2017). *Open Banking e PSD2: sfide ed opportunità per le banche.*

subordinati alla frammentarietà e all'assenza di interruzioni, caratteristiche tipiche dell'epoca postmoderna attuale, dando la possibilità all'individuo di godere dell'ubiquità di informazioni, servizi e l'accesso agli stessi in qualsiasi contesto spaziale o temporale.

Ma proprio ciò che getta le basi di tutto questo recente processo evolutivo e su cui maggiormente si indirizzerà il seguente trattato è una direttiva la cui ufficiale emanazione avviene nel 2018, la PSD2. (abbreviazione di Payment Services Directive 2, tradotto, Direttiva sui servizi di pagamento 2). Viene introdotta come parte di una serie di direttive dell'Unione Europea per disciplinare e stimolare l'innovazione, aumentare la sicurezza di pagamenti e prelievi e proteggere i diritti dei consumatori.

Se da un lato PSD2 si concentra principalmente sui servizi di pagamento, con i suoi diversi obiettivi progressistici, di competitività e sicurezza, dall'altro è stata pubblicata, in tempi più recenti (2020), la direttiva DORA (Digital Operational Resilience Act), la quale mira ad obiettivi ancor più capillari e specifici rispetto a PSD2: è fondamentalmente incentrata sulla resilienza operativa nel settore finanziario digitale, con lo scopo di dare alle varie istituzioni finanziarie la capacità di gestire i rischi operativi e minacce cibernetiche, tutelarle quanto alla loro sicurezza nell'ambito finanziario digitale.

Si tratta in entrambi i casi di due cruciali normative dell'UE riguardanti il settore di cui sopra, promozione di sicurezza e stabilità in quest'ultimo, ma con finalità leggermente differenti: mentre la Direttiva DORA mira a migliorare la resilienza operativa nel settore finanziario digitale, la Direttiva PSD2 si concentra specificamente sui servizi di pagamento, promuovendo l'innovazione e l'apertura nel settore dei pagamenti virtuali.

Capitolo 1 - PSD2: scopo e struttura della direttiva c.d. PSD2

Genesi e principali obiettivi della direttiva

I servizi di pagamento sono cruciali nel settore finanziario; tradizionalmente forniti dalle banche, le istituzioni finanziarie non bancarie, nel corso del tempo, hanno guadagnato importanza. Tuttavia, l'attenzione è stata più focalizzata sulla solidità del sistema che sull'efficienza dei servizi di pagamento, infatti, negli ultimi anni, questo scenario è drasticamente mutato: tra le svariate cause del cambiamento in questione si annovera la PSD2.[2]

Per comprendere al meglio l'essenza della suddetta, motivo centrale dell'elaborato, è necessario fare un piccolo passo indietro: la prima Payment Service Directive (PSD) viene pubblicata il 13 novembre del 2007 ed entra in vigore nel 2009. Questa direttiva definisce la giurisdizione nella comunità europea limitatamente ai servizi di pagamento elettronici, introducendo nuovi fornitori di servizi di pagamento oltre a banche tradizionali e avendo sempre obiettivi di maggiore trasparenza per quanto riguarda commissioni e tassi di cambio; svolge inoltre un ruolo centrale nel velocizzare lo sviluppo dell'area di pagamento unica in euro (SEPA, Single Euro Payments Area), con lo scopo di efficientare e accelerare i pagamenti. E ancora, ha posto ingente enfasi sulla protezione dei consumatori e sulla promozione di un'ampia gamma di servizi di pagamento tra cui scegliere.[3]

Da qui l'esigenza della creazione di PSD2: una serie di sviluppi e sfide nel settore dei pagamenti; diversi sono i fattori a concorrere alla nascita di questa necessità come, ad esempio, l'attuale e celere evoluzione tecnologica, la maggiore apertura all'innovazione rispetto al passato, l'armonizzazione dei servizi di pagamento nell' UE attraverso un mercato unico europeo, la protezione e sicurezza dei consumatori…[4]

Proposito principale della direttiva è la creazione di un mercato dei pagamenti integrato, competitivo e innovativo all'interno dell'Unione Europea, che punti a un'ampia e capillare protezione del cliente, forte sicurezza nei pagamenti e facilità nella loro esecuzione.

Nello specifico, la PSD2 consta delle seguenti clausole: rendere più semplice e sicuro il processo di pagamento online, una migliore protezione dei servizi di pagamento per quanto riguarda frode, abuso e problemi a esso annessi, promozione di sistemi di pagamento innovativi e rafforzamento dei diritti di pagamento degli utenti usufruenti dei servizi.

Successivamente all'implementazione della PSD2, il mercato dei pagamenti ha continuato la sua perpetua evoluzione: sono emersi nuovi agenti di mercato, ulteriori metodi di pagamento, servizi e tecnologie: inevitabilmente, e come conseguenza, i bisogni degli utenti quanto a servizi di pagamento

[2] Pozzolo A. (2021). *L'ATTUAZIONE DELLA SECONDA DIRETTIVA SUI SERVIZI DI PAGAMENTO E "OPEN BANKING*".
[3] Pagamenti Digitali. (2022). *PSD2: Cos'è, obblighi e funzionamento della direttiva europea*
[4] BERTOLDI, M. *La direttiva sui servizi di pagamento: portabilità dei dati finanziari e sviluppo dell'open banking.*

sono cambiati; causa è sicuramente l'incalzante digitalizzazione della società. Tutto ciò ha provocato, nel mondo dei servizi di pagamento, la nascita di nuove sfide e rischi (questi ultimi soprattutto) da prendere attentamente in considerazione. Dunque, innovazione e soddisfazione dei bisogni degli utenti fanno parte dei fondamentali obiettivi della direttiva.

Il costante aggiornamento del mercato ha portato alla generazione di una vasta gamma di nuovi servizi e soluzioni di pagamento come gli "account-to-account mobile-initiated payments" (il termine "account-to-account mobile-initiated" si riferisce a una transazione finanziaria in cui un utente utilizza un'applicazione mobile per iniziare una transazione da un suo conto bancario a un altro conto bancario), lo sviluppo di diversi tipi di portafoglio (compresi gli strumenti di pagamento nei negozi fisici come il POS, spesso "contactless", ossia che non necessita inserimento della carta fisica nel dispositivo), l'uso di effetti indossabili come gli Smart Watches, la possibilità di pagare in negozi fisici tramite Smartphone semplicemente registrando i dati della propria carta di credito o debito sul wallet elettronico e tanti altri elementi di ultima generazione. [5]

La protezione dei consumatori costituisce un altro fondamentale obiettivo della direttiva. Le principali caratteristiche di protezione dei consumatori in PSD2 includono elementi come trasparenza delle condizioni per l'accesso all'uso dei servizi di pagamento, una chiara definizione dei diritti e degli obblighi per PSUs e PSPs (rispettivamente Payment Service Users e Payment Service Providers) dapprima che giunga il momento di pagare (una specie di consenso informato ma nell'ambito di cui si è trattato) i requisiti per il miglioramento della prevenzione delle frodi, le procedure di risoluzione delle controversie e così via.

Trattandosi di una direttiva fondamentale dal punto di vista economico e sociale, è soggetta a continui aggiornamenti (ciò in ragione del fatto che l'economia sia in costante evoluzione e quindi necessiti di svariati istituti giuridici che la regolino e facciano funzionare quanto più fluidamente), questi ultimi oggetto di ingenti investimenti da parte dell'industria finanziaria.

A titolo esemplificativo, i PSPs si sono trovati nella necessità di adattare e migliorare i propri sistemi al fine di implementare adeguatamente la procedura di autenticazione del cliente. Inoltre, i PSPs (addetti a loro volta alla gestione dei conti di pagamento) hanno dovuto predisporre l'accesso da parte di altri fornitori di servizi anch'essi di pagamento;

Altro fondamentale scopo della direttiva è quello di abilitare le autorità competenti al miglioramento del monitoraggio e supervisione delle attività dei nuovi PSPs e con accesso nel mercato dei pagamenti (già da tempo); mira, dunque, a un rafforzamento e maggiore inclusività degli enti economici.

[5] Commissione Europea (2022). *Targeted Consultation On The Review Of The Revised Payment Services Directive (PSD2)*

Con queste intenzionalità, PSD2 ha introdotto importanti cambiamenti nel settore dei servizi di pagamento; spiccano, tra questi, una procedura di passaporto più dettagliata per le imprese che operano in più Stati membri e la definizione di norme di tipo tecnico che stabiliscono le modalità di cooperazione e scambio di informazioni tra le autorità nazionali competenti. Inoltre, la direttiva prevede che gli Stati membri debbano stabilire regole per garantire che le autorità nazionali competenti (NCAs) siano autorizzate ad assicurare e monitorare la conformità alla direttiva. Queste nuove disposizioni mirano a migliorare la sicurezza e l'efficienza dei servizi di pagamento transfrontalieri nell'Unione Europea.[6]

In sostanza, quindi, la struttura della direttiva può per sommi capi essere rappresentata dalle seguenti disposizioni:

1) L'obbligo per i fornitori di servizi di pagamento di ottenere una licenza da parte dell'autorità di vigilanza finanziaria nazionale.

2) L'obbligo di implementare misure di sicurezza avanzate per le transazioni online, come l'autenticazione a due fattori.

3) La creazione di un nuovo tipo di soggetto, il TPP (Third Party Provider), che può accedere ai conti bancari dei consumatori per offrire servizi di pagamento innovativi.

4) L'introduzione di nuove regole per la gestione dei dati personali dei consumatori, compresi i dati finanziari.

5) L'obbligo per le banche di fornire ai TPP un accesso sicuro e standardizzato ai conti bancari dei consumatori.

6) L'obbligo per le banche di fornire ai consumatori un accesso online ai loro conti bancari attraverso API (Application Programming Interfaces) standardizzate.

[6] Commissione Europea (2022). *Targeted Consultation On The Review Of The Revised Payment Services Directive (PSD2)*

Misure e procedure regolanti le attività di pagamento della direttiva

La direttiva in questione comprende una serie di misure e procedure finalizzate alla regolamentazione delle attività dei pagamenti al dettaglio. In particolare, essa disciplina l'autorizzazione delle istituzioni di pagamento e la supervisione dei prestatori di servizi di pagamento, attraverso la definizione di una lista di PSPs che richiedono l'autorizzazione da parte di un'ulteriore istituzione di pagamento, nonché le modalità per ottenerla e le condizioni richieste per le entità autorizzate a fornire tali servizi.

Dopo l'entrata in vigore della direttiva nel gennaio 2018, sono emersi nuovi attori sul mercato e sono state sviluppate nuove soluzioni di pagamento, servizi e tecnologie. Tuttavia, la Commissione Europea ha altresì rilevato che, contemporaneamente, si sono verificati anche nuovi casi di frodi ai mezzi di pagamento. Tale fenomeno ha reso necessario l'adozione di ulteriori misure di sicurezza e protezione per i consumatori. La PSD2 ha avuto come fine quello di modernizzare il mercato dei pagamenti e creare spazio per lo sviluppo di nuovi servizi e provider di pagamento; il Titolo II della direttiva riguarda in particolare l'autorizzazione (licenza) dei prestatori di servizi di pagamento (ad esempio, i requisiti per la presentazione della domanda di autorizzazione, il calcolo dei propri fondi, ecc.), le esenzioni dalle autorizzazioni e il quadro di supervisione. L'obiettivo di queste disposizioni è quello di garantire la stabilità del mercato dei pagamenti e la protezione dei consumatori, promuovendo al contempo l'innovazione e la concorrenza nel settore dei pagamenti nell'Unione Europea.

L'articolo 35 della Direttiva sui servizi di pagamento 2 (PSD2) prevede l'accesso non discriminatorio dei prestatori di servizi di pagamento ai sistemi di pagamento. L'articolo 2(a) prevede un'eccezione per i sistemi di pagamento designati ai sensi della Direttiva 98/26/CE (Direttiva sulla finalità dell'insediamento, SFD). Tra il 12 febbraio e il 7 maggio 2021, la Commissione europea ha condotto una consultazione mirata, chiedendo pareri sulla SFD (acronimo di Settlement Finality Directive) per preparare una relazione da presentare al Parlamento europeo e al Consiglio. L'obiettivo di tale consultazione è stato quello di valutare l'efficacia della normativa esistente e di identificare eventuali lacune o aree che richiedono miglioramenti, al fine di garantire la sicurezza e l'efficienza dei sistemi di pagamento nell'Unione europea.

Come precedentemente citato, uno degli obiettivi di PSD2 è migliorare la trasparenza delle condizioni per la fornitura dei servizi di pagamento (*paragrafo 1.1: Principali obiettivi della direttiva*). Ad esempio, i prestatori di servizi di pagamento sono tenuti ad essere trasparenti su tutte le commissioni pagabili dal PSU al prestatore di servizi di pagamento, sul tempo massimo di esecuzione della transazione e sul tipo di informazioni fornite ai pagatori e ai beneficiari dopo l'esecuzione delle transazioni. Ci sono alcune eccezioni e differenze nelle disposizioni sulla trasparenza delle condizioni

e sui requisiti informativi per i pagamenti con/verso paesi al di fuori dell'UE (questi ultimi vengono denominati "transazioni a una sola gamba").

PSD2 prevede anche diritti e obblighi per tutte le parti coinvolte, sia per gli utenti di servizi di pagamento che per i prestatori di servizi di pagamento. Queste misure sono volte a rendere i pagamenti più sicuri e protetti, garantendo un elevato livello di protezione per tutti gli utenti di servizi di pagamento in tutti gli Stati membri e a rafforzare i diritti dei consumatori. Il Titolo IV include, tra l'altro, alcune norme sulle spese applicabili, il tempo massimo di esecuzione, l'irrevocabilità, il diritto al rimborso, le regole per la responsabilità e i requisiti relativi all'accesso ai conti di pagamento (chi ha accesso, come e in quali circostanze). Inoltre, contiene requisiti per il rischio operativo e di sicurezza e per l'autenticazione forte del cliente.[7]

[7] Commissione Europea (2022). *Targeted Consultation On The Review Of The Revised Payment Services Directive (PSD2)*

Capitolo 2 - Open banking e PSD2: come cambia il sistema bancario a seguito della direttiva

Uno sguardo generale all'open banking: quali fattori lo abilitano e chi sono i principali attori del mercato dell'Open Banking

Per dare un incipit all'argomento dell'open banking è essenziale darne una lineare definizione: l'open banking riguarda la pratica di condividere in modo sicuro e controllato i dati finanziari di un cliente tra diverse istituzioni (a loro volta finanziarie) per mezzo dell'uso di tecnologie digitali. Sostanzialmente consente agli utenti di dare il consenso affinché loro dati finanziari vengano condivise con terze parti autorizzate (come banche o ulteriori intermediari finanziari) al fine di offrire una gamma di servizi innovativi e personalizzati in base al cliente. La trasmissione delle informazioni personali creditizie può attuarsi attraverso interfacce e API aperte: in tal modo si conferisce alle operazioni maggiore trasparenza, ulteriore scelta per i consumatori e più concorrenza quanto all'offerta da parte delle terze parti autorizzate.

È proprio per merito della direttiva PSD2 che nasce l'Open Banking, entrambi nell'ambito dei pagamenti digitali e dei servizi finanziari costituiscono concetti strettamente correlati: da una parte la PSD2 rappresenta un quadro regolamentare che promuove l'apertura dei servizi finanziari attraverso l'open banking; l'implementazione della direttiva ha in più reso obbligatoria l'apertura dei dati delle banche alle terze parti autorizzate, consentendo così lo sviluppo di nuovi servizi innovativi e l'integrazione dei pagamenti in modo più sicuro e conveniente per i consumatori. L'Open Banking è ormai diventato un fenomeno mondiale, fautore del profondo e continuo cambiamento del settore dei servizi finanziari: ha permesso l'ingresso di nuovi attori come le Fintech e ha spinto le banche tradizionali a rivedere i loro modelli di business per adattarsi a questo nuovo scenario. L'Open Banking ha abilitato una nuova modalità di "fare banca", basato sulla cooperazione tra diversi attori del mercato e ha consentito la creazione di un ecosistema digitale in cui i consumatori hanno accesso a un'ampia gamma di servizi attraverso canali innovativi. Le partnership tra banche e Fintech, insieme alle acquisizioni nel mercato, dimostrano il dinamismo del settore e l'attenzione crescente verso l'Open Banking.

La PSD2 ha introdotto il concetto di "open banking", stabilendo norme che consentono ai PSUs di condividere in modo sicuro determinati dati del loro conto di pagamento con fornitori terzi. In particolare, PSD2 impone ai fornitori di servizi di pagamento di fornire l'accesso agli account di pagamento dei propri clienti a terze parti autorizzate (TPP) attraverso interfacce di programmazione delle applicazioni (API). Questo consente ai TPP di accedere a informazioni sul conto di pagamento

dell'utente (come saldo e transazioni), al fine di offrire servizi aggiuntivi, come l'iniziazione di pagamenti o l'aggregazione di conti da diverse banche in un'unica "interfaccia utente".[8]

Nel contesto dell'Open Banking, l'utente non accede direttamente ai servizi online offerti dalla propria banca (che funge da gestore dati), bensì utilizza un'applicazione terza fornita da un Third Party Provider (TPP), che filtra e aggrega i dati ed offre servizi personalizzati all'utente in base alle sue richieste e alle logiche commerciali del TPP stesso. In altre parole, il TPP agisce come intermediario tra l'utente e la banca, consentendo all'utente di accedere ai propri dati bancari e di usufruire di servizi aggiuntivi offerti dal TPP. L'obiettivo di questa regolamentazione è quello di favorire l'innovazione nel settore dei servizi finanziari, aumentare la concorrenza tra i fornitori di servizi di pagamento e migliorare la protezione dei consumatori.[9]

L'apertura dei conti correnti ai servizi di Open Banking delle terze parti, anch'essa regolamentata dalla PSD2, ha segnato un passaggio epocale che ha connesso il mondo bancario tradizionale ai nuovi servizi Fintech. Oggi il pagamento digitale assume maggior valore quando viene offerto in un contesto integrato, poiché rappresenta un elemento di **servizio completo** offerto al cliente finale. Una esperienza d'uso in cui il cliente fruisce di un servizio digitale, ma deve poi utilizzare modalità scollegate "**out-of-band**" ("out of band" si riferisce a una modalità di comunicazione che avviene al di fuori del canale principale o predefinito utilizzato per la comunicazione) per pagarne il costo, perde sempre più di significatività. Allo stesso tempo, è sempre più evidente che i dati provenienti dai conti dei clienti hanno un valore molto ampio e sono in grado di attivare servizi e funzionalità che vanno oltre quelli previsti dalla PSD2.

Inoltre, l'open banking è un fenomeno emergente che sta registrando una notevole diffusione in tutto il mondo. Attualmente, più di 60 paesi hanno adottato iniziative o pratiche di Open Banking, ciascuno con un approccio specifico in relazione alle esigenze del proprio mercato domestico. Il mercato suo mercato è in costante crescita e nel 2018 tocca il valore di 7,29 miliardi di dollari, con una previsione di raggiungere i 43,15 miliardi di dollari entro il 2026, con crescita annua composta del 24,4%. Inoltre, il numero di utenti dell'Open Banking sta aumentando rapidamente a livello globale, passando da 24,7 milioni nel 2020 a una previsione di 132,2 milioni entro il 2024, con una crescita annua media del 50%. Il mercato europeo è attualmente il più grande a livello globale, con una previsione di circa 63,8 milioni di utenti attivi entro il 2024.

Dopo una prima fase iniziale, durante la quale il sistema bancario tradizionale ha adottato un approccio sostanzialmente difensivo nei confronti dell'Open Banking, si è verificato un cambio di strategia da parte degli incumbent: essi stanno ora cercando forme di collaborazione con i soggetti

[8] Commissione Europea (2022). *Targeted Consultation On The Review Of The Revised Payment Services Directive (PSD2)*

[9] CBI, (2021). *The Global Open Banking Report*

più innovativi al fine di sperimentare soluzioni inedite e ampliare l'offerta di servizi a vantaggio della propria clientela. Inoltre, si sta assistendo a una progressiva diffusione del fenomeno della "platformisation" (ovvero la tendenza delle aziende di creare e gestire piattaforme digitali per fornire servizi o prodotti ai propri clienti[10]) anche nel mondo dei pagamenti, grazie alle logiche "Open" introdotte dalla PSD2.

Per di più il settore dell'Open Banking sta progressivamente evolvendo verso prospettive ancor più ampie come l'Open Finance grazie alle numerose possibilità offerte dalle tecnologie attuali. Tuttavia, la sfida principale risiede nell'armonizzare il contesto normativo e gli standard di base in modo da sostenere e incentivare innovazione e fluidità nella fruizione dei servizi. In particolare, è fondamentale stabilire regole comuni per i servizi di base, come l'identificazione del cliente e la sicurezza delle transazioni, per tutelare privacy e sicurezza dei dati finanziari. La collaborazione tra fornitori di servizi finanziari, legislatori e regolatori è essenziale per creare un quadro normativo adeguato e favorire la concorrenza nel settore finanziario.

[10] Kenney, M., & Zysman, J. (2016). *The rise of the platform economy. Issues in Science and Technology, 32(3), 61-69.*

Tra PSD2 ed Open Banking: quali sono i fattori che spingono i Paesi verso il mondo "Open" e i diversi approcci

"L'Open Banking è un fenomeno globale che ha trasformato profondamente il Settore dei Servizi Finanziari, spingendo gli operatori finanziari a reinventare i loro Modelli di Business, facendo leva sulla collaborazione con nuovi attori del mercato."[11]

Tra tutti, il mercato britannico può essere considerato come quello che ha saputo sfruttare nel modo più efficace il paradigma dell'Open Banking promosso dalla PSD2, grazie anche alle scelte delle autorità di settore. La Competition and Markets Authority (CMA) inglese ha infatti stabilito fin da subito l'utilizzo di specifiche tecniche per le API destinate ai servizi di AIS e PIS delle principali banche inglesi, garantendo così piena interoperabilità all'interno del paese.

Prima della Brexit, la maggior parte dei TPP che operavano in Italia erano di nazionalità inglese. Con l'uscita del Regno Unito dall'Europa, il regime del "passaporto" è stato soppresso e i TPP inglesi hanno dovuto stabilire una propria sede in Europa per poter continuare a offrire i propri servizi in Italia. Ciò ha portato ad una redistribuzione del mercato dell'Open Banking europeo, scenario di paesi in costante aggiornamento in termini di innovazione finanziaria.

Purtroppo, l'Italia non è ancora tra questi. L'Open Banking, tramite l'introduzione della PSD2 in Europa, si è diffuso anche in Italia, con banche tradizionali e players non bancari che hanno sviluppato servizi Open Banking più semplici con l'intento di rimanere competitivi. L'ecosistema Open Banking italiano è composto da banche tradizionali, neo-banche e Terze Parti (TPP) come Fintech e provider utility che offrono servizi di pagamento.[12] Tuttavia, solo il 36% delle banche registra alti tassi di utilizzo dell'Internet Banking tra i clienti e la maggior parte di queste dichiara che i servizi Open Banking sono utilizzati da meno del 5% clienti digitali a causa degli investimenti significativi richiesti e delle barriere tecnologiche. Infatti, la maggior parte dei soggetti che offrono i nuovi servizi introdotti con la PSD2 nel nostro paese sono ancora di matrice straniera. Questo dato è particolarmente significativo, dato che questi servizi sono per definizione digitali e fruibili a distanza.

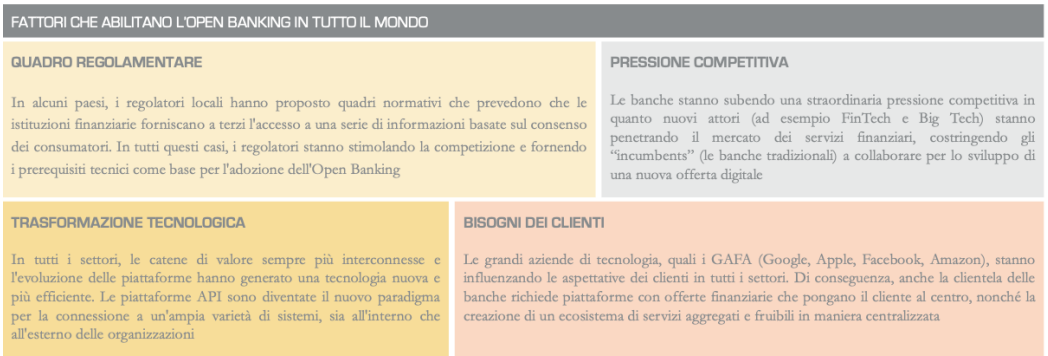
[11] CBI, (2021). *The Global Open Banking Report*
[12] CARDU, L. (2021). *Open Banking: origini e sviluppo all'interno del sistema bancario e finanziario di Italia, Francia e Germania.*

Ricerche dimostrano quindi che l'Open Banking è un fenomeno ormai diffuso a livello globale: a oggi, quasi 60 paesi (da quelli leader come Australia, Regno Unito e Unione Europea a quelli emergenti come Nigeria, Bahrain, Sud Africa) hanno avviato iniziative in ambito Open Banking, sebbene con diversi approcci, modalità e ritmi di adozione.

Con riferimento all'Unione Europea, l'analisi evidenzia che quasi tutti i principali operatori finanziari hanno sviluppato una "proposition" in ambito Open Banking spinti dalla direttiva, partendo da servizi base come AIS e il PIS e, in alcuni casi, arricchendola con servizi a valore aggiunto (VAS). L'offerta Europea si concentra principalmente sui dati di Account Information e Payment Initiation (63%). Tuttavia, inizia ad emergere una nuova categoria di servizi, l'Open Finance, che si basa sui dati riferiti ad investimenti, assicurazioni e dati di prestito (14%).

In Italia, sempre più players stanno dirigendo la loro attenzione verso l'Open Banking, anche se questo fenomeno non è ancora pienamente sfruttato: si prevede che le aziende aumentino gli investimenti nel mercato e intraprendano attività di educazione finanziaria per aumentare la consapevolezza dei clienti nei confronti dell'Open Banking e massimizzare i suoi benefici nei prossimi anni.

Dall'osservazione delle diverse configurazioni dell'Open Banking in tutto il mondo emergono alcuni fattori ricorrenti che favoriscono il suo sviluppo. Questi fattori includono cambiamenti normativi, nuove esigenze dei consumatori, aumento della concorrenza nel mercato dei servizi finanziari e rapido cambiamento tecnologico che sta interessando il mercato dei servizi finanziari (come illustrato nella figura).



[13]

In riferimento agli ecosistemi "Open", i principali attori coinvolti sono:

a) Banche tradizionali: istituzioni finanziarie con sedi fisiche e filiali, autorizzate a ricevere depositi e concedere prestiti, oltre a fornire servizi finanziari come gestione patrimoniale, cambio valuta e cassette di sicurezza.

b) Banche digitali: istituzioni finanziarie che operano esclusivamente online o tramite applicazioni, allontanandosi dal modello basato sulle filiali fisiche.

[13] CBI, (2021). *The Global Open Banking Report*

c) FinTech e fornitori di tecnologia: mirano a migliorare e automatizzare l'esperienza degli utenti nella fruizione dei servizi finanziari, offrendo software e algoritmi per gestire operazioni e processi finanziari.
d) Iniziative collaborative: promuovono l'innovazione nell'ecosistema Open Banking attraverso la condivisione di regole, standard e modelli di business, e garantiscono l'interoperabilità tra tutti gli attori dell'ecosistema.
e) Iniziative di standardizzazione: affrontano tematiche di interazione tra operatori e armonizzazione del settore, definendo standard condivisi per supportare la creazione di un ecosistema bancario aperto.
L'Open Banking sta diventando globale, ma i drivers che guidano l'adozione sono diversi a seconda dei paesi. In Europa e nel Regno Unito, l'adozione è stata spinta dalla PSD2 per aumentare la concorrenza nei servizi finanziari. In Nigeria, l'Open Banking mira a includere la popolazione non "bancarizzata", mentre in Australia è stato innescato da iniziative sulla privacy dei dati. In Bahrain, l'Open Banking e l'Open Data Economy sono considerati strumenti per attirare investimenti stranieri e creare valore nell'economia locale. Una "Open Data Economy", ovvero l'ecosistema economico che si basa sull'utilizzo e la condivisione di dati aperti, ossia dati digitali liberamente accessibili e utilizzabili da chiunque, se ben strutturata potrebbe favorirne l'innovazione.
Paesi come l'Arabia Saudita e il Canada non hanno ancora formalmente lanciato iniziative di Open Banking, mentre l'Australia ha pienamente implementato la regolamentazione dal 2019. Alcuni Paesi procedono a velocità differenti, come il Messico, dove la "FinTech Law" è stata istituita nel 2018 ma non sono stati compiuti ulteriori passi verso l'apertura dei dati, mentre il Brasile ha già sviluppato un framework in ottica Open Finance. Poi ci sono Paesi come l'UE che hanno adottato un approccio pienamente regolamentato, e Paesi come gli USA in cui le iniziative di Open Banking sono generalmente avviate dai principali operatori di mercato; dunque, sono ambientate in un contesto più "privatizzato".
Quanto agli approcci "Open", questi possono essere suddivisi in tre categorie principali: prescrittivo, facilitativo e market-driven.
L'approccio prescrittivo si basa sull'emissione di regole specifiche da parte delle autorità locali per definire il quadro normativo e tecnologico di riferimento. Questo approccio favorisce l'adozione e l'alta sicurezza, ma può limitare la sperimentazione di servizi innovativi e comportare costi elevati di conformità.
L'approccio facilitativo, invece, prevede la pubblicazione di linee guida da parte delle autorità locali per facilitare la collaborazione tra gli operatori del mercato e promuovere l'interoperabilità. Questo approccio può accelerare l'adozione dei modelli "Open" e incoraggiare la collaborazione, ma può anche essere limitato dalla mancanza di standard API condivisi.

Infine, l'approccio market-driven si basa sulla co-creazione di standard di interoperabilità da parte dei principali operatori di mercato, in assenza di regole esplicite o linee guida da parte delle autorità locali. Questo approccio incentiva l'innovazione e la sperimentazione di nuovi servizi, ma dipende fortemente dalla prontezza del mercato e dalla mancanza di standardizzazione per la condivisione dei dati.

Sostanzialmente, ciascuno di questi approcci presenta vantaggi e svantaggi e la scelta dell'approccio migliore dipende dalle caratteristiche specifiche del mercato e degli obiettivi dell'adozione dei modelli "Open".

Offerta Open Banking in UE: banche tradizionali e digitali, FinTech e Tech Providers

La PSD2 ha svolto un ruolo fondamentale nel favorire l'adozione dell'Open Banking in Europa soprattutto per quanto riguarda la riduzione di barriere all'ingresso nel mercato dei fornitori di terze parti e aprendo le porte a nuove opportunità di business.

Grazie alla PSD2, il numero di Account Servicing Payment Service Providers (ASPSP) e di Third Party Provider (TPP) è aumentato notevolmente, con un aumento del 300% delle entità TPP dal 2019. Ciò ha consentito di stimolare la concorrenza e la cooperazione nei servizi finanziari, aprendo la strada a nuove partnership tra aziende del settore.

Inoltre, molte aziende hanno scelto di acquisire società già operanti nel mercato dell'Open Banking per accelerare il processo innovativo e ampliare la propria offerta di prodotti e servizi. Tuttavia, l'Open Banking presenta anche alcune sfide, tra cui la sicurezza dei dati e la privacy dei clienti.

E quindi rappresenta una grande opportunità per le banche e le FinTech per differenziare il proprio business e generare nuovi ricavi, ma richiede anche una forte attenzione alla sicurezza dei dati e alla privacy dei clienti.

Le banche tradizionali e digitali, le FinTech e i Tech Providers sono attori chiave nel settore finanziario e hanno ruoli distinti nel panorama finanziario odierno.

Le banche tradizionali sono istituzioni finanziarie consolidate con una lunga storia nel fornire servizi bancari: sono strettamente regolate da normative specifiche e operano attraverso una rete di filiali fisiche, offrendo una vasta gamma di servizi finanziari, come depositi, prestiti, carte di credito e gestione patrimoniale.[14]

Esistono inoltre le banche digitali che, al contrario delle tradizionali, costituiscono banche operanti principalmente online senza filiali fisiche (come Hype, ad esempio). Sono basate unicamente sulla tecnologia e offrono servizi bancari attraverso applicazioni e piattaforme digitali. Totalmente concentrate sull'efficienza e l'accessibilità, offrono spesso servizi bancari convenienti e innovativi.

Si hanno poi le FinTech (Financial Technology), ossia imprese pionieristiche nell' utilizzo della tecnologia per fornire soluzioni finanziarie; operano in diversi ambiti quali pagamenti digitali, prestiti peer-to-peer, consulenza finanziaria automatizzata e gestione patrimoniale. Sono spesso caratterizzate dalla loro agilità, velocità e capacità di adattarsi rapidamente alle nuove esigenze del mercato.

Infine, i Tech Providers sono aziende tecnologiche che forniscono soluzioni altrettanto tecnologiche, infrastrutture o servizi di supporto alle banche tradizionali, alle banche digitali e alle Fintech. Dispongono di piattaforme di pagamento, sistemi di sicurezza informatica, servizi di cloud computing, analisi dei dati e molto altro. I Tech Providers sono essenziali per l'evoluzione e

[14] Fagnani, R. (2020). *Banche tradizionali, virtuali e pericolo FinTech.*

l'innovazione del settore finanziario, fornendo alle altre aziende strumenti e tecnologie per migliorare i loro servizi.

Sommariamente, quindi, le banche tradizionali e digitali rappresentano gli attori tradizionali del settore bancario, mentre le FinTech e i Tech Providers portano innovazione e soluzioni tecnologiche avanzate. L'interazione tra queste diverse entità sta contribuendo a ridefinire il panorama finanziario, proponendo nuove opportunità e sfide nel mondo dei servizi bancari e finanziari.

E l'Open Banking è esattamente un paradigma che prevede la cooperazione tra questi diversi attori del settore finanziario, insieme a iniziative di Collaborazione ed iniziative di Standardizzazione. Questi attori hanno obiettivi diversi ma condividono la stessa finalità: offrire servizi finanziari sempre migliori e semplici da utilizzare ai loro clienti.

Standard Open Banking: linee guida per l'adozione della PSD2

In sostanza, gli standard Open Banking rappresentano un insieme di linee guida e specifiche tecniche che aiutano le istituzioni finanziarie e le FinTech a progettare e implementare le API. L'obiettivo principale della standardizzazione delle API è quello di definire un insieme comune di standard che facilitino l'integrazione tra gli attori del mercato, promuovano la concorrenza tra i giocatori già presenti e i nuovi entranti, e garantiscano la sicurezza delle transazioni finanziarie.

Gli standard API sono diventati sempre più importanti con la diffusione dell'Open Banking e sono stati adottati da numerose iniziative come la Berlin Group, la Polish API, l'Open Banking UK e la STET. Grazie al lavoro di queste iniziative, le istituzioni finanziarie possono beneficiare di una serie di requisiti riguardanti l'uso e l'implementazione delle API per essere conformi alla PSD2. Ciò facilita l'esperienza degli sviluppatori, accelerando l'innovazione, e consente alle banche di beneficiare di un alto livello di sicurezza e funzionalità.

Il nuovo framework Open Finance si prefigge l'obiettivo di andare oltre l'ambito dei pagamenti e abbracciare l'intero panorama finanziario, consentendo l'integrazione di una vasta gamma di servizi finanziari attraverso le API. In questo modo, Open Finance rappresenta una naturale evoluzione dell'Open Banking e potrebbe aprire nuove opportunità di business per le banche e le FinTech, consentendo loro di offrire servizi più completi e personalizzati ai propri clienti. A tal proposito, Berlin Group ha avviato i lavori per lo sviluppo del framework Open Finance in collaborazione con altri stakeholder del settore finanziario e delle istituzioni europee, al fine di definire standard aperti, comuni e indipendenti per consentire l'interoperatività tra gli attori del mercato. L'obiettivo è di creare un ambiente di innovazione competitiva, garantendo al contempo la protezione dei dati e la sicurezza delle transazioni finanziarie per quanto riguarda gli standard tecnici per la PSD2, anche se forse non quanto alcune si vorrebbe a livello comunitario. Data la natura della Direttiva, è improbabile che alle banche e agli altri attori venga concesso pieno controllo su come implementare la sicurezza, poiché ciò potrebbe inequivocabilmente aprire la strada a varie vulnerabilità. Tuttavia, resta da vedere se ogni aspetto sarà specificato e obbligatorio e quale evoluzione avrà l'applicazione degli standard. [15]

[15] Mansfield-Devine, S. (2016). *Open banking: opportunity and danger. Computer Fraud & Security, 2016(10), 8-13.*

Il futuro dell'Open Banking: quali saranno le opportunità e le sfide

"L'Open Finance rappresenta una grande opportunità per l'industria finanziaria per creare innovazione collaborativa, a vantaggio della clientela Corporate e Retail, anche grazie al lavoro aggregativo di ecosistemi precompetitivi come CBI. Le banche che continueranno a investire in innovazione tecnologica, competenze digitali e sostenibilità saranno le protagoniste della trasformata arena competitiva internazionale"

Liliana Fratini Passi

CBI S.c.p.a. – Direttore Generale

L'Open Finance rappresenta un'opportunità chiave per il futuro del settore finanziario, poiché consente l'accesso ai dati finanziari dei consumatori da parte di terze parti attraverso API. Ciò permette di creare nuovi servizi finanziari, migliorare l'esperienza del cliente e aumentare la concorrenza nel settore finanziario. Le iniziative regolamentari dell'Unione Europea e le iniziative di standardizzazione degli operatori di mercato sono fondamentali per fornire un quadro normativo e tecnologico solido per lo sviluppo dell'Open Finance.

I casi d'uso Open Finance stanno diventando sempre più comuni, con servizi come aggregatori di informazioni sugli investimenti e servizi di "checkout loan" che rappresentano alcune delle soluzioni più innovative. Tuttavia, è importante notare che ci sono ancora molte opportunità inespresse nel settore dell'Open Finance e che è necessario continuare ad innovare e sviluppare nuovi servizi e soluzioni.[16]

Ciò significa che le banche possono fornire servizi di credito, investimenti, assicurazioni, onboarding e certificati, integrando le proprie offerte di Open Banking.

Per sfruttare appieno le opportunità offerte dall'Open Finance, le banche devono investire nella creazione di nuovi ecosistemi pan-europei, che consentano di testare nuovi modelli di business e di

[16] CBI, (2021). *The Global Open Banking Report*

ottenere sinergie per arricchire l'offerta senza aumentare i costi fissi. Inoltre, le banche devono contribuire attivamente ai tavoli regolamentari per partecipare allo sviluppo dell'ecosistema Open Banking e affrontare le decisioni di business chiave.

L'adozione dell'Open Finance richiede anche l'integrazione di competenze necessarie, attraverso partnership e collaborazioni con altre aziende del settore fintech. In questo modo, le banche potrebbero sfruttare appieno le opportunità di business dell'Open Banking e dell'Open Finance, mantenendo sempre un forte contatto umano con i propri clienti retail e corporate. L'Open Finance rappresenta quindi una grande opportunità per le banche, ma richiede un impegno costante nel perseguimento di una trasformazione digitale continua ed efficace.

Per estendere l'adozione di servizi API oltre i pagamenti, è necessario anticipare la trasformazione digitale. Questo richiede un'attenta analisi dei requisiti del mercato e delle esigenze dei clienti, così come la capacità di innovare e adattarsi rapidamente ai cambiamenti del mercato.

Per creare quindi nuovi ecosistemi pan-europei, gli operatori di mercato dovrebbero collaborare con altri attori del mercato, tra cui Fintech, regolatori e altri fornitori di servizi finanziari. Questa collaborazione può aiutare a testare nuovi modelli di business, come il “Banking-as-a-Service” (BaaS) e accelerare il Time to Market.

Per sfruttare appieno le opportunità di business dell'Open Banking è necessario integrare le competenze necessarie. Gli operatori di mercato dovrebbero considerare quindi affiliazioni con Fintech, startup e altre organizzazioni per acquisire le competenze tecniche e di business necessarie per innovare e sviluppare soluzioni Open Finance.

Capitolo 3 - Cybersecurity nei pagamenti

Sfide della cyber-sicurezza e strumenti per implementarne la strategia ed efficacia

Tema detenente ruolo fondamentale della direttiva è, come si può intuire dai paragrafi prcedenti, la cybersicurezza, che prospetta nel corso dei prossimi mesi ed anni numerose ed impegnative sfide con lo scopo di aumentare la propria funzionalità e rendimento.

Viene presentata il 25 maggio 2022 la Strategia nazionale di Cybersicurezza 2022-2026 predisposta dalla ACN, nonché Agenzia Cybersicurezza Nazionale, la quale propone ben 82 misure utili ad agevolare una più proficua collaborazione fra pubblico e privato, sovvenzionata altresì da finanziamenti, incentivi, agevolazioni e sgravi fiscali.

Le parole del Presidente Draghi a tal proposito: "…anche tenuto conto dell'elevata qualità e dei massicci investimenti realizzati dai principali alleati e partner internazionali. È dunque necessaria una puntuale rivisitazione nella concezione e nella visione strategica dell'architettura nazionale di cybersicurezza. […] Per realizzare questa nuova visione, l'Italia ha costruito un ecosistema di cybersicurezza fondato sulla collaborazione tra i settori pubblico e privato. Al contributo delle istituzioni, si affianca quello attivo degli operatori economici - in particolare dei gestori delle infrastrutture da cui dipende l'erogazione dei servizi essenziali dello Stato - del mondo dell'università e della ricerca e della società civile. Tutti devono farsi parte attiva nel proteggere i propri assetti informatici, nel rispetto delle norme riconosciute a livello internazionale. I produttori e fornitori di beni e servizi ICT svolgono un ruolo di primo piano. A loro è richiesto di fornire prodotti e soluzioni tecnologiche che soddisfino adeguati requisiti di cybersicurezza. L'obiettivo è rafforzare la resilienza di dispositivi e apparati ICT, a partire dal 5G e dal cloud, anche al fine di aumentare la fiducia dei cittadini.

È nostra intenzione intensificare i progetti di sviluppo tecnologico per arrivare a disporre di un adeguato livello di autonomia strategica nel settore e quindi garantire la nostra sovranità digitale. Per farlo, sarà cruciale stanziare fondi adeguati, con continuità."

Come ben si può constatare nella vita di tutti i giorni, l'avvento tecnologico e la velocità supersonica con cui avviene la sua stessa evoluzione, oltre a progresso, cambiamenti in positivo, porta anche a innumerevoli rischi che col tempo aumenteranno in maniera esponenziale a pari passo con l'avanzare della tecnologia.[17]

La transizione digitale del sistema Paese, tra cui gli attacchi cyber, la dipendenza dalle tecnologie sviluppate da grandi aziende controllate dai governi, e la diffusione di fake news e disinformazione online, rientrano fra questi. Questi rischi possono avere conseguenze significative sull'erogazione dei

[17] ACN. (2019). *Strategia Nazionale per la Sicurezza Cibernetica 2019.*

servizi essenziali di un Paese, sul suo PIL e sulla sua reputazione. La strategia proposta mira a rafforzare la resilienza del sistema Paese attraverso un uso sicuro delle tecnologie, l'autonomia strategica nella dimensione cibernetica, l'anticipazione dell'evoluzione delle minacce cyber, la gestione delle crisi cibernetiche e il contrasto della disinformazione online, nel rispetto dei diritti umani, dei valori e dei principi fondamentali.

Conseguentemente e in concomitanza a questi rischi, esistono quindi delle sfide che la politica deve affrontare.

Tra queste si ritrovano temi come assicurare una transizione digitale cyber resiliente della Pubblica Amministrazione e del tessuto produttivo, vale a dire un adeguato scudo protettivo per attacchi e incidenti virtuali, fondamentali per la corretta e fluente fruibilità dei servizi da parte del cittadino. In tal modo potrà usufruirne in maniera fiduciosa e consapevole. [18]

A ciò si aggiunge la questione di genere, poiché le donne ad intraprendere studi informatici e simili costituiscono un numero meramente esiguo, ancora meno coloro che si specializzano in cybersecurity.

Altra importante sfida risiede nel trovare autonomia strategica nazionale nel settore digitale, in ragione del fatto che l'Italia è fra quei paesi che dipendono ancora da sistemi tecnologici di altre nazioni. Ovviamente questo la rende meno monitorante su quelli che sono i dati trasmessi ed elaborati: più si è indipendenti tecnologicamente dalle altre nazioni più sarà possibile attuare politiche di sovranità delle informazioni.

Ancora, è importante puntare su strategie di difesa attiva quanto ad attacchi cibernetici: occorre anticipare la minaccia cibernetica e cercare di prevederla nel miglior modo disponibile e attutirne quanto più possibile i dannosi impatti che può provocare.

Sarà anche importante imparare a gestire in maniera quanto più efficiente le crisi cibernetiche, e dunque è richiesta una continuativa coordinazione fra tutti i soggetti pubblici e privati interessati e prontezza nel fornire un set preimpostato di misure nel momento in cui una crisi cibernetica dovesse sopraggiungere.

Ultima sfida (ma non per importanza) che la cybersicurezza nazionale dovrà fronteggiare sarà contrastare la disinformazione online: principale obiettivo di quest'ultima è condizionare quello che sarebbe lo spontaneo esercizio delle libertà fondamentali, specialmente a ridosso di momenti politicamente importanti: in questi frangenti la disinformazione online è una minaccia che ha necessità di essere combattuta proprio affinché il singolo possa esercitare i suoi diritti fondamentali senza essere influenzato da nozioni non veritiere e che possano falsare le sue decisioni in ambito di

[18] ACN. (2019). *Strategia Nazionale per la Sicurezza Cibernetica 2019.*

scelte politiche, e quindi su larga scala su quelle che poi dovrebbero essere le scelte dei governi nazionali e comunitari.

Dato il consistente numero di sfide che la cybersicurezza nazionale si propone di affrontare, è necessario, al fine di vincerle, implementare e migliorare quella che è la strategia da applicare: per far ciò è opportuno un programma di investimenti e leve finanziarie, già previsto e stilato dall'Agenzia per la Cybersicurezza Nazionale (nonché ACN).

Con lo scopo di rendere più efficace la strategia di cybersicurezza nazionale, si prevede di stanziare dei fondi nazionali. Queste sovvenzioni saranno rivolte a progetti che mirano al raggiungimento dell'indipendenza tecnologica di cui sopra si è trattato ed altresì ad aumentare i livelli di cybersicurezza nazionali.

Saranno altrettanto stanziati finanziamenti dei programmi Orizzonte Europa ed Europa Digitale: il primo volto a rendere più facile la collaborazione e al rafforzamento dell'influenza che ricerca e innovazione possono avere nello sviluppo delle politiche UE, sostenendo inoltre una maggiore diffusione di tecnologie di eccellenza oltre che creazione di nuovi posti idi lavoro, competitività industriale e crescita economica. Europa Digitale mira invece a rendere i cittadini più consapevoli e competenti nell'ambito tecnologico, così da rendere più veloce la ripresa economica; il programma finanzia progetti in settori come intelligenza artificiale, cybersicurezza, uso diffuso delle tecnologie digitali nell'economia, nella società e ulteriori grandi campi.

Ultimo strumento per l'implementazione cibernetica nazionale, non per rilevanza, il PNRR.

Questo programma, di importanza cruciale nello scenario socio-economico-politico italiano, mira nell'ambito tecnologico ad una maggiore digitalizzazione dei processi e dei servizi per i cittadini. Il PNRR prevede uno stanziamento di 623 milioni di euro in progetti volti allo sviluppo di servizi all'avanguardia per la gestione del rischio cyber: l'Italia è la prima nazione a beneficiare del programma Next Generation EU, il quale fornirà il Dispositivo per la ripresa e resilienza (RRF) e REACT-EU. Il primo vede la presentazione di un pacchetto di investimenti e riforme: in Italia rientra il PNRR che si articola in 6 missioni differenti tra cui digitalizzazione, innovazione, competitività. L'intento è il raggiungimento di un'autonomia tecnologica nazionale, che vede come principi fondamentali della trasformazione digitale della PA sia cybersicurezza che resilienza.

Il piano di attuazione vede coinvolti nell'intervento i più importanti attori nazionali della cybersicurezza, nel pubblico e nel privato: servizi cyber nazionali, interventi di potenziamento della resilienza cyber per la PA e laboratori di scrutinio per la certificazione tecnologica.[19]

[19] ACN. (2019). *Strategia Nazionale per la Sicurezza Cibernetica 2019.*

Principali obiettivi della strategia: protezione, risposta e sviluppo. Il piano di implementazione

Per affrontare al meglio queste sfide, l'ACN si pone tre obiettivi da raggiungere: protezione, risposta e sviluppo.

La protezione degli asset strategici nazionali richiede un approccio sistemico per gestire e ridurre il rischio. Ciò comprende la definizione di norme e l'adozione di misure, strumenti e controlli per consentire al Paese di effettuare una transizione digitale resiliente. È importante sviluppare strategie e iniziative per verificare e valutare la sicurezza delle infrastrutture ICT, inclusi gli aspetti di approvvigionamento e supply-chain con impatto nazionale.

Affinché il livello di protezione risulti efficace e perduri nel tempo l'ACN propone sette diverse misure da adottare: il potenziamento delle capacità del Centro di Valutazione e Certificazione Nazionale (CVCN) dell'Agenzia per la Cybersicurezza Nazionale e, negli ambiti di competenza, dei Centri di Valutazione (CV) del Ministero dell'Interno e della Difesa, la definizione ed il mantenimento di un quadro giuridico nazionale aggiornato e coerente in materia di cybersicurezza, la conoscenza approfondita del quadro della minaccia cibernetica, il potenziamento del livello di maturità delle capacità cyber della Pubblica Amministrazione, lo sviluppo di capacità di protezione per le infrastrutture nazionali, la promozione dell'uso della crittografia come strumento di cybersicurezza e l'implementazione di un'azione di coordinamento nazionale, coerente con le iniziative adottate a livello europeo e in sinergia con i Paesi affini.

Quanto all'obiettivo risposta, per affrontare le minacce cibernetiche a livello nazionale, è necessario coinvolgere tutti gli attori dell'ecosistema di cybersicurezza e utilizzare capacità di monitoraggio, rilevamento, analisi e risposta a livello nazionale. Una risposta tempestiva ed efficace richiede anche un sistema di gestione delle crisi cibernetiche nazionale e transnazionale, l'integrazione dei servizi cyber nazionali in diversi ambiti, esercitazioni periodiche di sicurezza cibernetica e resilienza, la definizione di una procedura nazionale per l'attribuzione di attività cibernetiche ostili, il contrasto al cybercrime e il rafforzamento delle capacità di deterrenza cibernetica.

E in ultima istanza, uno sviluppo consapevole e sicuro delle tecnologie digitali e della competitività industriale è fondamentale per la nazione. La ricerca e l'innovazione tecnologica sono patrimoni essenziali per l'Italia, con importanti potenzialità di espansione. Negli ultimi anni, sono stati avviati numerosi strumenti e iniziative per supportare lo sviluppo delle capacità del sistema nazionale di ricerca, la trasformazione digitale e l'innovazione tecnologica, come il PNRR, le leggi di bilancio e il Piano Nazionale Impresa 4.0.

Per accrescere ulteriormente questo impegno, è necessario sviluppare il ruolo del Centro Nazionale di Coordinamento (NCC) e del Centro europeo di competenza per la cybersicurezza nell'ambito industriale, tecnologico e della ricerca (ECCC), supportando lo sviluppo e il potenziamento

dell'autonomia strategico-tecnologica e digitale dell'Unione europea e dell'Italia, riducendo la dipendenza da tecnologie extra-UE. È inoltre fondamentale realizzare un "parco nazionale della cybersicurezza", che metta a sistema competenze e risorse per fornire le infrastrutture tecnologiche necessarie per la ricerca e lo sviluppo nella cybersecurity e nelle tecnologie digitali. Sarà necessario, inoltre, introdurre nuovi meccanismi e soluzioni incentivanti per supportare il continuo sviluppo industriale, tecnologico e della ricerca, e continuare a promuovere l'innovazione tecnologica e la digitalizzazione della Pubblica Amministrazione e del tessuto produttivo del Paese. [20]

[20] ACN. (2019). *Strategia Nazionale per la Sicurezza Cibernetica 2019.*

Ciò che rende più sicuri i pagamenti, norme che proteggono i soggetti deboli e soluzioni proposte dalla resilienza: finalità e nuovi obblighi del regolamento DORA

Il 16 dicembre 2020, la Commissione Europea e l'Alto Rappresentante dell'Unione per gli affari esteri e la politica di sicurezza hanno presentato la Strategia Europea sulla Cybersecurity, che è una componente chiave del piano europeo di transizione digitale, del recovery plan e della strategia europea sulla sicurezza. L'obiettivo principale della strategia è migliorare la prevenzione, la resilienza e le capacità di risposta agli incidenti nel campo della cybersecurity per enti pubblici e privati, autorità competenti e l'Unione nel suo complesso. La strategia prevede due proposte legislative: la revisione della Direttiva NIS, conosciuta come "NIS 2.0", e una nuova Direttiva sulla resilienza delle Entità Critiche. Queste azioni dimostrano l'importanza crescente delle questioni di cybersecurity nell'agenda comunitaria. La strategia si basa su tre settori di intervento: resilienza, sviluppo delle capacità operative e promozione di un ciberspazio globale e aperto. Tra le iniziative strategiche vi è la riforma della Direttiva NIS, il miglioramento della cybersecurity dei prodotti connessi, l'adeguamento degli obblighi di sicurezza e di notifica degli incidenti per gli operatori di servizi essenziali e i fornitori di servizi digitali.

La proposta per la revisione della direttiva NIS introduce diverse modifiche: modifica l'ambito di applicazione distinguendo tra soggetti essenziali e soggetti importanti. Introduce anche un quadro normativo per la divulgazione delle vulnerabilità e istituisce un registro europeo delle stesse. Rafforza la cooperazione attraverso la creazione di una rete europea per le crisi informatiche (EU-CyCLONe) e promuove la condivisione delle informazioni tra i soggetti NIS.

La proposta prevede anche nuovi obblighi per la gestione e la segnalazione dei rischi di cybersecurity, inclusi requisiti di base per le misure tecniche e organizzative di gestione del rischio. Inoltre, stabilisce l'obbligo di notifica delle minacce informatiche significative da parte dei soggetti NIS.

Complessivamente, la proposta mira dunque a migliorare la protezione della cybersecurity, promuovere la cooperazione pubblico-privato e facilitare lo scambio di informazioni per affrontare le sfide attuali e future. [21]

Ricollegandosi invece al discorso resilienza, è importante citare il Digital Operational Resiliance Act, nonché acronimo di DORA. Il 24 settembre 2020 la Commissione Europea presenta il pacchetto sulla finanza digitale, in cui è presente la proposta di una strategia di regolamento sulla resilienza operativa digitale. Il 21 novembre 2021 il Consiglio d'Europa ha adottato la sua posizione sul Regolamento ed è stata poi emanata la bozza definitiva il 28 giugno del 2022. Si ipotizza che questi venga emanato

[21] Brighi, R., & Chiara, P. G. (2021). *La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto UE. Federalismi. it, 21, 18-42.*

entro il 2023 e che sia applicabile 24 mesi dopo la pubblicazione in GUCE (Gazzetta Ufficiale delle Comunità Europee).

Ma entrando nel vivo del regolamento: quali gli obiettivi che si pone? DORA mira a creare un quadro normativo sulla resilienza operativa digitale grazie a cui tutte le imprese (fra cui bancarie, finanziarie, assicurative) garantiscono di poter far fronte a tutti i tipi di malfunzionamenti e minacce connessi alle TIC (Tecnologie dell'Informazione e della Comunicazione), al fine di prevenire e mitigare le minacce informatiche.[22]

Per "Resistenza Operativa Digitale" si intende la capacità dell'entità finanziaria di creare, assicurare e riesaminare la propria integrità operativa da un punto di vista tecnologico, garantendo, direttamente o indirettamente, tramite il ricorso ai servizi offerti da fornitori terzi di TIC (fornitori terzi di "Tecnologie dell'informazione e della comunicazione", un'impresa che fornisce servizi digitali e di dati, compresi i fornitori di servizi di cloud computing, software, servizi di analisi dei dati e centri di dati, esclusi i fornitori di componenti hardware e le Telco, nonché le società di telecomunicazioni), l'intera gamma delle capacità connesse alle TIC necessarie per garantire la sicurezza delle reti e dei sistemi informativi impiegati dall'entità finanziaria, su cui si fondano la costante offerta dei servizi finanziari e la loro qualità.

In sintesi si potrebbero racchiudere le finalità del regolamento e ciò che cambierà attraverso la sua emanazione partendo innanzitutto dalla premessa che DORA mira a stabilire una base molto più chiara affinché i regolatori finanziari e le autorità di vigilanza dell'UE possano assicurare che le imprese rimangano finanziariamente resilienti (e quindi siano solide) e che siano in grado di mantenere le operazioni durante una grave interruzione operativa, che siano dunque capaci di rispondere finanziariamente agli eventi sfavorevoli.

Si può per sommi capi riassumere il contenuto del regolamento in 4 aspetti fondamentali:

regolamentare i fornitori terzi di servizi TIC critici (CTPP) e i fornitori di servizi cloud (CSP), includendoli nel perimetro normativo. Le autorità di vigilanza europee (ESA) avrebbero il compito di monitorare questi fornitori, richiedere informazioni, effettuare ispezioni e sanzionare in caso di violazioni.

Standardizzare le regole locali per i test di resilienza operativa digitale in tutta l'UE, garantendo una maggiore coerenza e uniformità delle pratiche tra gli Stati membri.

Armonizzare le regole di gestione del rischio ICT nel settore dei servizi finanziari, utilizzando come riferimento le linee guida esistenti per garantire una maggiore efficienza e uniformità delle prassi.

[22] Parlamento Europeo. (2021). *Digital Operational Resilience Act (DORA).*

Armonizzare la classificazione e la segnalazione degli incidenti e promuovere la creazione di un unico hub dell'UE per la segnalazione degli incidenti più gravi da parte degli istituti finanziari.[23]

DORA simboleggia una grande novità nell'ambito digitale: il Regolatore ha interesse nel normare punti prima non inclusi come Resilienza tecnologica e il rafforzamento della supervisione e del controllo degli outsourcing tecnologici; insieme a quest'ultimo il comparto finanziario si appresta a implementare importanti riforme volte a rafforzare i presidi di sicurezza tecnica e di governo societario. In particolare, sarà introdotto un regime europeo di sorveglianza diretta sui fornitori critici di servizi informatici e di telecomunicazione al fine di garantire un elevato livello di sicurezza dei dati e di ridurre i rischi di incidenti informatici. Tale iniziativa rappresenta un importante passo avanti verso l'armonizzazione dei presidi di sicurezza tecnica e di governance nel comparto finanziario, offrendo maggiore tutela ai clienti e alle istituzioni finanziarie.

Inoltre, DORA copre entità finanziarie tradizionali come istituti di credito, borse, gestori di fondi, compagnie di assicurazione, istituti di pagamento e moneta elettronica, nonché fornitori di servizi di criptovaluta, emittenti di cripto-asset ed emittenti di token.

Quanto alla sua struttura, il regolamento prevede 9 capi e 56 articoli. Gli obblighi che stabilisce in merito a sicurezza delle reti e sistemi informativi sono svariati, e mirano a raggiungere un alto livello di resilienza operativa digitale.

Fra questi si trovano obblighi applicabili alle entità finanziarie in materia di gestione dei rischi delle tecnologie dell'informazione e della comunicazione, segnalazione alle autorità competenti degli incidenti gravi connessi alle TIC, test di resilienza operativa digitale, condivisione di dati e di informazioni in relazione alle vulnerabilità e alle minacce informatiche, misure relative a una solida gestione da parte delle entità finanziarie e infine dei rischi relativi alle TIC derivanti da terzi.

Sono altresì presenti obblighi relativi ad accordi contrattuali stipulati fra fornitori terzi di servizi di TIC, un quadro di sorveglianza per questi ultimi allorché forniscano i loro servizi a entità finanziarie e norme sulla cooperazione tra autorità competenti e norme sulla vigilanza e ancora, l'applicazione da parte delle autorità competenti in relazione a tutte le questioni trattate dal presente regolamento.[24]

Delineato il quadro generale che illustra il contenuto del Regolamento di cui si è trattato, che incarna le vere e proprie fondamenta della sicurezza cibernetica quanto a pagamenti online, è altrettanto rilevante definire quali sono effettivamente gli elementi che garantiscano il più possibile la sicurezza dei pagamenti digitali.

[23] Parlamento Europeo. (2021). *Digital Operational Resilience Act (DORA).*
[24] Parlamento Europeo. (2021). *Digital Operational Resilience Act (DORA).*

Anzitutto è opportuno riportare che negli ultimi decenni la maggior parte delle banche ha spostato gran parte della loro clientela su canali digitali ed in particolar modo la pandemia ha fatto sì che si intensificasse il bisogno di strutture bancarie sempre più digitalizzate.
E quindi, quali sono le tecnologie che rendono possibile lo sviluppo di processi di sicurezza delle banche e cosa ha in serbo il futuro circa fruibilità e sicurezza?
La normativa europea delega l'istituzione di regole specifiche sulla sicurezza a un'autorità tecnica, la European Banking Authority. Il sistema adotta un regime di responsabilità a favore del consumatore, che viene protetto salvo in caso di dolo o colpa grave.
Circa le principali misure di sicurezza previste, si potrebbe partire dalla tokenizzazione: quest'ultima è una tecnologia che protegge i dati sensibili delle carte di credito sostituendoli con un token generato algoritmicamente. Ciò rende i pagamenti più sicuri e convenienti per i clienti, poiché non devono inserire continuamente i dettagli della carta. O ancora, l'autenticazione biometrica e il codice OTP: la prima è un metodo che utilizza caratteristiche biologiche uniche come impronte digitali, voce o riconoscimento facciale per verificare l'identità dell'utente. Il secondo è acronimo di "One-Time Password" o "Password monouso", ossia un codice numerico o alfanumerico generato in tempo reale e utilizzato per autenticare l'identità di un utente durante un accesso o una transazione online, valido per un'unica volta ed avente durata limitata nel tempo. Queste tecnologie di recente divulgazione hanno vantaggi e svantaggi e sono utilizzate come misure di sicurezza ovviamente aggiuntive per proteggere i dati dei clienti.
Inoltre, si ha altresì l'autenticazione basata su certificato: questo tipo di verifica utilizza un certificato digitale per identificare un utente o un dispositivo prima di concedere l'accesso a un'applicazione o a una rete. Questa tecnica di autenticazione è combinata con metodi di verifica tradizionali come l'immissione di una password o di un PIN. I vantaggi includono l'autenticazione reciproca e l'assenza di hardware aggiuntivo, mentre gli svantaggi sono la necessità di conoscenze tecniche e la vulnerabilità a eventuali attacchi.
La parola d'ordine, più comunemente denominata "password", è un'altra delle diverse modalità per garantire quanto più possibile la sicurezza nel processo di pagamento: rimane il metodo più consueto per certificare l'identità del soggetto pagante e richiede l'inserimento di un nome utente e di un codice univoco per accedere all'applicazione fungente da intermediario per il pagamento (esempio: Paypal, Satispay, Hype) nel momento in cui si voglia effettuare un pagamento online. Le aziende cercano di prevenire l'uso di password facili da indovinare, mentre l'autenticazione a due fattori richiede un secondo codice casuale. I vantaggi delle password includono la loro semplicità ed economicità,

mentre gli svantaggi includono la vulnerabilità a eventuali violazioni dei server contenenti le informazioni di accesso e la possibilità di smarrirle o dimenticarle.[25]

Ciò di cui sopra si è trattato si riferisce inequivocabilmente alla pratica, ed è bene anche indicare quello che dal punto di vista normativo tutela e protegge i soggetti deboli nell'istante pratico di pagamento e non solo: anche qualora dovesse sopraggiungere una minaccia cibernetica che pone il soggetto debole a rischio, in quanto il mondo finanziario è continuamente esposto a pericoli informatici di svariate tipologie.

Grande importanza è costituita dalla difesa proattiva delle entità finanziarie nel contesto delle minacce, attraverso la realizzazione di penetration test avanzati commisurati ai rischi specifici di ciascuna entità. A livello europeo, la metodologia TIBER-EU costituisce il modello di riferimento per la conduzione di tali test. In Italia, il TIBER-IT si rivolge a diverse tipologie di entità finanziarie che possono sottoporsi al test su base volontaria, mantenendo la responsabilità della gestione dei rischi correlati. La Guida nazionale TIBER-IT definisce la metodologia, le fasi e i ruoli dei diversi attori coinvolti nella conduzione dei test.[26]

Anche temi come cancellazione dei dati e TIA, ossia "Transfer Impact Analysis", ricevono una significativa regolamentazione al fine di proteggere i soggetti deboli: dopo la sentenza Schrems II, i soggetti che trasferiscono dati fuori dall'UE/SEE devono verificare se la legge o la prassi del paese di destinazione offre gli stessi livelli di garanzia dei diritti offerti dal GDPR. Se ciò non è verificato, gli esportatori devono adottare misure supplementari per garantire un livello di protezione equivalente allo standard dell'UE. Tuttavia, le clausole contrattuali standard e le norme vincolanti d'impresa potrebbero non essere sufficienti a legittimare il trasferimento verso i principali Big Player come Amazon, Google, Microsoft e Facebook, a causa dell'accesso privilegiato alle agenzie di sicurezza americane ai dati di tali società. Anche le consociate europee delle società statunitensi sarebbero soggette alle leggi degli Stati Uniti, il che renderebbe difficile il trasferimento di dati verso queste società. Gli esportatori di dati devono quindi effettuare e dimostrare di aver effettuato una valutazione circa l'effettiva capacità delle misure di sicurezza adottate di garantire il rispetto dei diritti equivalente a quello offerto dal GDPR. Si prevede quindi di strutturare uno schema di Transfer Impact Analysis (TIA) per dimostrare di aver valutato l'adeguatezza delle misure adottate, in particolare per i principali contratti di attività esternalizzate e/o in cloud con Microsoft, Amazon Web Services e Google Analytics. Questo schema deve essere realizzato nel rispetto dei principi di accountability e di risk based approach.

[25] PagamentiDigitali.it. (2021). *Come garantire la sicurezza dei pagamenti digitali*

[26] Banca d'Italia, Consob, IVASS (2019). *Guida nazionale TIBER-IT - Test di penetrazione avanzati per entità finanziarie italiane*

Quanto a trattenimento e alla cancellazione dei dati, normativa che tratta la questione in analisi è il GDPR, già menzionato precedentemente: il "General Data Protection Regulation" è, come si può evincere dalla denominazione, un regolamento circa la protezione delle generalità e i dati degli utenti. Nello specifico, recita: "… *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"*; vale a dire che ogni dato personale di ciascun utente ha una propria "scadenza", sopraggiunta la quale il dato deve tassativamente essere eliminato.

Alcune fattispecie prevedono tempi stabiliti da leggi o obblighi contrattuali, anche convenzionali. Tuttavia, è inderogabile che il tempo di detenzione dei dati debba sempre essere limitato e proporzionale allo scopo medesimo.[27]

[27] Regolamento Europeo n. 679/2016. (2016). *Regolamento generale sulla protezione dei dati (GDPR).*

Capitolo 4: Investimenti, acquisti e nuove Tecnologie dell'Informazione e della Comunicazione

Definizione di ICT ed il loro ruolo negli investimenti per la crescita economica

Il modello di ICT si sta stabilendo nel contesto socio-giuridico attuale da vent'anni all'incirca[28]: le tre lettere sintetizzano l'acronimo di "Information and Communication Technology". Si riferisce all'insieme di tecnologie e strumenti che consentono di elaborare, trasmettere e ricevere informazioni attraverso sistemi di telecomunicazioni. Queste tecnologie includono l'hardware, il software e le reti di comunicazione, nonché tutte le applicazioni e i servizi connessi alla gestione e alla diffusione delle informazioni.[29]

È noto al giorno d'oggi come le ICT costituiscano parte integrante della quotidianità di ognuno e del tessuto sociale delle economie sviluppate, tant'è che non si riuscirebbe ad immaginare una società moderna priva di queste.

Queste tecnologie portano di giorno in giorno a rapidi e al contempo profondi cambiamenti nei paesi sviluppati dal punto di vista economico, condizionando ed incidendo sulla produzione di beni e servizi, sistemi produttivi, infrastrutture ed organizzazione aziendale.

Ingente utilizzo delle tecnologie ICT è oramai effettuato anche dalla PA stessa, oltre che dai cittadini, per l'erogazione di servizi sempre più tempestivi ed economici, quest'ultimo motivo fondamentale del grande incremento di utilizzo delle stesse negli ultimi tempi.

Le imprese, invece, utilizzano le ICT per le loro attività produttive, rendendo in tal modo i processi più efficienti ed offrendo prodotti di volta sempre più innovativi.

Si può dunque affermare che queste tecnologie creino nuova domanda, nuovi mercati e ancora, nuovi settori produttivi, costituendo un motore propulsivo per lo sviluppo economico grazie alla loro elevata pervasività e alla loro capacità di consentire processi produttivi immediati e funzionali.

È incontestabile che ICT ed internet rappresentino un'infrastruttura economica di grande rilevanza e che, oltre ad indurre forte innovazione di prodotto e quindi forti cambiamenti strutturali in svariati settori economici, anche maggiore efficienza nella produzione dei prodotti stessi e dei servizi, dunque delle stesse prestazioni aziendali.

Gli investimenti in ICT rendono oggi il mercato più competitivo (la logica è la seguente: più investo in nuove tecnologie dell'informazione, più i miei canali di distribuzione e comunicazione saranno migliori rispetto a quelli degli altri, più mi affermo sul mercato e più si alzano le probabilità di essere dominante in quest'ultimo) oltre che produttivo. Tra questi, per fare un esempio, si annoverano

[28] Capello, R., & Spairani, A. (2003). *Apprendimento collettivo, ICTs e performance delle PMI. Economia e politica industriale, (2003/118).*

[29] Agenzia per l'Italia Digitale (AGID). (s.f.). *Cosa sono le tecnologie dell'informazione e della comunicazione (ICT)*

investimenti di grande successo come le AI (Artificial Intelligence) o ancora, le criptovalute: il primo elemento riguarda un campo di studio e ricerca che si concentra sullo sviluppo di sistemi e algoritmi in grado di imitare o simulare l'intelligenza umana. L'obiettivo dell'AI è quello di consentire alle macchine di apprendere, ragionare, comprendere e prendere decisioni in modo autonomo, simile a come farebbe un essere umano. È ormai una componente della tecnologia utilizzata in molteplicità di settori come, ad esempio ed estremamente rilevante nel caso in trattazione, l'automazione dei processi. Quanto alle seconde, infine, si tratta di una forma di valuta digitale che utilizza la crittografia per garantire transazioni sicure e controllare la creazione di nuove unità. La criptovaluta più famosa è il Bitcoin, ma ne esistono molte altre, come Ethereum, Ripple e Litecoin. Si basano sul cd. blockchain, una tecnologia che registra in modo sicuro tutte le transazioni effettuate rendendole sicure, caratterizzate da anonimato e tracciabilità, entrambi valori di cui si fa portatrice la PSD2. Entrambi i settori presentano vantaggi e sfide uniche, si identificano come attori principali del cambiamento delle modalità con cui ci si approccia alla tecnologia e al denaro e si rileva abbiano un impatto che continua a crescere in modo esponenziale sulla società. L'intelligenza artificiale offre la promessa di migliorare l'efficienza, l'automazione e la previsione dei processi, ma solleva anche preoccupazioni riguardo all'automazione del lavoro e alla sicurezza dei dati. Le criptovalute offrono la possibilità di una maggiore libertà finanziaria e di transazioni sicure, ma sono soggette a volatilità di prezzo e a questioni regolamentari.

Rispostando il focus sulle ICT nel generale, alcune politiche di promozione delle infrastrutture delle comunicazioni o di promozione della domanda ICT possono avere effetti positivi sull'economia a diversi livelli. Infatti, quando vengono implementate correttamente, queste politiche possono stimolare la crescita economica, generare nuove opportunità di lavoro, aumentare la disponibilità di capitale e risorse imprenditoriali e migliorare la qualità della vita delle persone.[30]

La diffusione sempre più ampia delle tecnologie dell'informazione e della comunicazione rappresenta uno dei fattori trainanti per la crescita economica a livello globale. Grazie alla sua pervasività, l'ICT stimola la domanda di prodotti e servizi non solo all'interno del proprio settore, ma anche in altri settori dell'economia. Questo perché la produzione di beni e servizi ICT richiede input e collaborazioni con settori che non appartengono all'ambito delle tecnologie dell'informazione e della comunicazione. L'aumento della domanda di ICT, quindi, genera un effetto moltiplicatore sulla produzione di altri settori dell'economia, creando opportunità di crescita e sviluppo in diversi ambiti produttivi. Attualmente e negli ultimi anni, quindi, l'aumento degli investimenti in ICT genera un circolo virtuoso che alimenta la produzione e stimola la crescita economica, grazie agli effetti diretti

[30] Di Carlo, C., & Santarelli, E. (2011). *Il ruolo dell'ICT nella crescita economica in Italia. Mondo digitale, 37, 3-8.*

e indiretti prodotti dalle ICT stesse. In questo modo, viene logico supporre che le ICT abbiano un effetto moltiplicativo sulla crescita economica.[31]

[31] Di Carlo, C., & Santarelli, E. (2011). *Il ruolo dell'ICT nella crescita economica in Italia. Mondo digitale, 37, 3-8.*

Identità digitale del consumatore e virtualizzazione delle relazioni tra le controparti del rapporto economico-giuridico

Il nuovo concetto dell'identità digitale emerge a partire dal nuovo regolamento dell'Unione Europea GDPR[32]: l'identità digitale del consumatore e la virtualizzazione delle relazioni tra le controparti del rapporto economico-giuridico sono concetti che rivestono un ruolo sempre più importante nella società digitale odierna: l'identità digitale del consumatore si riferisce all'insieme di informazioni e attributi che identificano un individuo in contesti digitali. Mentre nell'era predigitale l'identità veniva principalmente stabilita attraverso documenti cartacei e riconoscimento facciale, l'avvento della tecnologia ha portato a una crescente necessità di gestire e verificare l'identità online. L'identità digitale può includere informazioni come il nome, l'indirizzo, la data di nascita, i dati finanziari e altre caratteristiche che permettono di riconoscere un individuo e consentono l'accesso a servizi online e transazioni.

La virtualizzazione delle relazioni economico-giuridiche, d'altra parte, riguarda il processo di trasformazione delle interazioni e delle transazioni tra le parti coinvolte in un rapporto economico o giuridico in contesti digitali. Ciò implica l'utilizzo di tecnologie digitali e piattaforme online per facilitare e gestire queste relazioni. Ad esempio, anziché firmare documenti cartacei o incontrarsi di persona, le parti coinvolte in una transazione possono scambiarsi informazioni e accordi tramite piattaforme digitali sicure. La virtualizzazione delle relazioni consente una maggiore flessibilità, rapidità ed efficienza nei processi commerciali e giuridici.

Questi concetti sono strettamente legati all'evoluzione delle tecnologie digitali e alla crescente adozione di strumenti online. L'identità digitale del consumatore e la virtualizzazione delle relazioni economico-giuridiche sono importanti per promuovere la fiducia, la sicurezza e l'efficienza negli ambienti digitali. Allo stesso tempo, sollevano questioni di sicurezza, protezione dei dati e privacy che richiedono attenzione e regolamentazione opportune.

Sviluppare e gestire un'identità digitale sicura e affidabile, insieme alla virtualizzazione delle relazioni economico-giuridiche, rappresenta una sfida significativa ma necessaria nella società digitale.

Il periodo pandemico vissuto dal 2020 sino a tempi recenti rientra a suo modo nel novero delle risposte adattative dalle relazioni fisiche, reali fra esseri umani e ciò che loro circonda: il domandarsi sulle probabili trasformazioni della propria identità e modi di socializzare passa in particolar modo anche attraverso la mediazione delle Tecnologie dell'Informazione e della Comunicazione. È

[32] Bianca, M. (2019). *La filter bubble e il problema dell'identità digitale. MediaLaws—Rivista di diritto dei media (2), 39-53.*

evidente come, l'impatto del Covid-19 sul sistema socioeconomico mondiale avrebbe portato a conseguenze ancora più drammatiche se l'offerta ICT non fosse stata quella disponibile in quei mesi. La virtualizzazione dei contatti (e contratti) è stato proprio ciò che nelle fasi di totale chiusura ha concesso di mantenere quel minimo di contatto fra le persone: è indubbio che questa lunga parentesi sospensiva della normalità, soprattutto grazie alla presenza dei dispositivi digitali, sia stata indiscutibilmente fonte di accelerazione dei processi telematici in ambito sociale, politico, giuridico, economico e via dicendo.[33]

Al giorno d'oggi è altresì consuetudine sentir parlare di "consumatore digitale": la Commissione Europea prospetta in continuazione misure a tutela dei consumatori proprio in funzione e a favore di questa nuova figura, tra cui il "New Deal" per i consumatori.

Il pacchetto di misure attualmente in fase di approvazione dalla Commissione è principalmente progettato per affrontare le "sfide future" che si presentano nella politica dei consumatori, considerando l'ambiente economico e tecnologico in rapida evoluzione: la digitalizzazione e il progressivo avanzo della tecnologia rendono di giorno in giorno sempre più innovativi non soltanto i mercati e l'offerta, bensì anche i costumi e le preferenze dei consumatori.

Se si prende come esempio l'ambito energetico, l'approccio regolatorio in questo settore: tramite lo spostamento dell'attenzione dalla prospettiva dell'offerta a quella della domanda si è riconosciuto al consumatore un ruolo centrale e dinamico.

Questa progressiva importanza attribuita al consumatore all'interno di questo mercato è sorretta anche dall'introduzione di nuove metodologie che permettono a chi vende di offrire contratti avanguardistici e servizi su misura, personalizzati.[34]

Il progresso delle ICT ha reso e tutt'ora rende possibile la fruizione di servizi aventi valore aggiunto per il cliente, il quale ora stipula contratti "demand side response" i quali possibilitano la diminuzione della domanda in tempo reale nei periodi di più intensi e di picco.

Nella fattispecie, il New Deal si propone di porre al centro dell'attenzione il vero e proprio consumatore digitale che compera beni e servizi sui mercati online. Si tratta palesemente di un consumatore aggiornato, che però, dinanzi al meccanismo delle piattaforme virtuali potrebbe sentirsi "disarmato", non in possesso di indicazioni limpide e adeguate al fine di tutelare la sua posizione allo stesso modo di come accade sui mercati fisici, tradizionali.

Un recente studio per la Commissione Europea ha inoltre sottolineato come sia evidente che vi sia una notevole asimmetria informativa fra utente-consumatore e piattaforme. Proprio in ragione di

[33] Redazione, L. (2020). *Mutamenti dell'identità personale nella contemporaneità digitalizzata. Rosmini Studies, (7), 1-7.*

[34] Ammannati, L. (2019). *Il paradigma del consumatore nell' era digitale: consumatore digitale o digitalizzazione del consumatore? Rivista Trimestrale di Diritto dell'Economia.*

questo fatto, come si è menzionato in sovraimpressione, gli organi costituzionali europei sono in mobilitazione per attuare regolazioni sostanziali mirate a dare più contezza riguardo quelli che sono i rischi degli utenti, parte debole del rapporto contrattuale poiché difettano di sufficienti risorse cognitive rispetto alla controparte, e quindi di conseguenza incapaci di prendere decisioni informate. Malgrado i dati siano accessibili a entrambi le parti del rapporto, è solo l'impresa quella capace di sfruttarli a proprio vantaggio: si tratta di informazioni riguardanti le scelte di consumo dei singoli individui, conosciute come "product use information", che vengono raccolte ed elaborate dalle imprese per il loro significativo valore economico, ma che i consumatori non sono in grado di valutare adeguatamente. Pertanto, sarebbe auspicabile combinare la disponibilità di informazioni sulle caratteristiche del prodotto, chiamate "product attribute information", con l'utilizzo dei dati relativi alle abitudini di consumo da parte dei clienti. Entrambi questi approcci possono generare un prezioso patrimonio di conoscenza essenziale per la regolazione dei mercati caratterizzati da asimmetrie informative. Viene da sé che l''uso diffuso delle nuove tecnologie digitali consente la raccolta e l'organizzazione dei dati relativi alle scelte e alle operazioni di consumo degli individui. Questo ha un duplice effetto: da un lato, fornisce al consumatore informazioni utili per conoscere la struttura dei prezzi e le caratteristiche di utilizzo dei prodotti o servizi, consentendo una scelta più consapevole. Dall'altro lato, la raccolta e l'elaborazione dei dati da parte delle piattaforme comporta una crescente personalizzazione o profilazione, sfruttando la conoscenza dei limiti cognitivi degli utenti per influenzarli individualmente.

Tuttavia, questa personalizzazione rappresenta una sfida per la regolazione a tutela del consumatore. I regolatori non possono ignorare questa sfida, altrimenti si rischia di compromettere la capacità di autonomia decisionale del consumatore.[35]

[35] Ammannati, L. (2019). *Il paradigma del consumatore nell' era digitale: consumatore digitale o digitalizzazione del consumatore? Rivista Trimestrale di Diritto dell'Economia.*

Il nuovo ruolo del consumatore e diffusione dell'ICT nei pagamenti elettronici e nelle attività sul web – indagini su imprese

È risaputo (anche da chi poco se ne intende) che la diffusione dell'ICT nei pagamenti elettronici e nelle attività di rete costituisca un fenomeno sempre più rilevante e che le tecnologie dell'informazione e della comunicazione abbiano creato nuovi orizzonti nel settore dei pagamenti, consentendo transazioni online sicure, veloci ed efficienti.

Secondo diverse fonti, si registra un aumento significativo nell'adozione dei pagamenti elettronici da parte delle imprese e dei consumatori. Sempre più aziende offrono opzioni di pagamento digitali, come carte di credito, bonifici e portafogli digitali, per consentire transazioni online e ridurre la dipendenza dai pagamenti in contanti.

Inoltre, l'ICT ha permesso lo sviluppo di nuovi modelli di business e l'emergere di attività di rete, come il commercio elettronico, le piattaforme di sharing economy e le reti sociali. Queste attività sono diventate sempre più diffuse e hanno rivoluzionato il modo in cui le persone interagiscono, fanno acquisti e conducono le proprie attività.

La propagazione del fenomeno ICT nei pagamenti elettronici e sul web gioca ancora oggi un ruolo chiave e si prospetta come una tendenza in continua crescita, spingente verso un futuro sempre più digitale ed interconnesso. Proprio per questo si sta pian piano assistendo all'estinzione del contante: la società diventa di anno in anno sempre più cash-less e come conseguenza le banche tradizionali arrancano.

Dal punto di vista delle transazioni in posti fisici, in Italia si registrano ben 80 milioni di carte di pagamento ed oltre 2 milioni di POS: vi è una salda infrastruttura e una solida base quanto a strumenti per i pagamenti elettronici, in via di ulteriore sviluppo e destinata a migliorare.[36]

Banca d'Italia effettua tre indagini campionarie sulla diffusione dei pagamenti elettronici e circa servizi di rete nelle piccole e medie imprese. Si è registrata l'identificazione di un sentiero di crescita nell'uso delle ICT insieme a quelle che sono le politiche volte alla promozione della loro diffusione al fine di rendere il sistema produttivo più competitivo ed efficiente.

Dall'indagine si rileva che la maggior parte delle aziende su territorio italiano sono dotate di un proprio sito e-commerce e che il divario tra Sud e Centro-Nord si sta nel tempo dissolvendo; circa il 50% delle aziende ha adoperato misure di sicurezza come firma elettronica e altre precauzioni circa la cybersecurity nei pagamenti. Questo consente di avere, oltre che una maggiore sicurezza in termini di operazioni da compiere, di rendere queste ultime snelle e automatiche.[37]

[36] Garonna, P., & Stefano, P. (2013). *Italia 2020: Finanza e ICT per l'Agenda Digitale.*

[37] Banca d'Italia. (2010). *Diffusione dell'ICT nei pagamenti elettronici e attività sul web.*

Collegandosi al tema barriere, nel caso appena descritto relative alla semplicità dell'utilizzo, è importante sottolineare un altro essenziale vantaggio: l'eliminazione di ogni limite geografico e temporale, in qualsiasi parte e momento del pianeta, senza che vi sia la parte interessata alla vendita nel processo d'acquisto, procedendo di tempo in tempo verso un tipo di commercio sempre più globalizzato e disarticolato.[38]

Cambia completamente il rapporto giuridico-economico fra impresa e consumatore: quest'ultimo assume molta più autorevolezza e potere nel processo d'acquisto.

Il settore in cui ci si serve di più della rete è emerso essere quello dei servizi bancari online: il 90% se ne avvale per la maggior parte di incassi e pagamenti da ricevere ed effettuare nel corso delle procedure operative.

Quasi il 75% delle imprese che utilizzano i servizi bancari online preferiscono il corporate banking interbancario per gestire la tesoreria aziendale quando hanno rapporti con più banche. La diffusione di questo servizio varia in base alle dimensioni aziendali. Tuttavia, l'utilizzo del web per le transazioni con le controparti bancarie è marginale in operazioni meno standardizzate, come i finanziamenti o il trading su titoli, dove la relazione di clientela è importante. In questi casi, la fiducia nella controparte e la disponibilità di un'ampia offerta di servizi informativi online, uniti alla standardizzazione dei servizi bancari di pagamento, sono elementi chiave per l'utilizzo delle nuove soluzioni offerte dalle banche. E ancora, l'applicazione di prezzi vantaggiosi rispetto alle operazioni allo sportello e le misure di sicurezza adottate dalle banche per proteggere le proprie reti sono fattori che favoriscono l'adozione di tali servizi da parte delle imprese.[39]

[38] Calzavara, M. (2019). *L'evoluzione dell'e-commerce e il suo impatto nelle relazioni business-to-consumer. Analisi e prospettive.*

[39] Banca d'Italia. (2010). *Diffusione dell'ICT nei pagamenti elettronici e attività sul web.*

Conclusione

Finalità principale dell'esaminazione di questo argomento è stata quella di illustrare nel modo più peculiare, inclusivo e globale possibile quelli che sono processi, misure e regolamentazioni dietro il mondo dei pagamenti e della cybersicurezza, evidenziando come seguentemente alle varie rettifiche legislative a livello comunitario e nazionale il mercato abbia subito modifiche e implementazioni.

L'avanzare del progresso tecnologico in ambito giuridico e finanziario ha inevitabilmente portato ad effetti perlopiù positivi: grazie all'entrata in vigore di direttive come PSD2 e DORA si ha la possibilità di osservare come l'innovazione non smetta mai di essere presente nella società con il passare del tempo e anche di riconoscere che l'assenza di rischi e contro, come in ogni ambito della vita umana, sia un qualcosa a cui aspirare fattibilmente utopico ed impossibile.

PSD2 e DORA rappresentano il coronamento di una legiferazione che prova in tutte le modalità esistenti ad essere democratica e stimolante per il vero e proprio progresso umano: si è giunti ad un punto della storia giuridica in cui è difficile immaginare una prassi legale che sia più inclusiva di questa. Ciò non vuol significare che il miglioramento non debba costituire un'ambizione a cui aspirare costantemente, ma che comunque si è giunti ad un livello di giurisdizione al passo con i tempi che corrono e le innovazioni che a questi vengono attribuite.

Da un lato PSD2 persegue la competitività degli enti finanziari nell'ambito dei pagamenti, dando ampio spazio al mondo dell'Open Banking, a sostenere la trasparenza delle operazioni e proclamare la protezione dei diritti dei cittadini a livello economico, dall'altro DORA che stimola la concorrenza nell'ambito digital-finanziario con obiettivi leggermente diversi rispetto alla prima.

Con l'aumento e l'implementazione di questo tipo di regolamentazione i mercati virtuali e fisici continueranno ad avere una crescita inarrestabile, si auspica sempre entro quelli che sono i limiti che non vadano a ledere i diritti fondamentali dell'individuo (per fare un esempio pratico, confidando nel fatto che considerevoli innovazioni come l'Artificial Intelligence non vadano, in un futuro, a sostituire quelle che sono azioni che consentono all'uomo di esercitare i suoi diritti).

I consumatori avranno esponenzialmente la necessità di effettuare transazioni più veloci, comode e ridotte al minimo della loro operatività e che l'esperienza di pagamento sulle piattaforme online si avvicini sempre di più a quella nei posti fisici, è un effetto abbastanza logico: la legge e l'innovazione abituano l'individuo ad agire in un certo modo, di volta in volta in maniera diversa e sintetica. Già adesso, colossi come Amazon e altre grandi imprese hanno ideato modalità affinché questo avvenga (ad esempio, su Amazon, se si visualizza un articolo qualsiasi, sottostante alla voce "aggiungi al carrello" è stata introdotto il tasto "acquista subito", in maniera tale da invogliare subito il cliente ad acquistare il bene così da non avere più di qualche momento per pensarci e, in secondo luogo, per rendere il processo di compravendita dalla durata di pochi millesimi di secondo e di un semplice

passaggio, un click), mettendo in atto (forse anche inconsciamente per il consumatore) una sorta di manipolazione e pressione psicologica, frutto di una buona strategia di marketing. L'individuo dovrà essere in grado di stare al passo dell'innovazione tecnologica, senza farsi abbindolare da questi impercettibili stratagemmi, o meglio: sfruttare la rapidità dei passaggi per operare in condizioni più "comode", sempre però ponendo l'attenzione alla misura in cui questi meccanismi entrano nella sua stessa vita; finché non andrà ad interferire negativamente sulla libertà umana e, nel caso specifico di questo elaborato, sulle transazioni finanziarie, fin quando le minacce cibernetiche non costituiranno un problema invalicabile per il soggetto fisico (e con la trovata di Amazon, ci si sta probabilmente appropinquando verso il limite), sinché le sfide proposte non risulteranno obiettivi inarrivabili per l'uomo, il progresso legislativo e digitale non potrà far altro che portare esiti positivi ai mercati e alla società medesima.

In conclusione, la cybersicurezza è ormai un elemento essenziale per lo sviluppo del sistema dei pagamenti digitali. Le due direttive PSD2 e DORA rappresentano strumenti normativi fondamentali per fronteggiare con destrezza le sfide della digitalizzazione dei pagamenti, promuovendo un ambiente sicuro e affidabile per le transazioni finanziarie online. Tuttavia, è fondamentale mantenere un approccio vigilante e continuare a investire nella ricerca e nello sviluppo di nuove tecnologie e strategie per proteggere i sistemi di pagamento da minacce sempre più sofisticate e diffuse.

Bibliografia

- ACN. (2019). *Strategia Nazionale per la Sicurezza Cibernetica 2019.*
- Agenzia per l'Italia Digitale (AGID). (s.f.). *Cosa sono le tecnologie dell'informazione e della comunicazione (ICT)*
- Ammannati, L. (2019). *Il paradigma del consumatore nell' era digitale: consumatore digitale o digitalizzazione del consumatore? Rivista Trimestrale di Diritto dell'Economia.*
- Banca d'Italia, Consob, IVASS (2019). *Guida nazionale TIBER-IT - Test di penetrazione avanzati per entità finanziarie italiane*
- Banca d'Italia. (2010). *Diffusione dell'ICT nei pagamenti elettronici e attività sul web.*
- BERTOLDI, M. *La direttiva sui servizi di pagamento: portabilità dei dati finanziari e sviluppo dell'open banking.*
- Bianca, M. (2019). La filter bubble e il problema dell'identità digitale. MediaLaws—Rivista di diritto dei media (2), 39-53.
- Brighi, R., & Chiara, P. G. (2021). *La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto UE. Federalismi. it, 21, 18-42.*
- Bruni, M. (2017). *Open Banking e PSD2: sfide ed opportunità per le banche.*
- Calzavara, M. (2019). *L'evoluzione dell'e-commerce e il suo impatto nelle relazioni business-to-consumer. Analisi e prospettive.*
- Capello, R., & Spairani, A. (2003). Apprendimento collettivo, ICTs e performance delle PMI. Economia e politica industriale, (2003/118).

- CARDU, L. (2021). Open Banking: origini e sviluppo all'interno del sistema bancario e finanziario di Italia, Francia e Germania.
- CBI, (2021). *The Global Open Banking Report*
- Commissione Europea (2022). *Targeted Consultation On The Review Of The Revised Payment Services Directive (PSD2)*
- Di Carlo, C., & Santarelli, E. (2011). *Il ruolo dell'ICT nella crescita economica in Italia. Mondo digitale, 37, 3-8.*
- Fagnani, R. (2020). Banche tradizionali, virtuali e pericolo FinTech.
- Garonna, P., & Stefano, P. (2013). *Italia 2020: Finanza e ICT per l'Agenda Digitale.*
- Kenney, M., & Zysman, J. (2016). *The rise of the platform economy. Issues in Science and Technology, 32(3), 61-69.*
- Mansfield-Devine, S. (2016). Open banking: opportunity and danger. Computer Fraud & Security, 2016(10), 8-13.
- Pagamenti Digitali. (2022). *PSD2: Cos'è, obblighi e funzionamento della direttiva europea*
- PagamentiDigitali.it. (2021). *Come garantire la sicurezza dei pagamenti digitali*
- Parlamento Europeo. (2021). *Digital Operational Resilience Act (DORA).*
- Pozzolo A. (2021). *L'ATTUAZIONE DELLA SECONDA DIRETTIVA SUI SERVIZI DI PAGAMENTO E "OPEN BANKING".*
- Redazione, L. (2020). *Mutamenti dell'identità personale nella contemporaneità digitalizzata. Rosmini Studies, (7), 1-7.*

- Regolamento Europeo n. 679/2016. (2016). *Regolamento generale sulla protezione dei dati (GDPR).*