Università degli studi di Napoli "Federico II"

Dipartimento di Economia, Management, Istituzioni

DOTTORATO DI RICERCA IN MANAGEMENT

XXXII ciclo

Tesi di Dottorato

"Impatto dell'innovazione nell'industria assicurativa: Insurtech e analisi sul valore della supply chain"

Coordinatore del dottorato

Prof.ssa Cristina Mele

Candidato ***Relatore***

Dott. Alfonsoluca Adinolfi Prof.ssa Clelia Mazzoni

INDICE

Introduzione

L'innovazione attraverso le nuove tecnologie è un motore fondamentale del cambiamento nel settore finanziario e ciò ha portato a incommensurabili guadagni di efficienza, anche se questi cambiamenti possono inizialmente essere accompagnati da incertezza e dubbi. Negli ultimi anni, tale innovazione è avvenuta sulla scia dei nuovi sviluppi tecnologici e il fenomeno è stato spesso descritto come "FinTech". Poiché i servizi finanziari trattano prodotti immateriali, l'innovazione tecnologica si presta bene a ridurre i costi di transazione e ad accelerare l'erogazione dei servizi. Anche se ciò è avvenuto nel corso della storia della finanza, la recente proliferazione di connessioni internet, home computing e dispositivi mobili e lo sviluppo di applicazioni ha portato alla possibilità di abbassare la barriera per l'ingresso sul mercato, aprendo la strada ad una maggiore concorrenza o "perturbazione" del settore finanziario. Tuttavia, l'utilizzo della tecnologia e dell'innovazione come tecnologia "dirompente" può

essere risultare di difficile interpretazioni agli attori tradizionali che contraddistinguono il mercato internazionale ed in particolare quello domestico. Il settore assicurativo non fa eccezione: gli sviluppi tecnologici offrono nuove possibilità di nuovi metodi di prestazione di servizi e maggiori opportunità di raccolta dati che possono portare a una migliore identificazione dei rischi e a misure di mitigazione, che vengono denominate "InsurTech". Rispetto al FinTech, l'AssicurTech, è più spesso legata al miglioramento dei servizi per i privati, rispetto alle imprese. L'innovazione è generalmente considerata uno sviluppo positivo, che offre convenienza ed efficienza. Ad esempio, l'avvento degli sportelli bancomat ha aiutato le persone ad avere accesso al contante anche fuori dall'orario di lavoro e ha ridotto i costi per le banche. I miglioramenti delle reti di comunicazione e della capacità di elaborazione hanno portato a processi di pagamento più rapidi. Le richieste di risarcimento assicurativo possono essere elaborate tramite piattaforme online, con meno tempo per l'elaborazione. I siti di confronto permettono di

confrontare i prodotti di diversi prodotti assicurativi. Il modo in cui il settore assicurativo risponde alle innovazioni tecnologiche a livello economico e sociale, fornendo nuovi processi e polizze assicurative che integrano tali cambiamenti risulta fondamentale per lo sviluppo del settore stesso. Ad esempio, l'economia della condivisione ha reso le start-up, come l'Uber, rendendo disponibile il *ridesharing* in modo più comodo e più ampio. Mentre l'assicurazione RC auto commerciale sarebbe un requisito per i tassisti, i tassisti di Uber potrebbero non avere la copertura adeguata in quanto spesso si tratta di un'attività secondaria o di un lavoro a tempo parziale. Le compagnie di assicurazione stanno già rispondendo a questo caso specifico, ma presenta una domanda più ampia su come l'assicurazione risponde a nuovi rischi che non si adattano allo stile di vita tradizionale e/o all'attività economica di privati o imprese. Dato che la sottoscrizione si basa in gran parte sull'analisi dei dati storici per effettuare la valutazione del rischio di un assicurato, l'assicurazione, a prima vista, appare

particolarmente adatta per l'analisi dei "grandi dati". I grandi dati e la catena di blocco sono stati argomenti importanti in molti discorsi assicurativi della tecnologia. InsurTech ha attirato grandi investimenti in capitale di rischio, e l'andamento dei finanziamenti indica che molte start-up sono considerate dagli investitori come commercialmente redditizie in un'economia di mercato. Negli ultimi anni sono state prodotte più informazioni e tracce digitali nel mondo di quante ne fossero state create in tutti gli anni precedenti della civiltà umana. Questo fa emergere sia rischi nuovi, legati al nostro alter ego digitale, sia bisogni di servizi nuovi per gestire rischi tradizionali, aprendo un grande dibattito sulle conseguenze per un settore chiamato a gestire rischi di lungo periodo, quale quello assicurativo. I *big data*[1] stanno mutando il mestiere della protezione, perché aiutano a comprendere l'evoluzione dei rischi non più solo in funzione di

[1] In statistica e informatica, la locuzione inglese *big data* ("grandi [masse di] dati"), o in italiano *megadati* indica genericamente una raccolta di dati informativi così estesa in termini di *volume*, *velocità* e *varietà* da richiedere metodologie analitiche e tecnologie specifiche/particolari per l'estrazione di valore o conoscenza

fattori sociodemografici, ma anche in relazione alle abitudini individuali. In aggiunta, la crescita esponenziale dell'*Internet of Things* ha ridefinito il rapporto non solo tra i professionisti e i consumatori, ma soprattutto la relazione che gli individui hanno con la realtà che li circonda, che è diventata sempre più "smart", interattiva e interdipendente. Ma cosa si intende per "*big data*" e per "*Internet of Things*"? I *big data* sono dati che superano i limiti dei database tradizionali, ma non solo; per *big data* si intendono anche le tecnologie finalizzate ad estrarre da essi conoscenze e valore. In pratica, potremmo definire i *big data* l'analisi di quantità incredibilmente grandi di informazioni. In considerazione della loro enorme estensione in termini di volume, ma anche delle loro intrinseche caratteristiche, quali la velocità e la varietà, i *big data* richiedono tecnologie e metodi analitici specifici, che possano portare all'estrazione di valori di interesse. L'analisi corretta dei *big data* ha l'obiettivo principale di estrarre informazioni aggiuntive rispetto a quelle che sono ottenibili da piccole serie di dati. Ormai

da diversi anni, l'argomento dei *big data* è ritenuto particolarmente interessante da molte aziende, e gli investimenti in questo senso sono sempre più importanti. Al contempo, la *Connected Insurance*, altresì definito *IoT* (*Internet of Things*) assicurativo, è uno dei trend più rilevanti di innovazione del settore assicurativo. Questo nuovo approccio si basa sull'utilizzo di sensori telematici, per la raccolta e la trasmissione dei dati sullo stato di un rischio assicurato, e sull'utilizzo dei *big data*, per trasformare i dati grezzi in informazioni che possano essere utilizzate lungo la *value chain* assicurativa. Il settore assicurativo, considerato da sempre tradizionale e resiliente al cambiamento, è quindi oggi attraversato da un macro trend di innovazione digitale, che sta portando istituzioni con centinaia di anni di storia a ripensare il modello di business assicurativo, identificando quali moduli della propria *value chain* trasformare o re-inventare attraverso la tecnologia e l'utilizzo dei dati (la stessa dinamica è avvenuta in tutto il settore dei *financial services* e prende il nome di *FinTech*) (Braun

A., Schreiber F., 2017). Tutti gli step del *customer journey* del cliente e della *value chain* assicurativa vengono influenzati da questo fenomeno. L'impatto è diffuso sull'intera catena di valore assicurativa, con una progressiva frammentazione e con la possibilità di nuovi ingressi a vari livelli da parte degli operatori, come ad esempio: nella ricerca di una maggiore efficienza e riduzione dei costi nelle operazioni aziendali (ad es. con il ricorso a *smart contracts*[2]); nel disegno di nuovi prodotti (possibilità di micro-polizze e *sliced insurance,* polizze *pay-per-use* o *pay-as-you-drive*[3]); nel processo di *pricing,* con il ricorso a dati personalizzati e granulari; in nuove modalità di intermediazione e distribuzione con vendita digitale e *peer-to-peer*; nell'assistenza post-vendita *anytime/anywhere* con servizi continui (ad es. assistenza sanitaria, chiamate SOS in caso di incidente auto, localizzazione). Il modello *peer-to-peer* verrà

[2] Secondo la definizione data dall'IVASS, "Gli *smart contracts* sono contratti scritti in un linguaggio eseguibile da un computer, le cui clausole possono produrre azioni senza intervento esterno sulla base di informazioni ricevute in input ed elaborate secondo regole predefinite (ad es. pagamento di una somma se accade un determinato evento)".

dettagliatamente trattato e approfondito nel lavoro, si rimanda quindi in seguito per una sua corretta definizione. Si modifica il ruolo svolto dalle *app*[4], sempre più centrale nella vita quotidiana, tendenza che non è sfuggita al settore assicurativo che affina i propri modelli di *business*, innovando le modalità di contatto con la clientela, le coperture e i servizi ancillari e le forme di assistenza nella risoluzione di problemi connessi con l'offerta assicurativa. Questo ampio spettro di innovazioni interessa trasversalmente tutti gli step del *customer journey* assicurativo e riguarda tutte le differenti *business lines*, in primis l'auto, ma anche il resto delle *personal lines* – P&C[5], salute e vita– oltre ad estendersi fino alle *commercial line*. La tecnologia *IoT* sta portando alla creazione di nuove tipologie di coperture assicurative, non più generiche ma

[4] Il termine applicazione in informatica individua un programma installato o una serie di programmi in fase di esecuzione su un computer con lo scopo e il risultato di rendere possibile una o più funzionalità, servizi o strumenti utili e selezionabili su richiesta dall'utente tramite interfaccia utente, spesso attraverso un'elaborazione a partire da un input fornito dall'utente interagendo con esso. È dunque il risultato a livello utente dalla combinazione di risorse software e rispettive risorse hardwaredi processamento per la loro esecuzione.

[5] Porperty& Casualty è un acronimo che viene utilizzato per comprendere diverse tipologie di coperture assicurative in particolar modo riferibili alle coperture personali di beni e di responsabilità civile.

personalizzate sulla base delle esigenze dei clienti ed associate ad ulteriori servizi. L'esperienza consolidata a livello italiano e internazionale nell'ambito dei *telematics auto* ha insegnato come non esista un approccio *one size fits all*. Ogni Compagnia ha bisogno di progettare il proprio approccio alla *Connected Insurance* basato sulla propria strategia e sulle proprie caratteristiche specifiche. La capacità di avere a disposizione una serie illimitata di nuove fonti dati in tempo reale sta radicalmente mutando uno dei parametri fondamentali per le compagnie assicurative, cioè quello della valutazione del rischio: la vera sfida che si trovano a fronteggiare è non solo gestire le informazioni, ma capire come estrarre valore da una mole di dati mai vista prima. Il comparto assicurativo è attualmente impegnato nella pianificazione e nel rendere operativi e numerosi progetti di *digital transformation*, che permettendo alle aziende, da un lato, di stare al passo dei *big player* digitali e rispondere alle rinnovate esigenze della clientela, dall'altro di cogliere le opportunità offerte dalle nuove tecnologie in termini di

ottimizzazione dei processi operativi, automazione e riduzione dei costi. Ad esempio, i processi di gestione dei sinistri hanno rappresentato in passato una delle voci di costo maggiormente rilevanti per una compagnia assicurativa. A gravare su di essa contribuivano in maniera particolarmente importante la loro non uniformità (differenti processi e strutture per tipologia di sinistro), gli elevati costi di coordinamento degli interlocutori coinvolti (cliente, agente, perito, fiduciario, ecc.) e della relativa documentazione, ma anche numerosi fenomeni fraudolenti. Queste criticità hanno spinto le compagnie ad investire prioritariamente su questa area aziendale, cosa che ha reso oggi l'area sinistri più evoluta rispetto a quella commerciale, in special modo in Italia. La reingegnerizzazione dei processi ed il rinnovamento dei sistemi informatici ha portato enormi benefici alla divisione sinistri, generando un elevato livello di automazione e di coordinamento dei flussi informativi delle diverse aree coinvolte. I prossimi investimenti interesseranno aspetti *HR* (*Human Resources*), come l'estensione della mappatura delle

competenze *digital* a tutto il personale dipendente (e delle reti esterne) e l'allineamento tra i sistemi di *back-end* e *front-end*[6] (l'evoluzione dei sistemi di *back-end* andrà di pari passo con l'implementazione di un *front-end* scalabile e flessibile, in grado di consentire l'utilizzo delle nuove tecnologie e dei canali digitali *web* e *mobile* abilitati per la preventivazione e la vendita di polizze in modalità *self* e *multidevice*). L'innovazione di portafoglio, però, si presenta oggi limitata. Se da un lato stiamo assistendo ad un discreto successo dei prodotti abbinati a *connected devices*, come nel caso delle *black- box* (per le automobili), sono ancora in fase di sperimentazione soluzioni assicurative che permettono la connessione ed il monitoraggio degli eventi che riguardano l'abitazione (*white-box*) ed il

[6] I termini front end (in sigla FE) e back end (in sigla BE) (anche scritti, con grafia meno corretta, ma più comune, *frontend* o *front-end* e *backend* o *back-end*) in informatica denotano, rispettivamente, la parte visibile all'utente di un programma e con cui egli può interagire - tipicamente una interfaccia utente - e la parte che permette l'effettivo funzionamento di queste interazioni.

Il *front end*, nella sua accezione più generale, è responsabile dell'acquisizione dei dati di ingresso e della loro elaborazione con modalità conformi a specifiche predefinite e invarianti, tali da renderli utilizzabili dal *back end*. Il collegamento del *front end* al *back end* è un caso particolare di interfaccia.

comportamento e lo stile di vita della persona (*wearable device*). Per le compagnie, quindi, la sfida principale è rappresentata dalle modalità per essere un attore rilevante nell'ecosistema. Date queste premesse, la sfida per il settore è su due livelli: il primo livello è quello di introdurre questo tipo di pensiero creativo all'interno del processo della strategia aziendale; il secondo è di dotarsi delle competenze e degli strumenti per gestire l'ecosistema dei partner. Per le compagnie, quindi, la sfida principale è rappresentata dalle modalità per essere un attore rilevante nell'ecosistema. Date queste premesse, la sfida per il settore è su due livelli: il primo livello è quello di introdurre questo tipo di pensiero creativo all'interno del processo della strategia aziendale; il secondo è di dotarsi delle competenze e degli strumenti per gestire l'ecosistema dei partner. Allo stesso tempo, l'attenzione di questi nuovi operatori si è spostata da semplici soluzioni software ad attività che sono chiaramente in concorrenza con quelle delle compagnie di assicurazione e dei broker. In questo contesto, molti osservatori evocano instancabilmente

conseguenze devastanti per il settore assicurativo. Di conseguenza, la situazione ancora relativamente favorevole per gli operatori storici, che attualmente prevale potrebbe non perdurare a lungo. In combinazione con cambiamenti sostanziali delle esigenze e delle richieste dei clienti, le nuove tecnologie cominciano ad intensificare la concorrenza per erodere i margini. Offerte più rapide, una maggiore trasparenza e comparabilità, servizi più personalizzati e un processo di liquidazione dei sinistri semplificato stanno rapidamente diventando fattori essenziali di successo; allo stesso modo, i clienti si aspettano un *customer journey* digitalizzato attraverso tutti i punti di contatto. In risposta a questi sviluppi, l'industria assicurativa deve iniziare a digitalizzare la propria *value chain*. In un contesto di mercato in rapida evoluzione e guidato dalla tecnologia, l'agilità è essenziale e questo si rivela un problema per molte compagnie di assicurazione e broker che, tradizionalmente, sono innovatori piuttosto lenti. Come se per il momento questo non fosse abbastanza stressante, i nuovi concorrenti, chiamati

InsurTechs, stanno entrando nell'ecosistema assicurativo accelerando la trasformazione dell'industria e guidando l'innovazione con idee nuove, concetti intuitivi e tempi di reazione rapidi. Molti di loro stanno già progettando di andare oltre la semplice digitalizzazione della *value chain*[7], e mirano ad anticipare preventivamente le tendenze chiave e le esigenze future dei clienti per posizionarsi di conseguenza, fornendo servizi e soluzioni intelligenti piuttosto che semplici prodotti assicurativi.

[7] il concetto di value chain racchiude la logistica interna, le operazioni, la logistica esterna, il marketing e le vendite e i servizi. A supporto di tali attività, l'organizzazione predispone un'infrastruttura d'impresa, una gestione delle risorse umane, una ricerca tecnologica e gli approvvigionamenti.

A causa dei modelli di business innovativi, i professionisti del settore e gli investitori hanno espresso crescenti preoccupazioni sul fatto che i nuovi operatori potrebbero prima o poi mettere a repentaglio l'esistenza degli operatori storici a causa di una trasformazione dei mercati assicurativi così come li conosciamo. Tali attori devono quindi trovare risposte e adattarsi alle più recenti innovazioni tecnologiche per mantenere un vantaggio competitivo e ridurre la distanza dal cliente. Per mantenere la loro posizione, molti hanno iniziato a considerare le partnership con le imprese *InsurTech* come parte integrante della loro strategia di digitalizzazione. Un esempio di fruitori di questi modelli sono gli assicuratori digitali, che aggiungono un valore aggiunto significativo per il cliente attraverso una copertura personalizzata basata su un'ampia valutazione individuale del rischio. Allo stesso modo, veri e propri concetti *peer-to-peer*, che consentono il trasferimento del rischio direttamente ai mercati dei capitali,

potrebbero mettere in discussione la rilevanza primordiale delle compagnie di assicurazione e quindi portare ad una vera e propria disintermediazione. Quali aspetti costituiscono un'innovazione del modello di business? Qual è il significato di "*disruption*" [8] ? Come si può distinguere tra concorrenti tecnologici, società che promuovono la digitalizzazione del settore assicurativo e veri e propri "*disrupters*" che possono modificare radicalmente l'ecosistema assicurativo tradizionale? E infine, quali sono le risposte degli *incumbent*[9] adatte per fronteggiare le nuove sfide descritte? Nell'elaborato propostosi analizzeranno gli elementi connessi, indagando dettagliatamente l'attuale panorama *InsurTech*". Gli obiettivi principali saranno quelli di stabilire una comprensione comune dei concetti chiave,

[8] Significa cambiamento. È ciò che l'innovazione digitale sta portando nel mercato e negli stessi modelli di business. Tutti coloro che hanno un'attività non possono più ignorare questo cambiamento e devono fare i conti con il web, le sue logiche e con il fatto che ormai gli acquisti avvengono sempre di più online e il business si sta spostando sul web.

[9] Il termine "*incumbents*" da qui in avanti verrà utilizzato con riferimento agli attori tradizionali- storici dell'ecosistema assicurativo.

facilitare la navigazione in questo settore in rapida evoluzione e fornire un insieme di strumenti intuitivi per la valutazione del potenziale di crescita dei nuovi modelli,andremo in conclusione ad analizzare il nuovo probabile scenario che si verrà a creare per le imprese assicurative ed per il cliente finale consumer.

1. ELEMENTI DELL'INSURTECH

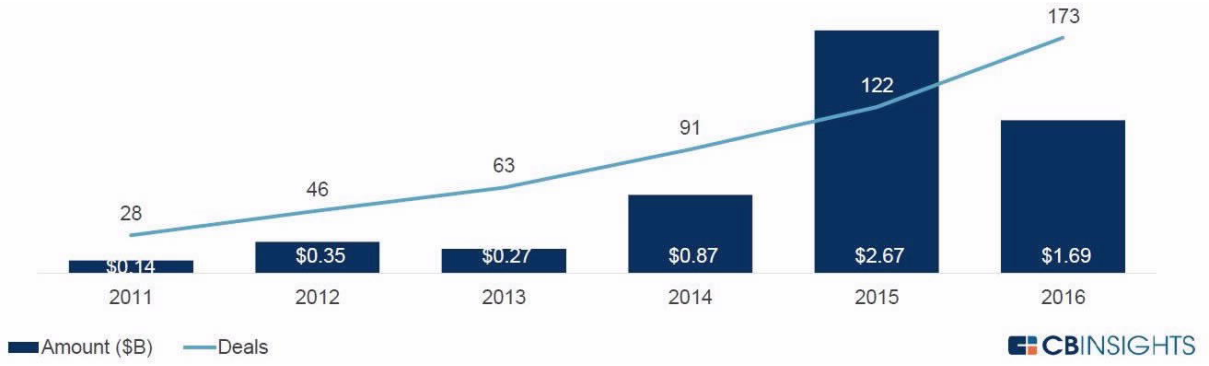
1.1. *Finanziamenti nell'insurTech*

I finanziamenti per le nuove tecnologie e l'innovazione nel settore assicurativo sono influenzati dalle più ampie possibilità di capitale di rischio ("VC") sul mercato. Negli Stati Uniti, le InsurTechs hanno beneficiato di un mercato ricco e competitivo per il finanziamento (ANIA, 2017) dei capitali di rischio e molte start-up assicurative hanno completato con successo una serie di cicli di finanziamento. D'altra parte, alcuni mercati non hanno una forte cultura del capitale di rischio, per cui l'approccio alla raccolta di capitali sarebbe diverso, con

fonti pubbliche che diventano più importanti. Ad esempio, la start-up francese, InsPeer, dispone di finanziamenti provenienti da diverse fonti pubbliche. Molti degli sviluppi tecnologici e delle innovazioni più ampi sono alla base di molti degli sviluppi InsurTech. Alcune delle tecnologie sono interdipendenti e una breve rassegna di esse è utile per stabilire un'interpretazione comune della loro natura. L'effetto rete dei telefoni cellulari e lo sviluppo di applicazioni per questi dispositivi ("App") ha permesso a molte aziende di raggiungere un pubblico più vasto di quanto fosse possibile in precedenza. La tecnologia mobile può funzionare in modi diversi per InsurTech, a seconda della generazione di reti mobili disponibili e dei tipi di telefoni cellulari più utilizzati. Gli smartphone e l'accesso a Internet consentono innovazioni basate sull'uso delle applicazioni. A tal fine sarebbero necessarie reti mobili che consentano messaggi brevi e telefoni cellulari prepagati, nonché trasferimenti di dati di grandi dimensioni. Ciò è particolarmente importante per i mercati emergenti che hanno una bassa

penetrazione assicurativa e non dispongono di una rete di distribuzione ben consolidata. Come nell'esempio di BIMA, i telefoni cellulari hanno la possibilità di comunicare via SMS ai singoli individui su qualsiasi cosa, dalla copertura assicurativa per ricordare loro l'imminente ritiro del tempo di trasmissione per il pagamento dei premi. L'intelligenza artificiale è l'intelligenza esibita dalle macchine. Una macchina sarebbe considerata "intelligente" quando prende in considerazione il suo ambiente e agisce per massimizzare le possibilità di raggiungere l'obiettivo prefissato. E’ ampiamente utilizzato quando i programmi informatici sono sviluppati per avere funzioni cognitive come l'apprendimento e la risoluzione dei problemi. La ricerca sull'intelligenza artificiale si sta svolgendo in campi che comprendono il ragionamento, la conoscenza, la pianificazione, l'apprendimento, l'elaborazione del linguaggio naturale, la percezione e gli oggetti in movimento/manipolazione.

TAVOLA 1.1. Andamento dei finanziamenti di AssicurTech (2011-2016)



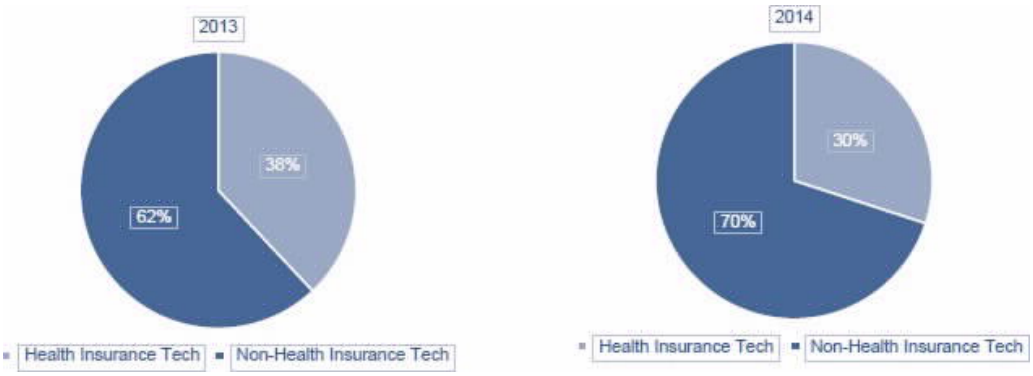
Fonte: CB Insights (2017a) Le *nuove imprese di assicurazione aumentano di $1,7B su 173 offerte nel 2016* www.cbinsights.com/blog/2016-insurance-tech-funding/ .[10]

Il 2015 ha visto livelli di finanziamento record per l'AssicurTech, con finanziamenti stimati in totale a 2 669 miliardi di dollari USA. Nel terzo trimestre del 2016 i livelli di finanziamento sono stati pari a 401 miliardi di dollari USA e il numero di transazioni nel

[10] *Fonte*: CB Insights (2017a) Le *nuove imprese di assicurazione aumentano di $1,7B su 173 offerte nel 2016*

terzo trimestre del 2016 è stato di 126, già superiore al numero di transazioni nel 2015 (*cfr*. figura 1). Va notato che nel 2015, quasi 1/3 dei finanziamenti è andato a Zhong An, un assicuratore cinese che è stato fondato nel 2013 con il sostegno di Alibaba Group Holding, che ha raccolto 931 milioni di dollari nel 2015, e che si dice stia pianificando una IPO.

TAVOLA 1.2. Attività assicurativa Tech negli Stati Uniti per area di intervento (salute vs. non-health)



Fonte: CB Insights (2017b), InsurTech Connect 2016 (ottobre) https://www.cbinsights.com/reports/ITC-insurance-tech-deck.pdf.

Nel 2016, il 59% delle operazioni InsurTech è andato alle start-up statunitensi, seguite da Germania (6%), Regno Unito (5%), Cina (5%) e India (3%) (CB Insights, 2017). Ciò potrebbe non corrispondere perfettamente allo status attuale dell'InsurTechs, ma è indicativo delle possibilità di VC sul mercato, in particolare per gli Stati Uniti, anche se l'Asian InsurTech è molto più debole rispetto ai più ampi finanziamenti di Venture Capital nella regione. Il numero di fondi di Private Equity che investono in nuove imprese InsurTech è passato da 55 nel 2012 a 141 nel 2016 YTD (CB Insights, 2017). Mentre la ripartizione degli investimenti nel settore assicurativo non è disponibile, gli investimenti nell'assicurazione malattia sono considerati forti e in crescita, assorbendo il 70% degli investimenti di InsurTech negli Stati Uniti (CB Insights, 2017). Allo stesso tempo, gli investimenti in start-up che forniscono canali di distribuzione commerciale sono aumentati in misura considerevole. Le start-up del ramo vita e delle rendite stanno attirando ingenti investimenti, così come le start-up di

assicurazioni sanitarie e dentali Anche le nuove imprese di assicurazione auto distribuzione/confronto costituiscono un'ampia coorte delle nuove imprese di assicurazione. Inoltre, gli assicuratori stanno fornendo strutture di finanziamento che consentirebbero loro di avere la possibilità di scegliere tra nuove tecnologie e innovazioni di successo che potrebbero sostenere le loro operazioni esistenti e migliorare l'esperienza dei clienti. Ciò è stato possibile sia attraverso opportunità di finanziamento generale dei VC [11], sia attraverso investimenti mirati di InsurTech, nonché attraverso la creazione di incubatori che ospitano imprenditori e dipendenti InsurTech. Diversi assicuratori hanno fornito investimenti alle nuove imprese InsurTech e alle start-up di Internet of Things ("IOT"). Il panorama più ampio dei finanziamenti per InsurTech è descritto sopra, ma uno sviluppo più interessante è stato il modo in cui gli riassicuratori [12] stanno finanziando

[11] Il venture capital è l'apporto di capitale di rischio da parte di un investitore per finanziare l'avvio o la crescita di un'attività in settori ad elevato potenziale di sviluppo.

[12] La riassicurazione è uno strumento di cui si servono le compagnie di assicurazione per assicurarsi a loro volta. È possibile, infatti, che esse non dispongano dei mezzi necessari

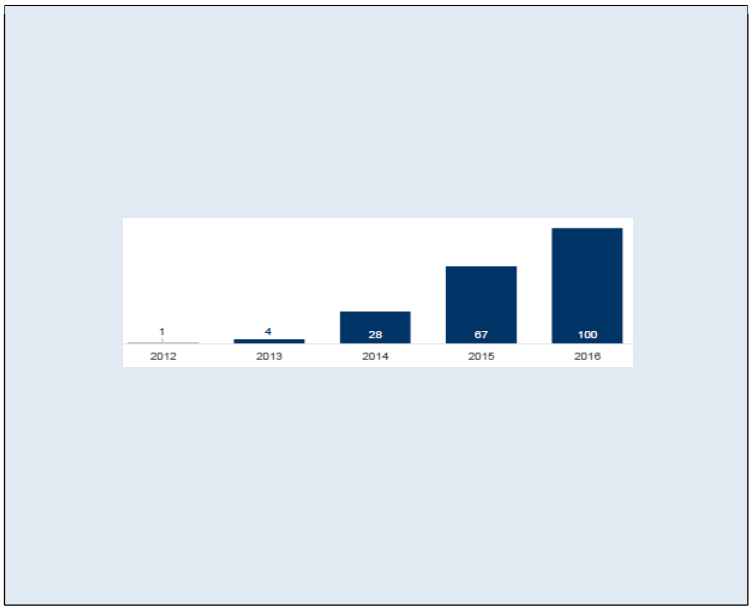
l’InsurTech. Alcuni dei maggiori assicuratori hanno creato fondi specifici e fondi di capitale di rischio per investire in start-up, anche per l'AssicurTech, indicando la probabilità di un maggiore investimento in InsurTech, e gli investimenti strategici che gli assicuratori esistenti faranno per assicurarsi di avere una partecipazione in una start-up che potrebbe essere in grado di scalare la loro attività. Il numero di contratti stipulati dai riassicuratori nel 2016 è stato di 100 contratti, contro 67 nel 2015 e 28 nel 2014. Riflettendo il panorama più ampio dell'InsurTech, ma con alcune differenze specifiche, gli riassicuratori statunitensi stanno effettuando la maggior parte degli investimenti in InsurTech, con il 64% delle operazioni effettuate (a differenza dell'effettivo livello di finanziamento, per il quale non sono disponibili dati) (CB Insight, 2017). Molto probabilmente riflettendo gli investimenti che Ping An Insurance ha fatto a Zhong An, e Taipang Insurance ha fatto in Alibaba Health, gli investimenti

---

ad indennizzare gli assicurati per disastri legati ad eventi di grande dimensioni (catastrofi naturali, danni a catena).Si tratta di uno strumento di primaria importanza per conferire stabilità al sistema finanziario globale.

riassicurativi cinesi rappresentano il 10% delle operazioni effettuate da riassicuratori. È possibile che, data la minore penetrazione dell'assicurazione in Cina, si preveda che il mercato possa svilupparsi sulla base dei nuovi modelli di intermediazione che si stanno introducendo in Cina. Gli riassicuratori francesi e britannici effettuano rispettivamente l'11% e il 6% delle operazioni degli riassicuratori (CB Insight, 2017). Molti degli accordi sono stipulati dal braccio strategico dei riassicuratori di VC. Ping An Venture ha effettuato alcuni dei maggiori investimenti in AssicurTech con oltre 20 operazioni. Axa Strategic Ventures ha anche completato 20 operazioni e insieme a Ping An sono stati i più attivi nella realizzazione di investimenti strategici.

TAVOLA 1.3. Investimenti tecnologici di start- up da parte di riassicuratori (2012-2016)



Gli assicuratori statunitensi MassMutual Venture, USAA, American Family Ventures, Transamerica e New York Life seguono con cinque o dieci contratti ciascuno. Dopo di che, gli assicuratori europei Allianz Ventures, MunichRE/HSB Ventures e Aviva Ventures continuano. Più storicamente, Axa Strategic Ventures, Transamerica Ventures e American Family Ventures sono stati gli investitori più attivi nell'investimento tecnologico privato dall'inizio del 2012. Axa ha fornito finanziamenti di avviamento per cinque start-up europee nell'ambito di un fondo istituito in Francia nel 2013, prima del lancio di Axa Strategic Ventures nel 2015. Il fondo di venture capital di 200 milioni di euro (223,47 milioni di USD) ha il mandato di investire in innovazioni nel settore assicurativo, nell'asset management, nella tecnologia finanziaria e nei servizi sanitari. Axa ha creato Kamet nel 2015, che è un incubatore InsurTech da 100 milioni di euro che lavora con imprenditori interni ed esterni. Axa ha recentemente investito 75 milioni di euro per acquisire una partecipazione dell'8% nella società di e-commerce Africa Internet Group ed è diventata l'unico fornitore di assicurazioni attraverso Jumia e altre piattaforme.

Allianz ha creato Allianz Ventures come centro per gli investimenti e le partnership con start-up, con l'obiettivo di focalizzarsi su cinque aree chiave: AssicurTech e gestione patrimoniale; mobilità e auto connesse; case e proprietà connesse; salute digitale; sicurezza informatica e intelligenza dei dati. Gli investimenti recenti includono una partecipazione minoritaria nel gestore patrimoniale digitale MoneyFarm. Allianz X è il "costruttore d'impresa" del gruppo che identifica, costruisce e scalare nuovi modelli di business nell'ambito dell'AssicurTech e in settori correlati come la catena a blocchi e l'intelligenza artificiale. Aviva ha lanciato una divisione di venture capital per investire in nuove attività digitali alla fine del 2015, con sede a Hoxton Square, il centro degli imprenditori digitali londinesi, con un fondo annuale di circa 20 milioni di sterline (24,8 milioni di dollari) da investire nei prossimi cinque anni. Il suo primo investimento è stato in Cocoon, un dispositivo intelligente per la sicurezza della casa che avverte i proprietari degli spostamenti e del suono all'interno della loro proprietà. Nel maggio 2016, Aviva ha annunciato una partnership con Founders Factory, un acceleratore digitale e

incubatore, diventando il suo partner finanziario esclusivo per i prossimi cinque anni, fornendo capitali e risorse per sostenere la crescita di oltre 200 aziende tecnologiche. Munich Re ha effettuato investimenti attraverso la sua divisione HSB Ventures in Slice Labs, un fornitore statunitense di assicurazioni on-demand, che ha lanciato un prodotto per gli host di homesharing utilizzando piattaforme come Airbnb, HomeAway, OneFineStay e FlipKey. L'assicurazione dura specificamente per il tempo in cui il proprietario agisce come un'azienda in modo che gli assicurati possono acquistare la copertura solo quando ne hanno bisogno. Munich Re si è assicurata il diritto di fornire capitale di sottoscrizione e licenze assicurative per l'assicuratore su richiesta Trov sul mercato statunitense. L'app di Trov consente ai clienti di assicurare singoli elementi come l'elettronica o le attrezzature sportive dal proprio smartphone e dà loro la possibilità di attivare e disattivare la copertura quando necessario. Nell'aprile 2016, la serie B di Helium da 20 milioni di dollari USA è stata guidata dal ramo d'impresa GV, ma anche Munich Re/HSB Ventures ha partecipato. La tecnologia dei sensori Helium

risiede nella sua capacità di utilizzare un sensore standard e collegarlo al Cloud Helium che permette al sistema operativo di controllare la temperatura di stoccaggio. In questo modo l'uso di tale tecnologia può proteggere da responsabilità derivanti, ad esempio, dal lasciare il frigorifero aperto in un ristorante o in un ospedale che non gestisce le scorte di vaccini. Ping An Ventures ha investito attivamente nel settore sanitario. La maggior parte degli riassicuratori sulle imprese di assicurazione o di riassicurazioni ha investito pubblicamente nelle nuove imprese solo negli ultimi due anni e nei settori in cui gli riassicuratori ritengono che vi sia una domanda di massa e un'applicazione pratica alle loro imprese. Axa Strategic Ventures, AIG e American Family Ventures hanno investito in start-up dell'internet. Oltre alle società di *private equity*[13],

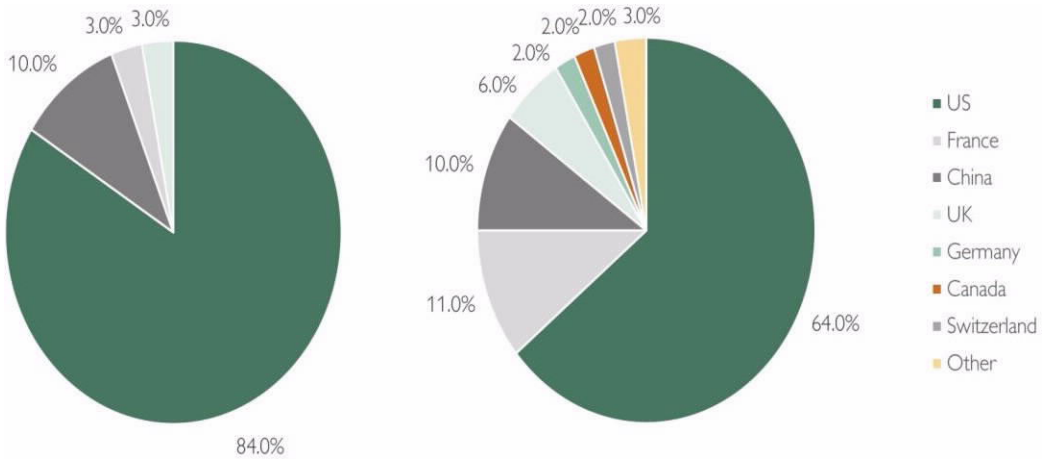
[13] Il private equity è una forma di investimento di medio-lungo termine in imprese non quotate ad alto potenziale di sviluppo e crescita (high grow companies) effettuata prevalentemente da investitori istituzionali con l'obiettivo di ottenere un consistente guadagno in conto capitale dalla vendita della partecipazione acquisita o dalla quotazione in borsa.
L'attività di private equity non comporta unicamente l'apporto di capitale di rischio, ma riguarda anche una serie di attività connesse e strumentali alla realizzazione dell'idea imprenditoriale; fondamentale è l'apporto professionale dello stesso investitore nell'attività della società, di fatto questi partecipa alle decisioni strategiche dell'impresa apportando le proprie conoscenze ed esperienze professionali lasciando all'imprenditore e al management la gestione operativa. Lo stesso investitore istituzionale può essere una figura di prestigio

negli ultimi due anni un numero crescente di compagnie di assicurazione e riassicurazione tradizionali hanno iniziato ad investire strategicamente nelle startup *InsurTech*.; a tal fine, la maggior parte di esse ha fondato società di *venture capital*. La TAVOLA 1.1., basata sui dati di *CB Insights*, mostra che il numero di operazioni private *tech* effettuate da assicuratori e riassicuratori è salito a 100 nel 2016, il che implica un tasso di crescita del 49% su base annua e un aumento di oltre il 250% rispetto al 2014. In linea con tale incremento, la gamma dei paesi in cui vengono effettuati gli investimenti si è notevolmente ampliata tra il 2013-2014 e il 2015-2016.

dell'ambiente finanziario, comportando notorietà per l'azienda stessa e facendo sì che il mercato stesso manifesti fiducia nella società al momento della sua quotazione.

Anche se il 64% degli affari ha ancora ad oggetto startup statunitensi, Francia (11%), Cina (10%) e Regno Unito (6%) sono ora considerevoli paesi target.

TAVOLA 1.4. Investimenti tecnologici di riassicuratori per area geografica



Fonte: The Current InsurTech Landscape: Business Models and Disruptive Potential

Anche se l’insieme delle start-up considerate come target per gli investimenti è piuttosto ampio, i canali di distribuzione digitale.

TAVOLA 1.5. Investimenti degli assicuratori nelle startup

Insurtech

Fonte: CB Insights (2017)

Oltre agli investimenti diretti nelle startup, gli assicuratori e i riassicuratori, che vanno da *AXA* e *Allianz* a *Munich Re* e *Swiss Re*, hanno cercato di implementare sistemi digitali attraverso la costituzione di acceleratori e incubatori o instaurando partnership con le startup *InsurTech*. Munich Re, ad esempio, ha istituito un "Digital Partners Program"

attraverso il quale fornisce possibilità di sottoscrizione aggiuntive grazie alle piattaforme assicurative on demand Trov e Slice. Nello stesso tempo, supporta l'assicuratore P&C digitale Lemonade con una copertura riassicurativa Il caso di Munich Re verrà trattato nello specifico più avanti nel lavoro. Allo stesso modo, Swiss Re finanzia l'acceleratore Startupbootcamp InsurTech con sede a Londra.

Queste iniziative strategiche evidenziano il fatto che gli assicuratori tradizionali hanno iniziato a considerare le startup tecnologiche come parte integrante delle proprie strategie di digitalizzazione.

1.2. Scenario macroeconomico

Nonostante le condizioni relativamente performanti per il settore dei servizi finanziari nel corso del 2018, il settore assicurativo si troverà ad affrontare diverse sfide con opportunità da cogliere per gli operatori pronti ad affrontare il cambiamento e l'innovazione. In effetti, il settore è minato dall'erosione dei vantaggi strutturali del loro business - il fatto che in altri settori si sta generando nuovo valore per i clienti rispetto ai servizi finanziari e l'alto livello di concorrenza proveniente da attori non finanziari alternativi, come i grandi tecnici o le assicurazioni, sta aumentando molto rapidamente. L'analisi dei *megatrend* globali è necessaria per contestualizzare l'ambiente in cui gli assicuratori stanno operando con uno scenario globale del mercato in mente - a partire dalle tendenze demografiche, dalla crescente età media della popolazione, dalla digitalizzazione e dall'adozione di tecnologie che raggiungono nuovi livelli

con più di 5,1 miliardi di smartphone di proprietà delle persone, dalle conseguenze delle politiche monetarie e politiche che interessano il mercato globale con uno sguardo sui mercati emergenti e, infine, dalle considerazioni sullo spostamento della percezione del rischio da parte delle persone (Bain Report, 2017). Secondo un rapporto dell'ONU, la popolazione mondiale di 7,6 miliardi di persone dovrebbe raggiungere 8,6 miliardi nel 2030, 9,8 miliardi nel 2050 e 11,2 miliardi nel 2100. Anche supponendo che i livelli di fertilità continuino a diminuire, il tasso di crescita della popolazione è pari a +1,6% all'anno. La riduzione del livello di fertilità si traduce principalmente in un rallentamento della crescita demografica con un aumento dell'età media globale. Considerata la tendenza globale, si prevede che il numero di persone di età superiore agli 80 anni triplicherà nel 2050, passando da 137 milioni nel 2017 a 425 milioni nel 2050 e 909 milioni nel 2100. L'invecchiamento della popolazione dovrebbe avere un

impatto profondo sulle società, sottolineando le pressioni fiscali e politiche che i sistemi sanitari, pensionistici e di protezione sociale di molti paesi dovranno probabilmente affrontare nei prossimi decenni.

1.2.1. Politica monetaria

I bassi tassi di interesse continuano a dominare i mercati; la FED[14] ha chiuso il 2018 con un aumento del tasso di interesse tra il 2,25-2,50%. Tuttavia, la FED ha preparato il mercato ad una possibile riduzione dei tassi nel 2019, suggerendo probabilmente uno scenario futuro di recessione. Mentre la BCE mantiene invariati a 0,00%, 0,25% e -0,40% il tasso di interesse sulle operazioni di rifinanziamento principale e i tassi di interesse sulle operazioni di rifinanziamento marginale e sui depositi presso la banca centrale. La natura eccezionale dello scenario economico pone nuove sfide per tutti gli

[14] La Federal Reserve Bank (o *Fed*), è la banca centrale responsabile della stabilità monetaria e finanziaria negli Stati Uniti. Fa parte di un sistema più ampio, noto come *Federal Reserve System*, con 12 banche centrali regionali, situate nelle principali città degli Stati Uniti.

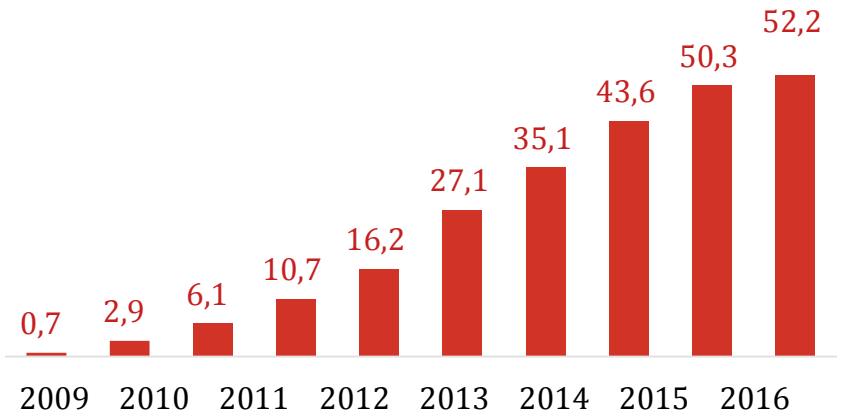
operatori economici, in particolare per gli assicuratori del ramo vita. In effetti, il ruolo socioeconomico svolto per tanti anni, come ad esempio nell'offrire soluzioni pensionistiche e nel finanziare l'economia può finire. Tuttavia, come affermato dal Rapporto dell'Associazione di Ginevra, l'esposizione delle diverse strutture delle compagnie di assicurazione sulla vita varia da un paese all'altro, il che comporta strategie di gestione del portafoglio da eseguire in funzione delle specifiche condizioni di mercato. I recenti annunci di aumenti tariffari da parte di Stati Uniti e Cina puntano in questa direzione. Una potenziale guerra commerciale potrebbe ridurre la crescita del PIL dei mercati interessati, compresi gli Stati Uniti, fino al 2% nel periodo 2018-2020. Ciò potrebbe avere un impatto negativo su I diversi rami assicurativi. Nel 2018 i paesi emergenti sono stati caratterizzati da politiche economiche divergenti, con un miglioramento generale delle condizioni di investimento, una bassa volatilità

finanziaria e una minore fragilità del settore bancario, una ripresa in alcuni settori merceologici e un rafforzamento delle prospettive macroeconomiche globali. Anche se vi sono diversi rischi che minacciano queste economie, come il tasso di inflazione, le valute deboli e l'aumento delle tariffe commerciali, il PIL dei mercati emergenti è cresciuto del 4,7% nel 2018 rispetto al 2017 e si prevede un aumento del 4,9% rispettivamente nel 2019 e nel 2020 (McKinsey, 2018). I premi dei mercati emergenti globali sono aumentati grazie alle economie emergenti trainate da un notevole incremento dei flussi di capitale, compresa la crescita transfrontaliera dei prestiti e del credito, sostenuta da bassi costi di finanziamento. Nel 2017, la quota di mercato emergente dei premi globali ha rappresentato il 18,8% del totale e si prevede che raggiungerà il 28% della quota totale in 10 anni. Il grafico 1 illustra la crescita dei premi Vita e Danni & Casualty relativi alle principali aree geografiche, mostrando il grande

potenziale dei mercati emergenti con l'Asia al primo posto in termini di crescita attesa dei premi. La Cina è il principale contributore dell'andamento positivo delle economie emergenti, trainato soprattutto dall'inarrestabile espansione del mercato cinese delle assicurazioni sulla vita. Tuttavia, per il 2019 si prevede un rallentamento della crescita della Cina rispetto ai risultati del 2016-17, in considerazione delle iniziative normative che incidono sulla vendita di prodotti di risparmio a breve termine e della richiesta di miglioramento della qualità delle vendite. Il numero globale di utenti internet ha raggiunto un nuovo record lo scorso anno, con 4 miliardi di persone che rappresentano oltre il 50% della popolazione totale. Nell'ultimo anno sono stati registrati quasi 250 milioni di nuovi utenti. La crescita massiccia del numero di utenti internet è stata trainata dagli smartphone accessibili e dai piani di dati mobili. Infatti, più di 200 milioni di persone hanno acquistato il loro primo dispositivo mobile nel 2017 e

più di 5,1 miliardi utilizzano attualmente un telefono

TAVOLA 1.2.1.: Crescita della quota mobile



cellulare. Il crescente interesse per Internet riguarda anche il tempo trascorso a navigare in rete - come di seguito illustrato nella TAVOLA 1.2.1. "Crescito della quota mobile" - con una media di sei ore al giorno per utente. Il digitale è diventato una parte essenziale della vita delle persone, influenzando le scelte dei consumatori e le decisioni aziendali. La ricca esperienza internet è in un continuo stato di flusso continuo. Si tratta dello sviluppo di nuovi telefoni oggi in uso, come l'aumento dei dispositivi connessi, l'ingresso vocale, la ricerca di immagini, il traduttore istantaneo e l'indirizzamento

visivo. L'Italia è caratterizzata da un mercato assicurativo maturo, basato sulla mutualità e spesso caratterizzato da un sistema di legacy[15] in atto. Gli investimenti in innovazione sono stati molto scarsi da decenni, soprattutto se confrontati con altri Paesi europei, più proattivi verso il cambiamento anche in un contesto di

affari tradizionali. Nonostante ciò, il mercato delle startup Insurtech inizia ad essere attivo anche in Italia, con alcune di esse in espansione oltre i confini nazionali. Nell'elenco che segue viene fornita una panoramica delle aziende più promettenti nate in Italia:

(i) Neosurance. Questa startup opera nel settore assicurativo istantaneo. Grazie all'ultima soluzione tecnologica adottata, è possibile per i clienti ricevere sul proprio smartphone proposte di copertura assicurativa in base alle loro reali

[15] Un sistema legacy, in informatica, è un sistema informatico, un'applicazione o un componente obsoleto, che continua ad essere usato poiché l'utente (di solito un'organizzazione) non intende o non può rimpiazzarlo.

esigenze. In questo modo sono in grado di coprire un singolo oggetto o un singolo arco di tempo. Fase di seed funding di Eu700k da diversi Business angels nel 2017

(ii) Axieme. Questa società opera nel campo delle assicurazioni peer-to-peer. Il modello si basa sulla possibilità di condividere il rischio di incidente con altre persone. Queste persone acquistano insieme una copertura assicurativa per un bisogno comune e in caso di assenza di sinistri, i premi raccolti dalla "folla" vengono restituiti agli abbonati.

(iii) YOLO. È il primo gruppo di fornitori di servizi assicurativi e di intermediazione, completamente digitale. You Only Live Once è un'innovativa piattaforma online che permette di attivare coperture assicurative pay-per-use e di

sottoscrivere coperture on demand tramite dispositivi mobili. L'assicuratore si occupa di viaggi, merci, coperture personali e salute. Aumento di capitale di di circa un milione di Euro registrato nel 2017.

(iv) Tiassisto24. Questa piattaforma ha lo scopo di aiutare gli agenti nella creazione e nell'acquisizione di lead online. Il modello funziona con un "marketplace" dove da un lato i clienti presentano la loro richiesta di copertura assicurativa con tutti i dettagli rilevanti, dall'altro le compagnie di assicurazione "competono" proponendo un'offerta al cliente che sceglierà quella migliore. In questo modo i consumatori possono ottenere prezzi più bassi e gli assicuratori possono migliorare la qualità del loro portafoglio eseguendo un'offerta *ex ante*. Per concludere questa panoramica sul mercato assicurativo

italiano, vale la pena di notare come l'offerta assicurativa italiana sia in forte ritardo rispetto a quella di altri Paesi europei, soprattutto per quanto riguarda i premi per l'assicurazione Non Auto. Questo lascia spazio all'introduzione di molte soluzioni innovative e su misura per soddisfare le esigenze dei clienti. Pertanto, anche in Italia, la condivisione dell'economia, la riduzione dei premi e la digitalizzazione sono pilastri fondamentali su cui fare leva per attrarre i clienti più giovani e costruire un rapporto più stretto, trasformando il business dalle radici.

1.3. Gli investimenti delle imprese assicurative

Gli algoritmi fanno parte dell'IA[16], dove ovvero esiste la programmazione per realizzare un compito a determinate

[16] L'intelligenza artificiale è una disciplina recente che negli anni ha fornito un importante contributo al progresso dell'intera informatica. Essa è stata inoltre influenzata da numerose discipline fra le quali la filosofia, la matematica, la psicologia, la cibernetica, le scienze cognitive. L'intelligenza artificiale studia i fondamenti teorici, le metodologie e le tecniche che consentono di progettare sistemi hardware e sistemi di programmi software atti a fornire

condizioni. Algoritmi ben noti includono sistemi di navigazione stradale o giochi di scacchi per computer. Nel settore finanziario, il trading algoritmico, come il trading ad alta frequenza, è molto diffuso, con istruzioni di trading pre-programmate per eseguire ordini di trading di grandi dimensioni. L'algoritmo seguirebbe una serie di istruzioni condizionali per effettuare un ordine di compravendita ad una velocità e frequenza che non è possibile per un trader umano.

La consulenza robotica, o consulenza automatizzata, sta diventando sempre più importante, in particolare per le piattaforme di investimento e di risparmio online. Può coprire un'ampia gamma di servizi, ma è essenzialmente un "modello di consulenza automatizzata on-line che ha la capacità di fornire consulenza in modo più efficiente in termini di costi" (HM Treasury and FCA, 2016). Per il settore assicurativo, la consulenza robotizzata per la

---

all'elaboratore elettronico prestazioni che, a un osservatore comune, sembrerebbero essere di pertinenza esclusiva dell'intelligenza umana.

gestione degli investimenti è in fase di sviluppo e viene sempre più utilizzata per le quotazioni con consulenza automatizzata e offerte calcolate tramite algoritmi. Invece di una consulenza diretta o combinata con una consulenza diretta, la consulenza robotica può fornire una guida e un'esecuzione automatizzata su varie decisioni finanziarie. La consulenza automatizzata potrebbe aiutare le tasche della popolazione che non hanno accesso alla consulenza finanziaria a ottenere un contributo in modo più efficiente in termini di costi rispetto a un consulente umano. Tuttavia, a seconda di come è strutturato l'algoritmo che fornisce la consulenza, potrebbe anche portare a consigli inadeguati che vengono forniti inavvertitamente.

Per "contratto intelligente" si intende qualsiasi contratto che sia in grado di autoesecuzione o di esecuzione. Sono scritte come codice di programmazione che può essere eseguito su un computer o una rete di computer piuttosto che in linguaggio legale su un documento stampato. Questo codice può definire regole e conseguenze rigorose

che emulano un documento giuridico tradizionale, indicando gli obblighi, i benefici e le sanzioni dovute a entrambe le parti che si trovano in varie circostanze. I contratti intelligenti consentono alle persone di commerciare e fare affari con sconosciuti, di solito utilizzando Internet, senza la necessità di un grande sito di un'autorità centralizzata per fungere da intermediario. Il limite di un contratto intelligente è che un programma può non sapere cosa sta accadendo nel mondo fisico o reagire a eventi imprevisti, non essendo quindi in grado di eseguire un'azione che era alla base del contratto.

I contratti intelligenti spesso si basano su catene di blocchi o sulla tecnologia di contabilità distribuita (DLT). Un esempio di contratto intelligente che utilizza DLT è una valuta criptata, come il Bitcoin. Ethereum è una delle più grandi piattaforme per contratti intelligenti e blockchains. La tecnologia Blockchain o distributed ledger (DLT) è un protocollo per lo scambio di valori o dati su Internet che non richiede un intermediario. Il protocollo della

tecnologia blockchain è quello di creare un database condiviso e criptato delle transazioni e di altre informazioni. Esempi di formiche e greggi di oche sono stati dati per dimostrare come sarebbe una società a catena di blocco perfetta; decentrata ma coordinata. La tecnologia è quella di stabilire una catena sempre più lunga di blocchi di dati. Ogni blocco ha un registro compatto delle transazioni convalidate dai partecipanti alla blockchain, e la premessa della blockchain è che le informazioni nei blocchi sono vere. Una volta che la transazione è stata convalidata e registrata, la registrazione memorizzata è irreversibile. Blockchain originariamente si riferiva al database dove tutte le transazioni Bitcoin sono registrate e memorizzate. Il 2015 ha visto livelli di finanziamento record per l'AssicurTech, con finanziamenti stimati in totale a 2 669 miliardi di dollari USA. Nel terzo trimestre del 2016 i livelli di finanziamento sono stati pari a 1 401 miliardi di dollari USA e il numero di transazioni nel terzo trimestre del 2016 è stato di 126, già superiore al numero

di transazioni nel 2015 (cfr. figura 1). Va notato che nel 2015, quasi 1/3 dei finanziamenti è andato a Zhong An, un assicuratore cinese che è stato fondato nel 2013 con il sostegno di Alibaba Group Holding, che ha raccolto 931 milioni di dollari nel 2015, e che si dice stia pianificando una IPO. Il settore assicurativo si è recentemente interessato alle applicazioni Blockchain. Alcune grandi compagnie hanno effettuato importanti investimenti per esplorare e sfruttare le potenzialità di questa tecnologia per il loro business, puntando alla semplificazione delle attività operative e alla fornitura di nuovi prodotti. Entrando nel segmento P&C, la capacità di auto esecuzione di contratti intelligenti abilitati dalla tecnologia Blockchain supporterà l'alleggerimento dei processi operativi aziendali, ad esempio accelerando la gestione dei sinistri riducendo lo sforzo umano. L'obiettivo è quello di fornire un'esperienza senza soluzione di continuità ai clienti che possono ricevere il loro denaro anche prima di reclamarlo, dal momento che il contratto si esegue

automaticamente quando viene rilevato un incidente e rimborsa l'abbonato non appena l'evento si verifica (e non appena vengono definite le responsabilità). Un esempio è l'assicurazione contro i ritardi, in cui i contratti intelligenti potrebbero rimborsare automaticamente i viaggiatori in caso di ritardo del volo o del treno. Attraverso i contratti smart scompaiono anche molte ambiguità legate ai tradizionali contratti testuali, poiché tutte le clausole sono codificate nel sistema di contratti smart che si autoabilita. I contratti smart potrebbero abilitare le polizze assicurative *pay-per-use*, affidandosi all'internet degli oggetti per l'attivazione automatica. I premi assicurativi di viaggio, ad esempio, potrebbero essere riscossi solo se le coordinate GPS dei clienti confermano che si trovano all'estero, o i premi assicurativi per le auto pagati solo quando i clienti stanno guidando. D'altra parte, esistono molti svantaggi, legati alla mancanza di efficienza dei libri contabili distribuiti esistenti rispetto alle soluzioni già esistenti e alla necessità di sviluppare ecosistemi che rendano ragionevole

la creazione di una rete Blockchain. Mentre la ripartizione degli investimenti nel settore assicurativo non è disponibile, gli investimenti nell'assicurazione malattia sono considerati forti e in crescita, assorbendo il 70% degli investimenti di InsurTech negli Stati Uniti. Allo stesso tempo, gli investimenti in start-up che forniscono canali di distribuzione commerciale sono aumentati in misura considerevole. Le start-up del ramo vita e delle rendite più in generale stanno attirando ingenti investimenti, così come le start-up di assicurazioni dedicate alla linea retail. Inoltre, gli assicuratori stanno fornendo strutture di finanziamento che consentirebbero loro di avere la possibilità di scegliere tra nuove tecnologie e innovazioni di successo che potrebbero sostenere le loro operazioni esistenti e migliorare l'esperienza dei clienti. Ciò è stato possibile sia attraverso opportunità di finanziamento generale dei VC, sia attraverso investimenti mirati di InsurTech, nonché attraverso la creazione di incubatori che ospitano imprenditori e dipendenti InsurTech. Diversi

assicuratori hanno fornito investimenti alle nuove imprese InsurTech e alle start-up di Internet of Things (IoT). Il panorama più ampio dei finanziamenti per InsurTech è descritto sopra, ma uno sviluppo più interessante è stato il modo in cui i riassicuratori stanno finanziando l' InsurTech. Alcuni dei maggiori assicuratori hanno creato fondi specifici e fondi di capitale di rischio per investire in start-up, anche per l'AssicurTech, indicando la probabilità di un maggiore investimento in InsurTech, e gli investimenti strategici che gli assicuratori esistenti faranno per assicurarsi di avere una partecipazione in una start-up che potrebbe essere in grado di scalare la loro attività. Riflettendo il panorama più ampio dell'InsurTech, ma con alcune differenze specifiche, i riassicuratori statunitensi stanno effettuando la maggior parte degli investimenti in InsurTech, con il 64% delle operazioni effettuate (a differenza dell'effettivo livello di finanziamento, per il quale non sono disponibili dati. Molto probabilmente riflettendo gli investimenti che Ping An Insurance ha fatto

a Zhong An, e Taipang Insurance ha fatto in Alibaba Health, gli investimenti riassicurativi cinesi rappresentano il 10% delle operazioni effettuate da riassicuratori. È possibile che, data la minore penetrazione dell'assicurazione in Cina, si preveda che il mercato possa svilupparsi sulla base dei nuovi modelli di intermediazione che si stanno introducendo in Cina. Gli riassicuratori francesi e britannici effettuano rispettivamente l'11% e il 6% delle operazioni degli riassicuratori (CB Insight, 2017). Molti degli accordi sono stipulati dal braccio strategico dei riassicuratori di VC. Ping An Venture ha effettuato alcuni dei maggiori investimenti in AssicurTech con oltre 20 operazioni. Axa Strategic Ventures ha anche completato 20 operazioni e insieme a Ping An sono stati i più attivi nella realizzazione di investimenti strategici. Gli assicuratori statunitensi MassMutual Venture, USAA, American Family Ventures, Transamerica e New York Life seguono con cinque o dieci contratti ciascuno. Dopo di che, gli assicuratori europei Allianz Ventures,

MunichRE/HSB Ventures e Aviva Ventures continuano. Più storicamente, Axa Strategic Ventures, Transamerica Ventures e American Family Ventures sono stati gli investitori più attivi nell'investimento tecnologico privato dall'inizio del 2012. Axa ha fornito finanziamenti di avviamento per cinque start-up europee nell'ambito di un fondo istituito in Francia nel 2013, prima del lancio di Axa Strategic Ventures nel 2015. Il fondo di venture capital di 200 milioni di euro (223,47 milioni di USD) ha il mandato di investire in innovazioni nel settore assicurativo, nell'asset management, nella tecnologia finanziaria e nei servizi sanitari. Axa ha creato Kamet nel 2015, che è un incubatore InsurTech da 100 milioni di euro che lavora con imprenditori interni ed esterni. Axa ha recentemente investito 75 milioni di euro per acquisire una partecipazione dell'8% nella società di e-commerce Africa Internet Group ed è diventata l'unico fornitore di assicurazioni attraverso Jumia e altre piattaforme.

Allianz ha creato Allianz Ventures come centro per gli investimenti e le partnership con start-up, con l'obiettivo di focalizzarsi su cinque aree chiave: AssicurTech e gestione patrimoniale; mobilità e auto connesse; case e proprietà connesse; salute digitale; sicurezza informatica e intelligenza dei dati. Gli investimenti recenti includono una partecipazione minoritaria nel gestore patrimoniale digitale MoneyFarm. Allianz X è il "costruttore d'impresa" del gruppo che identifica, costruisce e scalare nuovi modelli di business nell'ambito dell'AssicurTech e in settori correlati come la catena a blocchi e l'intelligenza artificiale.

Aviva ha lanciato una divisione di venture capital per investire in nuove attività digitali alla fine del 2015, con sede a Hoxton Square, il centro degli imprenditori digitali londinesi, con un fondo annuale di circa 20 milioni di sterline (24,8 milioni di dollari) da investire nei prossimi cinque anni. Il suo primo investimento è stato in Cocoon, un dispositivo intelligente per la sicurezza della casa che avverte i proprietari degli spostamenti e del suono

all'interno della loro proprietà. Nel maggio 2016, Aviva ha annunciato una partnership con Founders Factory, un acceleratore digitale e incubatore, diventando il suo partner finanziario esclusivo per i prossimi cinque anni, fornendo capitali e risorse per sostenere la crescita di oltre 200 aziende tecnologiche. Munich Re ha effettuato investimenti attraverso la sua divisione HSB Ventures in Slice Labs, un fornitore statunitense di assicurazioni on-demand, che ha lanciato un prodotto per gli host di homesharing utilizzando piattaforme come Airbnb, HomeAway, OneFineStay e FlipKey. L'assicurazione dura specificamente per il tempo in cui il proprietario agisce come un'azienda in modo che gli assicurati possono acquistare la copertura solo quando ne hanno bisogno. Munich Re si è assicurata il diritto di fornire capitale di sottoscrizione e licenze assicurative per l'assicuratore su richiesta Trov sul mercato statunitense. L'app di Trov consente ai clienti di assicurare singoli elementi come l'elettronica o le attrezzature sportive dal proprio smartphone e dà loro la possibilità di attivare e

disattivare la copertura quando necessario. Nell'aprile 2016, la serie B di Helium da 20 milioni di dollari USA è stata guidata dal ramo d'impresa GV, ma anche Munich Re/HSB Ventures ha partecipato. La tecnologia dei sensori Helium risiede nella sua capacità di utilizzare un sensore standard e collegarlo al Cloud Helium che permette al sistema operativo di controllare la temperatura di stoccaggio. In questo modo l'uso di tale tecnologia può proteggere da responsabilità derivanti, ad esempio, dal lasciare il frigorifero aperto in un ristorante o in un ospedale che non gestisce le scorte di vaccini.

Ping An Ventures ha investito attivamente nel settore sanitario.

La maggior parte degli riassicuratori sulle imprese di assicurazione o di riassicurazioni ha investito pubblicamente nelle nuove imprese solo negli ultimi due anni e nei settori in cui gli riassicuratori ritengono che vi sia una domanda di massa e un'applicazione pratica alle loro imprese.

Axa Strategic Ventures, AIG e American Family Ventures hanno investito in start-up dell'internet degli oggetti in auto, casa, industriale e altri segmenti, mentre Axa, AmFam, USAA e MunichRe/HSB hanno effettuato investimenti separati per l'internet degli oggetti.

1.4. Canali distributivi attraverso nuovi modelli

Come anticipato, l'industria assicurativa vive un momento di transizione: quello che oggi chiamiamo "*InsurTech*" - riferendoci a tutto ciò che è innovazione *technology driven* nell'industria assicurativa - potrà avere impatti rilevanti per l'intero comparto. Ad esempio, la tecnologia *mobile*, che comprende smartphone, tablet e app, ha avuto un enorme impatto negli ultimi anni nella vita delle persone e delle aziende.

Le app sono lo strumento adatto per una relazione più intima con il cliente; a testimonianza di questo, le nuove versioni introdotte nel mercato presentano un maggiore orientamento alle sue esigenze rispetto alle precedenti. Se

inizialmente rivestivano un ruolo comprimario nell'offerta dei servizi assicurativi, le applicazioni per *smartphone* stanno ora attuando delle sofisticazioni che introducono interessanti profili di innovazione. Al riguardo si segnala una app che, da un lato, offre agli intermediari un'interazione con la clientela in tempo reale, dall'altro consente al cliente e alla sua famiglia di monitorare la situazione assicurativa complessiva, ricevere assistenza attraverso i sistemi di localizzazione, avere alla portata offerte e polizze in tempo reale. Secondo quanto riportato dall'*IVASS*[17], il quadro generale del mercato assicurativo italiano, caratterizzato da un calo della produzione, mostra nei primi sei mesi del 2018 segnali di vivacità nel lancio di nuove offerte, anche nel modo di concepire le varie tipologie di coperture per rispondere alla crescita diffusa di incertezza e all'aumento dei connessi bisogni di protezione da parte di persone e imprese. Cambiano gli stili di vita

[17] L'Istituto per la vigilanza sulle assicurazioni (noto con l'acronimo IVASS) è un'autorità amministrativa indipendente che esercita la vigilanza sul mercato assicurativo italiano, per garantirne la stabilità e tutelare il consumatore.

degli italiani e cambiano anche le assicurazioni, che consentono di tutelarli con prodotti nuovi. Per le polizze sull'abitazione e a tutela della persona spesso si ricorre a formule modulari, uno strumento che scompone i prodotti nelle loro garanzie principali e che consente al cliente di ricostruire un *package* su misura. Sono sempre più diffuse le partnership e le sinergie tra compagnie e le startup *InsurTech*. Attualmente in Italia il settore danni sembra essere quello maggiormente influenzato, registrando un forte cambiamento soprattutto nelle aree che ruotano intorno alle coperture assicurative auto, casa e persona. Concentriamo quindi il focus della nostra analisi sui settori assicurativi *Motor*, *Healt & Home*, indagando come questi sono influenzati dalla digitalizzazione.

1.4.1. P2P insurance

La condivisione dell'economia è diventata un concetto diffuso in tutto il mondo, in vari settori industriali. Questo principio si scatena grazie al rapido e innovativo sviluppo

tecnologico. Esistono piattaforme ben note come Airbnb e Booking.com, con l'obiettivo di rivoluzionare il settore dell'ospitalità. O quelle come Uber e BlaBlaCar, che forniscono entrambe soluzioni di condivisione dei trasporti all'interno della città e tra città, rispettivamente. Nel settore bancario, stanno emergendo molti prestatori P2P, come il LendingClub, il Funding Circle, ecc.

L'impatto principale di tutte queste piattaforme è l'eliminazione dei tradizionali concetti di business, intermediari e costose infrastrutture. Di conseguenza, tutte le aziende ottengono una riduzione dei costi per i clienti finali.

Alcuni dei più popolari giocatori di assicurazione P2P[18] in tutto il mondo sono Friendsurance, Lemonade, Inspeer, PeerCover, Guevara, TongJuBao, ecc. I prodotti offerti da queste start-up sono presenti in tutte le linee di business,

[18] La tecnologia di rete logica Peer to Peer, abbreviata anche come P2P, permette di creare una rete dove non esistono server e client esclusivi, poiché ogni dispositivo collegato è sia client che server. Lo sviluppo di questa rete logica è dovuto alla possibilità di condividere con gli altri i dati presenti sul proprio PC.

inclusi Vita, Salute e P&C. Tuttavia, la maggior parte di loro sono specializzati in una sola linea di prodotti. Sono tutti caratterizzati da modelli di business simili, in formati leggermente diversi. L'idea principale alla base del concetto di assicurazione P2P è quella di creare un pool comune finanziato dai membri della comunità che sono disposti a condividere il rischio insieme. Questi gruppi di membri sono formati online. In alcuni casi il pool viene creato da membri della comunità/famiglia, sottolineando la fiducia tra loro, mentre in alcuni modelli i pool vengono creati da membri che non hanno relazioni personali. Il secondo modello è ragionevolmente più scalabile, ma con un livello inferiore di fiducia tra i membri. Potenzialmente, questo può essere un potenziale fattore scatenante per il problema delle false dichiarazioni. Questo problema sembra essere una delle maggiori sfide che gli assicuratori P2P non comunitari si trovano ad affrontare.

Normalmente, le società P2P addebitano una commissione

per il suo funzionamento, ad esempio, Lemonade addebita una commissione fissa del 20%. Una parte dei fondi è utilizzata a fini riassicurativi. Vale a dire, il player di assicurazione P2P deve rimanere protetto contro gli scenari avversi quando il pool assicurativo è vuoto. ad esempio, Lemonade è riassicurato presso i Lloyd's di Londra, pagando per la riassicurazione circa il 20% del valore del pool. Molto probabilmente, l'elemento più interessante offerto dalle P2P InsurTechs, è la possibilità di ottenere rimborsi dal pool, nei casi in cui ci sono ancora delle disponibilità nel pool alla fine dell'anno. Gli assicurati possono utilizzare il denaro o possono anche prorogare la loro polizza assicurativa per l'anno successivo senza alcun trasferimento e le relative spese di transazione. Nel caso della Lemonade, esiste una polizza "Restituzione", in base alla quale il denaro rimasto nel pool viene trasferito a cause scelte dai membri al momento dell'acquisto di una polizza assicurativa.

In conclusione, le piattaforme assicurative P2P riescono a

portare fiducia reciproca e un modello di business e di pricing trasparente ai membri della comunità e agli assicurati, a ridurre la necessità di infrastrutture e personale costosi, riducendo così i costi fissi e operativi, e ad aumentare la customer experience offrendo nuove funzionalità e riducendo il premio totale pagato.

1.4.2. Motor

I dispositivi telematici automatici sono piccoli gadget inseriti nelle auto e solitamente collegati a qualche applicazione per trasmettere e presentare i dati. Questi dispositivi sono dotati di sensori che consentono loro di tracciare e monitorare il comportamento di guida, come la velocità, la distanza percorsa, le accelerazioni e le frenate brusche. Sono anche in grado di localizzare un'auto, analizzare il consumo di carburante, fornire avvisi di manutenzione basati sulla diagnostica del veicolo, registrare gli incidenti, fornire assistenza stradale, ecc. Tutte queste funzionalità portano ad un nuovo livello di

esperienza per i conducenti.

Tuttavia, le compagnie di auto telematica hanno un enorme potenziale nel settore assicurativo. Più precisamente, questi dispositivi consentono alle compagnie di assicurazione di raccogliere dati sui loro clienti, che servono come input preziosi per la determinazione dei prezzi e la sottoscrizione dei prodotti assicurativi auto. In questo modo, le compagnie di assicurazione sono in grado di abolire parzialmente la polizza "one price" per tutti i clienti e di adattare i premi assicurativi ai profili di rischio dei loro clienti. Inoltre, la tecnologia telematica automatica consente di ottenere sconti premium in base ai modelli di guida registrati. La funzionalità che molti di questi giocatori offrono è il supporto in caso di emergenza. Alcuni dei dispositivi telematici automatici possono registrare gli incidenti d'auto e avviare automaticamente le chiamate di emergenza. Questa funzionalità può facilmente prevenire incidenti mortali. Alcuni dei giocatori più popolari in

questo campo sono TrueMotion, Metromile, DriveWay, DriveSpotter, Telematic, Citymile, Accscore, Zubie, ecc. Ci sono alcuni esempi di partnership tra start-up di autotelematica e compagnie di assicurazione. In particolare, Progressive ha collaborato con Zubie per fornire agli assicurati un modello di pricing basato sui premi. Si prevede di sfruttare i punteggi di guida da Zubie, per offrire sconti premium per i conducenti sicuri. Il concetto di telematica automatica apre lo spazio per prodotti assicurativi basati sull'uso. Ci sono quindi esempi come TrueMotion, che offre agli assicuratori una piattaforma end-to-end per fornire prodotti assicurativi basati sull'uso. Tuttavia, ci sono esempi come Cuvva, che riesce a distribuire direttamente la polizza di assicurazione auto basata sull'uso senza l'uso di dispositivi telematici, ma solo con l'applicazione mobile. Aviva, una compagnia di assicurazioni, ha creato anche l'applicazione Aviva Drive per fornire sconti sui premi. AXA ha inoltre sviluppato l'applicazione Drive Coach per consentire agli

utenti di analizzare, modificare e migliorare il loro comportamento di guida. Allo stesso tempo, consentirà di definire un modello di prezzo su misura. Tutte queste applicazioni sono in grado di monitorare il comportamento di guida tramite sensori mobili. Queste soluzioni consentono potenzialmente alle compagnie di assicurazione di fissare meglio i prezzi dei loro prodotti e, di conseguenza, di ridurre i costi di rischio/capitale. In particolare, se la compagnia di assicurazione è in grado di gestire meglio il rischio, all'inizio dell'anno sarà in grado di destinare meno risorse alle riserve di capitale destinate alla gestione dei sinistri.

1.4.3. Wereables

Gli oggetti da indossare sono dispositivi elettronici intelligenti (dispositivi elettronici con microcontrollori) che possono essere indossati sul corpo come impianto o accessori. Gli oggetti da indossare sono un buon esempio della tecnologia dell'internet degli oggetti, in quanto

"cose" come l'elettronica, il software, i sensori e la connettività sono dispositivi che consentono agli oggetti di scambiare dati attraverso internet con un produttore, un operatore e altri dispositivi collegati, senza richiedere l'intervento umano. In quanto tali, gli oggetti da indossare sono abbastanza applicabili all'attività assicurativa, così come la linea di prodotti Salute e Vita.

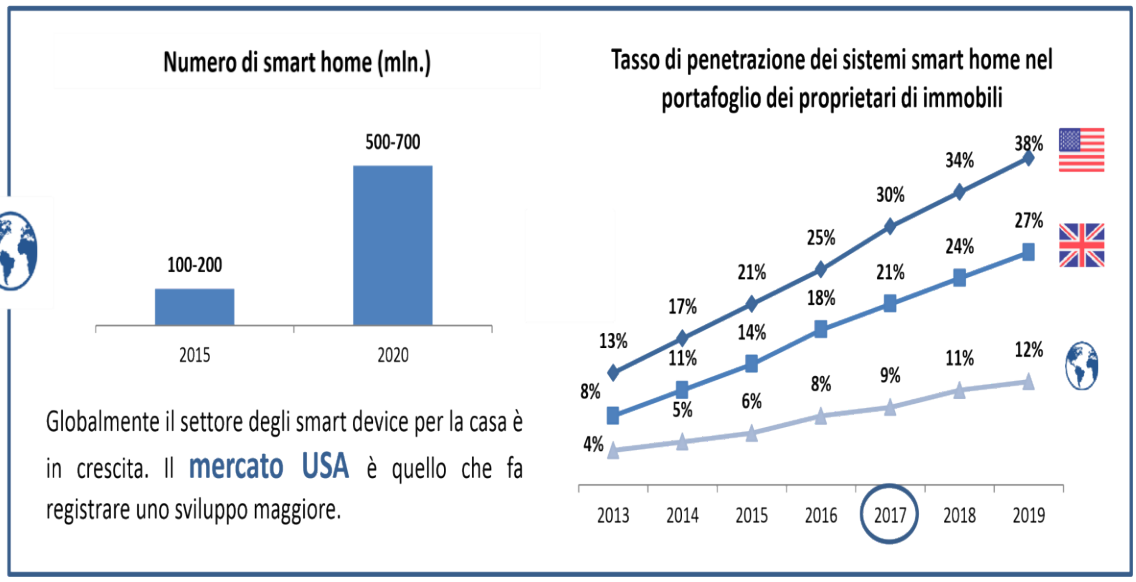
Gli oggetti da indossare sono in grado di tracciare lo stile di vita utilizzando sensori incorporati. In genere si collegano con il software per inviare dati approssimativi per ulteriori interpretazioni. La raccolta dati e il monitoraggio sanitario in tempo reale rendono la tecnologia degli articoli indossabili molto utilizzabile nel settore assicurativo. Questa tecnologia consente di migliorare la tariffazione e la sottoscrizione delle polizze assicurative. Consente inoltre un'offerta di sconti sui premi, che si basa esclusivamente sullo stile di vita dell'assicurato. Dispositivi indossabili collegati all'applicazione mobile sono adatti anche quando si tratta

di fitness coaching, imparando ai consumatori cosa fare e come vivere in modo più sano. Alcuni dei giocatori più noti in quest'area sono FitSense e Sureify. Un buon esempio è FitSense, che agisce come un prodotto con etichetta bianca che consente alle compagnie di assicurazione di impegnarsi con i clienti e personalizzare le loro polizze assicurative sfruttando i dati raccolti tramite dispositivi indossabili e digeriti attraverso l'applicazione mobile. Anche le compagnie di assicurazione mirano a sviluppare una propria soluzione interna. AXA ha sviluppato una piattaforma Health Keeper che viene distribuita sotto forma di app, progettata per aiutare i clienti a tenere traccia delle loro attività, ottenere l'accesso ai servizi sanitari e di benessere, ecc. Analogamente alla telematica automatica, gli oggetti da indossare facilitano anche una migliore gestione del rischio e una politica dei prezzi su misura. Di conseguenza, riduce i costi di rischio/capitale. Inoltre, aumenta anche l'esperienza del cliente.

1.4.4. Home Insurance

Nell'area *Property* gli Stati Uniti detengono il ruolo di leader del mercato, mentre l'Italia si sta appena affacciando nel settore (OECD, 2017).

TAVOLA 1.4.4. Numero di smart home



Stare al passo con i bisogni specifici del cliente e offrire, quindi, prodotti maggiormente personalizzati è la nuova linea che diverse imprese stanno già mettendo in atto, con polizze multirischio che, nei casi più all'avanguardia, si

integrano con l'ingegneria domotica e con la tecnologia dell'*IoT*[19]. L'interesse nelle soluzioni *smart home* non è solo incentrato sulla sicurezza dell'abitazione ma anche sul risparmio energetico.

In Italia il comparto *Property* è fortemente sotto assicurato: il 16% dei principali gruppi assicurativi italiani offre polizze con abbinati *device IoT*; l'84% dei gruppi assicurativi italiani non ha integrato le loro polizze *property* con dispositivi *IoT*, ma si limita ad offrire coperture tradizionali (incendio, furto, RC capofamiglia) e alcuni servizi in partnership con centri di riparazione convenzionati.

Il comparto *property* europeo offre in generale un limitato numero di polizze abbinate a dispositivi *IoT*. Quelle presenti si basano su servizi semplici come *alert* via SMS. Le compagnie stanno valutando se entrare in questo

[19] L'Internet of Things (IoT o Internet delle cose) è una tecnologia che permette di massimizzare le capacità di raccolta e di utilizzo dei dati da una moltitudine di sorgenti (prodotti industriali, sistemi di fabbrica, veicoli di trasporto…) a vantaggio di una maggiore digitalizzazione e automazione dei processi, della facoltà di sfruttare machine learning e intelligenza artificiale per creare nuovi business e servizi a valore per clienti e consumatori

comparto in modo più incisivo, considerando la forte componente tecnologica e concorrenza di *big player*. Seguendo alcune *best practice* internazionali, una possibile soluzione potrebbe prevedere partnership con aziende tecnologiche per sviluppare prodotti e servizi evoluti.

Nel 1° semestre del 2017 le compagnie assicurative italiane, come riscontrato nella seconda metà del 2016, proseguono nel lancio di polizze multirischio, talvolta contraddistinte dall'uso della tecnologia, come nel caso di un nuovo prodotto che si serve di un dispositivo *home box* per segnalare eventuali allarmi, notifiche all'utente tramite app sul proprio smartphone, con l'ausilio di diversi sensori. Tutti i *devices* sono autoinstallanti e in comodato d'uso e con la formula *full optional* (in quella Base, per ogni utenza della casa, è prevista l'assistenza con l'invio di personale qualificato in loco e l'estensione di garanzia degli elettrodomestici per difetto di conformità).

1.4.5. Comparatori ed Aggregatori

I siti web di comparazione dei prezzi sono già diventati di moda per molte nicchie di mercato. La gente li usa per confrontare i prezzi di vari beni, servizi finanziari, carte di credito, prestiti, voli, ecc. Queste aziende collaborano con i rivenditori e li servono come affiliati/broker. Questi partner sono a pagamento per ogni acquirente che ha visitato il loro sito web attraverso il sito web di confronto dei prezzi, o per ogni visitatore, a seconda del trattato compilato. A tale riguardo, i siti di confronto dei prezzi rappresentano i generatori di piombo per un'impresa che vende il prodotto. Gli aggregatori generano "traffico caldo" per le aziende che hanno i loro prodotti elencati sul sito web di confronto dei prezzi. "Traffico caldo" è declinabile in maniera efficace per i clienti già alla ricerca di un prodotto specifico, che sono, ragionevolmente, più propensi a maturare l'atto d'acquisto. Tuttavia, questi siti sono abbastanza popolari anche nel settore assicurativo. I siti web di confronto dei prezzi delle assicurazioni

consentono al cliente finale di cercare il prodotto assicurativo necessario e di ottenere preventivi da varie compagnie di assicurazione. Automaticamente, può confrontare tra più polizze assicurative e selezionare quella più adatta. Attraverso il sito web, un cliente può anche acquistare un prodotto, poiché gli aggregatori lo reindirizzano direttamente alla compagnia di assicurazione/sito del broker che vende una particolare polizza assicurativa per la quale ha optato. Alcuni dei giocatori famosi in quest'area sono Confused.com, GoCompare.com, Moneysupermarket, PolicyBazaar, BankBazaar.com, HealthCare.com, ecc. Queste aziende ha già ottenuto grandi successi e volumi, diventando uno dei principali canali di distribuzione assicurativa nell'era moderna. Tutti questi siti web sono utilizzati gratuitamente dai clienti. Prendono un taglio dalla compagnia di assicurazione per ogni prodotto assicurativo distribuito attraverso la piattaforma. Gli aggregatori agiscono come moderni broker, facendo tutto il business online e mirando

a trasformarsi in soluzioni scalabili con una vasta base clienti, per diventare partner di vendita cruciali per i grandi incumbent assicurativi. Di conseguenza, le compagnie di assicurazione possono ridurre i costi di acquisizione clienti e di marketing, utilizzando queste piattaforme di distribuzione. Allo stesso tempo, ai clienti viene garantita una maggiore trasparenza nel processo decisionale.

1.4.6. Sharing Economy

L'intera catena del valore assicurativo può essere perturbata da nuovi modelli di business basati sulla condivisione dell'economia e sulla digitalizzazione che porteranno a cambiamenti radicali nei prodotti, nel marketing, nei prezzi e nella distribuzione. Man mano che i prodotti condivisi si diffondono sempre più, soprattutto tra i giovani, le compagnie devono fornire un'assicurazione senza eredità per dare agli utenti un prodotto immediato, intelligente e con un'esperienza senza

soluzione di continuità. Un punto cruciale per sfruttare questo mercato, che si prevede crescerà ad un ritmo molto rapido anche negli anni a venire, è la capacità degli assicuratori di rendere le persone consapevoli dei potenziali rischi in cui incorrono utilizzando prodotti condivisi. Gli assicuratori hanno la possibilità di aumentare i ricavi sviluppando prodotti specifici per la condivisione delle attività economiche, concentrandosi sulla condivisione delle corse, sulla condivisione degli spazi di casa e degli uffici. La differenziazione tra gli assicuratori sarà data dalla loro reputazione, dall'esperienza degli utenti che saranno in grado di fornire e dalla varietà dei prodotti offerti.

La forza lavoro su richiesta è un'altra tendenza rilevante. La cosiddetta Gig Economy sta creando nuovi lavoratori e, allo stesso tempo, un nuovo bisogno di assicurazioni. Le coperture personali sulle automobili o le tradizionali assicurazioni per responsabilità civile non pagano i sinistri quando si utilizzano gli articoli per il lavoro. Una

soluzione in questo contesto potrebbe essere quella di offrire una copertura non per la responsabilità civile, ma per la copertura personale (ad esempio contro le malattie). Questa tendenza lascia spazio alla disintermediazione effettuata dalle piattaforme stesse (ad esempio Uber, Airbnb). Gli assicuratori devono seguire rapidamente questa tendenza e coprire questi margini di attività non sfruttati.

2. REGOLAMENTAZIONE NELL'INSURTECH E RISCHI EMERGENTI

2.1. *Regolamentazione assicurativa*

Mentre le innovazioni sono in genere uno sviluppo positivo, vi sono una serie di potenziali ramificazioni politiche e normative che possono creare incertezze e limitazioni nello sviluppo delle imprese. In termini di politica di concorrenza, la possibilità di avere nuovi operatori sul mercato attraverso l'applicazione di innovazioni e nuove tecnologie potrebbe portare a una

maggiore utilità per i consumatori. La logica del diritto o della politica di concorrenza è quella di migliorare il benessere dei consumatori e l'efficienza della produzione e dell'offerta, il che porterebbe a prezzi più bassi e a una scelta più ampia. La possibilità di nuovi concorrenti sotto forma di start-up e una scelta più ampia grazie all'innovazione e alla tecnologia potrebbe determinare una serie di sviluppi positivi per la concorrenza nel mercato assicurativo.

Quando le start-up vogliono diventare assicuratori o broker assicurativi, esistono requisiti potenzialmente proibitivi, in particolar modo legati alla capacità economica da soddisfare che assume vesti differenti anche nei vari paesi dell'Unione Europea. Forse per questo motivo, ci sono pochissime start-up InsurTech che hanno ottenuto licenze di sottoscrizione assicurativa, e la maggior parte ha licenze da broker. Anche se a fini prudenziali questi requisiti sono una pietra angolare importante per garantire la tutela degli assicurati, essi potrebbero potenzialmente costituire un

ostacolo all'ingresso di nuovi operatori sul mercato, se del caso. Nel settore finanziario vi è una costante tensione sul giusto equilibrio tra regolamentazione finanziaria e concorrenza, e questo è molto importante nel contesto delle tecnologie innovative.

Per affrontare questo problema, alcune autorità di regolamentazione finanziaria hanno creato piattaforme per consentire alle start-up FinTech di sperimentare la loro tecnologia e allentare alcuni dei requisiti normativi all'interno della piattaforma. L'Innovation Hub della Financial Conduct Authority (FCA) del Regno Unito è uno dei primi ad applicare l'approccio "regulatory sandbox". Anche l'Autorità Monetaria di Singapore (MAS) ha adottato l'approccio "sandbox" normativo. L'Australia's Securities and Investment Commission (ASIC) ha istituito un Innovation Hub per mitigare i rischi, impegnandosi tempestivamente con gli innovatori FinTech e aiutando i nuovi entranti a comprendere i requisiti normativi. Negli ultimi mesi anche la Hong Kong Monetary Authority e la

canadese Ontario Securities Commission hanno lanciato piattaforme simili. Queste piattaforme sono tutte concepite per favorire l'ingresso di nuovi operatori che incoraggerebbero una maggiore concorrenza e innovazione sul mercato, a tutto vantaggio dei consumatori. L'approccio normativo sandbox crea intenzionalmente uno spazio per la tecnologia assicurativa da sperimentare in un regime normativo diverso da quello regolare. Sebbene si tratti di fasi iniziali degli approcci, varrebbe la pena di capire quando le tecnologie sono considerate di successo e scalabili, come saranno graduate nel quadro normativo regolare. In futuro, ciò sarà importante per garantire l'applicazione di condizioni di parità di condizioni di concorrenza nella fase appropriata. Un importante sviluppo in corso tra MAS, FCA e la Australian Securities and Investment Commission sono gli accordi bilaterali di cooperazione tra le autorità che consentono loro di fare riferimento a imprese innovative che cercano di entrare nei rispettivi mercati. Ciò contribuirebbe a consentire alle

nuove imprese di trasferire i loro modelli d'impresa su base transfrontaliera, aiutando le imprese a scalare le dimensioni quando se ne presenta l'opportunità.

Un'altra considerazione importante, in particolare per i paesi in via di sviluppo, è se sia opportuno disporre di un quadro normativo specifico per consentire l'introduzione di nuovi prodotti assicurativi mirati a rischi specifici limitati, di basso valore e che possono beneficiare di una maggiore penetrazione delle polizze assicurative, pur avendo un impatto limitato sugli assicurati. Ad oggi, un numero di paesi (Brasile, India, Messico, Messico, Pakistan, Perù, Filippine, Sudafrica, Taiwan e altri paesi africani (Capgemini, 2017)) hanno una regolamentazione specifica in materia di microassicurazione.La microassicurazione può essere vantaggiosa anche nei paesi OCSE[20], come dimostra l'esempio della start-up Trov. Trov è un'assicurazione on-demand per beni mobili, che può

[20] L'OCSE è stata istituita con la Convenzione sull'Organizzazione per la Cooperazione e lo Sviluppo Economico, firmata il 14 dicembre 1960 ed entrata in vigore il 30 settembre 1961, sostituendo l'OECE, creata nel 1948 per amministrare il cosiddetto "Piano Marshall" per la ricostruzione postbellica dell'economia europea

essere accesa e spenta attraverso un dispositivo mobile. L'app mobile consente di tracciare in tempo reale il valore dell'inventario dei beni e i premi assicurativi. Con i minori costi di transazione che la tecnologia mobile può comportare, la microassicurazione può trovare un modo per essere fornita più facilmente anche nei mercati assicurativi sviluppati.

Nell'era delle nuove tecnologie, le normative assicurative che probabilmente ne risentiranno sono le regole di governance e le regole di condotta del mercato. Le linee guida dell'OCSE sulla governance degli assicuratori raccomanda che i membri del consiglio di amministrazione e i dirigenti con responsabilità strategiche stabiliscano controlli interni che garantiscano il rispetto delle leggi, dei regolamenti e delle norme applicabili, nonché una struttura di incentivazione che promuova una condotta corretta nei confronti dei consumatori e dei contraenti. Le funzioni di controllo sono tenute a valutare l'adeguatezza delle politiche, dei processi e delle procedure, nonché a

individuare e seguire le eventuali carenze.

I Principi fondamentali dell'assicurazione della IAIS[21] stabiliscono che i requisiti per la conduzione degli affari devono essere stabiliti in modo da garantire l'equo trattamento dei clienti, sia prima, durante o dopo la stipula del contratto. Ciò dovrebbe basarsi sul comportamento etico degli assicuratori, agendo in buona fede e sul divieto di pratiche abusive. Mentre le nuove tecnologie e le innovazioni possono consentire agli assicuratori di fornire prodotti adeguati alle esigenze di un cliente non è chiaro come possano garantire che il processo sia equo e trasparente.

Se un assicuratore adotta nuove tecnologie o innova processi/prodotti, dovrebbe considerare se sono state fatte le opportune considerazioni in materia di controllo interno, oltre ad essere appropriato in termini di comportamento

[21] L'Associazione internazionale degli organi di vigilanza nel settore assicurativo (International Association of Insurance Supervisors [IAIS]), fondata nel 1994, persegue l'obiettivo di promuovere una sorveglianza sulle assicurazioni efficace e coerente sul piano globale e contribuire alla stabilità finanziaria a livello mondiale. Ciò è volto a garantire l'equilibrio, la sicurezza e la stabilità dei mercati assicurativi a tutela degli stipulanti.

sul mercato. Un certo numero di paesi sono impegnati in un discorso più ampio, ad esempio, sulle automobili autonome, che avrà un impatto sulla copertura assicurativa auto. Il recente incidente mortale causato da un'auto che si guida da sola negli Stati Uniti ha portato all'attenzione la realtà delle auto autonome e su come garantirne la sicurezza. Insieme a ciò, come deve ancora essere risolta completamente la responsabilità di un'auto di questo tipo in un incidente. Il Regno Unito e gli Stati Uniti hanno condotto consultazioni che toccano la questione e il modo in cui i proventi di tali consultazioni avranno probabilmente un impatto sul modo in cui altri mercati reagiscono.

2.2. Regolamentazione della consulenza tecnologica

Con il diffondersi dell'IA[22] e della consulenza robotica,

[22] L'Artificial Intelligence è il ramo della computer science che studia lo sviluppo di sistemi hardware e software dotati di capacità tipiche dell'essere umano ed in grado di perseguire autonomamente una finalità definita prendendo delle decisioni che, fino a quel momento, erano solitamente affidate agli esseri umani. Le capacità tipiche dell'essere umano riguardano, nello specifico, la comprensione ed elaborazione del linguaggio naturale (Nlp – Natural Language Processing) e delle immagini (Image Processing), l'apprendimento, il ragionamento e la

potrebbe esserci incertezza sulle modalità di applicazione dell'attuale regolamentazione. Ad esempio, in Nuova Zelanda, l'attuale regolamento prevede che la consulenza sia fornita da una "persona fisica". I cambiamenti previsti in Nuova Zelanda mirano ad ampliare la definizione di consulenza al fine di accogliere le innovazioni tecnologiche e richiedono che gli enti che forniscono consulenza robotica siano autorizzati e tenuti agli stessi requisiti di altri tipi di consulenti (New Zealand Ministry of Business, Innovation and Employment, 2016). I servizi completamente automatizzati non sono autorizzati a fornire consulenza in Canada e qualsiasi servizio di consulenza robotica deve fornire un certo accesso alla consulenza personalizzata di un consulente.

Le autorità di regolamentazione di diverse giurisdizioni hanno valutato come la consulenza basata sulla tecnologia

---

capacità di pianificazione e l'interazione con persone, macchine e ambiente. A differenza dei software tradizionali, un sistema IA non si basa sulla programmazione (cioè sul lavoro di sviluppatori che scrivono il codice di funzionamento del sistema) ma su tecniche di apprendimento: vengono cioè definiti degli algoritmi che elaborano un'enorme quantità di dati dai quali è il sistema stesso che deve derivare le proprie capacità di comprensione e ragionamento.

dovrebbe essere regolamentata in futuro. L'Australian Securities & Investment Commission (ASIC) [23] ha pubblicato nell'agosto 2016 una guida regolamentare sulla consulenza robotica ai clienti al dettaglio. La guida sostiene che i requisiti di qualificazione per i fornitori di consulenza robotizzata sono gli stessi di quelli dei normali consulenti e definisce i requisiti per testare gli algoritmi utilizzati e i controlli e i processi di governance in atto.

Nell'aprile 2016, la US Securities Exchange Commission (SEC)[24] ha approvato una norma proposta dalla Financial Industry Regulatory Authority (FINRA) che richiede che gli sviluppatori di negoziazioni algoritmiche siano registrati come commercianti di valori mobiliari e siano soggetti agli stessi requisiti di qualificazione dei commercianti di valori mobiliari per ridurre la

[23] L'Australian Securities and Investments Commission è un ente governativo australiano indipendente che funge da regolatore aziendale dell'Australia. Il ruolo di ASIC è quello di applicare e regolare le leggi sulle società e sui servizi finanziari per proteggere i consumatori, gli investitori e i creditori australiani.

[24] SEC (Securities and Exchange Commission) Organo federale statunitense di vigilanza dei mercati di borsa (Commissione per i titoli e gli scambi) creata nel 1934.

manipolazione del mercato (SEC, 2016). Le autorità europee di vigilanza (Autorità bancaria europea, Autorità europea degli strumenti finanziari e dei mercati e Autorità europea delle assicurazioni e delle pensioni aziendali e professionali) hanno pubblicato un documento di discussione comune sull'automazione della consulenza finanziaria, esaminando i potenziali benefici e rischi di tali innovazioni al fine di determinare eventuali misure regolamentari supplementari necessarie per affrontare la consulenza finanziaria automatizzata (Comitato congiunto delle autorità europee di vigilanza, 2015).

I regolamenti e le consultazioni in corso indicano la necessità di coerenza con la regolamentazione della consulenza finanziaria umana e di un adeguato controllo dei rischi e della governance della consulenza fornita dal robot. Il tipo di consulenza fornita dalla piattaforma deve indicare chiaramente se la consulenza generica o personalizzata. Se la consulenza è determinata da una consulenza personalizzata, è necessario disporre di

processi chiari per quanto riguarda le modalità di determinazione dell'idoneità per il cliente. Gli algoritmi utilizzati per l'automazione dovrebbero essere ampiamente testati e i controlli in atto per garantire che le procedure siano in atto per garantirne il corretto funzionamento.

C'è anche la questione se gli algoritmi possono avere pregiudizi che, intenzionali o meno, possono portare a consigli inappropriati. Ciò potrebbe avere un impatto sugli assicurati su una base più ampia rispetto ai consulenti, in quanto il pregiudizio sarebbe integrato e chiunque utilizzi l'algoritmo sarà soggetto ad esso. Un'altra questione che è stata evidenziata è che la consulenza robotica e gli algoritmi di gestione del rischio potrebbero portare ad un aumento della prociclicità.

2.3. *Questioni relative alla privacy e alla protezione dei dati nel nuovo contesto macroeconomico*

La tecnologia che coinvolge grandi dati è complessa, opaca e spesso non interpretabile. Per questo motivo,

anche chi sviluppa la tecnologia per l'utilizzo di grandi dati potrebbe non comprendere appieno l'impatto o l'uso appropriato dei dati. Le imprese dovrebbero essere in grado di dimostrare che il loro uso dei dati è appropriato e, per quanto possibile, privo di errori.

Per quanto riguarda i grandi dati e l'analisi dei dati da parte degli assicuratori, le norme sulla privacy e sulla protezione dei dati dovrebbero essere affrontate in modo rigoroso e l'uso eticamente incerto dei dati dovrebbe essere pienamente valutato. Da questo punto di vista, il regime più ampio di protezione dei dati avrà un grande impatto sul modo in cui questo aspetto viene affrontato. Inoltre, quando vengono introdotti obblighi di notifica per le violazioni dei dati, gli assicuratori dovranno garantire che le banche dati siano in grado di soddisfare tale requisito. D'altro canto, è probabile che gli obblighi di notifica contribuiscano anche allo sviluppo di mercati assicurativi informatici autonomi.

Nell'attuale regime dell'UE, ad esempio, i trasferimenti

transfrontalieri di dati non sono consentiti se non a favore di una giurisdizione adeguata o se l'esportatore di dati non ha attuato un meccanismo legittimo di trasferimento dei dati (conformemente alla direttiva UE sulla protezione dei dati (95/46/CE) e al regolamento generale dell'UE sulla protezione dei dati.

Per essere considerata una giurisdizione adeguata, il GDPR [25] estenderà i requisiti previsti dalla direttiva affinché la giurisdizione abbia, tra l'altro, lo stato di diritto fondamentale e la protezione giuridica dei diritti umani, l'accesso ai dati trasferiti da parte delle autorità pubbliche, e agenzie per la protezione dei dati efficaci e funzionanti, impegni internazionali e altri obblighi in relazione alla protezione dei dati personali. Per il trasferimento di dati all'interno del gruppo societario, GDPR richiede che le imprese abbiano norme vincolanti d'impres. che sono

[25] Il GDPR è un regolamento attraverso il quale la Commissione Europea intende rafforzare la protezione dei dati personali di cittadini dell'Unione Europea.Il GDPR in Italia sostituisce e abroga le norme del codice per la protezione dei dati personali (DLgs. 196/2003) con esso incompatibili.

giuridicamente vincolanti e si applicano a tutti i membri del gruppo di imprese previste nell'attività economica congiunta, e che siano soggette all'approvazione di DPA[26] del BCR.

Nell'UE, gli accordi di esternalizzazione e gli accordi di distribuzione devono essere concordati con cautela, in termini di chi controlla ed elabora i dati. Ai sensi dell'attuale direttiva UE sulla protezione dei dati, il trattamento dei dati personali non può aver luogo se non vi sono motivi legittimi per farlo, il che, secondo GDPR, imporrà agli assicuratori (responsabili del trattamento dei dati) di effettuare una "valutazione d'impatto sulla protezione dei dati" prima del trattamento dei dati personali. Gli assicuratori sono tenuti ad attuare consensi sufficienti e protocolli efficaci per la raccolta, il trattamento e l'elaborazione di tutti i dati che l'assicuratore controlla.

[26] Nella pratica, definite le prestazioni che date, e non cambiatele nell'esecuzione del contratto se non volete che cambino per fatti concludenti. Il DPA e' quindi una condizione generale privacy aggiuntiva per specificare le prestazioni fornite nel rispetto della privacy.

Inoltre, ai sensi del GDPR, i responsabili del trattamento dovranno notificare le violazioni dei dati personali all'autorità di controllo competente, ove possibile, entro 72 ore dalla conoscenza della violazione, a meno che il responsabile del trattamento non sia in grado di dimostrare che è improbabile che la violazione comporti un rischio per i diritti e le libertà degli interessati. Le notifiche agli interessati devono inoltre essere effettuate "senza indebiti ritardi" se la violazione può comportare un rischio elevato per i loro diritti e le loro libertà. Le imprese possono essere multate fino a 20 milioni di euro o al 4% del fatturato globale annuo nell'ultimo esercizio finanziario, a seconda di quale dei due importi sia maggiore, per inosservanza del GDPR. Il 2018 vede nascere in Italia di una nuova figura professionale all'interno di aziende ed enti di medie e grandi dimensioni: è quella del DPO, il Responsabile protezione dati. Il suo avvento è concomitante con l'entrata in vigore del GDPR, il Regolamento generale sulla protezione dei dati 2016/679. Suo infatti il compito di

supervisionare l'attività del Responsabile della Privacy e del Titolare del Trattamento dei Dati sensibili. Avanzano così nuove opportunità di impiego, avanzamenti professionali e nuove fonti di guadagno. Ma tutto ciò ha un risvolto della medaglia: la presa in carico delle responsabilità sui dati utilizzati in azienda la cui privacy deve essere garantita e il cui uso deve essere autorizzato. Il DPO infatti, pur non avendo una responsabilità diretta su questi aspetti, non è esente dal dover rispondere in prima persona ai danni e alle eventuali sanzioni che un uso improprio o una cattiva protezione degli stessi può provocare.

Il DPO (Data Protection Officer), altrimenti detto Responsabile protezione dati, è una figura professionale non nuova a livello internazionale, ma piuttosto sconosciuta in Italia. Questa nuova figura professionale è stata introdotta dal Regolamento generale sulla protezione dei dati 2016/679(GDPR),

pubblicato sulla Gazzetta Ufficiale europea L. 119 il 4 maggio 2016 e divenuta obbligatoria a partire dalla sua entrata in vigore lo scorso 25 maggio 2018.

Figura storicamente già presente in alcune legislazioni europee, il DPO è una persona che deve avere un ruolo aziendale (sia esso soggetto interno o esterno) con competenze giuridiche, informatiche, di risk management e di analisi dei processi. La sua responsabilità principale è quella di osservare, valutare e organizzare la gestione del trattamento di dati personali (e dunque la loro protezione) all'interno di un'azienda (sia essa pubblica che privata), affinché questi siano trattati nel rispetto delle normative privacy europee e nazionali. Questo soggetto è già conosciuto nel mondo anglosassone con il termine di Chief Privacy Officer (CPO); Privacy Officer, Data Protection Officer o Data Security Officer.

L'art. 39 del Regolamento europeo sulla protezione dei dati personali indica i principali compiti del DPO

(Responsabile della protezione dei dati). Andiamo ad elencarli.

i. Il responsabile della protezione dei dati (DPO) è incaricato dei seguenti compiti:
    a) informare e fornire consulenza al Titolare del trattamento o al Responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
    b) sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del Titolare del trattamento o del Responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la

formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;

c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35;

d) cooperare con l'autorità di controllo;

e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

ii. Nell'eseguire i propri compiti il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo. Il Regolamento sulla Data Protection, entrato in vigore il 25 maggio 2016, è

stato applicato a tutti i 28 Stati membri UE a partire dal 25 maggio 2018. Come previsto dall'art.37 del GDPR l'istituzione della figura del Data Protection Officer (in italiano Responsabile della protezione dei dati) è obbligatoria nei casi in cui in azienda:

a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;
b) le attività principali del Titolare del trattamento o del Responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati sularga scala;
c) le attività principali del Titolare del trattamento o del Responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9

(dati particolari | sensibili) o di dati relativi a condanne penali e a reati di cui all'articolo 10. L'articolo 9 del Regolamento al comma 1 definisce come categorie particolari di dati personali (ex dati sensibili) i dati che "*rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona*".

In pratica il GDPR indica che siano tenuti ad avere il DPO:

- Gli Enti pubblici;

- Le Aziende private dove le ″core activities″ del titolare del trattamento o del responsabile del trattamento ″consista in trattamenti richiedenti il monitoraggio sistematico su larga scala;

- Le Aziende private dove le attività principali del titolare del trattamento o del responsabile del trattamento *"riguardano il trattamento, su larga scala, di informazioni sensibili o di dati relativi a condanne penali e a reati"*.

Tuttavia, si tenga presente che la designazione obbligatoria di un DPO può essere prevista anche in casi ulteriori in base alla legge nazionale o al diritto comunitario. Inoltre, anche ove il regolamento non imponga in modo specifico la designazione di un DPO, può risultare utile procedere a tale designazione su base volontaria. Il Gruppo di lavoro "Articolo 29", così come il Garante della privacy italiano, incoraggiano un approccio "cautelativo": si noti infatti che il GDPR obbliga a prevenire e mitigare i rischi secondo un concetto proattivo, il che significa da una parte certamente tutelare i diritti e le libertà degli interessati, ma anche e soprattutto valutare preventivamente l'impatto che alcune scelte possano avere sull'immagine dell'organizzazione e sulla continuità operativa dell'organizzazione.

Il DPO può essere un dipendente oppure un soggetto esterno che sia totalmente libero di svolgere in modo indipendente i suoi compiti. Nel dettaglio i suoi compiti sono molteplici, dall'analisi della mappatura aziendale, delle procedure fino alla gestione documentale cartacea e informatizzata via web. Al DPO sono richieste quindi, oltre alle competenze giuridiche e informatiche, anche quelle organizzative e di controllo dettate dal delicato compito di assistere il titolare o il responsabile del trattamento dei dati affinché la gestione degli stessi dati personali sia conforme e rispetti la normativa in materia di privacy.

Difficilmente una RC professionale copre anche i rischi derivanti dalla nuova carica DPO. Dopo aver verificato con un consulente assicurativo le coperture previste dalla propria polizza, è altresì possibile abbinare alla garanzia di RC professionale anche una apposita assicurazione di difesa legale, essenziale per completare il pacchetto di garanzie a difesa del patrimonio del professionista (anche qualora fosse un dipendente aziendale), che può essere esposto a sanzioni

in caso disattenda gli obblighi che la legge prevede per la propria professione.

2.3.1. RegTech

RegTech è un'area emergente in FinTech, che utilizza tecnologie per risolvere i requisiti normativi e di conformità in modo più efficace ed efficiente. Date le varie riforme normative introdotte dopo la crisi finanziaria, RegTech ha il potenziale per garantire una più efficace osservanza di normative complesse. Le tecnologie ritenute applicabili per RegTech includono l'apprendimento automatico e l'intelligenza artificiale, la biometria, l'interpretazione di dati non strutturati come e-mail e post di Facebook e l'uso di interfacce di programmazione delle applicazioni (API). Tali strumenti possono essere applicati su aree quali l'aggregazione di grandi dati, la modellizzazione del rischio di stress-testing, il monitoraggio della conformità ai requisiti patrimoniali, l'aggiornamento dei manuali di conformità, il

miglioramento dei programmi antiriciclaggio e di Know-your-Customer (KYC) e la prevenzione delle frodi e delle violazioni interne.

RegTech è un'area in cui i paesi che hanno sviluppato approcci normativi nei confronti di FinTech hanno beneficiato maggiormente delle start-up, con il 31% delle start-up RegTech incorporate nel Regno Unito, contro il 20% negli Stati Uniti (Mulder, 2016).

Per le assicurazioni, ad esempio, esistono piattaforme di analisi dei dati che consentono di convertire i dati interni delle istituzioni finanziarie in formati di reporting normativo, e questo potrebbe essere applicato al settore assicurativo. Esistono diverse piattaforme Know-your-customer (KYC) che possono utilizzare dati esterni e aperti per verificare l'identità del cliente. Poiché le iniziative di modernizzazione della solvibilità richiedono che i gestori patrimoniali degli assicuratori siano in grado di segnalare gli investimenti in modo trasparente, le soluzioni RegTech potrebbero fornire agli assicuratori una

piattaforma che consenta loro di cogliere il proprio asset under-management in una semplice interfaccia. Mentre nell'ambito di RegTech vengono proposte diverse soluzioni per le assicurazioni, in particolare per la prevenzione delle frodi e la conformità alla solvibilità, un settore emergente è il modo in cui le compagnie assicurative possono garantire che i loro algoritmi siano conformi alle norme di comportamento sul mercato. Alcune start-up stanno lavorando per affrontare le conseguenze indesiderate degli algoritmi, per garantire che gli istituti finanziari, comprese le compagnie di assicurazione, possano integrare gli algoritmi nella loro interfaccia con i clienti e la gestione del rischio aziendale in modo corrispondente all'obiettivo di efficienza ed efficacia dei processi aziendali, riducendo al minimo i rischi potenziali degli algoritmi. ORCAA è una start-up tecnologica con sede a New York, fondata da un data scientist per effettuare audit di algoritmi. Il modello utilizzato viene esaminato in quattro fasi: la raccolta e

l'integrità dei dati, l'obiettivo dell'algoritmo, la base in cui l'algoritmo è stato costruito, e il monitoraggio e l'aggiornamento dell'algoritmo. Gli algoritmi sono noti per l'uso di alcuni proxy, come il codice postale, che potrebbe portare ad un trattamento ingiusto di alcuni segmenti della popolazione a seconda di come viene modellato l'algoritmo.

Un settore in cui la regolamentazione finanziaria è stata relativamente esposta ad algoritmi è quello delle negoziazioni ad alta frequenza, dove gli algoritmi di negoziazione sono utilizzati per eseguire negoziazioni automatizzate ad alto volume e ad alta velocità sui mercati finanziari. Le autorità di regolamentazione finanziaria, come il Federal Reserve Board e l'Autorité des Marché Financiers francese avevano pubblicato rapporti sull'argomento; tuttavia, un'operazione di fondi comuni di investimento ha portato a un ritiro di massa da parte del commercio ad alta frequenza e al successivo crollo del Dow Jones ("Flash Crash") nel maggio 2010 (McQuivey,

2017). Nel 2013 la Germania ha adottato l'High-Frequency Trading Act, in base al quale le imprese di negoziazione ad alta frequenza, non precedentemente controllate dalla BaFin, devono essere controllate dalla BaFin. Le imprese sono tenute a garantire che i mercati non siano distorti o interrotti. La regola di tagging dell'algoritmo impone alle borse di implementare regole che richiedono a tutti i membri della borsa di contrassegnare tutti gli ordini generati algoritmicamente con una chiave univoca quando vengono inviati ad una borsa tedesca, in modo da consentire al sistema di sorveglianza del mercato di allocare tutti gli ordini all'algoritmo di generazione .La Commissione europea ha emanato uno standard tecnico per la direttiva sui mercati degli strumenti finanziari (MiFID)[27] II, che sarà attuato nel

[27] La MiFID II (entrata in vigore: 3 gennaio 2018) ha come obiettivo lo sviluppo di un mercato unico dei servizi finanziari in Europa, nel quale siano assicurate la trasparenza e la protezione degli investitori.
Sono previste varie disposizioni che, in quanto ispirate al dovere di agire nel miglior interesse del cliente, garantiscono una corretta informazione per gli investitori, si occupano dei potenziali conflitti di interesse tra le parti e richiedono un'adeguata profilatura del risparmiatore.

2018, sulle modalità di attuazione degli articoli relativi alle negoziazioni ad alta frequenza nell'aprile 2016. Il monitoraggio degli algoritmi è complesso e richiede competenze speciali e spesso le autorità di regolamentazione e di vigilanza non sono in grado di comprendere o valutare gli algoritmi e/o se i grandi dati vengono utilizzati in modo appropriato. Nel settore assicurativo, gli usi noti degli algoritmi sono legati principalmente all'interfaccia con la clientela, anche se le iniziative in materia di solvibilità spingono probabilmente gli assicuratori a utilizzare algoritmi anche per la misurazione della solvibilità.

Le autorità di regolamentazione dovrebbero considerare come affrontare l'uso di algoritmi e grandi dati da parte degli assicuratori che garantiscano che siano sviluppati in modo appropriato ed evitino, per quanto possibile, distorsioni e conseguenze indesiderate. In particolare, si potrebbero effettuare prove di stress per determinare come

la consulenza robotizzata affronterebbe in determinate condizioni di mercato estreme.

2.3.2. MonitorTech

La *MonitorTech* serve a mappare in tempo reale ciò che accade all'interno delle istituzioni finanziarie. È quasi impossibile per le persone tenere traccia di tutte le informazioni disponibili; infatti, a questa necessità rispondono i computer. Gli esempi di applicazione della *MonitorTech* non mancano: il cliente utilizza il proprio conto per riciclaggio di denaro? il cliente oppure un dipendente utilizza informazioni privilegiate? i trader negoziano senza tener conto degli imposti limiti di rischio? un cliente potrebbe non essere in grado di pagare il mutuo?

2.3.3. ReportTech

La ReportTech supporta le istituzioni finanziarie per le segnalazioni delle operazioni alle Autorità di Vigilanza nazionali ed europee. Esempi di tipologie di segnalazioni:

le transazioni in titoli, il superamento dei limiti di credito, segnalazioni alle Autorità Fiscali, bilanci trimestrali, rapporti e analisi sui rischi effettivi.

2.3.4. DataExchangeTech

Una delle tendenze più recenti in atto riguarda la progressiva "perdita di indipendenza" delle istituzioni finanziarie. Per fronteggiare i crescenti obblighi normativi che le istituzioni finanziarie si trovano a dover collaborare con altre istituzioni finanziarie e instaurare *partnerships* che creano valore aggiunto.

Ci sono grandi gruppi di aziende impegnate a collegare le parti interessate all'interno di un **ecosistema** finanziario. Pensiamo che, per fornire al cliente un prodotto finanziario preassemblato (ossia pacchetti unici, non modificabili, cui si può solo aderire o no i.e. fondi, polizze assicurative, strumenti strutturati o investimenti sui derivati, etc.) la banca prima deve fornire on-line il KID / KIID – un documento di due o tre pagine con le informazioni chiave

del prodotto -. Una banca ha disponibili circa 10.000 prodotti di investimento preassemblati – riconducibili a 100 società emittenti -; il conto è presto fatto, visto che in Europa ci sono circa 200 grandi banche si calcola che si tratta di circa 2 milioni di documenti.
La *DataExchangeTech* è non solo una necessità e un dato di fatto.

2.3.5. LegalTech

Le grandi istituzioni finanziarie impiegano innumerevoli legali e professionisti della *compliance* per rimanere aggiornati e per implementare i cambiamenti normativi. Gli adeguamenti normativi sono talmente tanti e in crescita che molte cose possono, ed iniziano, a sfuggire. Non solo occorre essere al corrente degli aggiornamenti di regolamenti e normative, ma occorre comprenderli e sapere a quali tipi di attività si applicano; e le attività possono essere in Paesi e Continenti diversi. L'informatica può fornire la soluzione.

2.3.6. ComplyTech

Le norme che i dipendenti del settore finanziario devono seguire sono molto complesse e possono accadere violazioni accidentali. D'altra parte, le politiche di *compliance* delle istituzioni finanziarie, a causa delle innumerevoli attività e possibilità, non sempre riescono a chiarire cosa i dipendenti possono fare e cosa, invece, non è permesso. L'informatica può assistere il business fornendo risposte ai casi reali che puntualmente si presentano.

2.3.7. Cyber Insurance

Ogni rischio che rappresenti per l'Azienda una possibile fonte di pregiudizio alla sua integrità materiale alla sua integrità patrimoniale ed alla sua business continuity deve essere gestito e fronteggiato con i mezzi appropriati, a cominciare da quelli che sono già a disposizione, provvedendo, se è il caso, a rafforzare le difese attraverso l'acquisizione di ulteriori mezzi di protezione. Questa

fase di potenziamento delle difese deve passare attraverso una attenta analisi che tenga conto dei costi da sostenere e dei benefici che se ne possono trarre, prima di prendere delle decisioni che rischino di risultare, col senno di poi, contro-producenti. Infine occorre alleggerire, per quanto possibile, il carico del rischio residuo mediante la pratica di trasferimento all'Assicuratore.

Il primo passo per sapere come affrontare correttamente un rischio è conoscerlo. Per perseguire questo obiettivo, preliminare, ma molto importante, dobbiamo dare una risposta a sei quesiti fondamentali, volti a conoscere i fattori interni del rischio i fattori esterni e le modalità di interazione fra i primi tre ed il quarto (Schober N. e Schober W., 2019). Vediamoli nel dettaglio: l'individuazione dell'interesse da proteggere, la stima del suo valore, l'identificazione del soggetto che ne è titolare, la conoscenza del ventaglio di accadimenti (o fattori esterni del rischio) che possono costituire un pericolo per la sua integrità e la valutazione della

probabilità che si verifichi un danno per effetto di ogni accadimento la valutazione dell' entità verosimilmente massima che può avere il danno per ogni accadimento. Ovviamente, a questa fase conoscitiva, deve far seguito la fase di intervento che avrà certamente dei costi, facilmente determinabili e dei benefici, la cui stima è però assai più aleatoria. Questa valutazione promiscua dovrà essere messa a bilancio, quale contropartita della risposta al quesito 6), ma perseguendo il sano proposito di fare un passo per volta, proveremo ad applicare i principi della fase conoscitiva al caso del *Cyber Risk*. Procedendo come appena detto, avremo fin da subito modo di renderci conto quanto poco questo nuovo rischio abbia in comune con quelli che siamo stati finora abituati a trattare. Poiché la soggettività che è già di per sé una caratteristica del rischio lo è, come vedremo, ancora a maggior ragione, nel caso del Cyber Risk, per rendere fluida l'esposizione, dovremo dare un nome al soggetto che corre il rischio: lo chiameremo per semplicità Assicurato, per coerenza con

la centralità che il tema assicurativo ha in questa trattazione, sebbene costretta a lasciare ampio spazio alla sua disciplina complementare, il Risk Management, se non altro per la congenita necessità di servirsene da puntello per non affogare, come vedremo, di fronte ad una probabilità che rischia seriamente di farsi certezza. Già nel cercare una risposta al primo quesito, ovvero individuare l'interesse da proteggere ci imbattiamo in una tipologia totalmente diversa rispetto agli interessi dei quali abbiamo trattato nell'affrontare i rischi tradizionali. Gli interessi sono costituiti principalmente (ma non solo) dai dati e dalle informazioni contenuti in forma digitale nelle memorie del computer dell'Assicurato, che può esserne il titolare oppure il detentore per conto di titolari terzi. In questo secondo caso, dati e informazioni sono un interesse dei soggetti terzi. L'interesse del soggetto che gestisce e conserva dati e informazioni (l'Assicurato) diventa il suo patrimonio, suscettibile di essere depauperato dall'azione risarcitoria che lo vedrà

obbligato nei confronti dei terzi titolari dei dati ed, in quanto tali, danneggiati. Abbiamo così trovato simultaneamente una risposta anche al terzo quesito. Per quanto siano dei beni del tutto immateriali e sfuggenti ad un criterio di valutazione oggettiva, i dati e le informazioni in forma digitale rappresentano comunque una entità statica, avente una collocazione, in qualche modo, fisica, nel sistema informatico o, al limite, presso la piattaforma Cloud. Essi costituiscono, come si è accennato, la parte più importante degli interessi connessi con l'uso di sistemi informatici, ma non esauriscono questo particolare insieme. Chi faccia uso del sistema informatico, fa anche uso della rete, per acquisire nuove informazioni e per comunicare. Gli strumenti che rendono possibile questa attività sono i siti internet e il servizio di posta elettronica. Lo sarebbero in teoria anche i motori di ricerca, che però, come avremo modo di vedere nel seguito, godono di un livello di vulnerabilità notevolmente inferiore. L'accesso in ogni momento a

questi siti deve essere salvaguardato. È facile comprendere che stiamo parlando di un interesse ancor più impalpabile, in quanto non si tratta più nemmeno di una entità, ancorché virtuale, quali sono le informazioni digitalizzate, bensì di una *facoltà (o libertà) di agire* che, per sua natura, è connessa in modo inscindibile con la funzione di immagazzinamento delle informazioni nelle memorie ad esse dedicate, come accade per esempio nel caso della posta elettronica. Come vedremo più avanti, la pirateria informatica è in grado di colpire anche questo interesse improprio, ma non per questo meno importante. La risposta al secondo quesito è quella che presenta le maggiori difficoltà. Se ci proponiamo di individuare il valore dell'interesse da proteggere, scopriamo che il patrimonio di informazioni non possiede un valore proprio e, ancor meno, se consideriamo quella parte di esso che abbiamo identificato nella *facoltà di agire*, ma l'importanza strategica di poter continuare a disporre di queste forme improprie di patrimonio, unitamente

all'importanza, ancor più strategica, che quello dei dati e delle informazioni digitalizzate non sia messo a disposizione né a conoscenza di soggetti estranei, rappresentano un valore totalmente soggettivo e verosimilmente non patrimoniale, che sfugge ad ogni criterio tradizionale di stima, ma la cui perdita potrebbe mettere a repentaglio la sopravvivenza stessa dell'Azienda. Passiamo ora a cercare una risposta al quarto quesito. Quanto abbiamo fin qui visto rivela sostanzialmente la presenza di due possibili fattori esterni di rischio:

- la perdita della facoltà di accesso al patrimonio di informazioni e alla comunicazione;
- la fuga delle informazioni dalla gabbia virtuale costruita attorno ad esse per garantirne la riservatezza.

Il primo evento può derivare da perdita, alterazione o distruzione dei dati e questo può verificarsi anche per effetto di eventi cosiddetti tradizionali (come il caso di

incendio della sala server), oppure per fatti che, pur essendo meno frequenti fra gli eventi assicurati contro i danni, mantengono il carattere dell'accidentalità, come il blackout elettrico, il guasto tecnico, l'errore di programmazione o, infine, l'atto di infedeltà di uno o più dipendenti. Tuttavia, l'evento che domina la scena di questo rischio è l'atto doloso esterno, compiuto da soggetti che dedicano la loro vita alla ricerca di metodi sempre più sofisticati e sempre meno opponibili, per violare la privacy dei sistemi informatici. Il secondo evento, quello della fuga di informazioni, tranne i casi dovuti ad infedeltà di dipendenti, può essere cagionato quasi esclusivamente da un atto di pirateria informatica, perpetrato a scopo di estorsione. Visto che non può essere assegnato alcun valore di scambio all'interesse che deve essere protetto, in quanto questo appartiene alla categoria delle proprietà intellettuali, per consentire una stima del danno, secondo un criterio assicurativo, si quantificano i costi per ripristinare la situazione ante sinistro. È un

criterio che richiama la garanzia sul Danno Ambientale, che assicura la contaminazione dell'ambiente, ma indennizza i costi di bonifica. Ne consegue che non esiste alcuna relazione fra il valore dell'interesse ed il costo sostenuto per ripristinarne l'integrità dopo il sinistro. Avendo identificato nei costi di ripristino l'onere economico del danno, il sesto quesito si trova ad avere una risposta alquanto semplificata rispetto ai rischi tradizionali. Nel caso del Cyber Risk, infatti non si pone il problema di stimare quanta parte del valore dell'interesse è coinvolta dal danno, dal momento che il danno, per come viene concepito, non è una quota parte del valore totale considerato. Non potrebbe che essere così, visto che il valore totale sfugge ad ogni criterio di misura finora conosciuto. Va osservato che i tentativi di ripristino non danno una reale garanzia di successo e, anche laddove il ripristino fosse tecnicamente riuscito, potrebbe non aver risolto il problema principale causato dal sinistro. La parte del problema che non viene e non

può venire risolto è dato dalla impossibilità di ottenere, con le buone o con le cattive maniere, da chi se ne fosse appropriato con metodi illeciti, la restituzione delle informazioni salvate in copia, la cui detenzione tiene viva la sua possibilità di reiterare a propria discrezione, la minaccia di divulgazione a scopo estorsivo. Qualora il patrimonio di informazioni colpito fosse di proprietà di terzi, si configurerebbe una responsabilità in capo a soggetti chiamati a conservare, gestire e trattare dati appartenenti a terzi, coperti da patto di riservatezza, derivante da azioni dolose compiute da sabotatori esterni, che non sono persone delle quali il gestore risponde per legge. Questi, invece, risponde solo dell'omessa o carente adozione di misure di difesa contro l'intrusione informatica e dell'omessa notifica agli interessati che, causa un attacco Cyber, i loro dati sono sotto sequestro oppure che corrono verosimilmente questo rischio. Risponderebbe della violazione in toto se la perdita o la divulgazione non autorizzata di dati e informazioni fosse

frutto di un incidente o di un atto di infedeltà dei dipendenti. Osserviamo che nel caso in cui il soggetto che patisce il danno è un terzo, viene un po' messo a margine l'aspetto dei costi di ripristino, che il gestore potrebbe peraltro essere chiamato a sostenere a proprio carico, ma la parte di danno che prenderebbe il sopravvento è l'obbligo risarcitorio derivante dalla divulgazione non autorizzata delle informazioni riservate. Trattandosi di un danno evidentemente non patrimoniale, si creano le condizioni per la richiesta di una somma a ristoro non prevedibile, in quanto dipende dalla richiesta del danneggiato e dall'aggiustamento che il giudice avrà apportato a tale richiesta nel momento in cui sarà chiamato a quantificare, non un risarcimento, ma un equo indennizzo. Le circostanze rilevate in merito al Cyber Crime sollevano una serie di problematiche di ordine giuridico che, come vedremo nel seguito, non sono del tutto semplici da risolvere. Venendo al quinto quesito l'ultimo al quale non abbiamo ancora dato una risposta,

scopriamo che Il Cyber Risk proviene da più fonti che si moltiplicano in breve tempo ed evolvono con grande rapidità verso una capacità di intrusione sempre maggiore ed, al tempo stesso, la classe di utenti che sono soggetti a patirne le conseguenze, si dimostrano indolenti e refrattari a comprendere la gravità del problema, fino a quando non vengono toccati sul vivo. Questa situazione paradossale si traduce in una probabilità di accadimento del danno talmente elevata, da potersi considerare ininfluente sulla valutazione del rischio. Una probabilità che può dirsi paragonabile a quella di restare colpiti attraversando, più e più volte, privi di protezione, una piazza nella quale numerosi cecchini sparano all'impazzata e senza posa, con dei mitragliatori, dotati di munizioni inesauribili. Una probabilità assai prossima al valore 1 (o se si preferisce il 100%) che lascia indeterminato solo il momento in cui il danno si possa verificare, quindi un parametro impalpabile che sfugge ad una

misurazione oggettiva, prerogativa questa che ricorda in qualche modo le caratteristiche del puro rischio del ramo vita. La categoria degli Assicuratori si è trovata pertanto costretta a fare i conti con un rischio che, per tutte le ragioni viste, rispetto a quelli tradizionali, poteva dirsi alieno nelle modalità con cui si manifesta e il proposito di assumerlo richiedeva un atto di coraggio senza precedenti. In nessun caso, nell'ambito dei rami danni, gli Assicuratori avrebbero assunto un rischio con questo livello di probabilità di accadimento, ma i fatti dimostrano che non si sono tirati indietro. Si può presumere che la vastità del fenomeno, accanto alla rapidità della sua crescita abbia fatto intravvedere le prospettive di un business assicurativo senza precedenti che, però, senza apportare adeguati correttivi, orientati ad una mitigazione manovrata del rischio, sarebbe stato un salto nel buio. Gli Assicuratori hanno dovuto così aguzzare l'ingegno ed agire su due fronti: limitando da un lato la propria esposizione con l'adozione di massimali a

misura della propria capacità assuntiva ed escogitando contromisure efficaci all'azione dei pirati informatici, imponendo successivamente agli Assicurati di farsi parte diligente nell'adottarle. Per raggiungere questo secondo risultato la categoria degli Assicuratori ha dovuto necessariamente fare ricorso a risorse esterne, per avvalersi di una competenza tecnica molto avanzata, in grado di aggiornarsi quotidianamente, sperando di restare al passo di corsa con cui evolve la regia di questo vero e proprio male del terzo millennio. Non tutti, però hanno dimostrato una pari ampiezza di vedute ed una pari consapevolezza di ciò cui stavano andando incontro. La risposta assicurativa, relativamente al panorama assicurativo italiano, si è fatta trovare impreparata, ma sta dando segni di recupero, anche se in ritardo rispetto ai Paesi trainanti dell'economia europea, ma ancor più rispetto agli Stati Uniti d'America.

2.4. Analisi comparata fra Cyber Risk e rischi tradizionali

Ricapitolando, rispetto ai rischi tradizionali, il Cyber Risk presenta delle evidenti differenze, riportate nella doppia tabella di seguito e alla pagina successiva, rappresentata separatamente per il caso di gestione di dati propri e per quello di gestione di dati di terzi:

Caso 1-Gestione dei dati propri

CARATTERISTICHE	RISCHI TRADIZIONALI (Property)	CYBER (CRIME) RISK
Interesse da proteggere	Entità materiali riconoscibili	Patrimonio di informazione e libertà di navigazione nel web
Valore dell'interesse	Il contro valore delle entità materiali	Indefinito
Eventi dannosi temuti	Eventi conosciuti reperibili anche dalle polizze	Perdita di dati - divulgazione di informazioni riservate
Probabilità dell'evento	Stima in base alle statistiche pluriennali	Quasi 100%
Stima del massimo danno	Basata su calcolo di concentrazione di valori	Costi preventivabili a priori disgiunti dal valore dell'interesse in gioco
Danno parziale	Quota parte del danno totale	Dato privo di senso

Caso 2-Gestione dei dati di terzi

CARATTERISTICHE	RISCHI TRADIZIONALI (RC)	CYBER (CRIME) RISK
Interesse da proteggere	Il patrimonio dell'assicurato	Il patrimonio dell'assicurato
Valore dell'interesse	Indefinito	Indefinito
Eventi dannosi temuti	Quelli ipotizzabili in base all'attività esercitata	Perdita di dati - divulgazione di informazioni riservate di terzi
Probabilità dell'evento	Stimata in base alle statistiche pluriennali	Quasi 100%
Stima del massimo danno	Basata sull'intensità dell'interazione con soggetti terzi	Incalcolabile

Confrontando le due tabelle, si osserva che nel caso della gestione di dati propri, il termine di paragone, necessariamente pescato nel settore Property, presenta delle differenze sostanziali su tutti i sei aspetti, corrispondenti ai sei quesiti di cui al paragrafo 1, con l'eccezione del quesito sull'identificazione del titolare dell'interesse che, come si può vedere, manca nella tabella, dato che la sua risposta risulta superata dall'unificazione della figura del titolare dell'interesse e dalla contestuale duplice forma che assume l'interesse fra il caso in cui il gestore sia proprietario dei dati e quello in cui li gestisca per conto di terzi. In compenso si può osservare

l'aggiunta di un aspetto ulteriore, non previsto nei quesiti, consistente nella definizione del danno parziale. L'aggiunta di questo ulteriore parametro è volta a mostrare come un aspetto così diffusamente presente nei rischi tradizionali attinenti i danni ai beni, perda di significato, quando è applicato al Cyber Risk. Nel caso del rischio relativo alla gestione di dati di terzi, invece, si riscontra una identità nei parametri che indicano la tipologia ed il valore dell'interesse, mentre il parametro indicante il danno parziale è stato omesso, in quanto in materia di RC non si assicura un bene, ma un obbligo risarcitorio, disgiunto dal valore di un interesse economico. In definitiva, la necessità di salvaguardare un rapporto sinistri/premi almeno accettabile nel ramo Cyber, ha indotto, in generale, gli Assicuratori a non limitarsi alla soluzione assicurativa, bensì a cercare delle sinergie con una strategia di Risk Management. È un percorso inevitabile, nell'intento di ridurre il tasso di probabilità che, allo stato grezzo del rischio, si presenta

ad un livello insostenibile. Quella che in questo caso risulta una scelta obbligata per non trovarsi in difficoltà fin dai primi anni di assunzione del rischio Cyber potrebbe essere d'auspicio e d'esempio nonché un'occasione per promuovere l'introduzione di questa importante disciplina nel costume dell'impresa italiana, anche nella gestione dei rischi tradizionali. Abbiamo visto in precedenza come l'azione del pirata informatico possa mettere il soggetto colpito nelle condizioni di dover rispondere civilmente nei confronti degli utenti che gli avevano affidato la conservazione, con facoltà di gestire e trattare i propri dati personali, sotto il vincolo del patto di riservatezza, avendo visto che l'hacker[28]

[28] Hacker è un termine della lingua inglese che designa una persona che utilizza le proprie competenze informatiche per esplorare i dettagli dei sistemi programmabili e sperimenta come estenderne l'utilizzo.

La parola deriverebbe dal verbo "To hack" non indicava più l'attività di saldare circuiti dalle strane sembianze, bensì quella di comporre insieme vari programmi, con poco rispetto per quei metodi o procedure usati nella scrittura del software "ufficiale". Significava inoltre migliorare l'efficienza e la velocità del software già esistente che tendeva a ingolfare le risorse della macchina. Ed è qui che successivamente si colloca una diversa radice del termine hacker, la forma sostantiva del verbo inglese "to hack" che significa "tagliare", "sfrondare", "sminuzzare", "ridurre", "aprirsi un varco", appunto fra le righe di codice che istruiscono i programmi software.

punta a minacciare proprio di violare tale patto facendo apparire tale violazione come fosse commessa da chi né è affidatario. In realtà, occorre riflettere su alcuni aspetti importanti che devono essere valutati con attenzione prima di dare per scontata una copertura assicurativa che, altrimenti, rischia di vedere svuotato, per una parte importante, il suo contenuto di garanzia, se non nella fase attuale, certamente nella prospettiva di un futuro, tutto sommato, imminente. È evidente che, alla percezione dell'utente, quello che accade è che il soggetto di fiducia è venuto meno al patto di riservatezza o all'impegno di conservare nella loro integrità originaria i dati affidatigli sulla cui base lo stesso utente aveva affidato dati ed informazioni proprie riservate, affinché potesse prestare un servizio di conservazione ed eventualmente di trattamento dei dati stessi, entro i limiti consentiti dal mandato. Agli occhi dell'utente non è visibile la differenza fra il caso in cui

la violazione sia frutto delle seguenti possibilità:

- di un errore umano;
- di un incidente tecnico;
- di un danno materiale all'hardware;
- di una disattenzione di carattere colposo;
- di un atto doloso, con movente di infedeltà di qualche dipendente addetto alla fase operativa della gestione dei dati
- dell'intervento esterno dell'hacker.

Pertanto, l'utente che subisca il pregiudizio da violazione della Privacy oppure da alterazione o perdita dei propri dati, può agire in giudizio nei confronti del gestore, in apparenza, inadempiente, ma il gestore cercherà di tutelarsi attraverso l'intervento del suo legale. Bisogna tuttavia prendere atto che il gestore è gravato da due ordini di responsabilità: una responsabilità diretta per divulgazione non autorizzata o

perdita di dati di terzi cagionata da un evento accidentale prodottosi nella sua sede, ovvero da un atto di infedeltà di un dipendente e unna responsabilità da culpa in vigilando, limitata al caso di inadempienza degli obblighi di tutelare i dati riservati con idonee misure di protezione, in conformità con le disposizioni di legge, qualora la perdita o la divulgazione dei dati sia stata causata da un atto di pirateria informatica. A queste due responsabilità ne va aggiunta una terza, che deriva dall'applicazione di normative di legge che al momento sono nelle more dell'entrata in vigore, (di questo parleremo diffusamente più avanti) e che riguarda l'obbligo di notifica, ovvero l'impegno di informare i titolari dei dati in gestione che essi sono soggetti ad attacco hacker esente o futuro. Il gestore ha dunque, in via prioritaria, l'onere di dimostrare che ricorre il caso b), posto che non riuscendo a produrre le prove in tal senso, esso risponderebbe verso i terzi danneggiati della violazione o della perdita di dati, a prescindere da come

ciò si sia verificato. In subordine la responsabilità del gestore è, sì, presunta, in quanto deve dimostrare la sussistenza degli elementi a sua discolpa e, riuscendovi, potrebbero essere rilevati degli elementi esimenti della responsabilità del gestore, ma non vi sarebbe nulla di scontato nelle conclusioni. Nell'ipotesi in cui egli riesca a produrre le prove a sua discolpa, può essere resa inoperante la garanzia assicurativa in materia di responsabilità civile, in ambito Cyber, ma non è detto che chi si riterrà danneggiato rinunzi alla tutela dei propri diritti ed anzi, a fronte di una eventuale sentenza sfavorevole in primo grado, la persegua in ogni sede, fino a vedere soddisfatte le sue pretese. In aggiunta a quanto detto, si inserisce un secondo elemento in grado di vanificare l'efficacia della garanzia assicurativa, ma in questo caso, senza che il danneggiato sia coinvolto. I due paragrafi che seguono contengono gli approfondimenti in merito alle due riserve cui si è accennato, la prima di carattere sostanziale, supportata

da motivazioni giuridiche e l'altra di carattere formale, attinente piuttosto la normativa contrattuale di polizza. Un primo aspetto, di carattere sostanziale, è che quando il pirata informatico viola il sistema del soggetto colpito, magari inibendo, con strumenti informatici, il titolare del sistema stesso all'accesso alle informazioni in esso contenute compie, sul patrimonio di informazioni digitalizzate, un atto che, sotto il profilo giuridico, non è diverso dal furto di beni materiali o, ancor più verosimilmente, dal sequestro di beni a scopo di estorsione. Proviamo dunque a fare un paragone con il caso di furto di merci in conto deposito e domandiamoci come si comporti la legge nei confronti del depositario che, a fronte di una richiesta del titolare delle merci, non avesse più la disponibilità delle merci affidategli in deposito, qualora la predetta perdita della disponibilità fosse da imputare a furto, rapina od altra forma di sottrazione illecita. In un caso di questo tipo verrebbero meno i presupposti di dolo e colpa che devono

caratterizzare il fatto affinché possa essere definito illecito ai sensi dell'Art. 2043 del Codice Civile, perché il fatto che ha leso il diritto del titolare dell'interesse è compiuto dolosamente da un soggetto terzo, del cui operato il depositario non deve nemmeno rispondere per legge. Resterebbe, tuttavia uno spazio per definire una culpa in vigilando. Tuttavia, per valutare la legittimità di una simile imputazione, avrebbe una rilevanza determinante la modalità con la quale il depositario avesse prevenuto il furto, in rapporto al livello di appetibilità della merce custodita, dotando il suo deposito ed, in particolare, i suoi accessi di opportuni dispositivi di inibizione, rilevazione, monitoraggio e allerta, volti a creare un impedimento su più livelli, nei confronti di eventuali malintenzionati, al raggiungimento del loro scopo illegale. Per una esenzione più esaustiva, il depositario dovrebbe adottare anche misure di prevenzione e protezione contro i danni da incendio e da intemperie della natura, ma in questa

sede ci stiamo occupando più specificamente dei pregiudizi derivanti da atto illecito. Mutatis mutandis e spostando l'attenzione sul tema specifico della conservazione dei dati di terzi, il DLgs 196/2003 (Legge sulla Privacy), che tratta anche degli obblighi in capo ai soggetti (definiti responsabili all'Art. 4, comma 1-g del Decreto stesso) che, a fronte del rischio proveniente da atti di pirateria informatica, sono chiamati alla custodia della riservatezza dei dati di coloro che li affidano, definisce il livello minimo delle difese che il responsabile è tenuto a predisporre a protezione dei dati digitalizzati, ma lo fa in modo così generico da sottrarre, a chi ne debba giudicare l'idoneità, ogni riferimento che consenta di darne una valutazione oggettiva. L'Art. 31 – Obblighi di sicurezza, infatti recita: I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche

caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta. Sono state evidenziate in carattere grassetto le parole attinenti la prevenzione di attacchi informatici perpetrati dall'esterno. Resta il fatto che l'adozione di idonee e preventive misure di sicurezza costituisce una espressione della massima genericità, che è di scarso aiuto per l'organo giudicante e si presta a valutazioni soggettive, che risentiranno del livello di esperienza specifica, da parte del Commissario Tecnico d'Ufficio, che necessariamente il giudice di merito dovrà incaricare, in presenza di una vertenza. A questo proposito si anticipa, a livello di cenno, che in merito alla definizione precisa delle misure di protezione e prevenzione contro il cyber crime, sono

stati fatti importanti passi avanti, con il Regolamento Europeo N. 679 del 27 aprile 2016, che entrerà in vigore a maggio 2018 e del quale parleremo diffusamente più avanti. Al di là delle imprecisioni descrittive degli obblighi di tutela dei dati coperti da vincolo di riservatezza in capo a chi li gestisca, si comprende come, essendo la legge sulla responsabilità dei gestori di dati di terzi, a fronte di un attacco informatico esterno, inerente l'adeguatezza delle misure di protezione, di fronte ad un capo di imputazione a seguito di quello che, al di là dell'individuazione del colpevole diretto, rimane un episodio di divulgazione non autorizzata dal titolare delle informazioni, ossia una violazione di fatto della riservatezza, spetti al gestore di dimostrare che le misure da esso adottate fossero in linea con le disposizioni di legge. Se le misure di cautela (protezione e allarme) fossero da ritenersi idonee, col senno di prima, ma il giudizio su di esse richiedesse di essere rivisto alla luce della nuova esperienza in cui

ladri si fossero inaspettatamente dimostrati in grado di superare le difese preposte, si potrebbe invocare il caso di forza maggiore, che esonera il depositario dalla responsabilità della custodia (di dati) per conto di terzi. Naturalmente stiamo parlando di facoltà di avvalersi di normative esistenti, per esimere il soggetto che, in prima approssimazione, appare certamente responsabile dall'addebito fattogli da coloro che ne avessero subito un pregiudizio. Premesso che tale responsabilità è presunta come effettiva e lo rimane fintanto che non siano prodotte le prove contrarie, è doveroso ricordare che vi sono due ragioni determinanti per le quali la suddetta esenzione di responsabilità ha una probabilità assai remota di essere invocata: la prima ragione sta nella constatazione che l'indolenza che caratterizza il comportamento dell'utenza nei confronti del rischio informatico, fino a quando non viene personalmente colpita è una garanzia pressoché assoluta di trovare nel 100% dei casi una protezione informatica inadeguata,

circostanza questa che tiene viva la responsabilità di chi detiene dati di terzi; la seconda ragione è che la velocità con la quale progredisce l'abilità degli hackers è tale da rendere inadeguate anche le difese che fino a qualche giorno prima potevano essere considerate idonee; questa seconda circostanza rischia di rendere opinabile qualsiasi giudizio di idoneità delle difese predisposte. Vale la pena osservare che il ragionamento fatto fonda la certezza di operatività di una garanzia assicurativa sulla (quasi) certezza di una persistente inadempienza agli obblighi in capo agli Assicurati. Se però questo deve essere il presupposto della sopravvivenza della garanzia di responsabilità civile della Polizza Cyber, ci imbatteremmo in una situazione paradossale. Da un lato è prevedibile che il crescere dell'attività di pirateria informatica, a bocce ferme, porterà a ridurre la capacità assuntiva di un rischio, la cui quasi certezza dell'evento tenderà a rendere sempre meno sostenibile per gli Assicuratori che se ne faranno carico, creando così, nel

mercato, una domanda, determinata da una indiscussa necessità di tutela, alla quale non corrisponde una offerta adeguata. Dall'altro lato, l'entrata in vigore del Regolamento 679 dal maggio del 2018, del quale parleremo poco più avanti, con il carico di sanzioni che si porterà dietro, dovrebbe dapprima sgravare il carico assuntivo delle Compagnie, che alimenteranno così un'offerta divenuta asfittica. Se poi prosegue nei suoi effetti di sensibilizzazione, l'entrata in vigore del predetto Regolamento finirebbe per indebolire le ragioni che giustificano la sussistenza di questa garanzia, mentre l'auspicio, difficilmente esaudibile, è che, per le ragioni sopra viste, si creino quelle condizioni che ne renderanno del tutto superata la necessità. Al di là della riserva che stiamo trattando ed anche in presenza di una utopistica situazione nella quale tutti gli utenti si fossero messi in regola con le norme sulla cyber security, non v'è dubbio che si tenderebbe, in

giurisprudenza, a fare salvo il diritto al ristoro di chi vede leso un proprio interesse e probabilmente questo principio che traspare fra le righe della letteratura dottrinale, può indurre il giudice a stabilire, comunque sia, un equo indennizzo a favore del danneggiato. Questa conclusione sarebbe comunque ben lontana dall'aver sancito un addebito di responsabilità che, riguardando la violazione di una norma di legge, rischia di avere una rilevanza anche penale. Si osserva che questa conclusione è perfettamente compatibile con la constatazione già fatta in precedenza, che i danni cagionati a terzi da perdita o, peggio, da divulgazione delle loro informazioni digitalizzate, sono di evidente natura non patrimoniale, risarcibili quindi sotto l'egida dell'Art. 2059 C.C. Nel caso dell'attacco informatico, la circostanza in cui i pirati siano in grado di superare le difese anche più conservative poste in atto da chi deve difendere il

proprio sistema rappresenta non l'eccezione, bensì la quotidianità. Ciò costituisce un serio ostacolo alla lettura della effettiva responsabilità in capo al soggetto chiamato alla conservazione di dati di terzi ed al giudizio di legittimità di un'azione di responsabilità nei suoi confronti per non aver predisposto le difese idonee a proteggere il patrimonio intellettuale in affidamento dall'azione malevola di chi volesse violarne la riservatezza. Infatti, per quanto sofisticate siano le misure di protezione informatica, si è dimostrato che gli hackers trovano, prima o poi, il modo di superarle. In altri termini, di fronte alla rapidità con la quale progredisce la ars violandi degli hackers, e di fronte alla impari lotta che gli esperti informatici ingaggiano con loro per escogitare contro misure sempre più sofisticate, il giudizio di idoneità delle misure di protezione adottate diventa particolarmente fluido, costretto ad uniformarsi a criteri che si fanno sfuggenti e volatili. Si può affermare che, a fronte di un siffatto scenario, il livello

di idoneità delle protezioni anti-hacker richiama quello che in matematica è definito un asintoto, ovvero quel limite cui la curva (nel nostro caso, la curva che descrive il miglioramento dell'efficacia delle difese) si avvicina indefinitamente senza mai raggiungerlo. Sotto un altro punto di vista, questo limite di idoneità potrebbe essere visto come un traguardo in movimento continuo, la cui mobilità lo rende di fatto irraggiungibile, e per far riemergere una responsabilità da culpa in vigilando, non sarebbe sufficiente dimostrare che al momento dell'attacco esisteva una tecnica di difesa migliore rispetto a quella adottata, ma anche che il gestore dei dati che l'ha usata ne fosse consapevole e, ancora, che egli abbia omesso la diligenza di tenersi debitamente informato, ma anche non avendola omessa, che egli avesse il tempo materiale di apportare gli aggiornamenti alle difese informatiche, da quando è venuto a conoscenza dei nuovi metodi più aggiornati ed efficaci a quando ha avuto luogo l'attacco informatico. A

sostegno di questi dubbi, osserviamo che la nuova normativa europea, che va sotto il nome di Regolamento N. 679 del 27 aprile 2016, che entrerà in vigore nel 2018, stabilisce degli obblighi in capo alle Società che gestiscono nei propri sistemi informatici dati e informazioni di terzi. Tali obblighi riguardano:

- l'adozione di misure di protezione preventiva contro gli attacchi esterni;
- l'obbligo di notifica in capo al gestore nei confronti dei titolari delle informazioni e dei dati gestiti, dell'avvenuto o dell'imminente attacco hacker a danno dei predetti dati e informazioni;
- la denuncia all'Autorità ed ai titolari dei dati affidati in gestione di ogni attacco che dovesse provenire dall'esterno, del quale il gestore fosse a conoscenza, anche se deve ancora avvenire;
- l'adozione di una politica strutturata di Risk Management per la pianificazione degli interventi e per l'aggiornamento delle tecniche di intervento;

L’inadempienza rispetto agli obblighi previsti dalla normativa europea comporta delle sanzioni che vanno dal 4 al 6% del fatturato globale lordo dell’Azienda e possono raggiungere l’ammontare di 20 milioni di Euro. Si osserva che la normativa sanzionatoria prevista dal Regolamento 679 attiene non già la violazione della privacy conseguente ad attacco informatico, bensì la mancata adozione delle misure di protezione informatica e la mancata od omessa notifica dell’avvenuto attacco ovvero, se in grado di verificarlo, dell’imminenza dell’attacco, del rischio di subirlo o della consapevolezza di essere esposto ad un attacco cyber in grado di far perdere il controllo sulla riservatezza dei dati conservati per conto di terzi. L’entrata in vigore della normativa europea rende comunque necessaria una gestione del rischio CYBER che si ispiri ad un modello di Risk Management avanzato e rende del tutto inefficace una strategia che si limiti alla tutela di tipo assicurativo. Il Regolamento 679

di cui sopra integra il disposto dell'Art. 31 del DLgs 196/2003, superando la descrizione eccessivamente generica data da tale articolo e dando finalmente una connotazione specifica alla natura delle misure di difesa da adottare. Il Regolamento 679 fornisce, in definitiva, gli elementi che consentono al gestore di dati di terzi di mettersi in quelle condizioni ideali che lo esimerebbero della responsabilità, in caso di violazione, potendosi quest'ultima ascrivere a causa di forza maggiore.

2.5. *Aspetti giurisprudenziali relativi al "cyber crime"*

Il primo atto legislativo a livello europeo volto a disciplinare la materia sanzionatoria inerente i crimini informatici perpetrati attraverso l'uso della rete (web) risale al 2001. Si tratta della Direttiva n. 185 emanata a conclusione del Trattato di Budapest del 23/11/2001, entrata in vigore il 1° luglio 2004. Tale Direttiva concerneva i temi delle infrazioni penali

commesse via internet e su altre reti informatiche, e trattava temi più generali attinenti gli atti illeciti commessi attraverso il web, quali ad esempio le violazioni dei diritti d'autore, la frode informatica, la pornografia infantile e le violazioni della sicurezza della rete. Il Trattato di Budapest contiene inoltre una serie di misure e procedure appropriate, quali la perquisizione dei sistemi di reti informatiche e l'intercettazione dei dati. In Italia, il Trattato di Budapest è stato ratificato quattro anni più tardi con la Legge 18 marzo 2008, n. 48. L' obiettivo principale del Trattato di Budapest, enunciato nel preambolo, è perseguire una politica, in tema di diritto penale, comune per la protezione della società contro la ciber- criminalità, in special modo adottando legislazioni appropriate e promuovendo la cooperazione internazionale fra i rispettivi organi legislativi. Si tratta sicuramente di un impianto normativo importante ed avente fini del tutto condivisibili, anche se non possiamo esimerci dal

riconoscere che la capacità tecnologica della pirateria informatica internazionale, in termini di abilità nel rendersi difficilmente rintracciabile e localizzabile, ancor più che in termini di perforabilità dei sistemi di protezione informatici più sofisticati, è tale da poter, purtroppo, irridere una normativa scritta, ancorché frutto di una collaborazione internazionale, potendosi avvalere di una astuzia in grado di prendersi gioco dei tutori della legge. Non è un caso che, scorrendo nella Giurisprudenza, troviamo, almeno in ambito nazionale, una ricca legislazione a tutela dei cittadini che affidano a Società ed Enti i propri dati sensibili, oppure a tutela dei diritti di titolarità su contenuti letterari (diritti d'autore), ma assai poco in merito alla tutela dei soggetti che, gestendo dati di proprietà di terzi, sono esposti ad imputazione di responsabilità per violazione del patto di riservatezza, ancorché generato da un atto illecito esterno. In sostanza la legislazione si è mossa per proteggere il rapporto fra utente che mette a disposizione i

propri dati e/o informazioni ed Ente deputato a gestirli (vedi DLgs 109/2003) oppure a definire gli obblighi in materia di prevenzione e protezione in capo a soggetti che gestiscono dati di terzi (Regolamento 679/2016) e qualche volta si è dedicata al riconoscimento dei diritti derivanti dalla proprietà intellettuale. In questa direzione si è mossa anche l'Unione Europea con la Direttiva n. 24 del 15 marzo 2006, recepita in Italia dal DLgs 30 maggio 2008, n. 109. La legislazione non si è profusa nel legiferare a tutela delle vittime della pirateria informatica ed anche quando avesse accennato a farlo, come nel caso della Legge 18/3/2008 n. 48 che ratificava il Trattato di Budapest, si deve il più delle volte arrendere di fronte alla irreperibilità del colpevole. In questo scenario salta all'evidenza l'importanza del Regolamento 679, di cui si è parlato nel precedente paragrafo, ma soprattutto l'importanza di attenersi alle norme ivi previste. Alla luce di quanto fin qui riportato, la tempestiva notifica in

merito ad attacchi informatici siano essi appena subìti, in corso o imminenti, può essere uno strumento fondamentale per alleggerire il carico di responsabilità del gestore nei confronti degli utenti. I dati statistici raccolti da CLUSIT [29] (Associazione Italiana per la Sicurezza Informatica) forniscono un quadro preoccupante che vede crescere in numero e in gravità i casi di Cyber Attacco a danno di utenti pubblici e privati, oltre che in termini di danni economici. Da una statistica condotta dal gruppo assicurativo Allianz, risulterebbe che a livello mondiale i danni economici provocati dal Cyber Crime ammontavano nel 2012 a poco meno di 500 miliardi di Dollari, dei quali quasi il 25% ha avuto luogo negli Stati Uniti, seguiti a poca distanza dalla Germania, con il 21%, mentre in Italia il fenomeno non è ancora diffuso come nei Paesi

[29] Il Clusit, nato nel 2000 presso il Dipartimento di Informatica dell'Università degli Studi di Milano, è la più numerosa ed autorevole associazione italiana nel campo della sicurezza informatica.
Oggi rappresenta oltre 500 organizzazioni, appartenenti a tutti i settori del Sistema-Paese.

menzionati, essendosi registrato un dato complessivo di poco meno di 1 miliardo di Dollari, pari al 2 per mille del totale mondiale, con riferimento allo stesso anno. Il fatto che in Italia il fenomeno sia meno esteso non è affatto tranquillizzante, in quanto significa che nel nostro Paese il problema ha ancora un margine di crescita assai elevato e che registrerà una impennata tanto più pronunciata, quanto meno il problema sarà gestito in materia di prevenzione e pianificazione delle difese. Ovunque nel mondo, il problema è sotto stretto monitoraggio ed è stato pertanto possibile accertare che i danni cagionati alla società civile dalla pirateria informatica sono in continuo e costante aumento nel mondo ed anche l'Italia non è risparmiata dalla crescita di questo fenomeno. Per dare un ordine espositivo, viene spontaneo fare un distinguo fra quello che è l'atteggiamento dell'utente di rete nei confronti del pericolo di finire nel mirino della pirateria informatica, e quello che invece è il comportamento tenuto nei confronti

dello stato di emergenza quando l'evento temuto è diventato una drammatica realtà, ed a tal fine si riscontra nella posizione nei confronti del rischio potenziale una sostanziale indolenza dell'utente medio, mentre nei confronti dell'emergenza, uno stato di smarrimento aggravato da un senso di impotenza, che induce spesso ad affidarsi a chi si conosce meglio, senza operare una selezione sul grado di preparazione tecnica di coloro cui si rivolgono per cercare di mettere una pezza alla situazione di crisi. La criticità maggiore nel comportamento della popolazione dell'utenza si riscontra nella fase in cui si devono pianificare le difese preventive. In altri termini, se andiamo ad analizzare un campione di possibili bersagli di attacchi cibernetici, ma che non hanno ancora fatta l'esperienza di una intrusione da parte di hackers, troveremo un atteggiamento quanto meno scettico e spesso restio ad accettare l'idea che occorre farsi trovare preparati, nei limiti che le tecnologie oggi conosciute lo consentono. Il comportamento delle vittime

dell'attacco Cyber è quello che in ultima analisi determina le scelte da parte dei pirati della rete. Una risposta che dimostra una propensione per l'accettazione di pagare il riscatto, visto che questo ha delle dimensioni certamente sopportabili dalla singola vittima, è certamente in grado di dare un nuovo impulso all'attività di pirateria informatica, così come il ricorso a contromisure di prevenzione, di protezione, di tutela legale ed anche assicurativa dovrebbe dare un impulso all'affinamento delle tecniche di intrusione, al fine di renderle meno osteggiabili dalle contromisure che la tecnologia del momento è in grado di offrire. In sostanza si verifica una sorta di competizione tecnologica fra hackers e Società specializzate nell'escogitare contromisure sempre più sofisticate, ma è una gara nella quale gli hackers sono sempre un passo avanti e talvolta anche con vantaggi più consistenti. Il Risk Management langue da anni in una condizione di pecora nera delle strategie imprenditoriali nei confronti dell'universo

Rischi e danni. Un po' questa posizione in ombra è da attribuire ad una cronica imprecisione, che grava sia sulla definizione stessa di Risk Management, spesso scambiato per una funzione di interfaccia dell'Azienda con le Compagnie di Assicurazioni, che si traduce in ultima analisi in un presidio per trattare ad ogni scadenza la possibilità di ricavare un ulteriore riduzione del costo delle polizze. In altri casi il Risk Management è concepito secondo la sua struttura classica basata sui tradizionali quattro pilastri (Analisi, trattamento, ritenzione, trasferimento) e, in questa veste, finisce per ridursi all'enunciazione di una teoria che rimane però scollegata con la gestione effettiva del rischio Aziendale. Sono poche oggi, nel nostro Paese, le Imprese che mettono in atto una accurata strategia di Risk Management, pianificata, sistematica e monitorata. Nella sua forma più avanzata il Risk Management deve partire con il censo degli interessi da salvaguardare, ordinati secondo la scala di priorità più appropriata ed il vaglio delle possibili

cause di pregiudizio e delle modalità in cui questo si può verificare. Successivamente deve fare un censo delle misure di protezione e prevenzione necessarie e di quelle fra esse che sono disponibili, accanto ad una valutazione di fattibilità nel reperire o nei mettere in atto quelle mancanti, attraverso l'installazione di presidi fisici e l'instaurazione dei presidi procedurali ed organizzativi, con un occhio dedicato alla convenienza di ciascuna alternativa di intervento in base al rapporto costo / beneficio di ogni passo previsto dalla pianificazione. Per quanto l'affermazione che segue possa apparire contro-corrente, la freddezza nella scelta dell'intervento in base alla convenienza economica deve tenere conto di tutte le alternative, compresa quella di cedere al ricatto dell'estorsione, soprattutto quando si è consapevoli che ogni minuto che va ad aggiungersi al periodo di inaccessibilità ai propri dati, può far crescere costi e pregiudizi fino al raggiungimento ed, al successivo, superamento della soglia di sopportabilità finanziaria. In

tal caso vanno messi su un piatto della bilancia i pregiudizi da interruzione di attività parametrati sulla maggior durata dell'intervento tecnico che può portare allo sblocco senza cedere al ricatto dell'hacker, nonché del suo costo, mentre sull'altro piatto, l'ammontare del riscatto ed i pregiudizi che si saranno potuti contenere o ridurre, per aver scelto la soluzione più rapida. Nel fare queste scelte non si può tuttavia dimenticare che il cedimento al ricatto dell'hacker mette il ricattato nella condizione di vedersi addebitata l'imputazione di complicità con l'azione illecita della pirateria informatica. Questo aspetto, che ha sicuramente una valenza di carattere generale, diventa particolarmente critico quando il titolare legittimo dei dati sottoposti ad attacco a scopo di estorsione è un terzo rispetto al gestore dei dati stessi. È interessante annotare l'informazione che ci viene fornita dal Rapporto CLUSIT 2017, fresco di stampa, circa l'evoluzione (che il documento denomina maturazione) di uno specifico Cyber Risk

Management, che vede la diffusione presso numerose aziende italiane di una politica di RM che cresce attraverso un processo di evoluzione culturale, schematizzabile secondo tre livelli (denominati generazioni), così suddivise: Primo livello (generazione). Attività basata su valutazione di tecnologie orientata a identificare le vulnerabilità tecniche. Secondo livello: Diagnosi organizzativa e di processo e acquisizione della consapevolezza che il rischio informatico può venire anche dall'interno dell'Azienda. Terzo livello: valutazioni integrate tra organizzazione, processo e tecnologia – misurazione economica del rischio – definizione degli assets strategici - pianificazione della loro protezione e ottimizzazione delle risorse. Col primo livello inizia il percorso di acquisizione della consapevolezza del Cyber Risk con l'identificazione delle vulnerabilità tecniche. Questa attività preliminare deve partire necessariamente con l'individuazione fra gli innumerevoli dati ed informazioni memorizzate nei vari sistemi informatici

presenti in azienda, quelli che rivestono carattere strategico e ai quali va data la priorità nell'attività di definizione dei perimetri di protezione da fortificare. Lo spunto interessante del secondo livello è l'acquisizione della consapevolezza che il rischio informatico può venire anche dall'interno dell'Azienda. Questo elemento, oltre a prendere in considerazione la possibilità che il patrimonio delle informazioni strategiche è vulnerabile anche rispetto ad un atto di infedeltà di un dipendente o da un comportamento non ligio alle mansioni affidate (come il caso del dipendente che naviga in internet per motivi personali col computer aziendale, od anche semplicemente collegandosi alla porta USB per ricaricare la batteria dello smart-phone, esponendo così il sistema all'ingresso di virus e di programmi malware, che poi si diffondono attraverso la rete interna) ci ricorda, giustamente, che il rischio informatico non si limita al Cyber Crime, che è e comunque resta il fattore di rischio più significativo, ma comprende anche fatti derivanti da

disguidi tecnici o da comportamenti umani non necessariamente criminosi, quali errori e negligenze. È certamente apprezzabile che la gestione ed i trattamenti dei rischi possa evolvere attraverso la progressione di questi steps che sono, in defintiva, livelli crescenti di consapevolezza, (che il documento definisce livelli di maturità). Tuttavia, affinché questo encomiabile sforzo non si perda nei corridoi che portano alla cabina di comando dell'impresa, è necessario avere ben chiara la priorità della comunicazione, ricordando che questa risulta tanto più efficace, quanto meglio viene compreso il messaggio da chi lo deve ricevere. È pertanto opportuno che lo staff preposto al Risk Management, operi in stretta collaborazione col Chief Information Officer aziendale per presentare in forma congiunta degli schemi di awareness (mettere al corrente del pericolo) usando forme espressive che traducono in numeri di bilancio gli effetti temuti dai rischi che sono oggetto di analisi, in modo che l'impatto sul business aziendale e

quello sugli assets patrimoniali siano leggibili con facilità e con immediatezza da parte del CEO e che il questo, o comunque il top management impari a ragionare in termini strategici anche sulla gestione pianificata dei rischi, integrandola nelle valutazioni della strategia di impresa. Infatti uno dei più importanti intoppi nella affermazione di una politica di Risk Management integrato sta nel fatto che chi in Azienda ci crede profondamente è l'addetto responsabile, ovvero il Risk Manager, che però fatica a comunicare in linguaggio CEO i suoi timori per la sicurezza. Il documento tratto dal Rapporto CLUSIT 2017 accenna a questo difetto di comunicazione ed all'auspicio che venga superato, individuando nel terzo livello (generazione) di evoluzione del CRM la presenza dell'elemento che orienta la politica di RM verso questo traguardo: la quantificazione economica del rischio. Il Risk Management avanzato prevede anche la gestione separata del rischio attraverso la costituzione di

un Fondo di Auto-finanziamento. Per la consultazione di queste tecniche di gestione del rischio si rimanda al volume "IL RISK MANAGEMENT GLOBALE" edito da Assinews. Se diamo uno sguardo all'attività di management del rischio Cyber oltre frontiera, osserviamo che l'esperienza nei danni da pirateria informatica su scala globale vede in pole position gli Stati Uniti d'America. Sotto un profilo assicurativo il mercato americano è all'avanguardia, ma in un testa a testa con il mercato Britannico, che certamente non è secondo a nessuno in questo comparto. Esistono infatti validi prodotti assicurativi per la copertura del rischio Cyber su entrambi i fronti, talvolta proposti in abbinamento a servizi sia di assistenza informatica continuativa (24h/giorno – 7gg/settimana) di tipo tecnologico informatico, sia per il monitoraggio preventivo, che per il disaster recovery, che agisce secondo un piano di emergenza, in costante aggiornamento, da attivarsi ad attacco in corso o già

avvenuto. Un interessante progetto che ha visto una sua realizzazione in Italia nasce in parallelo all'esperienza americana, ma muovendosi con le proprie gambe, con un prodotto/servizio che si presenta persino più completo rispetto al suo omologo di matrice americana, in quanto comprende anche un servizio di assistenza legale, fornito da uno studio di notorietà internazionale. Si tratta di un progetto che non fa più affidamento cieco alla copertura assicurativa, ma la gestisce come risorsa esterna, da inserire e integrare nel quadro di una gestione a 360 gradi che parte dal monitoraggio delle fonti di rischio, allo studio di come fronteggiarle, alla messa a punto dei presidi necessari a proteggere il proprio interesse, salvaguardando in primo luogo quelli vitali per la sussistenza dell'Azienda. Questo prodotto domestico ha il merito di aver aperto in ambito nazionale, la strada verso una visione più moderna della gestione del rischio, come una nave rompighiaccio apre il cammino attraverso i ghiacci del Polo, per spianare la strada verso obiettivi di

sicurezza sempre più al passo coi tempi.

3. LA STRATEGIA OPERATORI TRADIZIONALI E DEGLI INCUMBENTS

L'obiettivo del presente capitolo è quello di analizzare la possibilità che una strategia digitale possa essere presa in considerazione ed implementata da parte degli operatori tradizionali del mercato. La trasformazione digitale potrebbe rivelarsi quindi una minaccia per gli operatori incumbent.

3.1. *Sviluppo di una innovativa strategia d'impresa attraverso i nuovi modelli di Business*

Le imprese di assicurazione, nonostante abbiano storicamente minore capacità di reazione ai cambiamenti, rispetto ad altri settori economici, si trovano oggi al punto di dover ridefinire le proprie priorità strategiche al fine di attuare la loro trasformazione digitale. Si trovano infatti di fronte ad un bivio: per sfruttare al meglio le

opportunità che offre la digitalizzazione dell'economia, dovranno reinventare le proprie attività. Il numero costantemente in crescita di dati forniti dai dispositivi IoT offre la possibilità di proporre e distribuire prodotti innovativi e digitalizzati. Inoltre, le possibilità offerte dalle tecnologie di cloud computing, facilmente implementabili e rapidamente accessibili, consentono alle imprese assicurative la possibilità di soddisfare maggiormente i propri clienti, con l'obiettivo di massimizzare la fidelizzazione i clienti. Le nuove tecnologie ed il loro conseguente impatto sul settore assicurativo rendono il rischio maggiormente gestibile e mitigabile, per mezzo di strumenti come l'intelligenza artificiale e l'apprendimento automatico. Al momento attuale, in cui le opportunità di sviluppo sono enormi, ma in cui, allo stesso tempo, la minaccia delle startup InsurTech si fa sempre più concreta, è necessario per gli operatori incumbent procedere con la digitalizzazione della catena del valore. Le compagnie assicurative

dovranno ridefinire il proprio comportamento e cercare di interpretare le necessità dei propri clienti, al fine di prendere decisioni che riguardino nuovi servizi e nuovi prodotti da collocare sul mercato, nuove modalità di distribuzione dei prodotti e nuovi segmenti di mercato da raggiungere. Come anticipato, quindi, sarà fondamentale servirsi di quei dispositivi e sensori intelligenti che possano monitorare lo stile di vita ed il comportamento degli assicurati. Si rende, quindi, necessaria l'implementazione di un database e di soluzioni tecnologiche, quali software e piattaforme, necessari per l'elaborazione della grande quantità di dati generata dai suddetti dispositivi. Questo è certamente il primo passo da compiere per ottenere successo all'interno della trasformazione digitale. Entrando maggiormente nel dettaglio, le compagnie assicurative dovranno realizzare un'esperienza "omnichannel" per i propri clienti. Anche in campo assicurativo, infatti, i clienti ricercano l'esperienza a cui sono abituati in altri settori, desiderano

poter accedere ai servizi offerti attraverso una vasta gamma di canali, senza interruzioni derivanti dal dover ripetere passaggi già compiuti o dal dover reinserire dati già forniti. In altre parole, sarà necessario procedere all'implementazione di piattaforme attive 24 ore su 24, per tutti i canali di distribuzione, funzionali per gestire i rapporti con i clienti e con i partner di vendita. Inoltre, ai clienti dovrà essere consentito di accedere facilmente ad un'area riservata tramite cui poter gestire le proprie polizze ed apportare modifiche (come ad esempio la modifica dell'indirizzo di fatturazione) e di poter, in qualsiasi momento, inoltrare un reclamo o denunciare un sinistro. Le imprese tradizionali, inoltre, dovranno, rivedere chiaramente le proprie linee di business al fine di fornire prodotti su misura a segmenti di clientela specifici ed integrare il servizio anche con prodotti non assicurativi, realizzando una strategia di cross-selling. Per realizzare queste priorità strategiche, le aziende assicurative dovranno rivedere i processi aziendali, la

forza-lavoro e la "customer experience". L'obiettivo ultimo della digitalizzazione dell'industria assicurativa è quello di creare prodotti sempre più mirati e "taylor made" per le esigenze della propria clientela, partendo dall'analisi dei dati comportamentali dei clienti stessi, rilevati attraverso l'utilizzo di apparecchi tecnologici. L'automazione dei processi, oltre a ridurre i costi operativi, aumenta la soddisfazione dei clienti, andando a toccare ogni fase della catena del valore, indipendentemente dalla linea di business o dal canale distributivo scelto. Qualora la rete di distribuzione e i processi di vendita rimanessero tradizionali, quindi governati da processi sostanzialmente manuali senza l'attuazione di processi automatizzati, vi è la possibilità concreta che la digital disruption contribuisca alla crisi delle aziende che non si adegueranno. Tuttavia, le aziende assicurative avranno bisogno non solo di automatizzare ulteriormente i processi di base, ma dovranno anche implementare l'utilizzo della robotica

con l'intelligenza artificiale e l'analisi avanzata dei dati, per poter prendere decisioni più consapevoli e più velocemente. Grazie alla grande quantità di dati generati tramite l'intelligenza artificiale e l'apprendimento automatico le compagnie assicurative possono sviluppare le loro capacità predittive, in modo tale da migliorare i processi operativi e mitigare il rischio. Le compagnie assicurative che desiderano implementare processi orientati al cliente, ma che, allo stesso tempo, siano anche efficienti, devono procedere con la digitalizzazione end-to-end, la strada da percorrere per ridurre significativamente gli interventi manuali. La tradizionale digitalizzazione dei processi, da sola, può, infatti, incrementare l'efficienza fino al 15-20%. Un'altra possibilità può essere quella di esternalizzare alcune singole fasi del processo, come l'inserimento dell'indirizzo o il fornire al cliente le istruzioni per i pagamenti, è una pratica piuttosto diffusa, pratica che può portare a riscontri positivi, nel caso in cui la clientela

reputi attraente la modalità con cui ha luogo l'interazione. Al giorno d'oggi, grazie all'utilizzo di strumenti digitali (smartphone, tablet, ecc) vengono generati una mole gigantesca di dati, consentendo, quindi, di ottenere il profilo della clientela in maniera più dettagliata e precisa e di progettare nuovi prodotti, migliorando la segmentazione del rischio e affinando le politiche di prezzo. I benefici che ne derivano per le imprese d'assicurazione saranno significativi, tra cui:

- Comprovato miglioramento nella fidelizzazione della clientela;
- Ulteriori opportunità di cross-selling, grazie alla maggiore interazione che si viene a creare con i clienti;
- La promozione attraverso i social media da parte dei clienti già fidelizzati che genera interesse tra gli utenti.

Per raggiungere un alto grado di automazione, si richiede, tuttavia, che le compagnie tradizionali

modifichino profondamente la loro architettura IT, dal momento che ogni livello è interessato dalla digitalizzazione. Si renderà, inoltre, necessaria una revisione del sistema di gestione dei reclami e dei sinistri con l'introduzione di nuovi sistemi di robotica o strumenti di gestione del flusso di lavoro aggiornati. Per guidare questo processo introduciamo cinque strategie di risposta generiche, ognuna delle quali è rivolta agli appartenenti ad un determinato campo della matrice InsurTech ne valutiamo l'adeguatezza e riportiamo i casi osservati sul mercato.

Osservare

I cosiddetti *lightweights*, vale a dire tutte le startup InsurTech che si posizionano su una traiettoria "sustaining", con capitale disponibile limitato, non richiedono una risposta immediata da parte degli assicuratori tradizionali, ma il loro obiettivo principale dovrebbe essere quello di raccogliere informazioni sul

modello di business delle startup, sulla tipologia dei loro clienti target e sulla struttura del prodotto offerto. Ciò non significa che gli incumbents devono sentirsi troppo sicuri di sé, dato che i lightweights sono in grado di realizzare importanti progressi in qualsiasi momento, il che migliorerebbe notevolmente la loro attuale posizione trovando facile accesso al capitale e realizzando vantaggi di scala. Per prepararsi adeguatamente a questo tipo di minacce, gli incumbents devono avere la capacità di reagire rapidamente al fine di riposizionarsi nel nuovo contesto competitivo. Anche se questa strategia sembra essere appropriata per contrastare la maggior parte dei lightweights, è generalmente complicato riuscire ad individuare i primi movimenti innovativi. Come indicato nel capitolo precedente, la startup tedesca GetSafe è nata inizialmente come broker digitale e ora sta diventando una vera e propria compagnia assicurativa. Tuttavia, alla luce del fatto che la loro offerta costituisce un'innovazione "sustaining" e che le loro prospettive di

successo sono attualmente alquanto incerte, si raccomanda agli assicuratori primari di seguire una strategia di osservazione.

Competere

Gli usual suspects, invece, superano i lightweights per quanto concerne il capitale disponibile. Dato che le loro offerte migliorano i prodotti e i servizi (sustaining innovation), è raccomandabile agli incumbents di entrare in diretta competizione con loro. Grazie infatti al loro notevole vantaggio in termini di potere di mercato, questi ultimi sono in grado di attaccare in modo aggressivo le nuove startup con l'obiettivo ultimo di escluderle dal mercato. È di fondamentale importanza che gli incumbents non ritengano, erroneamente, che tali imprese siano di scarsa rilevanza, poiché in tal caso si perderà l'occasione di intervenire nel momento cruciale e, senza aver preso le contromisure necessarie, la perdita di quote di mercato sarà ancora più costosa da recuperare. Nel loro

elaborato sul mercato assicurativo statunitense delle piccole imprese, Boston Consulting Group sottolinea che sia gli agenti indipendenti che gli assicuratori disposti a sostenerli sono tenuti a compiere alcune "no-regret moves" per entrare in competizione diretta con i broker digitali, come Knip. In altre parole, gli agenti dovrebbero entrare in concorrenza sviluppando servizi e offerte di vendita più incentrati sui clienti e consolidando le loro partnership con gli assicuratori, diventando così una componente importante dell'ecosistema assicurativo del futuro. Le compagnie di assicurazione, d'altro canto, dovrebbero sviluppare nuovi prodotti a struttura modulare, garantire che le loro capacità informatiche di e-commerce siano aggiornate e migliorare la capacità dei loro modelli di pricing. Ciò aiuterebbe a trasferire il loro processo di sottoscrizione nell'universo digitale, aumentando in misura significativa la loro efficienza.

Investire

Le startup classificate come minacce stanno già sviluppando prodotti e servizi "disruptive", ma attualmente sono ancora a corto di capitale. Ciò offre l'opportunità per gli incumbents, che dispongono di capitale elevato, di seguire una strategia di investimento, promuovendo l'innovazione al di fuori del proprio bilancio; non importa se l'innovazione origina da fondi di venture capital (come ha fatto Allianz nel 2015), da programmi di incubators e di accelerators (come l'accelerators InsurTech di Swiss Re) o dagli investimenti diretti in InsurTechs. Spostiamo la nostra analisi su un caso concreto. Le offerte dell'assicuratore on-demand Slice sono molto simili a quelle di Trov; tuttavia, con l'attuale livello di finanziamento (pari a circa 4 milioni di dollari), il capitale disponibile di Slice è strettamente limitato (Trov 92 milioni di dollari americani) e, di conseguenza, la prima startup è considerata un obiettivo interessante per gli assicuratori tradizionali che

perseguono una “strategia di investimento”. Un diverso approccio d’investimento è stato adottato dalla compagnia di assicurazione leader AXA, che ha lanciato nel 2015 il proprio incubatore InsurTech (AXA Kamet con 100 milioni di EUR) e il fondo di venture capital (AXA strategic ventures con 230 milioni di EUR). L’attività di quest’ultimo ha un orientamento internazionale, avendo uffici a San Francisco, New York, Londra e Parigi, e si rivolge in modo specifico alle assicurazioni verticali, ai servizi finanziari, ai software per le imprese e alle tecnologie finanziarie e assicurative (nei primi due anni sono stati effettuati 20 investimenti.

Sviluppare

I “disrupters”, vale a dire gli assicuratori dotati di un’innovazione “disruptive” già ben finanziata, non possono più essere affrontati con una strategia d’investimento. Poiché questi nuovi operatori sono potenzialmente in grado di plasmare l’attuale struttura del

mercato, gli incumbents non dovrebbero confidare ciecamente sulla loro attuale posizione e sulla loro clientela, ma rafforzare ulteriormente le proprie capacità. Ad esempio, gli assicuratori tradizionali dovrebbero concentrarsi sulla promozione della digitalizzazione, sullo sviluppo di tecnologie innovative all'interno dell'azienda, cercando allo stesso tempo di anticipare le future esigenze dei clienti. La strategia di sviluppo non è solo una risposta efficace contro i disrupters, ma garantisce anche vantaggi tecnologici nei confronti dei competitors affermati del settore assicurativo. Generali, ad esempio, ha recentemente avviato una partnership con Microsoft e ha iniziato a "sviluppare" internamente il progresso tecnologico. Secondo Generali, l'obiettivo di questa collaborazione non è solo quello di migliorare i processi operativi e l'efficienza operativa dei dipendenti e degli agenti, ma anche quello di creare nuovi prodotti assicurativi e modelli di business attraverso le innovazioni digitali (una piattaforma tecnologica digitale

mira a fornire una più efficace interazione e porta in primo piano la centralità del cliente211).212

Cooperare

Gli assicuratori tradizionali hanno anche la possibilità di cooperare con startup InsurTech che forniscono innovazioni "enabling". Abbracciando l'offerta tecnologica dei loro nuovi partner, gli incumbents sono in grado di ottenere vantaggi commerciali; inoltre, le partnership consentono loro di accedere allo stadio più all'avanguardia della digitalizzazione, senza essere esposti a rischi sconosciuti associati allo sviluppo interno di nuove tecnologie e a complesse attività d'investimento; allo stesso tempo, agli incumbents viene offerta un'importante opportunità per migliorare l'esperienza del cliente, mentre le startup continuano a cercare la loro posizione all'interno dell'ecosistema assicurativo. Tuttavia le compagnie assicurative tradizionali e le startup InsurTech presentano differenze significative,

concernenti diverse importanti dimensioni aziendali, che potrebbero ostacolare una proficua collaborazione. In particolare, sulla base di un'indagine empirica tra gli assicuratori e le startup, Celent rileva che le due dimensioni della "tolleranza al fallimento" e della "rapidità decisionale" hanno suscitato il maggior numero di divergenze tra gli intervistati. Inoltre i diversi progressi a livello tecnologico, ossia "sistemi IT all'avanguardia" rispetto ai "sistemi IT tradizionali", sono considerati un ulteriore ostacolo alla partnership, anche se questo è contemporaneamente uno dei principali fattori che spingono gli incumbents a collaborare con le startup InsurTech. Il vero problema è che gli assicuratori tradizionali incontrano gravi difficoltà ad adeguare le loro strutture all'interno di un'impresa già operante, continuando a tenere sotto controllo l'elemento della redditività. Un esempio recente di cooperazione di successo è la collaborazione tra Munich Re e Trov30

[30] *Munich Re* non è considerata la compagnia assicurativa tradizionale corrispondente a *Trov*. *Trov* offre un'innovazione "*disruptive*" nel mercato

negli Stati Uniti: Trov fornisce una piattaforma tecnologica mobile, che consente ai clienti di attivare e disattivare a piacimento la copertura assicurativa per specifici oggetti personali;31 l'obiettivo di Munich Re è quello di fornire tale servizio negli Stati Uniti, utilizzando la piattaforma tecnologica digitale di Trov. Il servizio facilita l'accesso ad un segmento assicurativo sotto-servito e genera dati in tempo reale sugli articoli assicurati, consentendo di fornire prodotti su misura.

Ignorare

Infine, gli assicuratori storici potrebbero confidare nelle barriere all'ingresso del settore assicurativo, vale a dire sulla sua elevata regolamentazione e sulla richiesta di requisiti patrimoniali elevati, e ignorare completamente la tendenza InsurTech. Tuttavia, occorre tener conto del fatto che tale strategia è altamente pericolosa; come disse William Edwards

esistente degli assicuratori elementari.

Deming (1900-1993), un fisico americano: “Survival is optional. No one has to change”. La trasformazione digitale rende necessario lo sviluppo di nuove competenze, dando vita a nuovi ruoli all’interno delle imprese (Simpson A., 2013). I processi automatizzati, infatti, rimpiazzano le attività manuali, riducendo lo svolgimento di attività ripetitive e la necessità di personale preposto a tali operazioni. I prodotti offerti diventano sempre più complessi e personalizzabili; si rende, quindi, necessario lo sviluppo di prodotti sempre più innovativi che richiedono personale in grado di calcolarne i rispettivi premi. Attualmente, le aziende tradizionali, stanno vivendo ciò che possiamo definire come ricambio generazionale: infatti, mentre, i nati negli anni ’50-60 del secolo scorso vanno in pensione, i giovani, nati nell’epoca digitale e quindi dotati di ampie conoscenze informatiche, si affacciano, per la prima volta, sul mondo del lavoro. Si viene, quindi, a creare un divario notevole nella

conoscenza organizzativa di queste due categorie di lavoratori: i giovani dipendenti dovranno essere affiancati da personale più esperto, che li supporti nell'andare a ricoprire il ruolo dei loro predecessori più anziani; allo stesso tempo, vi è, però, la necessità d'impiegare una forza lavoro digitalmente abilitata, per andare ad incrementare la produttività. Le imprese, devono, quindi, trovare il modo di riuscire a sfruttare le conoscenze tecniche e le lezioni impartite dai senior executive, e di riuscire a diffondere tali conoscenze attraverso tutta la struttura aziendale. Altrettanto importante è la necessità di andare a creare un ambiente di lavoro che riesca ad attirare i "millennial", esperti di tecnologia. Per restare competitive, quindi, le compagnie assicurative dovranno trasformare i propri uffici e le proprie agenzie in spazi di lavoro collaborativi e flessibili, al fine di evitare che i giovani lavoratori più talentuosi s'indirizzino verso altri concorrenti, che dispongono

di un ambiente di lavoro più moderno. Ruolo fondamentale in questa fase è quello ricoperto dal "CIO" (Chief Integration Officer), dirigente aziendale incaricato di garantire il coordinamento di tutti i sistemi che interagiscono all'interno dell'azienda. Questa figura professionale viene ad assumere un ruolo fondamentale nel collegare la strategia aziendale e l'implementazione dell'Information Technology, contribuendo ad identificare ed applicare le tecnologie emergenti alla roadmap aziendale (Techtrends Deloitte, 2015).

Inoltre, è possibile inserire proprio in questa fase di mutamento la figura del "CDO" (Chief Digital Officer), un professionista dotato di forti competenze tecnologiche e che, allo stesso tempo, conosca i processi aziendali. Tale figura professionale può rivestire un ruolo fondamentale all'interno dell'azienda evitando la duplicazione di alcune operazioni che possono essere svolte in automatico ed

elaborando una metodologia per una nuova valutazione della customer experience. La tecnologia digitale e la nuova valutazione della customer experience possono facilitare gli utenti, consentendo loro di muoversi rapidamente e senza problemi attraverso i diversi canali e punti di contatto con l'azienda. I clienti, infatti, si aspettano un servizio personalizzato e di alta qualità, su qualsiasi tipo di canale: nel rapporto face-to-face, via telefono, Internet o videoconferenza. I canali digitali, infatti, dovrebbero garantire una risoluzione più veloce dei problemi ed un accesso più rapido a risorse ed informazioni. Purtroppo, in realtà, tale situazione ad oggi è paradossalmente il contrario, nel senso che l'avvio della trasformazione digitale ha reso sotto alcuni punti di vista ancora più lenta e macchinosa l'operatività quotidiana. Tale situazione si riflette, il più delle volte nel fatto che i clienti cambiano frequentemente la loro Compagnia assicurativa di

riferimento, poiché la Compagnia che sembra aver intrapreso la strada della completa digitalizzazione risulta più attraente di una Compagnia tradizionale. Tali imprese, quindi, dovranno essere in grado di attuare una strategia che offra ai propri clienti esperienze nuove, personalizzate e differenziate con l'obiettivo ultimo di risolvere i problemi in maniera più veloce ed efficiente ed aumentare di conseguenza la fidelizzazione dei clienti stessi. L'obiettivo principale, quindi, per le compagnie assicurative, deve essere il ripensamento dell'esperienza del cliente, in maniera completa, e non limitandosi a correggere soltanto le inefficienze riscontrate lungo il percorso. Le esigenze e le preferenze manifestate dai clienti devono costituire sia il punto di partenza, sia l'ulteriore conferma, durante il processo di sviluppo. I clienti dovranno essere coinvolti nel processo stesso di sviluppo del prodotto, e tale sviluppo dovrà essere verificato secondo i feedback stessi che i clienti

forniranno. Importante e strategico sarà cercare di comprendere le reali esigenze dei clienti sin dall'inizio del processo di definizione di nuovi prodotti e processi. Alcune compagnie assicurative, stanno già sviluppando la possibilità di accesso ai propri dipendenti ai dati raccolti dalla compagnia stessa, in merito all'opinione dei clienti, dati costituiti principalmente dai feedback raccolti attraverso i social media o mediante il contatto telefonico con il servizio di assistenza. In definitiva, la rivalutazione e ridefinizione dei processi aziendali, della forza-lavoro e della "customer experience" non si rivelerà soltanto una strada per creare valore al giorno d'oggi, ma fornirà le basi per affrontare il futuro e le sfide sempre più stimolanti che la tecnologia saprà offrire nei prossimi anni. In altre parole, le startup InsurTech si affacceranno sul mercato già pronte sotto questi punti di vista della rivalutazione della customer experience, della forza-lavoro e dei processi aziendali

e i risparmi ottenuti da parte delle compagnie assicurative tradizionali in termini di riduzione dei costi dei processi (qualora applicati) si riveleranno fondamentali per competere ad armi pari sul mercato e per realizzare investimenti in prodotti e servizi innovativi. Una minaccia fondamentale per gli assicuratori tradizionali è rappresentata dal fatto che le innovazioni del modello aziendale, basate sulla tecnologia di alcune startup, possono portare ad una vera e propria disintermediazione. In altre parole, se le imprese InsurTech riusciranno a stabilire un percorso dal rischio al capitale più diretto ed efficiente, alcuni incumbents potrebbero trovarsi di fronte al pericolo di scomparsa, a causa della loro scarsa rilevanza oppure della concorrenza. Se questo scenario dovesse verificarsi, l'unica via di fuga per gli operatori tradizionali sarebbe una drastica innovazione dei loro modelli di business, in modo da

rivolgersi a mercati e segmenti di clientela completamente nuovi.

Come illustrato, diversi settori industriali hanno subito cambiamenti fondamentali nell'equilibrio di potere, dal momento che i nuovi operatori tecnologici come Uber, Facebook, AirBnB o Alibaba (KPMG, 2015) sono riusciti a conquistare i punti di accesso chiave al cliente; nello stesso tempo, la pressione sul settore bancario è in aumento dal momento che le società FinTech come LendingClub o Prosper hanno introdotto il concetto peer-to-peer, che collega prestatori e richiedenti senza la necessità di intermediari finanziari. Anche se un modello simile può essere più complesso da applicare nel settore assicurativo, gli esempi citati dimostrano che sarebbe imprudente ignorare tale possibilità. Che cosa succederebbe se i canali di distribuzione digitale fossero in grado di declassare le compagnie assicurative in veri e propri depositi di rischio? E se,

in uno scenario più estremo, le persone fossero in grado di trasferire i propri rischi anche senza compagnie di assicurazione?

3.2.*La risposta delle compagnie tradizionali*

Il settore assicurativo, storicamente, si è rivelato come uno tra i settori più conservativi e contrario nei fatti al cambiamento tecnologico, a causa principalmente dei seguenti fattori: la regolamentazione stringente, la complessità dei prodotti offerti e le ampie dotazioni patrimoniali delle grandi compagnie assicurative. Per decenni, quindi, si è mostrato come un settore con enormi barriere all'ingresso. Negli ultimi tempi, però, sono emersi nuovi concorrenti, le cd. startup InsurTech, a partire dai motori di ricerca delle polizze tradizionali offerte dalle compagnie cd. telefoniche. Un primo passo effettuato da parte delle compagnie tradizionali è stato quello di creare compagnie on-line, controllate al 100% dalle compagnie tradizionali,

ma che in prima istanza eliminano la rete degli intermediari eliminando di conseguenza i costi relativi alle provvigioni da rimettere agli agenti/broker. Ultimamente è stato un periodo difficile per il settore assicurativo. Con le aspettative dei clienti in rapida evoluzione che si combinano con le interruzioni digitali in un settore fortemente regolamentato, non c'è da stupirsi che molte organizzazioni stiano iniziando a sentirne il calore. E' doveroso pertanto identificare diversi fattori che negli ultimi anni hanno contribuito a creare un ambiente commerciale difficile per gli assicuratori. La concorrenza basata sui prezzi, i bassi livelli di crescita sia nei mercati maturi che nelle linee discrezionali, il calo della fedeltà dei clienti, le mutevoli richieste dei clienti e gli scarsi rendimenti degli investimenti del ramo vita hanno destabilizzato il settore e lasciato molte parti incerte sulla loro prossima mossa. Tra queste tendenze, le mutevoli richieste e aspettative dei

clienti stanno colpendo il settore assicurativo in modo particolarmente duro. Sebbene si tratti di un fenomeno ormai diffuso in tutti i settori, gli assicuratori non hanno necessariamente il rapporto più profondo e duraturo con i loro clienti per cominciare, il che rende la questione difficile da affrontare. I consumatori provano la scelta assicurativa come impersonale, dispendiosa in termini di tempo e costosa. L'assicurazione è un acquisto che non crea empatia immediata con le comuni logiche di prodotto e sia i consumatori che gli assicuratori trovano che non ci sono molti punti di contatto nel rapporto che hanno tra di loro. Spesso l'esperienza che i clienti hanno non è in linea con le loro esigenze e le loro aspettative, ma più in linea con i limiti dei prodotti che gli assicuratori offrono, e la scarsa esperienza dei clienti che essi forniscono. Questo potrebbe riguardare l'acquisto di nuovi prodotti o il percorso dei sinistri. Oltre a un cambiamento nelle

richieste dei loro consumatori, gli assicuratori devono anche affrontare cambiamenti nella composizione dell'ecosistema del settore. La perturbazione digitale e l'innovazione hanno portato alla creazione di startup assicurative, che sono in grado di offrire prodotti completamente diversi in un modo completamente diverso. C'è stato un enorme investimento nell'insurTech che è arrivato in termini di nuove capacità, offerte e servizi per i clienti delle compagnie di assicurazione tradizionali e questo sta iniziando a causare disordini. Alcuni esempi specifici potrebbero essere i modelli assicurativi peer to peer - come Friendsurance - che supportano la condivisione del rischio e la condivisione dei guadagni tra gruppi di pari per determinati rami di attività. In risposta a insurancetech, le compagnie di assicurazione tradizionali stanno iniziando a intraprendere le proprie iniziative digitali. Queste sono particolarmente evidenti per quanto riguarda l'uso dei

dati per ottimizzare l'esperienza del cliente, ad esempio aggregando i dati esistenti sul cliente per snellire il viaggio quando presenta una richiesta o un sinistro. "*L'altra cosa che ritengo interessante da questo punto di vista*", dice Paton, "sono i diversi approcci che le varie aziende stanno adottando per cercare di rispondere e creare le proprie innovazioni e disgregazioni. Abbiamo visto tutto, La tecnologia - come in tutti i settori industriali - ha un ruolo importante da svolgere nella trasformazione delle assicurazioni. Nuove opportunità si stanno creando grazie a strumenti come IoT, la telematica, l'analisi avanzata dei dati e le tecnologie che supportano le offerte basate sui consumi e le assicurazioni per l'economia della condivisione.Questi vantaggi tecnologici sono particolarmente apprezzati in un settore che ha dovuto affrontare una crescente regolamentazione, molte sfide normative moderne sono iniziate con la Direttiva Solvency II dell'UE nel

2009, e altri decreti sono seguiti. Il grande impatto di Solvency II dal punto di vista dell'innovazione è stato quello di aver dirottato la capacità dell'assicuratore di investire in nuovi settoriè stata seguita dalla Direttiva sulla distribuzione delle assicurazioni e da un controllo regolamentare sulla condotta in aree quali le linee personali. Le assicurazioni saranno ridisegnate dalle innovazioni apportate dall'intelligenza artificiale, dall'internet delle cose e dalla Blockchain .Sono opportunità che guidano la creazione di nuovi prodotti e il modello di interazione con la clientela, aumentando l'efficienza dei processi commerciali e migliorando la qualità del servizio. I consumatori italiani desiderano esperienze personalizzate e una maggiore interazione multicanale con le compagnie assicurative Il Global Insurance Distribution & Marketing Consumer Study 2017 – sondaggio che Accenture ha realizzato su oltre 32mila persone in Italia e nel resto del mondo – dimostra concretamente

come, oggi più che mai, sia diventato fondamentale ascoltare i consumatori per costruire con loro un rapporto sempre più diretto e significativo. A determinare il successo delle compagnie in questa rivoluzione del settore sarà infatti una nuova customer experience personalizzata, in grado non solo di soddisfare i bisogni e le crescenti aspettative dei clienti, ma di facilitare un'interazione continua e senza confini, supportata da un costante sistema di feedback capace di premiare i consumatori per la fedeltà e i comportamenti virtuosi mostrati. Il consumatore italiano, sottolineanmo i curatori della ricerca, desidera mantenere il controllo dell'interazione, pur senza rinunciare a un monitoraggio costante. Tra gli aspetti più interessanti: il 60% degli intervistati vorrebbe avere una customer experience multicanale, per interagire con la compagnia attraverso qualsiasi mezzo, fisico o digitale. Il 50% del campione vorrebbe inoltre avere

accesso immediato alla propria compagnia assicurativa in caso di bisogno, per esempio attraverso il proprio dispositivo mobile. Negli ultimi tre anni sono molto aumentati i consumatori italiani che si dichiarano disposti ad acquistare una polizza da "operatori del digitale" come Google, Amazon, Facebook ed Apple (GAFA). Questa propensione è passata dal 22% del 2013 al 38% del 2016, superando la media dei principali paesi Europei (32%) e avvicinandosi a valori di un mercato molto evoluto quale quello inglese (49%). Nell'era dei Living Service, assicurarsi una crescita profittevole sarà sempre più complesso per le Compagnie ancorate solo a modelli di business convenzionali. Per un efficace percorso di trasformazione verso i Living Service, riteniamo che le Compagnie dovranno puntare sul rendere sempre più efficiente il business tradizionale (semplificando prodotti, processi e la macchina IT) per arrivare a strutture costo più

competitive e investire il valore recuperato, da un lato per crescere nel business tradizionale portando a scala il digital in aree come digital marketing, analytics, mobile, e dall'altro per sperimentare in modo mirato nuovi modelli di business abilitati dalle frontiere aperte dalle tecnologie digitali ed ecosistemi. L'equilibrio tra business assicurativo e investimenti in nuovi trend tecnologici diviene quindi il fattore critico di successo per organizzazioni che devono ambire a diventare "partner" dei propri clienti nella loro quotidianità". Il "Living Insurer" adotta un modello di business customer centric, che integra tecnologie digitali e partnership strategiche con un network di aziende: l'obiettivo è quello di trasformare i prodotti e la relazione con il cliente in servizi attivi e dinamici, in grado di apprendere in modo continuo bisogni, intenti e preferenze, offrendo proposte rilevanti e coinvolgenti. È necessario che le Compagnie rivedano il proprio business principale per aumentare la

capacità di investimento: è possibile farlo attraverso una maggior competitività in termini di costi strutturali, che possa accrescere i profitti nel modello di business esistente (utilizzando, ad esempio, tecnologie cloud e sistemi di intelligent automation). E', questo, un punto di importanza critica, perché è dal core business che deriva la maggioranza delle revenues. Il "Living Insurer" deve utilizzare la nuova capacità di investimento per supportare il digital marketing e gli analytics (che permettono di acquisire nuovi insight operativi) e per migliorare le interazioni con i clienti da web e da mobile (un canale che dà la possibilità di attivare nuove richieste e espandersi in nuovi mercati). In questo modo è possibile che il core business continui a crescere almeno a singola cifra, per supportare l'evoluzione verso nuovi mercati. Diffondere la cultura digitale su tutte le funzioni aziendali in modo da rendere più efficiente la struttura dei costi delle compagnie e, allo stesso tempo,

automatizzare i processi standard per liberare risorse e generare valore incrementale da impiegare nella customer experience e avvicinare così le assicurazioni alle esigenze quotidiane del cliente. Una cambiamento che, a partire dai CEO, dovrà coinvolgere tutti i livelli organizzativi.

3.3. *Evoluzione della normativa con l'ingresso delle Insurtech*

Come anticipato, i nuovi concorrenti, le startup InsurTech, stanno riscontrando notevoli difficoltà nell'affacciarsi al mercato assicurativo, proprio in ragione della stringente disciplina di questo settore, che impone requisiti elevati in termini d'idoneità per ottenere l'autorizzazione ed in termini di capitale. L'imposizione di requisiti stringenti costituisce un elemento fondamentale, ai fini prudenziali, per garantire la tutela dei soggetti assicurati, e potrebbe rivelarsi un

ostacolo all'approccio digitale e alla concorrenza nel mercato assicurativo. Nell'era della tecnologia, le normative relative al settore delle assicurazioni maggiormente interessate sono le regole relative alla governance e le regole di condotta sul mercato. Nel luglio del 2016, l'OCSE ha avviato una pubblica consultazione sulla revisione della Raccomandazione relativa alle Linee Guida in materia di governance delle imprese di assicurazione (la Raccomandazione in questione era stata pubblicata nel 2011). Tali linee guida raccomandano che i membri del Consiglio di Amministrazione e i dirigenti con responsabilità strategiche stabiliscano una serie di controlli interni che garantiscano la conformità alle leggi, alle normative e agli standard vigenti, nonché uno schema d'incentivi che promuovano la correttezza dei comportamenti nei confronti dei contraenti e dei consumatori in generale.. I principi emanati dall' "Associazione internazionale dei supervisori assicurativi" (IAIS) stabiliscono, inoltre, che

deve essere garantito l'imparziale ed equo trattamento dei clienti: prima, durante e successivamente alla stipula del contratto. Le compagnie assicurative dovrebbero, perciò, adottare un comportamento in linea con il principio di buona fede e del divieto di pratiche abusive. Nel momento in cui le aziende d'assicurazione andranno ad adottare nuove tecnologie o ad innovare processi, così come a realizzare nuovi prodotti, dovranno valutare che siano state fatte le opportune considerazioni sul controllo interno e che siano state rispettate le regole di condotta del mercato. Relativamente invece l'utilizzo dei Big Data, la normativa risulta piuttosto complessa e, spesso, di difficile interpretazione. A questo riguardo, il Parlamento Europeo ed il Consiglio Europeo hanno emanato, ad aprile 2016, un nuovo Regolamento (Regolamento UE 2016/679) atto a garantire la protezione e la libera circolazione dei dati personali nell'Unione Europea, il cosiddetto "General Data Protection Regulation" (GDPR). Il suddetto

Regolamento si applica nel caso in cui vengano trattati i dati personali di soggetti che risiedono nell'Unione Europea, indipendentemente dal fatto che l'impresa che fa un utilizzo di questi dati abbia sede nell'UE o meno, ed è entrato in vigore a partire dal 25 maggio 2018. Il GDPR sancisce che le informazioni private siano eliminate senza indugio, nel momento in cui i dati non si rendano più necessari allo scopo per cui erano stati raccolti. L'impresa deve conservare i documenti che attestino il consenso rilasciato dal soggetto interessato in merito all'utilizzo dei propri dati: infatti, senza tale consenso, l'azienda potrebbe non avere il diritto di utilizzare i suddetti dati. Nella fattispecie in cui il trattamento dei dati da parte di un'impresa, particolarmente nel caso in cui preveda l'utilizzo di nuove tecnologie, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, si richiede, prima di procedere al trattamento, che venga effettuata una valutazione dell'impatto dei trattamenti previsti sulla

protezione dei dati personali. Inoltre, ai sensi del GDPR, i responsabili del trattamento dei dati saranno tenuti a notificare le eventuali violazioni dei dati personali all'autorità di vigilanza competente, ove possibile, non oltre 72 ore dopo essere venuti a conoscenza della violazione, a meno che il responsabile del trattamento non sia in grado di dimostrare che è improbabile che la violazione comporti un rischio per i diritti e le libertà delle persone interessate. Le notifiche devono essere fatte anche agli interessati senza indebito ritardo se la violazione può comportare un alto rischio per i loro diritti e le loro libertà. Le imprese potrebbero essere multate fino a 20 milioni di euro o il 4% del fatturato globale annuo dell'anno più recente, a seconda di quale sia maggiore tra i due valori, se non vengono rispettano le disposizioni del GDPR. Al fine, invece, di poter offrire un serivizio sempre più personalizzato occorre considerare le disposizioni della Direttiva (UE) 2016/97 del Parlamento Europeo e del Consiglio sulla

distribuzione assicurativa (la cosiddetta "Insurance Distribution Directive – IDD), che va ad abrogare la precedente Direttiva 2002/92/CE in materia d'intermediazione assicurativa. La suddetta Direttiva si applica a tutti i soggetti che a vario titolo concorrono alla vendita di prodotti assicurativi e, quindi, non solo alle imprese di assicurazione ed agli intermediari assicurativi, ma anche, ad esempio, ai soggetti che gestiscono i siti di comparazione, quando questi consentano di stipulare direttamente o indirettamente un contratto di assicurazione. La IDD prevede che l'adeguatezza dell'offerta alle caratteristiche dell'utente non debba essere affrontata esclusivamente nella fase di vendita, ma, al contrario, deve essere verificata durante l'intero processo di sviluppo del prodotto. Il produttore (manufacturer de-facto), durante lo studio del prodotto, dovrà, infatti, considerare il livello di conoscenza e di educazione finanziaria della clientela target, con l'obbligo d'identificare preventivamente i gruppi di

utenti per i quali il prodotto non è adeguato in termini di potenziali obiettivi o di caratteristiche finanziarie. Al fine di garantire la corretta rispondenza alle aspettative del cliente è prevista una costante verifica di adeguatezza non solo rispetto ai prodotti di nuova ideazione, ma anche per quelli già commercializzati e per quelli sottoposti a un "restyling". La verifica dell'adeguatezza viene, quindi, rafforzata nella fase precedente alla vendita, con responsabilità del product manufacturer a livello di formulazione del prodotto e da parte dei distributori nella fase di vendita. Alla luce di queste considerazioni, risulta evidente la portata della sfida che le compagnie assicurative devono affrontare nell'approcciarsi al mondo digitale: non dovranno soltanto dotarsi di tecnologie innovative al passo con i tempi ed attuare una strategia sempre più orientata al cliente, ma dovranno farlo nel rispetto delle normative e dei requisiti regolamentari che, nell'era dell'innovazione tecnologica, diventano sempre più stringenti.

3.4. *Successo digitale equivale al successo del settore?*

Sebbene il termine “disruption” sia oggi utilizzato in modo inflazionistico, le sue interpretazioni variano in modo significativo. Per evitare incomprensioni e stabilire un significato comune nel contesto del nostro studio, ci riferiamo alla ben nota “disruption theory”, elaborata da Clayton M. Christensen nel 1995. Nel loro studio principale, Bower e Christensen (1995)distinguono tra innovazioni “sustaining” e “disruptive”, e sottolineano che queste due tipologie hanno impatti diversi su un’azienda, che possono essere illustrati dal concetto delle cosiddette “traiettorie di performance”. Le innovazioni “sustaining” sono definite come miglioramenti di prodotti e servizi esistenti, destinati a gruppi di clienti noti, che possono avvenire gradualmente o attraverso salti importanti. Un esempio tipico di innovatori “sustaining” sono i produttori di

telefonia mobile, che continuamente sviluppano nuove generazioni di dispositivi intelligenti con crescenti funzionalità, come l'iPhone 7 Apple o il Samsung Galaxy S8. Un'altra caratteristica importante di un'innovazione "sustaining" è che spesso supera le esigenze dei clienti (ad esempio, solo pochi utenti sfruttano regolarmente l'intera gamma di funzionalità del proprio smartphone). Le innovazioni che provocano "disruption" sono invece prodotti e servizi che inizialmente si rivolgono all'estremità inferiore di un mercato esistente o ad un mercato completamente nuovo, e poi cominciano a spostarsi nel tempo progressivamente verso l'alto .Nella maggior parte dei casi, le rispettive imprese sono piuttosto piccole e dispongono solo di poche risorse e, anche se all'inizio le loro offerte sono inferiori a quelle degli incumbents, finiscono per rimpiazzare i mercati, i prodotti e i competitors esistenti. Secondo King e Baatartogtokh, le innovazioni "disruptive" sono caratterizzate da una

maggiore convenienza, un prezzo più basso e una minore complessità. Inoltre, l'elemento probabilmente più importante dell'innovazione disruptive è l'anticipazione delle esigenze future dei clienti: gli assicuratori tradizionali di successo tendono a porre molta enfasi sulle esigenze attuali e non adottano tecnologie o modelli di business che soddisfino i bisogni non dichiarati o futuri dei loro clienti; questo comportamento nel tempo può causare la loro destabilizzazione e la successiva scomparsa. Storicamente, le innovazioni con impatto "disruptive" hanno cambiato in modo sostanziale diverse industrie. Un esempio importante è il settore automobilistico. Alla fine del XIX secolo, le carrozze dei cavalli erano il mezzo di trasporto più utilizzato. Nel 1886 Carl Benz introdusse la prima automobile al mondo, la cosiddetta "Benz Patent Motorwagen"; a differenza dell'opinione pubblica diffusa, tuttavia, ciò costituiva solo un'innovazione "sustaining". Sebbene il trasporto fosse

diventato più facile e, in una certa misura, più comodo, il problema del costo del bene lo rendeva non destinabile al segmento più basso del mercato. L'innovazione "disruptive" in questo contesto è stata innescata più tardi dal lancio del modello T di Ford, il quale, grazie alla produzione di massa, e con l'aiuto di processi di assemblaggio, poté offrire il prodotto ad un prezzo contenuto. Ben presto, le carrozze più costose vennero rimpiazzate dalle automobili di serie, che soddisfacevano le esigenze dei clienti tradizionali. Insieme alle carrozze, anche le altre industrie collegate, come i carrozzieri, i carri e i produttori di alimenti per cavalli, subirono il cambiamento. In sintesi, i disrupters si distinguono dagli incumbents sotto vari aspetti in primo luogo, si tratta per lo più di imprese piccole e giovani, che dispongono di minori risorse rispetto agli operatori assicurativi tradizionali;32 inoltre, mentre gli operatori tradizionali si rivolgono a clienti sofisticati,

[32] Si noti che il vantaggio in termini di risorse degli operatori storici si manifesta anche in attività quali le relazioni con i clienti, il *know-how* del settore, ecc.

appartenenti alla fascia superiore del mercato, i disrupters orientano la loro offerta iniziale verso la fascia inferiore e offrono prodotti più semplici e funzionali a prezzi contenuti, guadagnando meno rispetto agli incumbents. Poiché questi ultimi in genere inseguono una maggiore redditività, i disrupters possono evitare la concorrenza diretta. Infine, i disrupters anticipano le esigenze e le richieste future dei clienti, mentre gli incumbents danno molta importanza ai loro clienti attuali. Di conseguenza la redditività della propria attività, inizialmente inferiore, non dissuade i disrupters dall'obbiettivo di diventare in futuro società affermate, aspirazione rafforzata anche dal fatto che gli incumbents potrebbero non essere in grado di innovare il loro modello di business in tempo, cioè prima che le richieste dei clienti siano accolte sistematicamente dai nuovi entranti nel mercato. I disrupters hanno in genere un'elevata propensione al rischio e poco da perdere, mentre le imprese tradizionali si trovano di fronte ad un

trade-off33 tra innovazione ed il successo attuale della loro attività. Oltre alle innovazioni "sustaining" e "disruptive", introduciamo adesso un terzo tipo di innovazione, che chiameremo innovazione "enabling". Le imprese che si muovono lungo questa linea forniscono tecnologie che possono aiutare gli incumbents a modernizzare le loro attività. Esempi per quanto riguarda il settore assicurativo comprendono le categorie InsurTech IoT, Big Data e Blockchain: i wereables consentono agli assicuratori del ramo vita di monitorare meglio lo stato di salute di una persona e, allo stesso modo, gli assicuratori danni/infortuni possono utilizzare dispositivi per la casa smart, come termostati, sensori di rilevamento e sistemi avanzati di allarme per segnalare rischi di incendio e furti.; i dati trasmessi dai dispositivi IoT, invece, possono essere analizzati con software e algoritmi forniti da startup Big Data e la tecnologia Blockchain consente agli

[33] "In economia un *trade-off* è una situazione che implica una scelta tra due o più possibilità, in cui la perdita di valore di una costituisce un aumento di valore in un'altra." Trade-off, https://it.wikipedia.org/wiki/Trade-off

assicuratori di memorizzare e rintracciare elettronicamente tutte le transazioni, completamente automatizzate e a prova di manomissione. Trovarsi su una traiettoria "disruptive", che può in ultima analisi portare al rimpiazzo o alla disintermediazione degli incumbents, non equivale sistematicamente al successo commerciale. In altre parole, solo perché un nuovo concorrente è considerato un perturbatore non necessariamente è destinato ad avere successo nel lungo termine. Il motivo è che il successo presenta molti più fattori determinanti, e non si limita al solo potenziale "disruptive". Naturalmente, le imprese di maggior successo sono caratterizzate da un modello di business innovativo, difficile da emulare, e da una tecnologia all'avanguardia, fattore di perturbazione che aiuta le imprese a raggiungere una forte posizione di mercato. Analogamente, un capitale adeguato successivo alla fase di vita iniziale dell'attività (un finanziamento di round A) e una profonda conoscenza del settore e dei clienti

sono fattori chiave di successo. Infine, per avere successo, le imprese devono chiaramente trasmettere elevato valore aggiunto ai loro clienti target. Come indicato in precedenza, il potenziale di "disruptive" è solo uno dei fattori che contribuiscono al successo aziendale. In questo capitolo proponiamo una matrice InsurTech intuitiva. Poiché la maggior parte delle recenti discussioni sull'InsurTech è incentrata sui livelli di finanziamento delle startup, decidiamo di seguire questa tendenza e di selezionare come secondo parametro il "capitale disponibile". Definiamo il finanziamento nelle fasi iniziali (fino al round A) come capitale disponibile "limitato" e il finanziamento nelle fasi successive (oltre il round A) come capitale disponibile "ampio". La nostra matrice distingue il potenziale pericolo originato dalle startup InsurTech per mezzo di cinque campi diversi:le imprese che promuovono innovazioni "sustaining" sono considerate lightweights (con capitale limitato) o usual suspects (con

ampio capitale), mentre le imprese che si trovano su una traiettoria "disruptive" sono classificate come minacce (con capitale limitato) o perturbatori (con ampio capitale); inoltre, le startup che introducono un'innovazione "enabling" sono denominate enablers. Esempi sono Bought by Many, Slice e Sherpa. Queste startup hanno modelli di business innovativi, soddisfano nuove esigenze dei clienti o si rivolgono a segmenti di nicchia del mercato, mirando a rendere l'assicurazione più semplice e di più facile utilizzo, ma data la loro limitata dotazione di capitale essi si configurano attualmente solo come minacce. Lemonade, Trov e Metromile, al contrario, hanno già raccolto finanziamenti oltre il round A, tutte e tre presentano caratteristiche "disruptive" e possono quindi essere considerate "disrupters". Diverse altre startup InsurTech hanno lanciato innovazioni "sustaining" piuttosto che "disruptive". Anche se gli assicuratori digitali, come ad esempio Ottonova e HavenLife, migliorano chiaramente

il modello di business assicurativo tradizionale, non possiedono le caratteristiche di un'autentica innovazione "disruptive". Allo stesso modo, i portali di confronto come Check24 e i broker digitali come Knip rendono il processo di acquisto dell'assicurazione più conveniente per molti clienti. Infine, la maggior parte delle startup InsurTech si considerano come enablers, con l'obiettivo di sostenere il settore assicurativo con i loro progressi tecnologici. Ciò è confermato anche da una recente dichiarazione di Startupbootcamp: "*InsurTechs are more likely to operate as enablers than disrupters. The majority of InsurTech startups are focused on activities that will help incumbent insurers to do a better job, rather than to steal their business. This is not to say insurers can afford to dismiss InsurTechs"*.

Conclusioni

La ricerca condotta ha voluto indagare il comparto assicurativo analizzandone i mutamenti degli ultimi periodi,rilevando i cambiamenti all'interno della globalità della filiera e degli stakeholders che ne fanno parte. E' evidente come le mutazioni avvenute in un settore estremamente poco incline ad evoluzioni abbia apportato migliorie in termini di servizio e costo all'utente finale che nel breve periodo ne trarrà giovamente attraverso un'offerta di prodotto estremamente "customizzata",dove l'atto d'acquisto risulti più semplice ed in linea con l'epoca attuale. D'altro canto per le imprese assicurative la continua guerra di costo,suggerita dall'utente finale che ancora vede in questo il driver principale della scelta assicurativa,nel lungo periodo non poterà giovamente in termini di ricavi; questo è falso ovviamente per gli incumbert e le insurtech più in generale che pongono le basi del modello attraverso la costruzione e vendita di un

prodotto assicurativo differente e che rappresenti una novità assoluta per l'utente finale spingendolo a non considerare il premio assicurativo come univa variabile durante l'acquisto. E' oltremodo evidente precisare che dallo studio sopra descritto vi sarà nel breve periodo una decrescita degli organici nelle comapgnie tradizionali seppure il comparto risulti ancora in crescita; va da se che diverse figure professionali(Underwriter,attuari,Periti) verranno sostituiti in maniera vorace dallingresso dell'intelligenza artificiale. Il settore assicurativo continua ad affrontare sfide su più fronti, tra cui l'incertezza macroeconomica e politica, i bassi tassi di interesse, la crescente concorrenza e i cambiamenti normativi. Il digitale offre agli assicuratori una soluzione a molti problemi. La sfida risiede nella coerenza tra le scelte e la loro esecuzione. La tecnologia sta cambiando la natura del rischio e sta rendendo possibili nuovi prodotti, servizi e canali. Per avere successo in questo ambiente gli assicuratori dovranno impegnarsi a fondo - e a volte essere

la forza trainante per la creazione di ecosistemi. Trovare il giusto ruolo e il modo di aggiungere valore in questo nuovo ambiente sarà fondamentale. Un risultato chiave della combinazione di disgregazione e adozione del digitale è che la convergenza intersettoriale che sta diventando sempre più importante e questo ci sta trasferendo ad una riprogettazione fondamentale delle catene del valore tradizionali, nonché alla necessità di entrare in nuovi contesti di business. Per gli assicuratori, la partecipazione a "partnership" di ecosistemi connessi digitalmente non è naturale e richiede comportamenti e approcci commerciali molto diversi rispetto alle norme vigenti. Cosa significa per il settore: In questo ambiente, gli assicuratori devono rispondere rapidamente: Diverse società insurTech puntano a offuscare le linee di settore - in particolare nell'ambito dei servizi finanziari - e mirano ad offrire un portafoglio completo di servizi. Per ridefinire i rapporti con i clienti e creare valore in qualsiasi ecosistema, gli assicuratori devono cercare di offrire servizi

ancillari ed innovativi oltre all'assicurazione ridefininendo il loro ruolo negli ecosistemi futuri valutando il ruolo delle tecnologie emergenti come blockchain, identificndone i loro punti di forza e, di conseguenza, acquisire o rendersi partner di aziende che possono contribuire a creare un'esperienza digitale integrata per i clienti. L'ingresso di GAFA (Google Amazon Facebook Alibaba) nel mondo assicurativo insieme all'ascesa delle InsurTechs sta creando forti stravolgimenti. Basti pensare che solo negli ultimi 12 mesi, ci sono stati 450 nuovi operatori InsurTech, prevalentemente focalizzati sulle vendite e sulla distribuzione. La maggior parte hanno cercato di fornire soluzioni specifiche per la catena del valore, e pochi hanno coperto la catena del valore end-to-end. I finanziamenti per queste aziende sono aumentati notevolmente, con 2,5 miliardi di dollari investiti a livello globale nel 2018, che riflettono un aumento annuo del 39% rispetto al 2017. La rivoluzione tecnologica in atto, se da un lato richiede notevole flessibilità nell'offerta, dall'altro, se ben orientata,

può cambiare il corso della storia: vengono poste nuove sfide ma soprattutto si creano nuove opportunità. La compagnia assicurativa deve avviare un processo di trasformazione per diventare un lifestyle coach, così da permettere al modello di passare da quello tradizionale, incentrato sulla prevenzione e sulla trasmissione di informazioni relative ai rischi, a quello di agente di cambiamento dei comportamenti, al fianco e vicino alle persone. La tecnologia è in grado di influenzare in modo significativo il comportamento dei clienti: gli utenti sono sempre connessi, si aspettano che tutte le funzioni previste siano disponibili in ogni momento e che tutte le richieste effettuate vengano immediatamente processate. Oggi, e ogni giorno sempre di più, ci troviamo di fronte un consumatore diverso, più consapevole, multitasking e interattivo, in grado di influenzare direttamente le aziende, anche grazie agli strumenti digitali. Un consumatore consapevole che si informa, che vuole sapere e conoscere l'offerta che gli viene proposta e, solo dopo averla valutata

– sotto tutti gli aspetti, non solo strettamente economici – decide. Le tecnologie, l'informatica e la digitalizzazione devono aiutarci a trovare soluzioni, a risolvere problemi e a prendere decisioni orientate al bene comune. Fino ad alcuni anni fa l'obiettivo principale dell'impresa era generare lucro per gli azionisti, oggi l'obiettivo principale è creare valore per il cliente, perché è importante monitorare e anticipare i cambiamenti di valore che le innovazioni tecnologiche abilitano per mantenere l'impresa "rilevante". Diventa fondamentale ragionare strutturalmente in termini di "valore" per il mercato e continuamente analizzare: in quale business opero? A chi vendo? Quale valore riceve il cliente? Qual è il fine vero per il quale il cliente compra il mio prodotto o servizio? Ci sono nuovi bisogni indotti dalla tecnologia o nuove modalità di soddisfare il medesimo bisogno? Questo modo di pensare non è ancora così diffuso e un esempio a tutti noto viene dal mondo della musica, in cui se ci si concentra sulla catena del valore si vede come è cambiata radicalmente la value

propositon del mercato, nuovi attori permettono di fruire solo dei brani preferiti e non dell'intero album, di fruirne on demand ed everywhere, suggeriscono al consumatore nuovi brani di suo gusto e così via. Sono spariti alcuni attori (si pensi ai distributori fisici) e ne sono nati di nuovi (si pensi alle piattaforme on line o ai grandi distributori digitali come iTunesDi fatto è cambiata la catena di valore dalla creazione del contenuto alle forme di fruizione dello stesso. Risulta evidente come la chiave di un'evoluzione porpositva sia quella della focalizzazione sul customer value,avendo chiaro qual è il valore che la nostra offerta dà, occorre concentrarsi sull'esperienza cliente. Con la digitalizzazione sono cambiate totalmente la strategia e i modi di relazionarsi con i clienti, sono nati i customer network, dove i clienti comunicano tra loro e non ricevono più informazioni solo dall'impresa che produce il prodotto/servizio, ma interagiscono con altri consumatori attraverso le piattaforme digitali. La competizione sulla "customer experience" è sempre più serrata e, per la

cosiddetta legge della “equivalent experience”, la miglior esperienza vissuta dal nostro cliente costituisce sempre un benchmark anche se “vissuta” in altri mercati. La sfida oggi è reinventarsi, confrontandosi non solo con concorrenti “simmetrici” del medesimo mercato, ma anche con le esperienze offerte da settori completamente differenti. L’impresa deve adattarsi in tempi rapidi ed essere veramente agile: non si tratta solo di adottare pratiche e modelli organizzativi agili e “alla moda”, ma di pensare in modo agile. Il cambio di mindset è cruciale. Le imprese analogiche operavano in un mondo lineare di “planning e control”, dove era possibile (e atteso) prevedere il futuro, si poteva avere il controllo dell’ambiente in cui si operava e replicare “best practices”. Oggi non è così, vista l’imprevedibilità del business, il mindeset digitale abbandona la logica volta a replicare le formule di successo passate, e incorpora la necessità di innovare, sperimentare e apprendere in modo continuo. Non si tratta solo di replicare il passato, ma di creare un

futuro nuovo. È necessario avere obiettivi strategici di business chiari come premessa per potersi concentrare e selezionare i dati rilevanti e avere da essi supporto nella definizione della direzione e delle decisioni da prendersi. Essere Data Driven vuol dire promuovere una cultura Data Oriented come fulcro della vita d'impresa, oltre che utilizzare architetture e metodologie per produrre, ottenere, sfruttare dati in logica di business. Il modello di business di piattaforma impatta tutti i settori, e può essere preso come riferimento per un modello di business in grado di generare valore, facilitando le interazioni dirette o indirette tra due o più tipologie di clienti differenti. La piattaforma facilita la relazione tra le differenti tipologie di clienti, crea l'esperienza del servizio e soprattutto porta a modelli di business scalabili, in cui, di fatto, non si possiedono i "mezzi di produzione" ma i "mezzi di connessione", abilitando nuovi modi di rispondere alle esigenze del cliente. Avere una strategia che incorpori elementi di business model tipico delle piattaforme, capire e anticipare

gli impatti che le piattaforme esistenti o potenziali avranno sul mercato in cui si opera è ormai inevitabile.

BIBLIOGRAFIA

Bill BRIGGS & Marcus SHINGLES, "Tech Trends 2015, The fusion of Business and IT" Deloitte;

Donatella CAMBOSU, "InsurTech, che cos'è e quali sono i suoi pilastri" InsuranceUp (Febbraio 2017);

CAPGEMINI & EFMA, "World Insurance Report 2017";

ANIA, (2017), Ania Trends 2012-2016.

ANIA, (2017), Indagine conoscitiva sulle tematiche relative all'impatto della tecnologia finanziaria sul settore finanziario, creditizio e assicurativo.

ANIA, (2017), The Italian insurance market and new investment trends under Solvency II .

ANIA,(2018),schema di decreto legislativo recante attuazione direttiva (ue) 2016/97 sulla distribuzione assicurativa.

Bain report , (2017), Customer Behavior and Loyalty in Insurance: Global Edition 2017.

Capagemini, (2018), World Insurance report 2018.

Cbinsight, (2017), How Blockchain is distrupting Insurance.

EY, (2017), Global Insurance trends analysis: an industry braving uncertain times.

EY, (2018), Insurance Innovation.

University of St.Gallen (2013);

GLOBAL PRIVACY ENFORCEMENT NETWORK (GPEN), "Report annual 2016";

GRUPPO UNIPOL, "Sharing Economy" Edizione 2017;

IVASS, "Indagine sui siti comparativi nel mercato assicurativo italiano" (Novembre 2014);

IVASS, "Quaderno n.8" Aprile 2017;

Roy JUBRAJ, Talbert THOMAS & Erik J. SANDQUIST, "Coming to Terms with Insurance
Aggregators: Global lessons for carriers" Accenture (2016);

Andrew A. KING & Bajir BAATARTOGTOKH, "How Useful Is the Theory of Disruptive Innovation?" MIT Sloan Management Review (2015);

KPMG, "Assicurazioni e social media – La presenza social delle compagnie e l'evoluzione del rapporto con il cliente" (2015);

MACROS CONSULTING – Osservatorio Insurance 2.0, "Social media e business assicurativo: nuovo mondo o mondo nuovo?" (Luglio 2013);

James MCQUIVEY, "Digital Disruption: Unleasing the Next Wave of Innovation" Forrester
Research (2013);

John MULHALL, Anudeep CHAUHAN, Claudia LINDSEY & Michael LYMAN, "The broker of the future: Winning in a disruptive environment" Accenture (2016);

MUNICH RE, "Reinvesting insurance for the Digital generation" (Gennaio 2017);

MORGAN STANLEY, "Evolution and Revolution in a Digital World" (2014);

OECD, "Draft recommendation of the council on guidelines on insurers governance";

OECD, "Technology and Innovation in the insurance sector" (2017);

ROLAND BERGER, "Copy them? Work with them? Or buy them? InsurTech and the digitization of insurance" (2017);

Benfield. A., Global Insurance Market Opportunities in Insurance Risk Study, AON Empower
Results, Eleventh edition, 2016.

Bower, J. L. and Christensen, C. M. (1995), Disruptive Technologies: Catching the Wave in Harvard Business Review,1995, 73 (1): 43-53.

Braun A., Schreiber F., The Current InsurTech Landscape: Business Models and Disruptive Potential, University of St. Gallen, 2017.

Cambosu, D., Insurance Tech, All Incubators and Specialized Accelerators in InsuranceUp, 2016.

Carbone M., Dabusti V., Connected Insurance, il nuovo paradigma assicurativo in Italian AXA Paper n.8: "Le sfide dei dati", 2016.

Celent, Success Factors for InsurTech / Incumbent Partnerships, 2017.

SAP, "How Insurers Can Prepare for the Digital Revolution" (2017);

SWISS RE INSTITUTE, "Technology and insurance: themes and challenges" (Giugno 2017);

VENTURE SCANNER, "Where in the World are Insurance Technology Startups?" - Q3 2017 (Agosto 2017);
Emmanuel VIALE & Christian SOUCE, "Insurers and social media: vast potential, significant challenges" Accenture (2012);

IVASS, (2018), Reclami ricevuti dalle imprese di assicurazione nel 2017.

McKinsey , (2017), Time for Insurance companys to face digital reality.

McKinsey, (2016), Making digital strategy a reality in insurance.

McKinsey, (2017), Digital distruption in insurance: cutting through the noise.

McKinsey, (2017), Insurtech - The threat that inspires.

McKinsey, (2018), Claims in the digital age: how insurers can get started.

McKinsey, (2018), Insurance 2030–The impact of AI on the future of insurance .

McKinsey, (2018), Insurance beyond digital: The rise of ecosystems and platforms .

BOSTON CONSULTING GROUP, "Thinking outside the blocks" (Dicembre 2016);

Alexander BRAUN & Florian SCHREIBER, "The Current InsurTech Landscape:
Business Models and Disruptive Potential", University of St.Gallen (2017);

APPLIED SISTEMS UK, "The Digital Brokerage: Developing a Digital Transformation Plan" (2016);
Joseph L. BOWER & Clayton M. CHRISTENSEN, "Disruptive Technologies: Catching the Wave" Harvard Business Review (1995);

Bill BRIGGS & Marcus SHINGLES, "Tech Trends 2015, The fusion of Business and IT" Deloitte;
Venture Scanner, Insurance Technology Market Overview-Q4, 2016.

Willis Towers Watson, WillisRe, CB Insights, Incumbent InsurTech Strategy in Quarterly InsurTech Briefing (Q1 2017), 2017.

Willis Towers Watson, WillisRe, CB Insights, Transaction Spotlight in Quarterly InsurTech Briefing (Q1 2017), April, 2017 pp. 19-20.

Willis Towers Watson, WillisRe, CB Insights, Q1 2017 Industry Theme in Quarterly InsurTech Briefing (Q1 2017), 2017.
Accenture, (2018), Insurance Tech Vision 2018.

Accenture, (2018), Fearless innovation: insurtech as the catalyst for the change within insurance.

Accenture, (2017), The everyday insurers, Insurance Day 2017

Tanguy CATLIN & Johannes-Tobias LORENZ, "Digital disruption in insurance: Cutting through the noise" McKinsey (Marzo 2017);

Clayton M. CHRISTENSEN, Michael E. RAYNOR & Rory MCDONALD, "What Is Disruptive Innovation?" Harvard Business Review (2015);

CISCO, "Digital Transformation for the Insurance Industry" (Gennaio 2017);

Shaun CRAWFORD & David PIESS, "Blockchain technology as a platform for digitization" Ernst Young (2016);

Oliver EHRLIC, Harald FANDERI & Christian HABRIC, "Masteri

ng the digital advantage in transforming customer experience" McKinsey&Company (Maggio 2017);

EUROPE ECONOMICS, "La distribuzione assicurativa in Italia e in Europa – Modelli, evoluzione e prospettive" (Dicembre 2013);

Michael FITZGERALD, "Success factors for insurtech/incumbent partnerships" Digital Insurance Agenda (Aprile 2017);