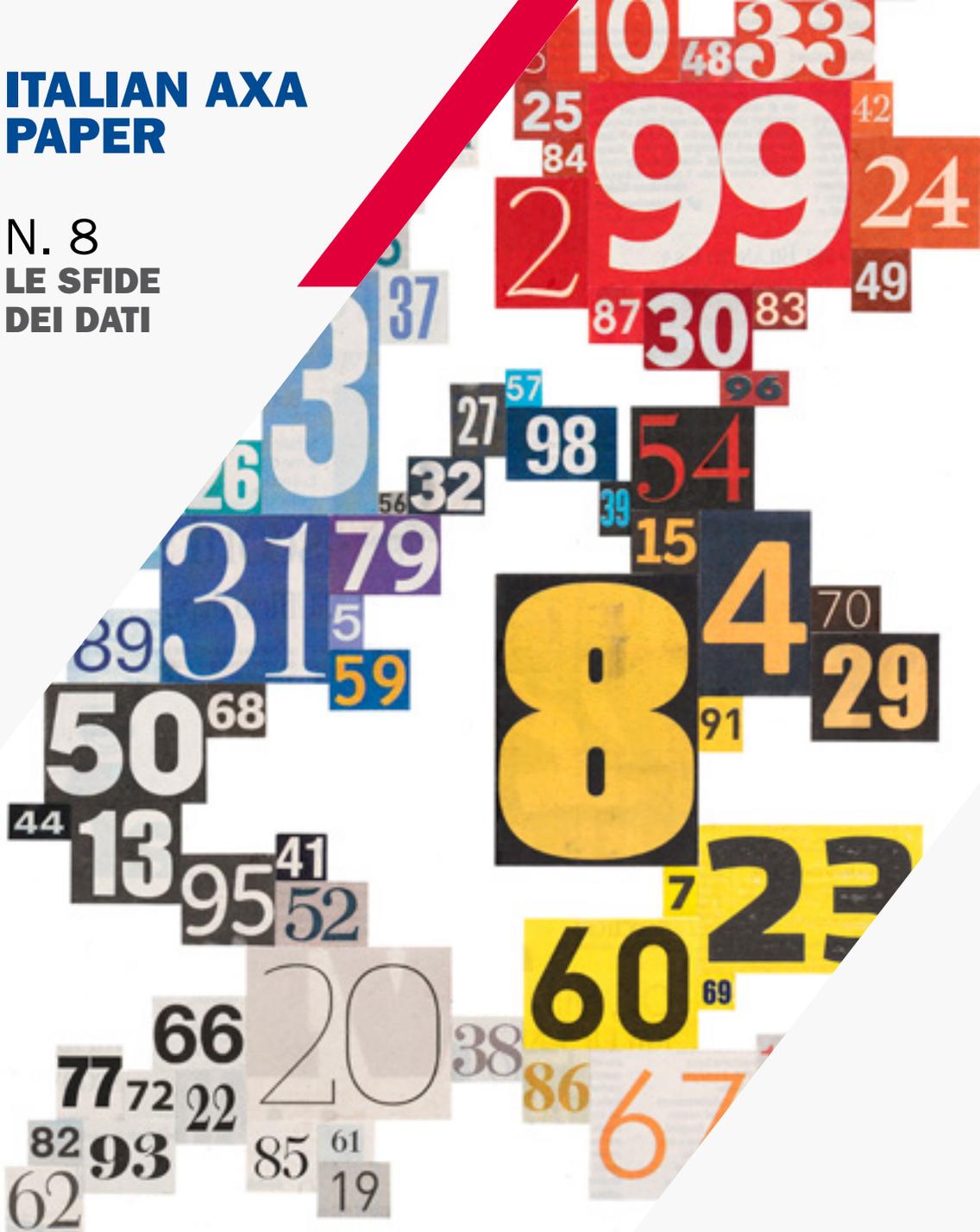


ITALIAN AXA PAPER

N. 8
LE SFIDE
DEI DATI



Verso le Assicurazioni 4.0?

Il settore assicurativo
e la rivoluzione dei dati

ridefiniamo / la protezione



SOMMARIO

EDITORIALE

Isabella Falautano, Direttore Communication, Corporate Responsibility & Public Affairs, AXA Italia 04

1. **I *BIG DATA*: QUALI OPPORTUNITÀ PER IL SETTORE ASSICURATIVO?**
A cura del Gruppo AXA 08

2. **SURVEY AXA-EPISTEME: GLI ITALIANI, IL LABIRINTO DEI DATI E IL RUOLO DEL SETTORE ASSICURATIVO**
Monica Fabris, Presidente, Episteme 14

3. **UN APPROCCIO OLISTICO ALLA SICUREZZA DEI DATI. AFFRONTARE I NUOVI RISCHI LEGATI AI *BIG DATA* E AL *CLOUD*: UN CASO RECENTE SULLA TRASPARENZA DEL SOFTWARE**
Bryan Ford, AXA Chair in Information Security and Privacy, Ecole Polytechnique Fédérale di Losanna 34

4. ***CONNECTED INSURANCE*, IL NUOVO PARADIGMA ASSICURATIVO**
A cura di ANIA e Osservatorio ANIA-BAIN su *Telematics, Connected Insurance e Innovation* 44

5. **COMPORAMENTI EMERGENTI DEI MILLENNIALS, TECNOLOGIE DI ROTTURA E INNOVAZIONE: RIFLESSIONI SUL FUTURO DELLE ASSICURAZIONI**
Federico Casalegno, Direttore MIT Mobile Experience Lab, Associate Professor of the Practice, MIT 58

In copertina

Adriano Attus

Numerage – Prima Serie, Tav. #5, 2014, collage, 30x40 cm

EDITORIALE

Isabella Falautano, Direttore Communication, Corporate Responsibility & Public Affairs, AXA Italia

Con l'*Italian AXA Paper n.8 - Le sfide dei dati* si vuole analizzare, da diverse angolazioni, la rivoluzione dei dati e il suo impatto su società e settore assicurativo, per stimolare una riflessione su come proteggere l'industria, l'economia e la società 4.0.

La *data revolution* non è un trend di passaggio, ma è il *game changer* del nuovo millennio. Nel 2015 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 "doppio 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.

L'*InsurTech* ha visto quasi 2 miliardi di dollari investiti nei primi 9 mesi del 2016, e già nel 2015 gli investimenti erano stati più che triplicati a livello mondiale, passando da 0,8 nel 2014 a 2,6 miliardi. Come ci ricorda l'analisi del Gruppo AXA, i *big data* stanno reinventando il mestiere della protezione perché aiutano a comprendere l'evoluzione dei rischi non più solo in funzione di fattori sociodemografici, ma anche in relazione alle abitudini individuali. La vera sfida è quindi non solo gestire, ma capire come estrarre valore da una mole di dati mai vista prima.

In questo quadro, come vivono gli italiani la società dei dati? Nell'indagine dedicata, Monica FABRIS, Presidente di Episteme, sottolinea come le persone abbiano, allo stesso tempo, un entusiasmo crescente per le opportunità

che la rivoluzione tecnologica offre, per esempio in termini di nuovi servizi, e una scarsa consapevolezza e una paura di perdita di controllo, in particolare sul tema privacy. Il vissuto ambivalente si traduce nel bisogno di una guida e di un punto di riferimento, con un nuovo ruolo per le assicurazioni del futuro: quello di PARTNER delle persone. Un modello incentrato sulla prevenzione, dove la compagnia diventa un *lifestyle coach* che non solo informa, ma aiuta le persone ad agire e modificare i comportamenti per anticipare i rischi prima che accadono.

Dalla ricerca emerge come il tema della privacy e della protezione dei dati sia tra i più sentiti dagli utenti della rete. La Cattedra AXA Bryan FORD, con un caso recente sulla trasparenza del

software, ci fa entrare nel mondo sconosciuto dei nuovi rischi connessi a *big data* e *cloud*. Un universo apparentemente lontano da noi e ancora poco esplorato, ma che, secondo gli esperti, è urgente affrontare con un approccio complessivo per non compromettere nessuna delle tre proprietà fondamentali della sicurezza dei dati: disponibilità, integrità e riservatezza.

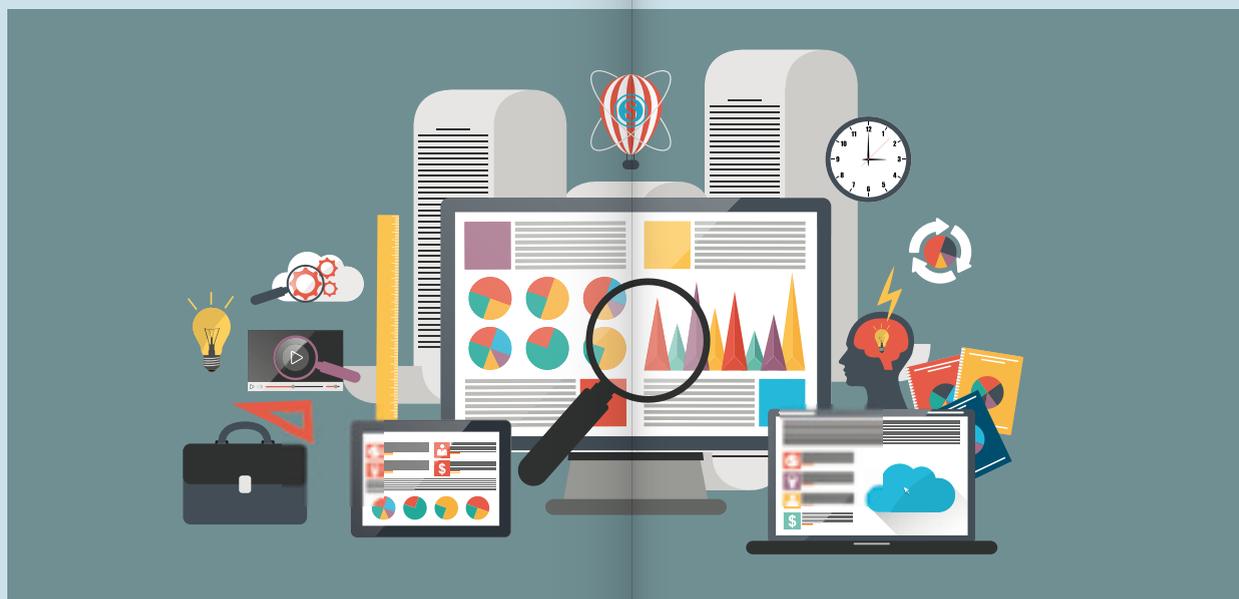
La *Connected Insurance*, ovvero tutte le soluzioni assicurative che prevedono l'utilizzo di sensori e della telematica per la raccolta, la trasmissione e la gestione dei dati di un rischio assicurato, è uno dei trend più rilevanti di innovazione del settore assicurativo. Il nostro paese gioca un ruolo da protagonista, come evidenziato nell'analisi di ANIA e dell'Osservatorio ANIA-Bain

sul tema. Ad oggi, infatti, la linea di business in cui viene maggiormente utilizzata è quella auto, dove l'Italia rappresenta circa il 50% di tutto il mercato a livello mondiale, candidandosi a essere il laboratorio per l'estensione ad altri rami, dalla casa alla salute.

Chiudono il *paper* le riflessioni sui comportamenti emergenti dei protagonisti dell'era dei dati, i *Millennials*, di Federico CASALEGNO del MIT, che ci ricorda come l'aspetto più critico di tutti gli sforzi verso l'innovazione sia tenere sempre al centro l'esperienza umana. Le tecnologie sono migliori quando arricchiscono, aumentano e soddisfano le nostre esperienze e non sono un sostituto dell'esperienza umana.

Gli algoritmi organizzano il mondo e contribuiscono al suo progresso, ma la realtà è sempre qualcosa in più della somma dei singoli dati che la compongono. Quel qualcosa in più è la mente umana, con la sua creatività, intuizione, capacità di prendere rischi e di commettere errori. Fino a trasformare i numeri in una forma d'arte, come ben rappresentato dall'artista e designer Adriano ATTUS nell'immagine di copertina.

In conclusione, un grazie a tutti coloro che hanno contribuito alla realizzazione di questo *paper*. Siamo convinti che, in un contesto sempre più "liquido", dove la velocità deve andare di pari passo con la capacità di andare a fondo, le imprese possano essere motori di un cambiamento a somma positiva, anche attraverso il dibattito pubblico e un dialogo costante con la società.





1. I **BIG DATA**: QUALI OPPORTUNITÀ PER IL SETTORE ASSICURATIVO?

A cura del Gruppo AXA*

I **big data** hanno trasformato il mondo delle assicurazioni, grazie a nuovi strumenti tecnologici per prevedere i rischi e analizzarli. Questa **rivoluzione digitale** consente di affrontare meglio le esigenze del cliente e di creare uno spazio per servizi innovativi in un settore in pieno cambiamento.

Negli ultimi cinque anni una vera e propria rivoluzione tecnologica ha cambiato radicalmente le nostre abitudini e l'attività delle imprese. Si tratta della rivoluzione dei **big data**, resa possibile dalla moltiplicazione degli usi e delle interazioni che ogni secondo creano una massa di dati enorme e che oggi è possibile sfruttare. Infatti, grazie ai **big data**, la raccolta, la conservazione e l'analisi dei dati personali hanno fatto straordinari passi avanti. Questa rivoluzione ha un impatto **disruptive** sul modo in cui il settore assicurativo sviluppa le proprie attività, ma suscita anche inquietudini fra i clienti, specie per quanto riguarda la **sicurezza**, la **riservatezza** e il **trattamento dei dati personali**.

Scopo di questo articolo è di presentare in che modo il settore assicurativo abbia portato i dati al centro del suo business e come la **protezione dei dati dei clienti** sia diventata un punto essenziale per gli assicuratori.

* Contributo da *Finance & Gestion*; Cécile Wendling, Head of R&D Foresight, e Niccolò Pagani, Public Affairs Team, AXA, Settembre 2016.



I DATI, UN RUOLO FONDAMENTALE NELLE ATTIVITÀ ASSICURATIVE

Il ruolo delle assicurazioni è proteggere le persone da eventi incerti e da imprevisti nel corso della loro esistenza.

A questo scopo, l'assicuratore deve capire e misurare i rischi in cui incorrono gli assicurati. Questo consente loro di fornire prodotti e servizi che corrispondano alle esigenze del cliente per prevenire i rischi e per porvi rimedio una volta che si sono verificati. Gli assicuratori usano quindi i dati in ogni passaggio della catena di valore, dall'ideazione del prodotto fino alla gestione del sinistro, passando per la sottoscrizione e la quotazione. La disponibilità dei dati e la loro qualità sono fattori essenziali per le assicurazioni e i *big data* offrono loro molteplici opportunità. L'uso dei dati disponibili permette agli assicuratori di valutare meglio i rischi ai quali sono esposti i loro assicurati, di proporre prodotti e servizi più personalizzati e quindi di garantire loro una migliore esperienza d'acquisto.

I *big data* danno così luogo a una vera rivoluzione nel mestiere dell'assicuratore: aiutano a comprendere l'evoluzione dei rischi non più solo in funzione di fattori socio-demografici, ma anche in relazione alle abitudini individuali.

UNA MIGLIORE CONOSCENZA DEL RISCHIO

Oggi lo sconvolgimento portato dai *big data* è particolarmente visibile nel campo delle assicurazioni auto. A partire dal 2014, infatti, molte compagnie hanno iniziato a sperimentare l'applicazione dei *big data* in questo ramo. Applicazioni collegate a una scatola nera consentono di raccogliere informazioni sulla

guida dei loro clienti e vengono poi incrociate con quelle dei GPS (frenata, accelerazione, velocità, comportamento in curva) al fine di stabilire un punteggio di guida e un profilo del guidatore basato sulla sua prudenza o sulla sua propensione al rischio.

Questo tipo di applicazioni basate sui *big data* premia, anche in termini di riduzione dei costi, i comportamenti virtuosi. I benefici per i clienti sono dunque chiari. AXA ha lanciato l'offerta di assicurazione auto con collegamento remoto YouDrive nell'ottobre 2015, dopo sei mesi di test cui hanno partecipato oltre 500 clienti.

Oltre alle assicurazioni auto hanno cominciato a svilupparsi altri progetti che utilizzano le informazioni rese disponibili dalla tecnologia dei *big data*. Un esempio è quello che nasce dall'unione fra *big data* e Internet delle cose. Questa combinazione permette agli apparecchi connessi in rete, come i rilevatori di fumo o di presenza, oppure le telecamere di videosorveglianza di diventare fonti di dati per rilevare i rischi d'intrusione, d'incendio e di accumulo di monossido di carbonio nelle abitazioni.

L'obiettivo di questa sperimentazione è analizzare meglio i rischi, capire se questo tipo di applicazioni consenta di prevenirli e di valutarne la ripercussione sui premi. Nell'ottobre 2015 AXA ha lanciato il suo progetto pilota di casa connessa, attraverso l'applicazione *Mon AXA*, in collaborazione con Myfox, Nest, Philips, Orange e Kiwatch.

NUOVI PRODOTTI E UN MAGGIOR NUMERO DI ASSICURATI

Le tecnologie *big data* consentono di trattare un enorme volume di dati che nessuno strumento classico di gestione dei dati o delle informazioni è in grado di analizzare. Così, oltre a una migliore conoscenza dei rischi, consentono anche la nascita di nuove forme di protezione, come le assicurazioni parametriche.

L'assicurazione parametrica è un modello di assicurazione che permette il risarcimento di un sinistro quando un indice, di solito meteorologico, supera una soglia prefissata che viene calcolata sulla base di dati climatici raccolti dai satelliti o da stazioni meteorologiche. Questa assicurazione garantisce una risposta a eventi naturali per i quali la stima del rischio era molto difficile fino adesso, come pure l'accesso al cliente e la distribuzione del prodotto assicurativo. I vantaggi del nuovo modello comprendono anche un indennizzo rapido e un costo di gestione dei sinistri molto basso. Il sistema infatti è automatizzato, e il processo di rimborso si avvia al raggiungimento di una soglia: per esempio se per un dato raccolto in un determinato periodo mancano all'appello 100 mm di pioggia, non c'è bisogno della perizia ma il pagamento avviene automaticamente. In questo modo l'assicurazione parametrica permette di limitare l'impatto dei mutamenti climatici sulle imprese nei Paesi sviluppati e di contribuire alla sicurezza alimentare nei Paesi emergenti, in particolare nei contesti in cui i mutamenti climatici scatenano eventi meteorologici più estremi e frequenti.

I *big data* e i dati satellitari possono dunque essere utilizzati con lo scopo di mappare meglio le zone vulnerabili alle catastrofi naturali, incrociando dati pubblici e informazioni interne alla compagnia

sui sinistri. In questa logica, AXA si appoggia dal 2014 all'analisi di immagini satellitari sempre più precise per fornire soluzioni innovative di assicurazione parametrica agli agricoltori dei Paesi in Via di Sviluppo.

LA LOTTA CONTRO LE FRODI

Oltre a misurare meglio i rischi dei clienti e consentire lo sviluppo di nuovi modelli di assicurazione i *big data* potrebbero contribuire a limitare le frodi. I *big data* potrebbero dare alle compagnie assicurative le quantità di dati necessarie a creare tecniche di rilevamento delle frodi, come l'analisi predittiva o lo *scoring*. Diversi grandi gruppi, fra cui AXA, usano già questa tecnica con lo scopo di rilevare i "segnali deboli" e contrastare i tentativi di frode.

UNA QUESTIONE DI GRANDE INTERESSE: LA PROTEZIONE DEI DATI PERSONALI

L'uso di tecnologie *big data* da parte degli assicuratori consente lo sviluppo di nuovi servizi, ma suscita anche inquietudini sulla riservatezza e il trattamento dei dati. Tuttavia, la raccolta di dati presso i clienti da parte degli assicuratori è giustificata nella misura in cui gli interessi delle compagnie sono allineati a quelli dei loro clienti, il che non è sempre vero per tutti i settori.

AXA ha preso posizioni molto chiare in termini di trasparenza ed etica. Ha, infatti, pubblicato nel giugno 2015 i propri impegni in materia di riservatezza e di protezione dei dati personali. AXA si impegna a non usare i dati senza l'accordo esplicito del cliente e a non venderli in nessun caso, e allo stesso modo a essere trasparente sul modo in cui i dati dei clienti sono raccolti, resi anonimi, conservati e utilizzati.

AXA ha creato a luglio 2015 anche un panel consultivo sulla questione della riservatezza dei dati (*AXA Privacy Advisory Panel*), che si riunisce due volte l'anno a Parigi. Il Comitato ha come scopo quello di definire regole chiare, responsabili e trasparenti sulla gestione dei dati personali e sensibili dei propri clienti. È composto da esperti provenienti da vari settori (specialisti di *big data*, di marketing, giuristi, esperti in comunicazione, esperti di sviluppo sostenibile, ecc.) e di personalità esterne al Gruppo (accademici, consulenti, ecc.).

In conclusione, i *big data* sono una rivoluzione. Potranno migliorare il modo in cui gli assicuratori capiscono e valutano i rischi, ma non cambieranno affatto la missione dell'assicuratore: proteggere i clienti contro i rischi e affrontarli quando si verificano.



2. SURVEY AXA-EPISTEME: GLI ITALIANI, IL LABIRINTO DEI DATI E IL RUOLO DEL SETTORE ASSICURATIVO

Monica Fabris, Presidente, Episteme

OBIETTIVI DELLA RICERCA

L'obiettivo generale di questa ricerca è **valutare come i cittadini consumatori italiani percepiscano l'essere immersi in un flusso continuo di dati**, analizzandoli sotto un duplice aspetto: **come fruitori** (soprattutto di quelli che vengono chiamati gli Small Data), **ma anche e soprattutto come produttori di tracce digitali** (i *big data*). Per esaminare questo tema è stato fondamentale dare concretezza alle situazioni e alle conseguenze generate dalla diffusione dei dati digitali, facendo emergere le esperienze dirette e quotidiane degli italiani. **I dati**, prodotti e usati, **vanno sempre ricondotti ai singoli contesti** in cui operiamo **e ancor di più alle finalità** con cui li creiamo/scambiamo/usiamo. Queste dimensioni sembrano ancora più significative della stessa natura delle informazioni che si stanno comunicando.

Già nel 2013 la sociologa Saskia Sassen sottolineava infatti **l'importanza del contesto** in cui i dati si usano e **della modalità d'uso**, dissuadendo dal pensare ingenuamente che esistano dati buoni o cattivi, utili o nocivi in sé. **Questa tesi trova conferma nella nostra ricerca**: esiste infatti una sorta di dicotomia, **una duplice prospettiva di visione sui *big data* che scaturisce dal sentirci di volta in volta o "cittadini", e quindi portatori di diritti, o "consumatori" alla ricerca del miglior prodotto/servizio.**

Il secondo macro-obiettivo che ci siamo posti con la ricerca è stato quello di indagare in maniera più puntuale **come**, sempre alla luce del tema dei *big data* e degli *small data*, **si modifichi il rapporto tra consumatori/clienti e aziende**, a partire dalle

aspettative e dalle nuove abitudini di consumo che, di settore in settore, si vanno definendo.

Strettamente collegato a questo tema è la **percezione dei benefici** che si possono ricavare lasciando una traccia digitale di sé, **sia in generale verso chi offre servizi e prodotti di consumo che per quanto attiene al grande tema della protezione.**

Infatti con l'irrompere dei *big data* è indubbio che **le sfide che solitamente deve affrontare chi si occupa di protezione – e a maggior ragione i player assicurativi – sono al tempo stesso moltiplicate quantitativamente ma anche trasformate qualitativamente.** Detto in altre parole i *big data* rappresentano una fonte di **opportunità unica** che, se da un lato espone le aziende e cittadini al pericolo di perdita di privacy e in un certo senso di libertà, dall'altro sono **uno strumento sempre più unico per erogare servizi e renderli esigibili (si pensi ad esempio alla *sharing economy*), per garantire la sicurezza individuale e collettiva, per prevenire incidenti e di anticipare i bisogni più o meno essenziali della vita di tutti i giorni.** E ancor più diventare un veicolo per **trasmettere stili di vita più corretti**, ma anche più sostenibili, consapevoli e responsabili.

NOTA METODOLOGICA, CAMPIONE, TERMINOLOGIA

È stata svolta una ricerca estensiva tramite tecnica CAWI (computer-assisted web interviewing) a un campione di **1675 individui dai 15 ai 74 anni per un totale di 3652 interviste, effettuate tra luglio e agosto 2016.**

Trattandosi di un campione composto da user internet si dovranno tenere presenti alcune caratteristiche sociodemografiche e socioculturali tipiche dei segmenti più evoluti della popolazione italiana: **alta scolarità, buona dimestichezza con la tecnologia, curiosità e apertura alle innovazioni. Queste caratteristiche, per quanto ancora non omogeneamente diffuse presso la popolazione italiana, sono senza dubbio in espansione, costituendo dunque un punto di vista molto interessante se si leggono i risultati di ricerca in chiave aspirazionale e prospettica.**

Un'ultima notazione doverosa consiste nell'accortezza riservata all'uso di termini altamente tecnici e ancora relativamente poco diffusi. Durante le interviste CAWI l'intervistato è stato accompagnato in **un percorso graduale di avvicinamento alla terminologia specialistica**, grazie alla possibilità di alternare domande "a brucia pelo" e formulazioni più articolate dei significati delle parole usate. Al fine di rendere più fruibile lo stesso rapporto, riportiamo i principali significati attribuiti ai termini specialistici.

BIG DATA: una raccolta di dati così estesa in termini di **volume, velocità e varietà** (disomogeneità) da richiedere **tecnologie e metodi analitici specifici** per l'estrazione di valore.

ALGORITMI: i processi di calcolo e di elaborazione dei dati che ne permettono la loro **intelligibilità**. In informatica **senza algoritmi non c'è automazione e programmazione**. Potremmo dire che se i *big data* costituiscono la materia informale, gli algoritmi sono il processo attraverso cui questa miniera di dati prende via via forma, dandoci la possibilità di **"estrarre il loro valore conoscitivo"**.

INTELLIGENZA ARTIFICIALE (IA): per semplificazione possiamo intendere sotto questo termine **la capacità di una macchina di eseguire forme di ragionamento tipiche e caratteristiche dell'intelligenza umana** (come ad esempio capacità evolute di comprensione del linguaggio naturale, di decifrazione delle emozioni, ecc.). Tra le caratteristiche più interessanti dello sviluppo dell'IA moderna ci sono: **l'apprendimento automatico, la capacità di interpretare le immagini e il riconoscimento facciale, l'elaborazione del linguaggio naturale.**

ROBOT: qualsiasi macchina automatizzata **capace di svolgere compiti e lavori al posto di uomini**, siano essi svolti in completa autonomia o sotto la guida di personale. Nelle **sfide future** dell'automazione c'è senza dubbio **la capacità di manipolare oggetti e muoversi e interagire in ambiente naturale** (non protetto o isolato, ma "abitato da persone"). La robotica si trova ad affrontare il cosiddetto paradosso di Moravec: "un ragionamento sofisticato richiede pochissima capacità di calcolo, mentre le capacità sensorie di basso livello (prendere un vasetto di vetro su un nastro trasportatore che ha perso il disallineamento prestabilito o manipolare un oggetto non rigido, come una pizza da impastare) richiedono enormi risorse di calcolo".

I RISULTATI DELLA RICERCA

UNO SGUARDO D'INSIEME

L'essere connessi non solo permea completamente le nostre vite, ma alimenta anche costantemente uno strato di tracce digitali che si accumulano incessantemente. Quello che di noi resta in rete si sedimenta e dà vita a nostri "doppi digitali", alter ego parziali tuttavia dotati di senso, comprensibili e soprattutto prevedibili grazie alla lettura offerta da algoritmi che sembrano comprenderci meglio di noi stessi.

Gli algoritmi sono all'origine della più grande rivoluzione del nostro stare in rete: il passaggio dall'essere connessi (e liberi di muoverci e cercare) all'essere guidati e orientati da queste potenti e invisibili procedure di calcolo (che ci suggeriscono cosa fare).

Lo sviluppo di nuove applicazioni di intelligenza artificiale rinnova dunque le aspettative nei confronti della tecnologia. Sempre più vicina, sempre più alleata – soprattutto nell'ampliamento delle possibilità di scelta di consumo e nel caso di macchine intelligenti nella difesa della salute. Si generano e si alimentano così nuove speranze salvifiche sollevate dall'evoluzione tecnologica.

Tuttavia questi mutamenti si accompagnano anche a preoccupazioni profonde: il timore è che il trionfo della razionalità possa indebolire i valori più umani della cura delle relazioni e della fiducia tra persone.

La paura maggiore è quella della perdita di controllo, in particolare sul tema privacy, del

condizionamento e di un uso improprio da parte di soggetti privati o comunque non vincolati a regole condivise.

Ciò considerato, si riesce a comprendere il sentimento ambivalente che viene associato al tema dei big data. Più in dettaglio emerge una dicotomia tra il vissuto dei big data in quanto cittadini e in quanto consumatori.

E per entrambe le identità (noi cittadini, noi consumatori) la prima conclusione a cui si giunge è che i big data generano nuovi bisogni di tutela. È qui che si apre per le assicurazioni l'importante occasione di rilanciare e al tempo stesso rinnovare il proprio ruolo.

Infatti, a partire dalle competenze di settore, alle assicurazioni i cittadini consumatori riconoscono un ruolo di garanzia:

- del rispetto tra le parti, colmando il gap di fiducia generato dall'automazione e dalla disintermediazione della *sharing economy*;
- della correttezza ed eccellenza nella erogazione dei servizi, anche in termini sociali di consolidamento delle pratiche virtuose;
- della trasparenza nel trattamento dei dati.

Le assicurazioni intercettano dunque le grandi aspettative che i cittadini hanno verso l'innovazione tecnologica, con possibili estensioni di competenze dalla copertura del profilo di rischio all'ambito della diffusione e promozione di prodotti tecnologici.

CYBERSOCIALITÀ: OLTRE LA VITA CONNESSA

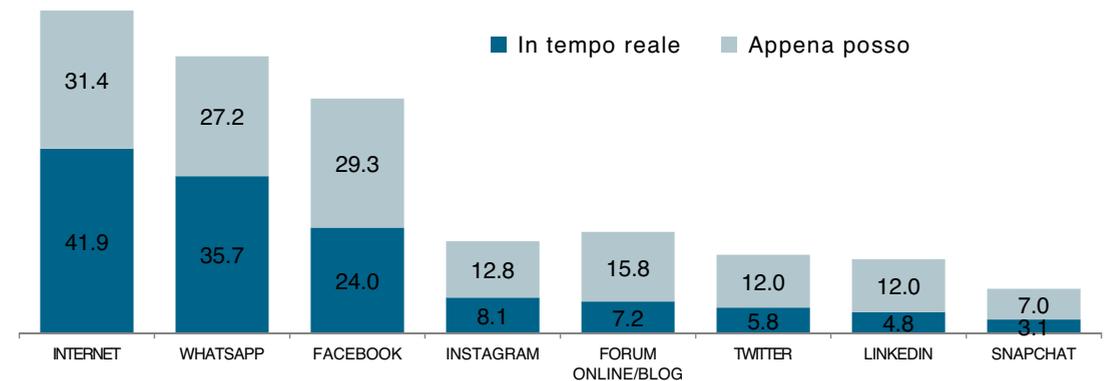
La nostra quotidianità si caratterizza per essere sempre disponibile e accessibile dalla tecnologia. Connetterci "appena possiamo" non significa "staccare dalla realtà", "fare pausa", ma districarsi in questo nuovo continuum restandoci sempre dentro.

Le tracce che i nostri comportamenti lasciano

nel mondo connesso sono diventate un "doppio digitale": un altro "noi" che è decifrabile e soprattutto prevedibile (nei gusti, nei comportamenti, nelle azioni), perché studiato e fatto interagire con altri doppi digitali.

Il tempo reale tende a cannibalizzare tutto il tempo restante nella formula dell'"appena posso": una disponibilità continua a interagire in ambito digitale ed essere rintracciati.

FIGURA 1. USO INTERNET E SOCIAL NETWORK IN UN GIORNO MEDIO (VALORI %)



Fonte: ATLAS 2016 Base: popolazione 15+74enni

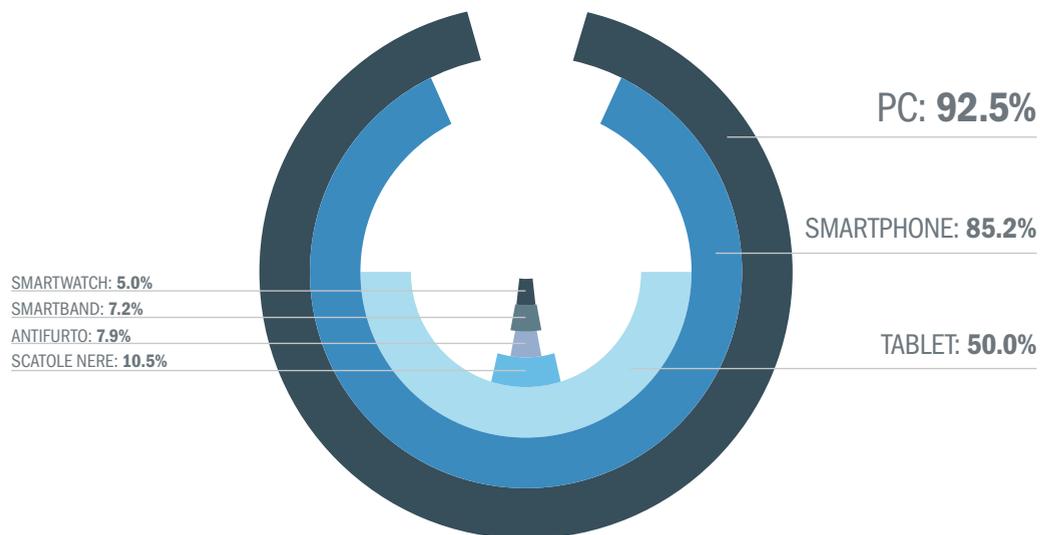
In una giornata tipo di un cittadino connesso, dotato di smartphone, possiamo infatti ipotizzare una molteplicità di usi che abbracciano le più comuni potenzialità del mobile: di tipo social, destinate alle comunicazioni con familiari e amici (Whatsapp, Facebook, ma anche più tradizionali come chiamate, sms, email); la ricerca di informazioni (dal meteo alla viabilità); di servizi

(come le app di navigazione e consultazione di mappe, le piattaforme di recensione e prenotazione di servizi, le app per i pagamenti, quelle mediche e di fitness, ecc.). L'uso della tecnologia (mobile, wearable, internet of things) permette a tutte le principali dimensioni della vita quotidiana (famiglia, affetti, casa, lavoro, tempo libero) di trasformarsi in traccia digitale,

di trasformarsi in documento e memoria e soprattutto di dare forma a un alter ego numerico e persistente. Al centro delle vite del nostro campione (gli italiani internet user) si trova

dunque il rapporto molto stretto, ormai intimo e simbiotico, con la tecnologia, come si evince dalle percentuali di possesso di dispositivi digitali.

FIGURA 2. POSSESSO PERSONALE DI DISPOSITIVI TECNOLOGICI (VALORI %)



Fonte: ATLAS 2016 Base: popolazione 15÷74enni

IL RAPPORTO CON LA TECNOLOGIA

L'intelligenza artificiale ricopre oggi un **nuovo protagonismo**, come strumento di supporto al fianco delle persone. Le aspettative verso la tecnologia sono quelle che si riversano su un **partner individuale**, capace cioè:

- nel presente, di offrire **soluzioni, indicazioni, risposte puntuali ai bisogni** (le app di servizio, i motori di ricerca);

- nel futuro, di trasformarsi in **prevenzione, consulenza evoluta, interpretazione della realtà** (crescita delle aspettative verso i robot sempre più intelligenti).

Allo stesso tempo, l'espansione della tecnologia chiama in causa il ruolo insostituibile del fattore umano: l'importanza della **sua tutela e la salvaguardia di rapporti di fiducia, anche in relazione alla *sharing economy*** (condivisione reciproca di informazioni, servizi, prodotti

esperienze). Emerge cioè **il tema centrale della garanzia del funzionamento del sistema**. Questa garanzia deve essere **al di sopra delle parti** e deve valere anche e soprattutto **tra persone che non si conoscono**. Solo così la *sharing economy* può appoggiarsi su entrambe le sue gambe: **la condivisione e la fiducia**.

Quando si parla di rapporto con il mondo digitale si intende innanzitutto l'uso di app di servizio: primi tra tutti i motori di ricerca. **Il digitale si afferma oggi infatti come strumento per la vita di tutti i giorni**, per i bisogni, più ancor che quotidiani, estemporanei e improvvisi: cercare un significato che ci sfugge, il nome di una persona, una strada.

L'altra faccia del connetterci 'appena possiamo' è infatti l' 'appena ne abbiamo bisogno': qui, ora, subito.

La tecnologia diventa anche un **compagno "sempre al lavoro"**: pensiamo ad esempio alla funzione continua di raccolta e segnalazione di informazioni utili, sconti, sistemi di accumulo di punti per premi che ci offrono le numerose tessere fidelizzanti (abbiano esse forme fisiche o virtuali, ci accompagnano oramai costantemente nei nostri acquisti). E così via, passando per i servizi di gestione dei pagamenti, del proprio conto corrente, delle polizze online.

FIGURA 3. FREQUENZA D'USO DI DISPOSITIVI TECNOLOGICI (VALORI %)

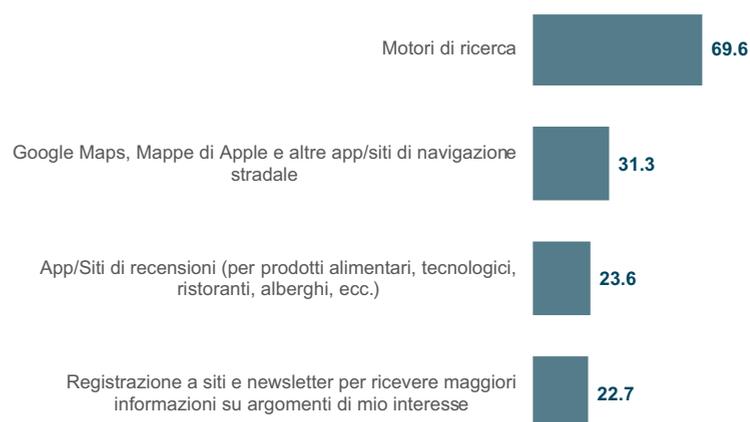


Fonte: ATLAS 2016 Base: popolazione 15÷74enni

La consapevolezza che in tutto ciò **il nostro uso della tecnologia ci espone a essere tracciati** è elevata, soprattutto quando si parla di motori di ricerca, servizi di geolocalizzazione, piattaforme di recensione di negozi e prodotti. In particolare **i motori di ricerca sono la punta dell'iceberg**

del nostro rapporto con il mondo digitale: nell'interrogarli ci sentiamo esposti e vulnerabili, perché **sentiamo di dipendere dalla possibilità stessa di domandare e cercare**, più ancora che legati alle singole richieste e alle singole ricerche.

FIGURA 4. LE APP CHE PIÙ DICONO DI NOI (POSSIBILI RISPOSTE MULTIPLE) (VALORI %)

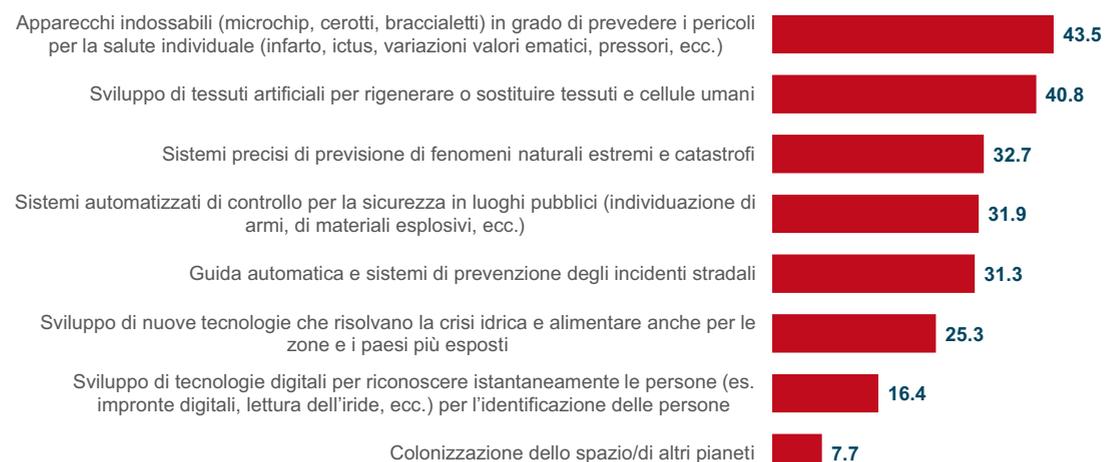


Fonte: ATLAS 2016 Base: popolazione 15÷74enni

Le aspettative verso la tecnologia si concentrano attorno alla **grande promessa salvifica** che anima la scienza e il progresso: la **capacità di guarire e di custodire la vita**. Ma più ancora che una risposta ex-post, una terapia di cura, sogniamo **la possibilità di mantenerci in salute, ridurre al**

minimo i rischi, di aumentare la nostra capacità di controllo e di autointervento, grazie a tecniche di monitoraggio, di simulazione e anticipazione dei pericoli, grazie infine alla **diffusione di buone abitudini e corretti stili di vita**.

FIGURA 5. ASPETTATIVE FUTURE VERSO LO SVILUPPO DI SOFTWARE E TECNOLOGIA INTELLIGENTE (VALORI %)



Fonte: ATLAS 2016 Base: popolazione 15÷74enni

In particolare verso le macchine intelligenti sono alte le aspettative per quanto attiene alla capacità di **riconoscere dei modelli di comportamento ricorrente** e di **ideare nuovi prodotti** sulla base di analisi dei comportamenti, individuati come

obiettivi, su cui puntare nei prossimi 5/10 anni. L'intelligenza artificiale è vista dunque come un completamento delle nostre capacità cognitive e come uno strumento per soddisfare i nostri sogni "segreti".

FIGURA 6. COSA FARANNO LE MACCHINE INTELLIGENTI NEI PROSSIMI 5/10 ANNI (VALORI %)



Fonte: ATLAS 2016 Base: popolazione 15+74enni

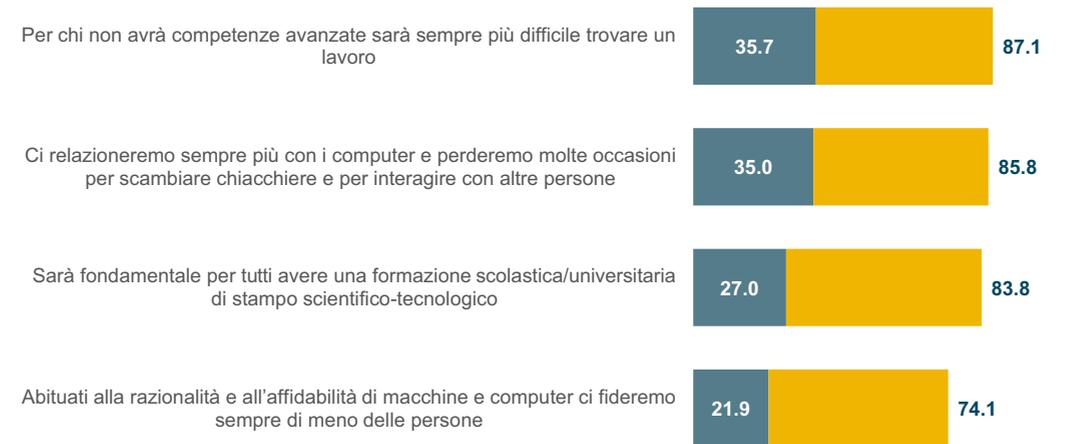
I robot suscitano dunque **grande curiosità ma anche alcune perplessità e paure**:

- per le **ricadute possibili sul mondo del lavoro e della formazione** (aumento della disoccupazione, maggiore selezione in entrata);
- per **l'impatto al momento sconosciuto sulle relazioni umane** (perderemo competenze relazionali, diventeremo più esigenti e impazienti di fronte alle manchevolezze e alle

fragilità caratteriali abituati all'efficienza delle macchine, ecc.);

Anche se si fatica in certi ambiti meno familiari a fidarsi delle macchine (i vantaggi offerti dai robo-advisor non sembrano essere tra le priorità degli italiani) emerge tuttavia **un'apertura verso i temi più prossimi alla vita quotidiana** (assistenza domestica agli anziani, svolgimento di lavori di casa).

FIGURA 7. GRADO D'ACCORDO (VALORI %)



Fonte: ATLAS 2016 Base: popolazione 15+74enni

FIGURA 8. INTERESSE PER I ROBOADVISOR (VALORI %)



Fonte: ATLAS 2016 Base: popolazione 15+74enni

FIGURA 9. INTERESSE PER ROBOT DOMESTICI (PER LA CURA DI ANZIANI E I LAVORI DOMESTICI) (VALORI %)

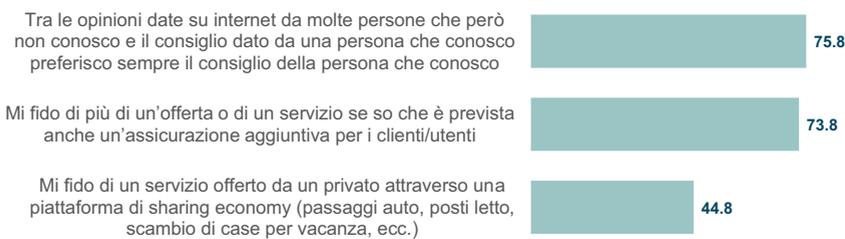


Fonte: ATLAS 2016 Base: popolazione 15+74enni

Le perplessità verso la digitalizzazione e la robotizzazione crescente si esprimono anche sotto forma di **richiesta di maggior tutele nell'erogazione dei servizi: i vantaggi di prezzo** risultanti dalla *sharing economy* da soli non bastano ad entusiasmare i cittadini-consumatori.

Serve anche una **rete di relazioni, fatta di consigli, pareri, garanzie dal volto più umano e tradizionale**. Detto altrimenti, il rapporto di fiducia è ancora al di là dall'essere assorbito apertamente dalla relazione con macchine intelligenti e software.

FIGURA 10. GRADO DI ACCORDO (MOLTO + ABBASTANZA) (VALORI %)



Fonte: ATLAS 2016 Base: popolazione 15+74enni

I BIG DATA TRA STRESS ED ENTUSIASMO

La **dipendenza dai motori di ricerca**, ma anche la **sovrastima delle proprie capacità nell'usarli**, lo **scarso controllo dei propri dati immessi nel sistema**, la **difficoltà a capire i meccanismi complessi** (gli "Algoritmi") che regolano la rete **provocano nei cittadini utenti una sensazione di spaesamento**, confusione e stress.

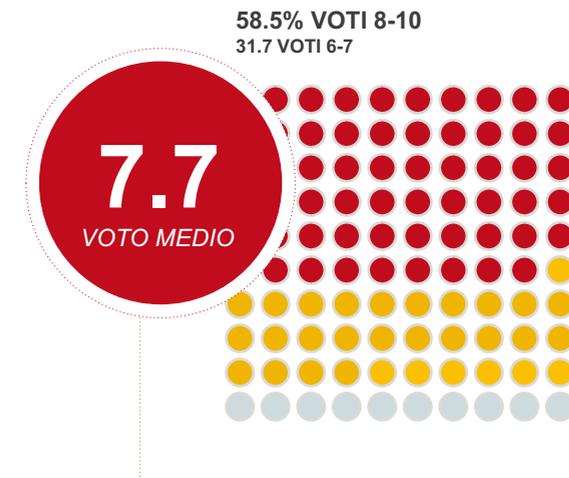
Di fronte alle potenzialità delle nuove tecnologie emerge una forte dicotomia: **come consumatori ci rallegriamo** e approfittiamo dei vantaggi derivati **dalla proliferazione di nuovi servizi**, ma **come cittadini ci sentiamo in balia delle aziende che governano la rete e gestiscono la miniera dei big data**, estromettendoci dal sapere che noi stessi contribuiamo a generare.

La vera rivoluzione dei *big data*, più che nell'accumulo enorme di dati – negli ultimi due anni abbiamo superato l'ordine degli *zettabyte* (10^{21}) – sta infatti **nella capacità di elaborare questa quantità di informazioni velocemente e con strumenti alla portata (quasi) di tutti**. Chi dunque riuscirà a sfruttare questo vantaggio conoscitivo?

Per quanto gli italiani dichiarino di possedere delle buone capacità di uso della tecnologia, **la possibilità di sfruttare pienamente la mole di informazioni che tutti quanti produciamo resta al momento una prerogativa delle aziende**.

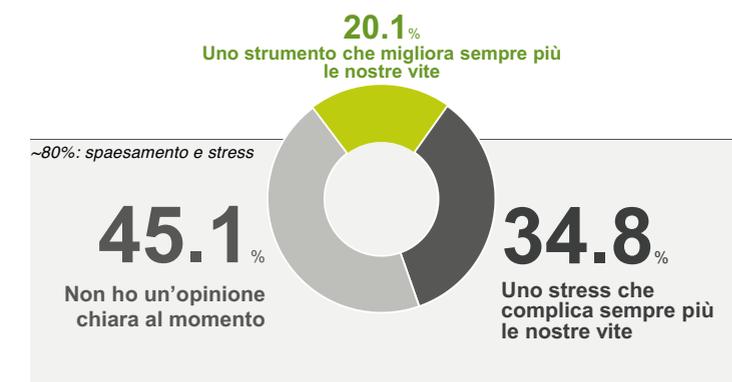
E proprio la possibilità di essere estromessi dai benefici di questa rivoluzione, pur vivendone gli eventuali effetti collaterali, genera nelle persone un **senso di inquietezza**.

FIGURA 11. AUTOVALUTAZIONE DELLE PROPRIE CAPACITÀ DI USARE MOTORI DI RICERCA (VALORI %)



Fonte: ATLAS 2016 Base: popolazione 15+74enni

FIGURA 12. COME VENGONO PERCEPITI I BIG DATA (VALORI %)

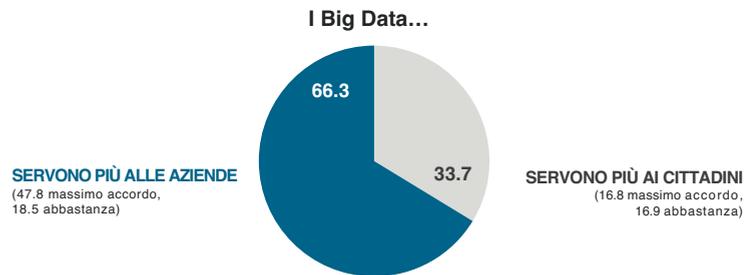


Fonte: ATLAS 2016 Base: popolazione 15+74enni

È significativo che, nonostante le aspettative verso le nuove tecnologie siano elevate, i *big data* in sé, come oggetto e materia prima da cui ricavare

nuova ricchezza, siano visti essenzialmente e al momento come **fonte di vantaggi per le aziende** più che per la società nel suo complesso.

FIGURA 13. A CHI SERVONO I BIG DATA (VALORI %)



Fonte: ATLAS 2016 Base: popolazione 15÷74enni

Ecco dunque che, a fianco delle grandi promesse (creazione di nuovi servizi e nuovi bisogni, aumento della varietà e delle opportunità), i *big data* incarnano paure radicate: perdita della *privacy*, perdita del controllo delle scelte. Dunque

le informazioni che produciamo, le nostre tracce digitali, non solo possono diventare uno strumento che "ci spia", ma anche che ci influenza, in modo più o meno esplicito e autorizzato, indirizzandoci verso quel determinato prodotto o servizio.

FIGURA 14. GRADO D'ACCORDO (MOLTO + ABBASTANZA) (VALORI %)



Fonte: ATLAS 2016 Base: popolazione 15÷74enni

PRIVACY VS SERVIZI: UN DIFFICILE EQUILIBRIO

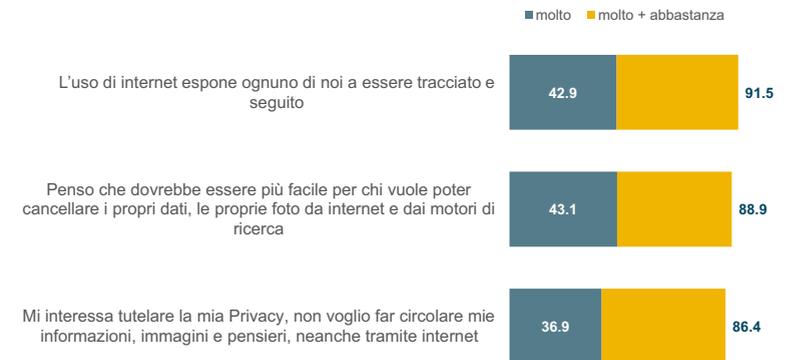
Il **tema della privacy** è altamente **sentito ed elaborato** dai cittadini utenti della rete. Si accompagna infatti a **comportamenti attivi e diffusi** verso la sicurezza online.

solo ognuno di noi vuole avere l'esclusiva nel montaggio della propria identità, ma bisogna garantire questo "controllo sull'ultima parola" anche nella sua radicale forma che si esprime nella volontà di autocancellazione, nel **diritto all'oblio**.

Esiste tuttavia un'area di conflitto tra la **grande voglia di raccontarsi e di farsi capire**, di vedere anticipati e assecondati i propri desideri e la **paura di perdere il controllo della propria immagine**, della propria storia, del racconto che ciascuno di noi vuole costruire di se stesso. Non

Oltre a questa nuova e peculiare paura, le preoccupazioni più diffuse restano quelle più frequenti e probabili, cioè quelle di **natura economica** riconducibili alla clonazione di carte di credito, al furto di codici personali, alle frodi.

FIGURA 15. GRADO D'ACCORDO (MOLTO + ABBASTANZA) (VALORI %)



Fonte: ATLAS 2016 Base: popolazione 15÷74enni

FIGURA 16. PREOCCUPAZIONI (VOTI MASSIMI: 6/7 E 7/7) (VALORI %)



Fonte: ATLAS 2016 Base: popolazione 15+74enni

IL RUOLO DEL SETTORE ASSICURATIVO

Le aspettative, le preoccupazioni e le non piene competenze degli utenti digitalizzati italiani sembrano indicare l'esistenza di **una grande possibilità per le assicurazioni**: quella di **assumere un ruolo di riferimento, di garanzia e di competenza, in grado di trasformare le attuali paure in opportunità**.

Il clima sociale è contrassegnato dalla preoccupazione. Lo studio dei trend rispetto al 2015 vede salire le **paure concrete** degli italiani e contemporaneamente **crescere la motivazione all'assicurarsi come strumento di pianificazione e di ampliamento del margine di gestione e protezione dai rischi**.

Il ruolo dell'assicurazione futura sembra dunque trasformarsi da **tutela "nel rischio" a tutela**

"al rischio", con un significativo cambiamento della dimensione temporale in cui si interviene: dall'"a posteriori" al "da prima" e "sempre".

Sempre dal confronto con il 2015, si rivela complessivamente **stabile la percentuale di assicurati**, mentre **diminuisce l'interesse generale a sottoscrivere polizze in futuro** (tengono Long Term Care, Rischi internet, Responsabilità civile). **L'interesse per le polizze online è buono**, tuttavia è subordinato alle **garanzie offerte da brand assicurativi conosciuti**.

L'assicurazione del futuro può avvantaggiarsi dell'**alto interesse verso prodotti e polizze caratterizzati da una forte componente tecnologica e di innovazione**. Grazie a questo interesse le assicurazioni potranno dunque proporsi pienamente come **erogatori di servizi di**

prevenzione e di supporto nel consolidamento di comportamenti virtuosi (scatole nere per auto, dispositivi salute, monitoraggio *smart* della casa/ "domotica").

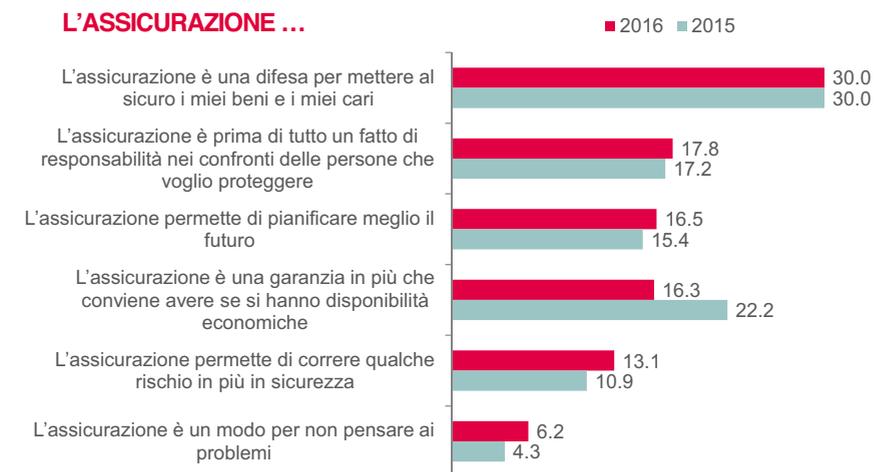
Per quanto riguarda infine **i canali distributivi**, si conferma **il valore della relazione personale con gli agenti** nei momenti topici di contatto con il mondo assicurativo (ascolto delle esigenze e assistenza in caso di necessità). Allo stesso tempo **crece la predisposizione verso l'online nelle fasi di comparazione e raccolta dei preventivi e nei servizi complementari** (es. simulazione apertura del sinistro).

Emerge dunque come sia di fondamentale importanza lo **sviluppo di tool che replichino le esperienze di fruizione online a supporto dei**

canali tradizionali. Per il settore assicurativo si aprono dunque importanti possibilità

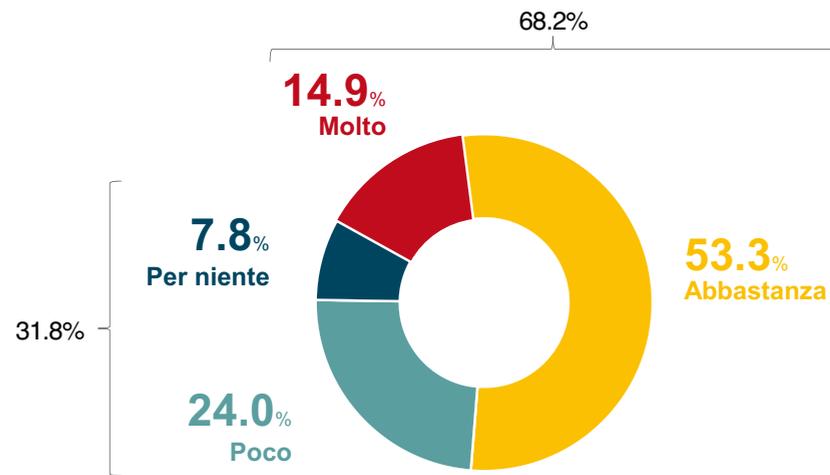
- sia di **natura commerciale**: verso un'**offerta Phygital** (valore relazione umana + personalizzazione del rischio), con **servizi ad alto valore aggiunto** resi possibili dalla tecnologia e digitalizzazione servizi complementari;
- sia **nello spazio sociale**, con la possibilità di esercitare un **ruolo di riferimento per le persone: rispetto delle norme; trasparenza e competenza nella gestione dei dati sensibili; prevenzione ed educazione di "impatto"**, capace di agire sui comportamenti; **mutualità per nuovi gruppi sociali emergenti**.

FIGURA 17. PERCHÉ ASSICURARSI (VALORI %)



Fonte: ATLAS 2016 Base: popolazione 15+74enni

FIGURA 18. INTERESSE AD ADOTTARE DISPOSITIVI TECNOLOGICI CHE INTEGRINO L'ASSICURAZIONE (VALORI %)



Fonte: ATLAS 2016 Base: popolazione 15÷74enni

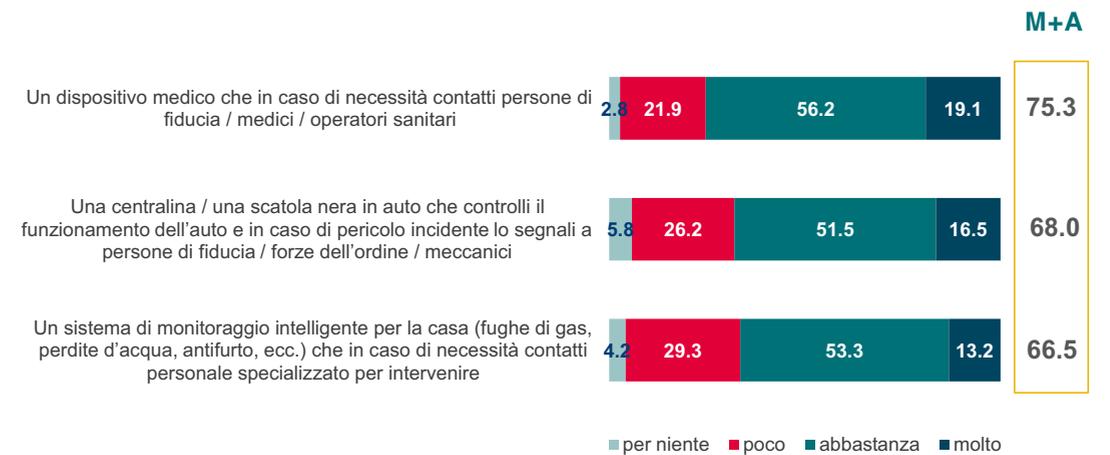
D'altra parte l'interesse per l'adozione di dispositivi tecnologici capaci di prevenire o monitorare il nostro stato di salute è uno dei capisaldi attorno a cui ruotano i nostri sogni sul futuro, per certi versi già presenti.

Infatti l'uso di braccialetti fitness e medici e scatole nere non solo è realtà, ma assolve alla duplice funzione di renderci più sicuri e soprattutto ci permette di comportarci meglio.

Ed è proprio questa una delle sfide più interessanti che si aprono per le assicurazioni del futuro: la capacità di agire sui comportamenti dei cittadini-consumatori, accompagnandoli responsabilmente verso una riduzione reale del rischio. Non più dunque solo gestione dei sinistri

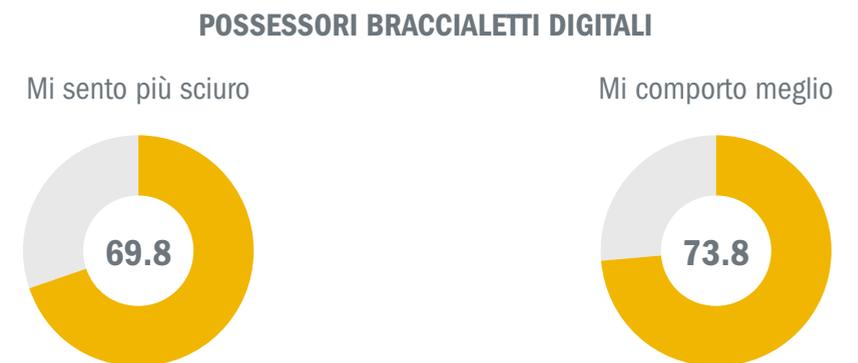
ex post. La compagnia assicurativa si trasforma così in un *lifestyle coach*, e il modello passa da quello tradizionale, incentrato sulla prevenzione e sulla trasmissione di informazioni relative ai rischi, a quello di agente di cambiamento dei comportamenti, al fianco e vicino alle persone.

FIGURA 19. INTERESSE PER IL POSSESSO DI DISPOSITIVI TECNOLOGICI (VALORI %)



Fonte: ATLAS 2016 Base: popolazione 15÷74enni

FIGURA 20. GRADO D'ACCORDO (MOLTO + ABBASTANZA) (VALORI %)

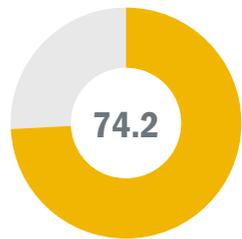


Fonte: ATLAS 2016 Base: popolazione 15÷74enni

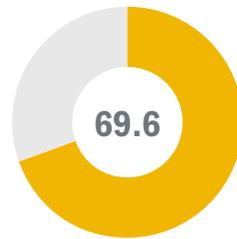
FIGURA 21. GRADO D'ACCORDO (MOLTO + ABBASTANZA) (VALORI %)

POSSESSORI SCATOLE NERE

Mi sento più sicuro

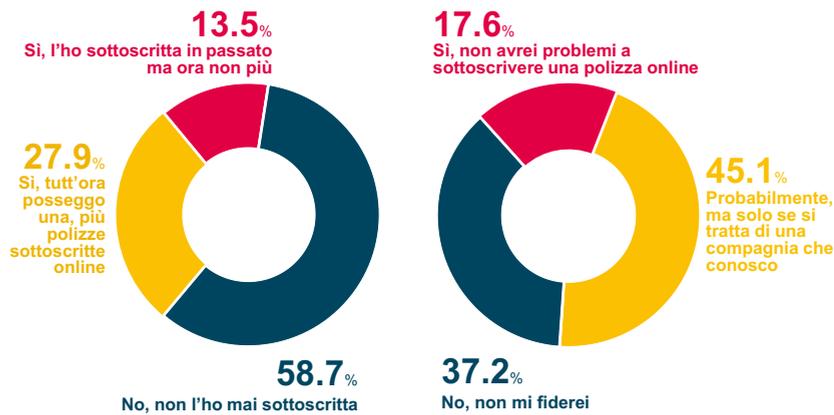


Mi comporto meglio



Fonte: ATLAS 2016 Base: popolazione 15÷74enni

FIGURA 22. SOTTOSCRIZIONE E INTERESSE PER POLIZZE ONLINE) (VALORI %)



Fonte: ATLAS 2016 Base: popolazione 15÷74enni

FIGURA 23. CANALI INFORMATIVI PREFERITI PER MOMENTO/SERVIZIO (VALORI %)

	Preferirei parlare con un agente assicurativo	Preferirei usare un servizio automatizzato	È indifferente
L'ascolto delle proprie esigenze di protezione	58.9	21.8	19.2
La presentazione di diverse soluzioni di assicurazione	47.2	30.5	22.2
L'illustrazione del funzionamento di apparecchi/dispositivi di sicurezza	47.2	27.7	25.2
La comparazione tra diverse proposte assicurative (coperture assicurative, costi, ecc.)	40.8	35.8	23.4
La simulazione/il racconto della procedura per aprire il sinistro e per chiedere consulenza/assistenza	45.8	30.7	23.5
L'assistenza, il momento in cui si vuole aprire il sinistro/si ha bisogno di consulenza	58.9	21.3	19.8

Fonte: ATLAS 2016 Base: popolazione 15÷74enni

3. UN APPROCCIO OLISTICO ALLA SICUREZZA DEI DATI. AFFRONTARE I NUOVI RISCHI LEGATI AI *BIG DATA* E AL *CLOUD*: UN CASO RECENTE SULLA TRASPARENZA DEL SOFTWARE

Bryan Ford, AXA Chair in Information Security and Privacy, Ecole Polytechnique Fédérale di Losanna

UNA CATTEDRA AXA DEDICATA ALLA SICUREZZA INFORMATICA E PRIVACY

Il lavoro degli informatici è essenziale per le nostre attività personali e professionali, a tal punto che a stento riusciamo a immaginare una vita senza di essi. Al tempo stesso, l'importanza conquistata da questo campo, compresi *cloud computing* e *big data*, ci costringe ora a esaminare attentamente i rischi che comporta e a trovare nuovi approcci per garantire la sicurezza dei nostri dati.

La maggior parte dei ricercatori si dedica a rafforzare una determinata proprietà di sicurezza, nonostante questo potrebbe voler dire trascurarne altre. Tuttavia, il Prof. Bryan Ford ritiene che la questione possa essere trattata solo in maniera olistica, affrontando simultaneamente le numerose domande che gli utenti pongono in merito ai sistemi di protezione dei dati. Inoltre, il Professore è sicuro che sia necessario iniziare a studiare immediatamente questa possibilità.

Pur non rinunciando alle potenzialità dei metodi di elaborazione più avanzati, gli **attacchi cyber** si fanno **sempre più sofisticati** e il rischio di guasti ai sistemi è sempre più concreto. Con questo programma di ricerca, il Prof. Ford punta a **identificare i rischi più urgenti, ma meno esplorati**, e a proporre **nuove soluzioni** per affrontarli.

Le tre proprietà principali della sicurezza dei dati sono la **disponibilità** (garanzia che i dati non vengano perduti o non divengano inaccessibili), l'**integrità** (dati né "corrotti" né manipolati in

malafede) e la **riservatezza** (dati né divulgati né utilizzati impropriamente). La sfida consiste nel **garantire ognuna di queste proprietà senza compromettere le altre**. Ad esempio, per verificare l'integrità dei dati occorre divulgarli, violando così la privacy dell'utente.

Il Prof. Ford ha già cominciato ad affrontare la questione creando **sistemi decentralizzati su piccola scala** che siano efficienti in termini di riservatezza, dotati di integrità di sistema e di tutele per la disponibilità. Il compromesso è stato il numero esiguo di utenti che questi sistemi erano in grado di sostenere. Tuttavia il suo lavoro precedente su un progetto chiamato "Dissent" ha dimostrato che, grazie a **tecniche innovative**, questi sistemi sarebbero in grado di **supportare come minimo migliaia di utenti**, il che li renderebbe pratici per l'implementazione nel mondo reale. In futuro il Prof. Ford migliorerà la struttura che ha concepito per consentirne l'uso nei **sistemi di comunicazione**, ma anche per realizzare strumenti sicuri capaci di preservare la privacy e per molte altre funzioni di primaria importanza, quali **applicazioni per il voto, soluzioni di archiviazione digitale** e l'uso di valute criptate come i **bitcoin**.

Secondo il Prof. Ford, mentre gli straordinari progressi nel campo dell'informatica rendono possibile quanto descritto sopra, la crescita del fenomeno del **cloud computing** introduce **nuovi rischi**, rendendo quelli già noti solo la punta dell'iceberg. A preoccupare il Professore non sono i problemi correlati direttamente al proprio provider di servizi su *cloud*, come i blackout che impediscono l'accesso, bensì i **rischi secondari**. Questi comprendono **servizi su cloud che**

possono apparire indipendenti, ma che in realtà dietro le quinte condividono risorse, **minando la sicurezza** normalmente conferita dalla ridondanza ovvero – aggiunta di parti duplicate per aumentare l'affidabilità¹ – in un sistema. Il tutto potrebbe creare **“correlazioni di guasto inattese e potenzialmente catastrofiche**, come ci insegnano i vari crac del settore finanziario”.

Inoltre, a richiedere attenzione urgente è **la sfida che il cloud computing aggiunge alla tutela degli artefatti digitali**². La tecnologia cambia rapidamente e le versioni divengono obsolete, mettendo a rischio la disponibilità a lungo termine. Grazie alle applicazioni basate sul *cloud* gli utenti non entrano mai in possesso di una copia completa e funzionale dell'elemento da custodire in una *repository*: basti pensare ai motori di ricerca o alla mappatura delle applicazioni in confronto al software di elaborazione testi installato direttamente sul computer. Quindi, come gli archivisti digitali possono catalogare su *cloud* artefatti di interesse storico ai fini della preservazione della cultura nel lungo periodo? Il progetto di ricerca del Prof. Ford vuole rispondere a domande come questa, che devono essere poste in una nuova era di *cloud computing*. In risposta ai rischi citati, il Professore progetterà anche **nuove architetture di sistema** in grado

di affrontare i problemi insorti, con l'obiettivo di sviluppare **metodi per la quantificazione dei rischi correlati alla violazione della privacy o a un guasto in un sistema**. Quindi procederà a creare **prototipi in grado di utilizzare queste misurazioni per riconfigurare i sistemi su cloud a rischio**. Iniziando subito il progetto, il Prof. Ford spera di comprendere i rischi e di sviluppare soluzioni “prima che il nostro tessuto socio-economico diventi indissolubilmente dipendente da un modello di elaborazione conveniente ma potenzialmente instabile”.

LE SFIDE DI FONDO EMERSE NEL RECENTE CASO DELLA TRASPARENZA DEL SOFTWARE*

Il recente scontro tra Apple e FBI rappresenta uno snodo centrale della nuova *Crypto War*. Il 16 febbraio 2016 l'FBI ha invocato l'*All Writs Act* del 1789, un'autorità a tutto tondo di assistenza all'*enforcement* della legge, chiedendo ad Apple di creare una versione su misura del suo iOS al fine di aiutare l'FBI a decriptare un iPhone utilizzato da uno degli autori della sparatoria di San Bernardino³. Il fatto che l'FBI abbia permesso ad Apple di rendere l'ordine di pubblico dominio lo stesso giorno rappresenta una rara eccezione alla tradizionale propensione dei governi per la segretezza.

* Contributo da *Freedom to Tinker, Princeton's Center for Information Technology Policy*, 10 marzo 2016, <https://freedom-to-tinker.com/2016/03/10/apple-fbi-and-software-transparency/>
Le opinioni e i contenuti riportati dall'autore sono strettamente personali e non rappresentano in alcun modo AXA.

¹ La ridondanza in ambito tecnologico è l'aggiunta di parti duplicate per aumentare l'affidabilità del sistema.

² In generale, un artefatto è qualsiasi fattore introdotto nella rappresentazione che non è o non era presente anche nell'oggetto in esame. Con il termine vengono indicati quei disturbi dei segnali digitali, analogici o delle immagini, dovuti alla tecnica di acquisizione, di codifica o a diversi fenomeni interferenti che alterino il reale risultato finale del processo. Il termine viene spesso utilizzato anche in campo chimico analitico, in diverse discipline utilizzando dispositivi ottici quali microscopi e telescopi e nelle procedure biomediche, per indicare diverse possibili interferenze in molti differenti campi di analisi.

³ Il 2 dicembre 2015 due attentatori di matrice islamica hanno attaccato il centro disabili di San Bernardino (California), cittadina di 200 mila abitanti a circa 100 chilometri a est di Los Angeles, uccidendo 14 persone e ferendone altre 2.

Le ragioni alla base dell'entrata in scena insolitamente "rumorosa" dell'FBI sono importanti, ma lo è ancora di più il rischio che, in seguito ad altri problemi, l'FBI e le altre agenzie governative possano utilizzare metodi più "dissimulati" per costringere le aziende a creare una *backdoor*⁴ nei propri software. Il presente contributo esplora non solo i rischi connessi alla trasparenza del software, ma anche in che modo le nuove misure tecniche possono contribuire a fare rimanere pubblico il dibattito sulle *backdoor* dei software.

L'ORDINE DI ASSISTENZA ALLA DECRIPTAZIONE

Le aziende operanti nel settore della tecnologia sono abitualmente *compliant* con le indicazioni governative sui dati in loro possesso. Tuttavia, nel caso in oggetto, i dati non si trovano in possesso di Apple, bensì all'interno di un iPhone criptato e viene ordinato ad Apple di creare un nuovo software che aiuti l'FBI ad aggirare la sicurezza di quell'iPhone. Sebbene Apple sia probabilmente in grado di eseguire dal punto di vista tecnico quanto richiesto dall'FBI, si è schierata inizialmente contro tale ordine con la seguente motivazione: "il Governo chiede che Apple crei una *backdoor* per eludere la cifratura sull'iPhone, rendendo le informazioni più riservate e personali dei suoi utenti vulnerabili a pirati informatici, ladri di identità, agenti stranieri ostili e sorveglianza governativa arbitraria".

Pretendere che un'azienda privata crei un nuovo "strumento forense" (*forensic tool*) su ordine del Governo, indebolendo la sicurezza dei dispositivi Apple e rivelando i segreti più intimi dei propri

utenti, potrebbe costituire una violazione del primo emendamento della Costituzione degli Stati Uniti. L'ordine è paragonabile ad esempio al chiedere a General Motors di realizzare un nuovo camion a cinque ruote entro il mese prossimo.

Probabilmente l'FBI sarebbe in grado di creare la propria versione di iOS munita di *backdoor*. Tuttavia, i dispositivi Apple accettano esclusivamente aggiornamenti software recanti una firma digitale basata su una chiave segreta presumibilmente controllata solo da Apple. *Presumibilmente*. Ci ritorneremo...

PERCHÉ COSÌ TANTA PUBBLICITÀ?

Una delle caratteristiche più interessanti e insolite di questo caso è la rapidità con cui il pubblico, cioè noi, è venuto a sapere della vicenda da Apple. L'FBI avrebbe potuto impartire quest'ordine in modo riservato, proprio come ha fatto per avanzare altre richieste analoghe di assistenza alla decriptazione nei confronti di Apple ma anche di altre aziende come Lavabit, il fornitore di servizi e-mail (ormai scomparso) utilizzato da Edward Snowden.

Apple ha addirittura richiesto espressamente che l'ordine dell'FBI fosse posto sotto segreto, ma l'FBI ha optato per uno scontro pubblico. I fatti relativi al caso minano le rivendicazioni dell'FBI riguardanti l'urgenza di accedere ai contenuti dell'iPhone: i killer non erano più in vita da tempo, la montagna di metadati relativi ai killer di cui l'FBI era già in possesso non ha rivelato alcun collegamento con altri terroristi e l'iPhone in questione era un telefono aziendale che i killer non si sono premurati di distruggere,

⁴ In informatica, codice o serie di comandi che consentono di accedere a un software o a un sistema informatico, conosciuti generalmente solo dal programmatore e usati in casi di emergenza o per l'ordinaria manutenzione.

come hanno invece fatto con i loro due telefoni personali.

L'interpretazione dei fatti, applicando il principio del Rasoio di Occam⁵, suggerisce che l'FBI sia meno interessata ai dati veri e propri di quanto non lo sia nei confronti del precedente giuridico costituito da un'eventuale vittoria in tribunale. L'iPhone in questione rappresenta un campo di battaglia scelto strategicamente, su cui l'FBI ritiene di poter vincere giocando la carta del terrorismo, anche se in verità questo specifico iPhone è di scarso o di nessun valore ai fini dell'intelligence.

In difesa di Apple si è schierata gran parte dell'opinione pubblica americana; organizzazioni e fondazioni di pubblico interesse quali CDT (*Center for Democracy & Technology*), ACLU (*American Civil Liberties Union*), EFF (*Electronic Frontier Foundation*); molti giganti della tecnologia tra cui Google, Intel, Microsoft, Cisco e Amazon; giornali come il New York Times e il Wall Street Journal, l'Alto Commissario delle Nazioni Unite per i Diritti Umani; persino l'ex direttore dell'NSA e altri ex alti funzionari del Governo degli Stati Uniti.

L'ALTERNATIVA DELLA RISERVATEZZA, PASSATA E FUTURA

A prescindere da questa battaglia pubblica, è altrettanto importante capire che l'FBI e i governi di tutto il mondo possono perseguire e spesso abbiano perseguito in segreto gli stessi obiettivi: Apple contro FBI è più un'eccezione che la regola. Basti pensare all'esito delle prime *Crypto Wars*, in cui il governo statunitense ha tentato di esigere la chiave di cifratura contenuta nel famigerato *chip Clipper*⁶. Nonostante abbia perso quella battaglia pubblica, il Governo non si è arreso, bensì ha semplicemente messo in ombra, di nuovo, il suo impegno volto a violare la cifratura.

Ad esempio, apparentemente l'NSA ha inserito di nascosto una *backdoor* in uno standard dell'agenzia governativa NIST (*National Institute of Standards and Technology*) per la generazione di numeri casuali, consentendo di violare tutti gli algoritmi di cifratura su un dispositivo. Per dimostrare i pericoli correlati al tentativo di tenere una *backdoor* accessibile solo ai "buoni", recentemente un pirata sconosciuto è riuscito a modificare la chiave e a impadronirsi di una copia latente di questo generatore di numeri casuali dotato di *backdoor* nei router della multinazionale ICT Networks.

⁵ Rasoio di Occam (*Novacula Occami* in latino) è il nome con cui viene contraddistinto un principio metodologico espresso nel XIV secolo dal filosofo e frate francescano inglese William of Ockham, noto in italiano come Guglielmo di Occam. Tale principio, ritenuto alla base del pensiero scientifico moderno, nella sua forma più immediata, suggerisce l'inutilità di formulare più assunzioni di quelle strettamente necessarie per spiegare un dato fenomeno: il rasoio di Ockham impone di scegliere, tra le molteplici cause e a parità di fattori, quella che spiega in modo più semplice l'evento. La formula è utilizzata spesso in ambito investigativo e di *problem solving*.

⁶ Il *chip Clipper* era un dispositivo di cifratura sviluppato dall'Agenzia per la sicurezza nazionale (NSA) statunitense che avrebbe dovuto essere adottato dalle compagnie telefoniche per cifrare le comunicazioni telefoniche. Annunciato nel 1993 e dismesso nel 1996, sia per la contrarietà emersa nel dibattito sulla sua adozione (possibile sorveglianza illegale da parte del governo sui cittadini), sia per lo sviluppo di software crittografici ad elevata affidabilità, disponibili gratuitamente su Internet.

Anche se a prevalere in questo nuovo round delle *Crypto Wars* è il buon senso, possiamo essere certi che il Governo statunitense e i governi di tutto il mondo continueranno a tentare di acquisire *backdoor* segrete. Naturalmente, i governi possono sfruttare *bug* nel software oppure vulnerabilità fisiche per accedere nei dispositivi personali. Tuttavia le *backdoor* segrete continueranno a costituire un potente richiamo. Sfruttare una *backdoor* nota è più semplice, più economico e meno rischioso rispetto alla creazione *ex novo* di una via di accesso personalizzata.

LA BACKDOOR PER L'AGGIORNAMENTO SOFTWARE

Quasi tutti i dispositivi personali moderni, compresi quelli di Apple, sono già dotati di una *backdoor* pronta per essere lanciata sotto forma di aggiornamenti software automatici convalidati da firme digitali. Un metodo con cui il Governo statunitense potrebbe acquisire una *backdoor* universale per i dispositivi Apple consiste, semplicemente, nell'esigere una copia delle chiavi segrete di Apple per la firma del software. Il Governo ha già manifestato l'intenzione di procedere proprio in questo modo, come ha preteso con le chiavi master del servizio di e-mail cifrate di Lavabit durante le indagini su Snowden. Potrebbe non trattarsi di una questione del tutto marginale se le chiavi per la firma del software di Apple fossero custodite su Moduli Hardware di Sicurezza (HSM) concepiti per impedire

l'estrazione o la clonazione di chiavi segrete. Tuttavia, in questo caso, il Governo potrebbe semplicemente imporre ad Apple di utilizzare la propria chiave segreta per produrre una firma digitale valida per la versione dell'iOS dotata di *backdoor* creata dall'FBI, mantenendo segreti sia questo processo sia l'esistenza dell'iOS munito di *backdoor*.

Sia che vinca la battaglia pubblica, sia che venga costretta a prestare il proprio aiuto in segreto firmando software con *backdoor* e immagini di *firmware*⁷, Apple si troverebbe comunque ad affrontare timori e sospetti fondati dell'era post-Snowden e nutriti da aziende e governi di tutto il mondo. Apple non è unica azienda esposta a questo rischio, bensì lo è qualsiasi organizzazione che crea e rilascia software. Persino il software *open source* non è immune, poiché è impossibile sapere con certezza se un aggiornamento software rappresenta o meno una versione compilata correttamente, ad eccezione dei casi in cui viene realizzata personalmente, cosa che ben pochi utenti fanno.

TRASPARENZA DEL SOFTWARE MEDIANTE LA CO-FIRMA DECENTRATA DEI TESTIMONI

In occasione di IEEE Security & Privacy 2016⁸, un gruppo di esperti, tra cui il sottoscritto, ha presentato un paper⁹ che introduce la *co-firma decentrata dei testimoni*, uno strumento tecnologico adottato da produttori di software come Apple per proteggere i propri utenti da

⁷ È un programma, ovvero una sequenza di istruzioni, integrato direttamente in un componente elettronico e non è immediatamente modificabile dall'utente finale. Ha lo scopo di avviare il componente stesso e consentirgli di interagire con altri componenti hardware tramite l'implementazione di protocolli di comunicazione o interfacce di programmazione.

⁸ È il più importante incontro annuale sulla sicurezza e sulla privacy on-line. L'Edizione 2016 si è svolta dal 23 al 26 maggio a San Jose (California, USA), <http://www.ieee-security.org/TC/SP2016/>

⁹ <http://dedis.cs.yale.edu/dissent/papers/witness-abs>

versioni contenenti una *backdoor* nascosta. In questo modo i produttori proteggono anche se stessi e i propri utili dai timori e dai sospetti globali inerenti il software con *backdoor*.

Con le firme digitali convenzionali, comunemente utilizzate per la maggior parte dei processi di firma di software e *firmware*, un solo soggetto (ad es. Apple) è in possesso della chiave segreta necessaria per produrre immagini di software valide accettate dai dispositivi e dai rispettivi sistemi di aggiornamento. Qualsiasi sistema di aggiornamento ben realizzato rifiuta ogni immagine software che non sia stata autenticata mediante un *certificato digitale* integrato nel dispositivo, il quale identifica con una cifratura il produttore del software per mezzo di una relazione matematica con la chiave di firma segreta. Le *best practice* per la firma del software prevedono già di custodire *offline* le chiavi di firma particolarmente sensibili: è il caso di ICANN (*Internet Corporation for Assigned Names and Numbers*), che ha introdotto DNSSEC (*Domain Name System Security Extensions*), specifiche ed estensioni nate con l'obiettivo di assicurare che la comunicazione avvenga in maniera corretta e sicura, con il flusso dati proveniente dall'IP corretto¹⁰. Comunque, come accennato sopra, tali misure non impediscono che l'organizzazione venga costretta ad abusare segretamente delle chiavi di firma.

Con la co-firma decentrata dei testimoni, un produttore di software imprime nei propri dispositivi e sistemi di aggiornamento un certificato digitale che non corrisponde solo alla loro chiave segreta, ma anche a quelle in possesso di un gruppo di testimoni indipendenti.

Tali testimoni possono comprendere altre aziende produttrici di software con cui è in atto una collaborazione, organizzazioni di pubblico interesse come ACLU, EFF o CDT oppure importanti aziende clienti o governi mondiali che desiderano garanzie di natura non solo verbale ma anche tecnologica dell'impegno alla trasparenza assunto dai produttori. A sua volta, prima di accettare qualunque immagine software, il sistema di aggiornamento del dispositivo verifica che l'immagine rechi non solo la firma del produttore, ma anche quella di un certo numero di testimoni designati. In sostanza, il dispositivo non accetta immagini software a meno che non rechino una "prova" crittografica attestante che quella particolare immagine è stata esaminata pubblicamente da (e in tal modo sottoposta a scrutinio di) un gruppo decentrato di soggetti indipendenti sparsi per il mondo in varie giurisdizioni.

LA SCALABILITÀ DELLA CO-FIRMA DEI TESTIMONI

Dal punto di vista tecnico, implementare la co-firma dei testimoni è piuttosto semplice se il numero di testimoni è ristretto. Un produttore di software potrebbe semplicemente creare un elenco di firme individuali per ogni nuova *release* del software, proprio come per centinaia di anni è stato fatto per le petizioni pubbliche. Tuttavia se occorre un gruppo esteso di testimoni – e a noi occorre per garantire che la massima trasparenza – radunare centinaia o migliaia di firme individuali per ogni *release* del software può diventare gravoso e inefficiente. Non solo: ogni dispositivo che necessita di convalidare un *download* o un aggiornamento dovrebbe verificare singolarmente

¹⁰ L'ente non profit statunitense, organizzato in sede internazionale, è infatti impegnato, tra le altre cose, nell'assegnare gli indirizzi IP ai domini di primo livello come .com, .org o .it. Per info: <https://archive.icann.org/tr/italian.html>

tutte queste firme, con conseguenti ritardi e ripercussioni sull'autonomia della batteria.

Il contributo tecnico fondamentale apportato dalla nostra ricerca consiste in un protocollo distribuito che automatizza questo processo e agevola il ricorso alla co-firma di ampi gruppi di testimoni decentrati. In sintesi: il protocollo prevede di comprimere centinaia o migliaia di firme in una firma singola, verificabile quasi con la stessa semplicità ed efficienza di una normale firma personale¹¹.

COME SI FA A SAPERE SE C'È UNA BACKDOOR?

Purtroppo, durante il processo di co-firma dei testimoni, gli indipendenti non sono necessariamente in grado di determinare immediatamente se una specifica immagine software contenga o meno una *backdoor*. In particolare, questo accade nel consueto caso in cui il codice sorgente è proprietario e il produttore di software firma e rilascia solo immagini binarie. Ciò nonostante i testimoni possono comunque garantire trasparenza in maniera proattiva assicurandosi che ogni immagine software esistente dotata di firma valida sia stata divulgata, catalogata e sottoposta a pubblico scrutinio.

Ad esempio, se in futuro i dispositivi Apple adottassero la co-firma decentrata dei testimoni e un governo tentasse in segreto di costringere Apple a firmare una versione di iOS 11.2.1 dotata di *backdoor*, il solo modo in cui la società di Cupertino potrebbe farlo sarebbe sottoporre la versione di iOS dotata di *backdoor* ai testimoni indipendenti per la co-firma. Anche

se tali testimoni non fossero necessariamente in grado di individuare la *backdoor*, potrebbero notare immediatamente che sono state firmate due diverse versioni di iOS denominate “versione 11.2.1”, vale a dire la versione standard e quella dotata di *backdoor*. Questa incongruenza, da sola, dovrebbe immediatamente rappresentare un campanello d'allarme e attirare l'attenzione delle imprese di tutto il mondo operanti nel settore della sicurezza, le quali potrebbero esaminare accuratamente le differenze tra le due immagini software.

Naturalmente, un governo potrebbe costringere Apple ad assegnare all'immagine dotata di *backdoor* un numero di versione diverso che la maggior parte dei suoi clienti non riceverà mai: ad esempio, “11.2.1.fbi” o il più anonimo “11.2.1.1”. Tuttavia, i testimoni sarebbero comunque in grado di stabilire l'esistenza di un'immagine iOS firmata ma non distribuita, attirando ancora una volta le attenzioni degli esperti sulla sicurezza, che procederebbero a un attento scrutinio.

Ovviamente Apple, oppure un suo dipendente in malafede, sarebbe comunque in grado di inserire una *backdoor* nascosta o un *bug* di sicurezza nelle *release* standard di iOS che *tutti* usano. I *bug* e le *backdoor* accidentali possono esistere per anni senza essere individuati, come dimostra ampiamente l'incidente di Juniper. Il software *open source* offre un vantaggio in termini di trasparenza, specialmente grazie alle *build* riproducibili, ma persino le *backdoor* a questo livello possono essere diabolicamente insidiose.

Ciò nonostante, le tecniche e gli strumenti per l'analisi del software sorgente e binario sono in

continuo miglioramento, e la co-firma decentrata dei testimoni è in grado di garantire che tutte le *release* di una distribuzione software siano pubblicamente note ed esposte a quest'analisi a opera di ricercatori di talento nel campo della sicurezza e di hacker etici di tutto il mondo. Un pirata che nasconde una *backdoor* in una *release* software disponibile al pubblico corre il rischio che possa essere scoperta in qualsiasi momento. La co-firma dei testimoni impedisce agli autori di attacchi di aggirare il rischio di essere scoperti, persino installando segretamente il software dotato di *backdoor* solo su determinati dispositivi sotto il controllo del pirata.

TRASPARENZA: APPROCCIO PROATTIVO VS. APPROCCIO RETROATTIVO

La co-firma decentrata dei testimoni non rappresenta il primo meccanismo crittografico di trasparenza. Ad esempio, l'infrastruttura a chiave pubblica (*Public Key Infrastructure - PKI*) utilizzata per la sicurezza delle connessioni web presenta punti deboli analoghi, ed esistono meccanismi di trasparenza come la *Convergence*, *Sovereign Keys*, *Certificate Transparency*, (...) per affrontare questo problema.

Oggi il *Certificate Transparency* di Google è standard nel browser Chrome. *Application Transparency* è una variante proposta del *Certificate Transparency*, adattata per i download e agli aggiornamenti software. Altre proposte correlate come *Perspectives* e *CONIKS* puntano a risolvere problemi analoghi rispettivamente in merito alle connessioni *Secure Shell* (SSH) – un protocollo di rete che consente lo scambio di dati su un canale protetto tra due computer – e alla messaggistica criptata *end-to-end*.

Tuttavia, i meccanismi di trasparenza sopra citati presentano due punti deboli rilevanti:

1. non incrementano in modo significativo il numero di chiavi segrete che un pirata deve controllare per violare qualunque dispositivo personale;
2. tali dispositivi non possono nemmeno rilevare in maniera retroattiva detta violazione, a meno che non siano in grado di comunicare attivamente con vari server Internet.

Ad esempio, anche con il *Certificate Transparency*, un pirata può creare un certificato *Extended Validation* (EV) per Chrome dopo aver violato o costretto solo tre soggetti: una *Certificate Authority* (CA) e due *log server*. Poiché numerosi CA e *log server* rientrano nella giurisdizione degli Stati Uniti, un attacco del genere è chiaramente alla portata del governo statunitense e qualora si verificasse, *Certificate Transparency* non è in grado di rilevarlo a meno che il dispositivo bersaglio non sia in grado di comunicare o far trapelare (*gossip*) il certificato falso ad altri soggetti su Internet, tutto questo dopo che il dispositivo ha accettato e iniziato a utilizzare il falso.

I meccanismi legati al *gossip* non sono in grado di garantire la trasparenza del software. Queste debolezze sono particolarmente gravi in termini di trasparenza, ovvero la questione principale del caso Apple contro FBI. Innanzitutto, se un dispositivo personale accetta e inizia a utilizzare un aggiornamento software dotato di *backdoor* prima di aver avuto l'occasione di diffondere informazioni sull'aggiornamento ad altri soggetti su Internet, il software munito di *backdoor* riesce a eludere la trasparenza semplicemente

¹¹ Per dettagli: <http://dedis.cs.yale.edu/dissent/papers/witness-abs>

disabilitando tale diffusione nel codice aggiornato. In secondo luogo, se per qualche ragione il pirata non fosse in grado oppure omettesse di eseguire questo passaggio piuttosto ovvio, egli può ancora eludere la trasparenza controllando il dispositivo o i suoi percorsi di accesso a Internet. Nel caso FBI contro Apple, ad esempio, l'FBI potrebbe eludere con semplicità la trasparenza basata sul gossip e tenere segreta la sua immagine iOS dotata di *backdoor* mantenendo il dispositivo disconnesso dal resto della rete Internet in seguito all'installazione dell'aggiornamento software munito di *backdoor*.

Questo punto debole della trasparenza basata sul *gossip* riguarda anche gli autori di attacchi che potrebbero non controllare il dispositivo in sé, ma il suo percorso di accesso a Internet. Ad esempio, la violazione di un fornitore di servizi Internet (*Internet service provider* - ISP) o di un *gateway* Internet aziendale può sconfiggere la trasparenza basata sul *gossip* bloccando costantemente l'accesso della vittima ai server di trasparenza in qualunque punto della rete. Anche se il dispositivo dell'utente è mobile, un servizio di intelligence nazionale come il *Great Firewall* cinese potrebbe sconfiggere la trasparenza basata sul *gossip* bloccando costantemente le connessioni dai dispositivi di una vittima designata ai server di trasparenza globali nello stesso modo in cui la Cina blocca già le connessioni a numerosi siti web e alla rete anonima Tor.

CONCLUSIONI

Il clamore della battaglia tra Apple e FBI è solo la punta visibile dell'imminente iceberg che rappresenta l'integrità del software e illustra sia l'importanza dei meccanismi di trasparenza del software, sia le sfide tecniche poste dalla

sicurezza di tali meccanismi. Gli attuali metodi basati sul *gossip* non sono effettivamente in grado di garantire la trasparenza se un pirata controlla il dispositivo bersaglio o il suo percorso di accesso a Internet, come accade nella vicenda tra FBI e Apple. Anche se gli aggiornamenti software fossero protetti da certificati delle autorità di certificazione più attendibili – *Certificate Transparency do Application Transparency* – l'FBI potrebbe comunque costringere Apple a firmare un aggiornamento software munito di *backdoor*, obbligare due *log server* statunitensi a firmare voci di registro false mantenendo al tempo stesso segreti l'aggiornamento software e le voci di registro, e isolare *offline* il dispositivo bersaglio in modo da impedirgli di diffondere i metadati relativi all'aggiornamento fasullo.

Al momento la co-firma decentrata dei testimoni è l'unico metodo noto per garantire la trasparenza e la responsabilità pubblica in situazioni come queste. Adottando un approccio proattivo, la co-firma dei testimoni fornisce ai dispositivi, una prova crittografica indipendente che un aggiornamento software è stato esaminato da numerosi soggetti indipendenti *prima* che l'apparecchio accetti o utilizzi il software. In questo modo le aziende come Apple potrebbero offrire ai propri clienti una garanzia solida che tutte le immagini software valide ed esistenti sono state divulgate pubblicamente prima che qualunque suo dispositivo in qualsiasi parte del mondo le consideri valide, anche se il dispositivo e/o la sua rete fosse sotto il controllo di un pirata che non dimostra lo stesso senso effimero per la pubblicità dell'FBI. L'attuale dibattito pubblico sulle *backdoor* nei dispositivi personali è di importanza cruciale per la nostra sicurezza, la nostra privacy e la nostra libertà personale ed è ugualmente importante garantire che il dibattito rimanga pubblico.



4. CONNECTED INSURANCE, IL NUOVO PARADIGMA ASSICURATIVO*

Matteo Carbone, Principal Bain, Fondatore e Responsabile Osservatorio ANIA-Bain sulla Connected Insurance e Viviana Dabusti, Executive Manager IRSA Servizi e formazione

SUMMARY

La *Connected Insurance* rappresenta un nuovo paradigma per il business 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 molto tradizionale e resiliente ai cambiamenti, è in una fase di notevole trasformazione e la *Connected Insurance* rappresenta uno dei principali trend in virtù dei potenziali impatti su: la **profitabilità** del business, la **produttività** in termini di volumi di vendite, la **vicinanza** ai clienti e la **resilienza** del portafoglio.

Nel corso della sua prima edizione, da gennaio 2016, l'Osservatorio sulla *Connected Insurance* ha razionalizzato i concreti risultati che questo nuovo approccio ha portato per il ramo auto (auto *telematics*) e le sperimentazione in corso sulle altre linee di business.

Il paradigma della *Connected Insurance* apre quindi incredibili opportunità al settore assicurativo, richiedendo una trasformazione digitale enorme del settore. Gli assicuratori possono svolgere un nuovo ruolo proattivo nel rapporto con i propri clienti: **dalla liquidazione alla prevenzione**.

In un mondo in cui gli analisti prevedono 10 oggetti connessi a persona nel 2020, in

crescita sino a 200 oggetti nel 2030-2040, ad esempio possiamo vedere la *value proposition* di protezione di una casa (a fronte di un canone mensile) come:

- Un servizio di prevenzione attiva per tutti i rischi che potrebbero verificarsi, basato sui dati provenienti dai sensori;
- Azioni proattive di intervento per limitare i danni e ripararle, in quei casi in cui la prevenzione non è sufficiente;
- La garanzia di un rimborso monetario limitato ai casi di "fallimento del servizio", il che significa che i due servizi di cui sopra non hanno funzionato come previsto.

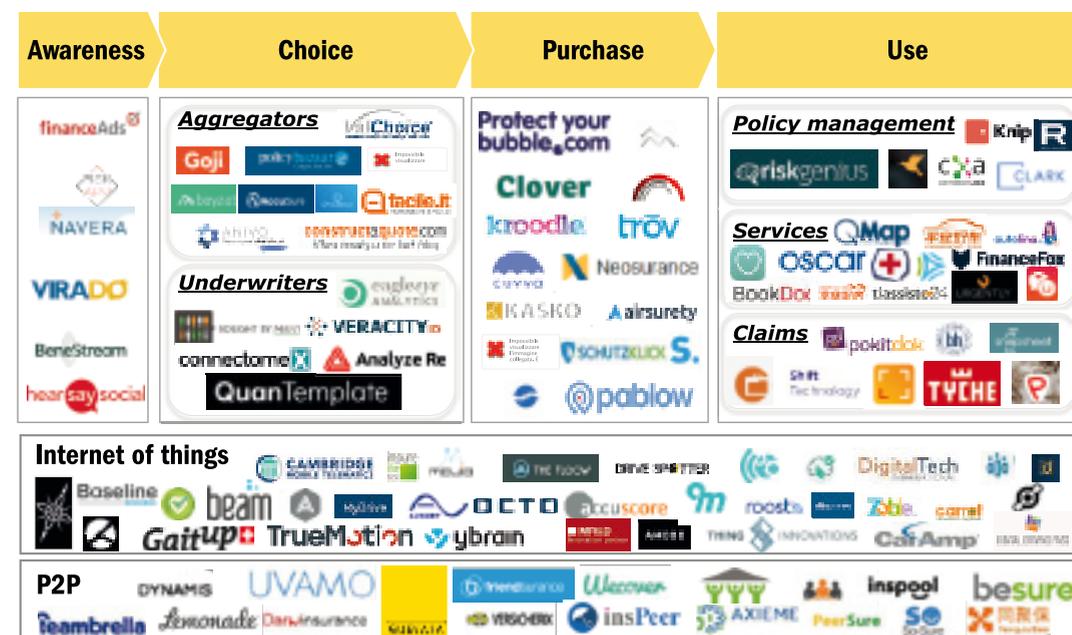
L'esperienza consolidata a livello italiano e internazionale nell'ambito dei *telematics* auto ha insegnato come non esista un approccio *one size fits all*. Ogni Compagnia ha bisogno di progettare il proprio approccio alla *Connected Insurance* basata sulla propria strategia e le proprie caratteristiche specifiche.

1 IL MACRO TREND DELL'INSURTECH

Il settore assicurativo, considerato tradizionale e resiliente al cambiamento, è 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.

Nel settore assicurativo si sta manifestando la stessa dinamica che è avvenuta in tutto il settore dei *financial service*, con startup e altre società che, attraverso la tecnologia, innovano uno o più step della *value chain* delle tradizionali istituzioni finanziarie. L'*InsurTech* ha visto quasi 2 miliardi di dollari investiti nei primi 9 mesi del 2016

rispetto ai \$2,6 B del 2015 e ai 0,74 miliardi di dollari del 2014. Tutti gli step del *customer journey* del cliente e della *value chain* assicurativa vengono via via interessati da questo fenomeno, come viene rappresentato un campione delle quasi 1000 startup *insurtech* presenti a livello internazionale.



Fonte: Bain, Osservatorio Connected Insurance - 2016

Si possono razionalizzare 6 macro aree in cui le start up si inseriscono:

1. **Awareness:** riguarda tutte le attività di creazione di consapevolezza nel cliente – persona o impresa – del bisogno assicurativo oltre agli aspetti di marketing dello specifico brand o offerta;

2. **Scelta** della soluzione assicurativa, all'interno del quale esistono due macro *cluster*: da un lato gli *aggregator*, che, secondo differenti modalità, hanno come caratteristica peculiare una comparazione di un ampio numero di differenti soluzioni e, dall'altro, gli *underwriter*, a cui sono riconducibili tutte le iniziative di innovazione delle modalità, per costruire una singola offerta per lo specifico cliente a

* Si ringrazia inoltre Dario Focarelli, Direttore Generale dell'ANIA, per il presente contributo.

prescindere dall'attività di comparazione;

3. Acquisto: ovvero le innovazioni focalizzate sulle modalità di perfezionare l'atto di vendita, incluso l'incasso dei premi;

4. Uso del prodotto assicurativo, che racchiude al suo interno tre step della *value chain* assicurativa molto differenti: la gestione della polizza, l'erogazione di servizi – che sempre più stanno diventando una parte importante della *value proposition* assicurativa – e da ultimo la gestione dei sinistri;

5. Internet of Things (IoT): in questa macro attività – trasversale alle attività sopra descritte – ricadono tutte le soluzioni hardware e software che rappresentano gli *enabler* di *Connected Insurance*, in primis il *motor insurance telematics*;

6. P2P, nel quale ricadono le iniziative che negli ultimi anni hanno iniziato a portare le logiche del *peer to peer* in ambito assicurativo, con uno spirito di fondo non distante da quello delle mutue assicurative.

Questo macro trend sta portando ad uno stato del settore molto più liquido, dove ciascuna *value proposition* può diventare l'integrazione di un insieme di molteplici moduli appartenenti a differenti player e, contemporaneamente, i confini diventano sempre più sfumati tra i ruoli classici di distributore, fornitore (magari proveniente da un altro settore), assicuratore e riassicuratore. In uno scenario come questo vengono rimessi in discussione i rapporti di forza – e di conseguenza la quota di *profit pool* di competenza – dei differenti attori e ciascuno potrà collaborare o competere in funzione dei contesti e dei momenti.

Un esempio concreto di questo fenomeno è Metromile che rappresenta il primo *insurtech newcomer* ad acquisire una compagnia di assicurazioni (Mosaic Insurance). Metromile è un provider che permette di “pagare per miglio” l'assicurazione, nata per tutti coloro che non hanno un importante utilizzo dell'auto come mezzo di trasporto, e che solamente occasionalmente ricorrono alla propria auto per effettuare dei viaggi.

A differenza delle altre assicurazioni *pay as you go*, che fanno pagare in base al comportamento di guida, Metromile fa pagare in base all'utilizzo effettivo del veicolo: attraverso un piccolo dispositivo wireless chiamato Pulse Metromile vengono contate le miglia percorse.

Attualmente gli investitori di Metromile sono numerosi e comprendono, tra gli altri: due grandi player assicurativi, Intact Financial Canada e China Pacific Insurance (CPIC), e top VC Index Ventures, New Enterprise Associates (NEA), First Round Capital, Mitsui e SV Angelo. Grazie a questi finanziamenti Metromile acquisterà una compagnia di assicurazione, Mosaic Assicurazione, per gestire direttamente la sottoscrizione delle proprie polizze e ricomprendere alcune coperture attualmente non offerte (ad esempio come l'assicurazione del trasportato).

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 a 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**.

2 IL NUOVO PARADIGMA DELLA CONNECTED INSURANCE

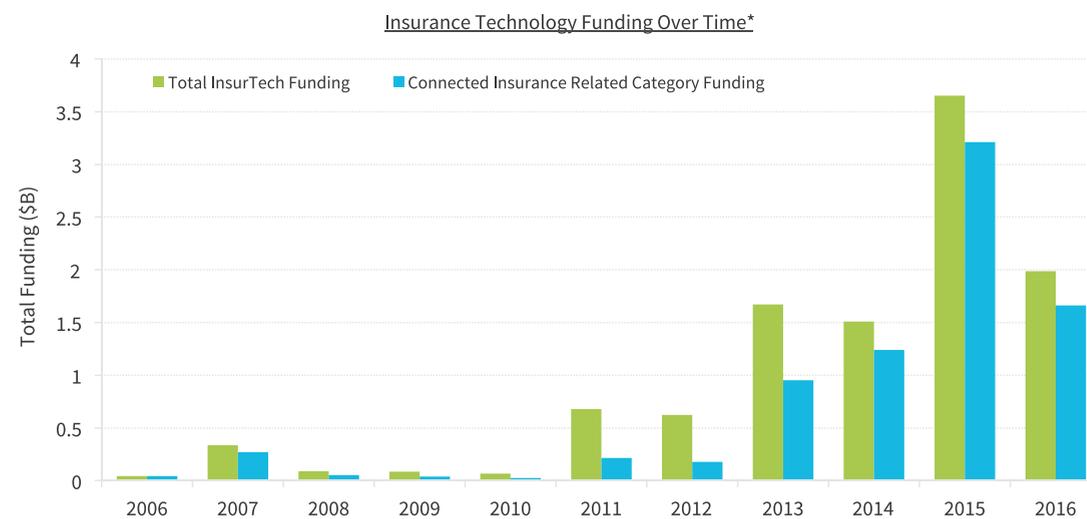
L'IoT assicurativo, altresì definito *Connected Insurance*, rappresenta uno dei trend più rilevanti di innovazione del settore assicurativo, così come efficacemente fotografato anche dal World Economic Forum 2015, oltre che quello che con un livello di maturità maggiore.

Secondo la definizione coniata nell'ambito dell'Osservatorio *Connected Insurance*, ricadono in questo ambito tutte le soluzioni assicurative che prevedono **l'utilizzo di sensori per la raccolta di dati relativi allo stato di un rischio assicurato e**

della telematica per la trasmissione a distanza e gestione informatica dei dati raccolti.

Si tratta ovviamente di un ampio spettro di innovazioni che interessano trasversalmente tutti gli step della *customer journey* assicurativa e riguarda tutte le differenti *business lines*, in primis l'auto, ma anche il resto delle *personal lines* – P&C, salute e vita – oltre ad estendersi fino alle *commercial lines*. Dai primi output dell'analisi che Venture Scanner sta effettuando per l'Osservatorio *Connected Insurance* emerge come la *Connected Insurance* rappresenti una parte rilevante dei fondi investiti nelle 1000 startup *insurtech* mappate a livello internazionale.

Overall InsurTech funding grew at a CAGR of 52% from 2011-2015, whereas the *Connected Insurance categories* have a 97% CAGR



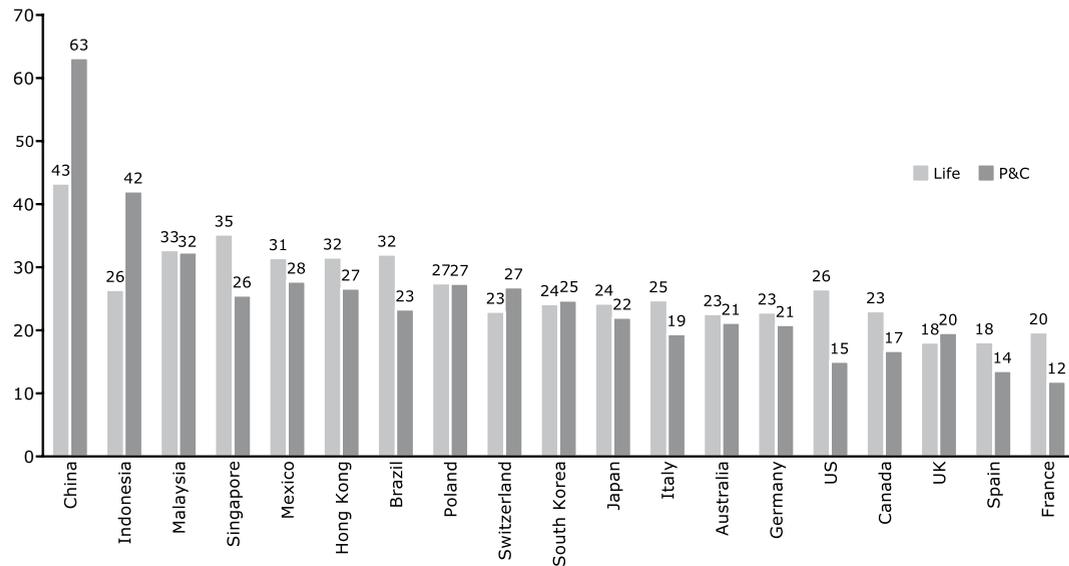
Fonte: Venure Scanner, Osservatorio *Connected Insurance*, 2016 (Esclusa dalla rappresentazione 2014 il funding post-IPO di un player assicurativo cinese)

Questo insieme di approcci assicurativi basati sul IOT rappresenta un'opportunità straordinaria per connettere il settore assicurativo con i propri clienti e con i loro rischi. Le opportunità di business per le compagnie di assicurazione riguardano due aspetti fondamentali: poter avere un impatto diretto sul conto economico assicurativo, ma anche aumentare l'interazione con i propri clienti (incrementare il livello di interazione e migliorare la *customer experience*, per ottenere fedeltà allargata).

Gli assicuratori possono svolgere un nuovo ruolo proattivo nel rapporto con il loro cliente: **from payers to cares**.

Tutte queste considerazioni sono emerse dal lavoro dei partecipanti all'Osservatorio *Connected Insurance* e trovano riscontro dalla ricerca Bain "Customer Behavior and Loyalty in Insurance: Global Edition 2016".

Percentage point difference in Net Promoter Scores between customers who had an interaction in the past 12 months and those who did not



Fonte: Bain, Customer Behavior and Loyalty in Insurance, Global Edition 2016

Con riferimento all'efficacia in termini di **aumento della fedeltà del cliente**, la figura precedente evidenzia come in tutti i paesi, a prescindere

dalla linea di business considerata, la differenza di soddisfazione tra i clienti che hanno avuto una interazione negli ultimi 12 mesi e quelli che non

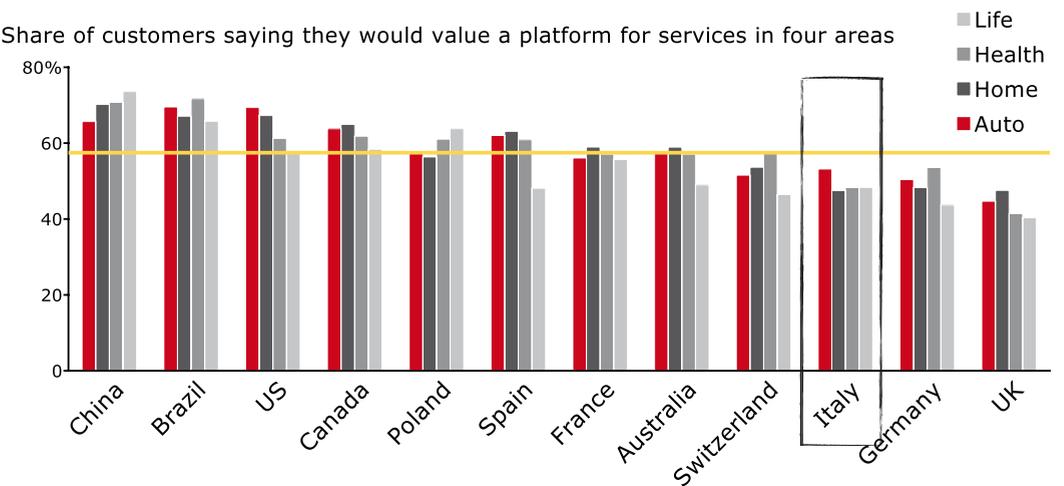
l'anno avuta sono molto elevate: in Cina questo effetto è particolarmente accentuato, ma si manifesta in modo consistente in tutti i paesi. In Italia la situazione è quasi simile tra le due linee di business: il gap di soddisfazione tra chi ha avuto un'interazione e chi non l'ha avuta è pari al 25% per il Vita e al 19% per P&C.

se poteva essere utile ottenere informazioni sui negozi di riparazione, nella casa avere indicazioni in merito ai fornitori di riparazione, nella salute informazioni su dove effettuare controlli sanitari, mentre nel vita consigli per il monitoraggio della propria salute.

Un'altra domanda a cui si è voluto dare una risposta riguarda quanti clienti danno valore ai servizi collegati copertura assicurativa. Per rispondere a questa domanda si sono considerati 4 item di interesse: auto, casa, salute e vita; per ognuno si è chiesto l'interesse verso piattaforme di servizi legati al bisogno assicurato: nell'auto

Dalla figura sotto è possibile cogliere la **forte propensione dei clienti verso questi ecosistemi di servizi**. Da questa *survey* circa la metà degli italiani ha risposto in modo affermativo a questa domanda, vedendo in tutte e 4 le linee di business considerate un'opportunità per ottenere soluzioni aggiuntive utili e adeguate al proprio stile di vita.

Share of customers saying they would value a platform for services in four areas



Auto	Home	Health	Life
Such as monitoring driving behavior, platform to buy or sell cars, getting advice on auto repair shops, antitheft services	Such as advice and discounts on home monitoring systems, recommendations for repair providers, real estate sales, flood monitoring	Such as health advice and monitoring, fitness-plan provider, doctor recommendations	Such as health advice/ monitoring, estate planning and legal advice

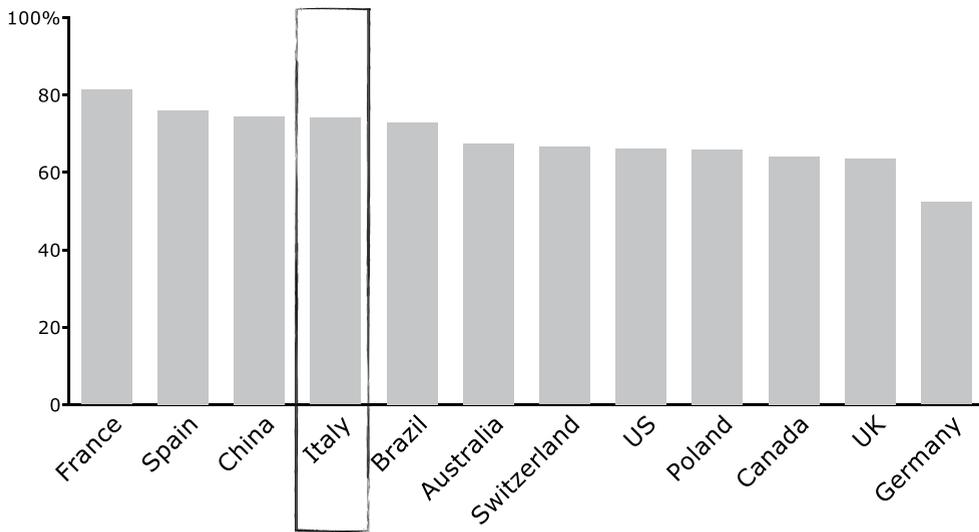
Fonte: Bain, Customer Behavior and Loyalty in Insurance, Global Edition 2016

Altro aspetto che è stato analizzato dalla ricerca riguarda la possibilità che i clienti vedano le compagnie di assicurazione come loro stessi potenziali fornitori di servizi aggiuntivi.

Si è chiesto quindi ai clienti di P&C e Vita interessati ai servizi aggiuntivi, oltre quindi alla

sola copertura assicurativa, se riuscissero ad immaginare una **compagnia di assicurazioni come erogatrice di questo tipo di servizi**: in Italia quasi l'80% degli intervistati ha risposto in modo positivo. Questa percentuale risulta essere tra le maggiori rilevate, al pari quasi di Cina e Messico.

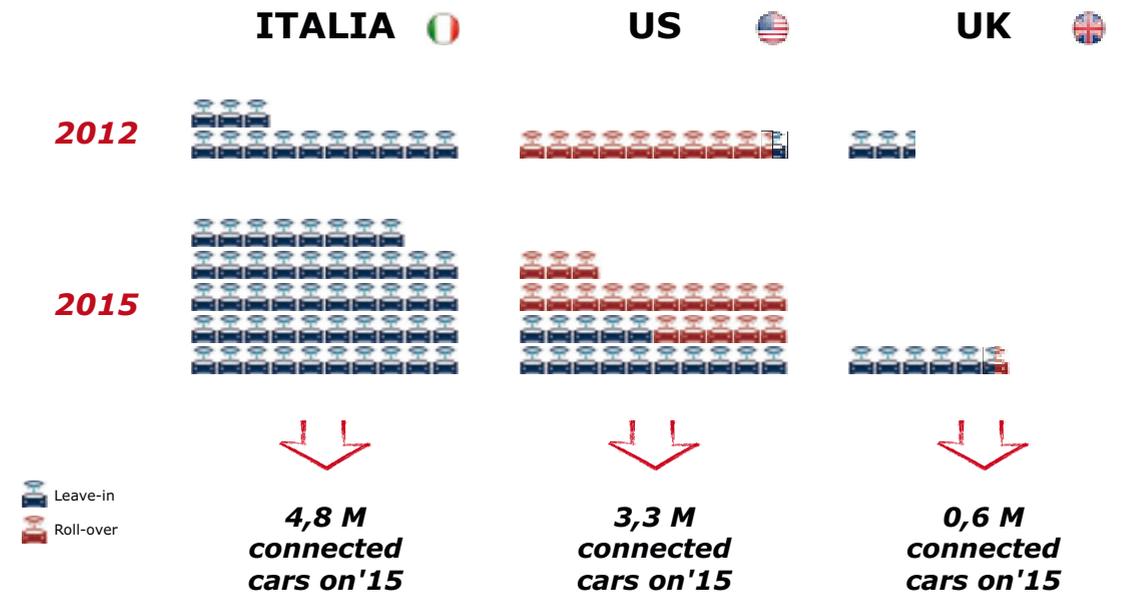
Among P&C and life customers interested in a platform for services that extend beyond insurance coverage, the share who can imagine an insurance company providing the platform



Fonte: Bain, Customer Behavior and Loyalty in Insurance, Global Edition 2016

Dai risultati sopra riportati emerge come il nuovo paradigma della *Connected Insurance* rappresenti un'opportunità straordinaria per il settore assicurativo nell'ottica di intercettare

questi desiderata dai clienti: un approccio nuovo che completa le finalità e le coperture assicurative più tradizionali.



Fonte: Bain, Connected Insurance Observatory 2016

Attualmente la linea di business in cui viene utilizzata maggiormente è quella Auto e il mercato italiano è il pioniere mondiale: basti pensare che nel 2015 a livello mondiale erano presenti poco più di 10 milioni di auto connesse con una polizza assicurativa *telematics*, di cui 4,8 milioni di in Italia, pari quindi a circa metà del mercato mondiale.

L'Italia è riconosciuta come **il mercato delle assicurazioni auto più avanzato a livello mondiale** per i *telematics* e, sfruttando l'esperienza fatta nel settore auto, sta affermando la sua posizione di laboratorio per la nuova **adozione di paradigma su altre linee di business**.

Il fatto che il mercato assicurativo italiano rappresenti lo stato dell'arte della *Connected Insurance* ha dato origine all'idea di creare un think tank – **Osservatorio Connected Insurance** – per contribuire a generare e promuovere l'innovazione nel settore assicurativo, offrendo una visione strategica e stimolando la discussione.

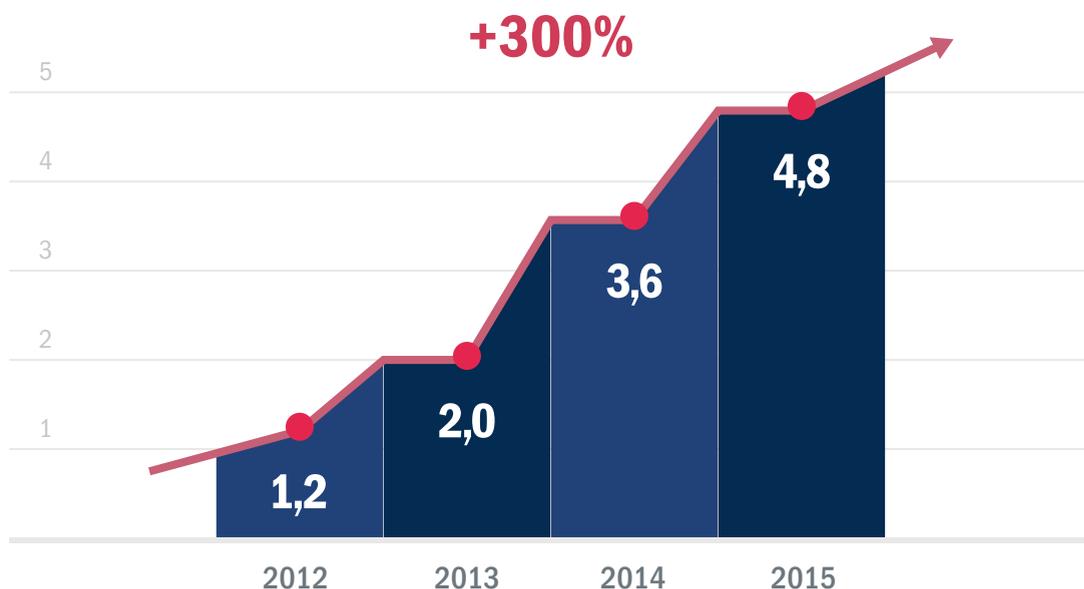
Nei prossimi paragrafi si analizzerà il mercato auto e quello degli altri rami per evidenziare gli aspetti più salienti della *Connected Insurance*.

2.1 AUTO TELEMATICS

Come già anticipato, attualmente l'Italia è considerata a livello internazionale la *best*

practice per i *telematics* auto e mostra un percorso significativo di crescita del parco installato.

Veicoli con scatola nera (in milioni)



Fonte: Ania, Osservatorio Connected Insurance 2016

Più del **70%** degli italiani mostrano un atteggiamento positivo² verso le soluzioni di assicurazione auto telematiche e 26 diverse compagnie di assicurazione presenti sul mercato offrono al momento queste prodotti; secondo i dati IVASS, il **16%** delle autovetture ad uso

privato assicurate nel secondo trimestre 2016 ha un contratto assicurativo telematico.

Questa rilevanza è stata confermata anche da un questionario fatto alle compagnie partecipanti all'Osservatorio, in cui veniva

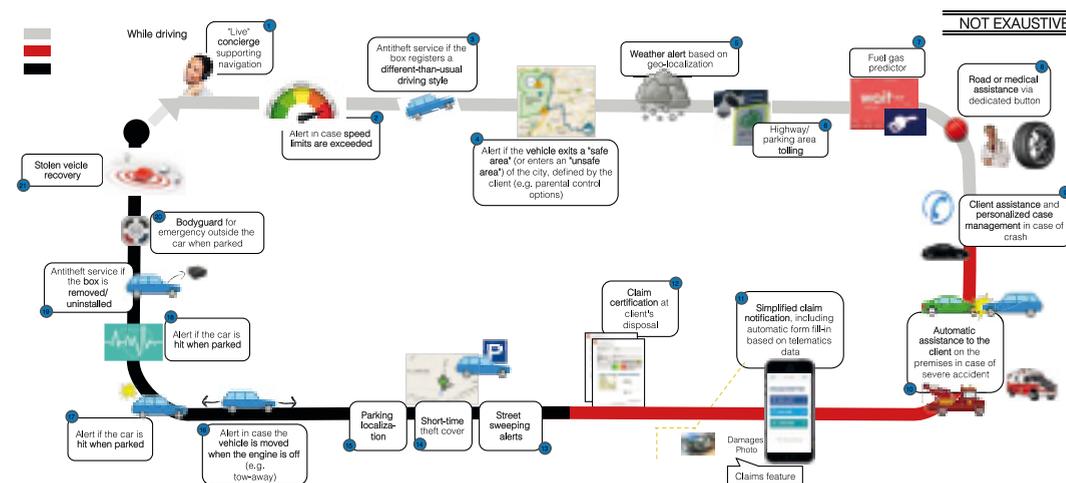
² L'osservatorio *Connected Insurance*, Bain & Company e SSI, hanno realizzato un'indagine sull'auto telematics nell'agosto 2016. La domanda di interesse è: "Sareste disposti ad accettare di avere una *Blackbox* montata sulla vostra auto oppure avere un'applicazione di guida sul vostro smartphone che monitori il vostro tragitto o che dia informazioni sui vostri comportamenti di guida al fine di ricevere servizi e uno sconto sul premio della vostra assicurazione auto?". Le risposte possibili erano su una scala da 1 a 5 (in cui 1 rappresentava la risposta "non è affatto probabile", mentre 5 quella "molto probabile"), sono state considerate positive le risposte con valore 4 e 5.

richiesto di rispondere a una domanda circa il livello di maturità: il 65% ha affermato che "il modo di gestire giorno per giorno l'attività di assicurazione auto era già influenzato dai *telematics*". Punti chiave del paradigma italiano:

- **la capacità di vendere i servizi telematics ai clienti:** secondo i dati dell'Osservatorio *Connected Insurance* più del 50% delle polizze *telematics* vendute in Italia prevedono servizi a valore aggiunto venduti ai clienti on top sul premio di polizza;
- **la capacità del box di fare self selection e l'utilizzo nell'ambito della gestione dei sinistri delle informazioni provenienti dal box.**
 - L'analisi del servizio attuariale ANIA su tutto il portafoglio assicurativo auto ha mostrato un rischio frequenza sinistri *risk adjusted* inferiore del 20% dei *telematics* rispetto a quello non-*telematics*;

- Molte compagnie di assicurazione adattano i loro processi sinistri in modo coerente con i *telematics*: il rilevamento delle collisioni e l'apertura del sinistro (FNOL), nonché il servizio di recupero dei veicoli rubati hanno dimostrato la loro efficacia nella mitigazione perdita. La *Connected Insurance* rinforza l'intero processo di gestione dei sinistri: la compagnia può semplificare la gestione dei sinistri utilizzando le informazioni strutturate e obiettive estrapolate dai dati grezzi dei sensori.
- **una retrocessione ai clienti di una parte significativa del valore generato dai telematics** attraverso uno sconto sulla garanzia RCA.

L'esperienza auto *telematics* ha già mostrato la capacità di reinventare il *customer journey* del guidatore creando quei *touchpoint* fondamentali per incrementare la *loyalty* del cliente.



Fonte: Bain, Connected Insurance Observatory 2016

2.2 IOT NELLE ALTRE LINEE DI BUSINESS

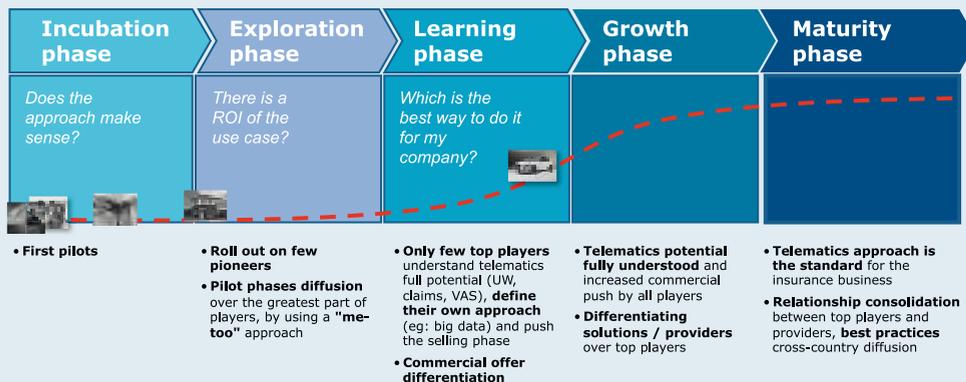
Il percorso di adozione della *Connected Insurance* può essere schematizzato in 5 fasi:

- 1. Fase di incubazione**, dove viene svolto il primo pilota per identificare l'approccio coerente con gli obiettivi di business;
- 2. Fase di esplorazione**, che prevede il *roll out* su alcuni pionieri e la successiva diffusione, in caso di esito positivo del *roll out*, della fase pilota; molto spesso l'approccio utilizzato dalle compagnie è di tipo "me-too";
- 3. Fase di apprendimento**, in cui si evidenzia una diffusa presenza delle soluzioni

proposte e le compagnie sviluppano un approccio personalizzato, spingendo la proposizione sul mercato;

- 4. Fase di crescita**, dove la diffusione della soluzione ha un ampio respiro e in cui si evidenzia un maggiore *push* commerciale;
- 5. Fase di maturità**, in cui la *Connected Insurance* diventa un approccio standard per assicurare un rischio e dove vengono diffuse tra i diversi paesi le *best practice*.

Attualmente in Italia anche **le altre linee di business si stanno avvicinando a questo nuovo paradigma**, così come confermato dalla indagine fatta ai membri dell'Osservatorio.



Per i partecipanti all'osservatorio, i *telematics* auto rappresentano l'area più matura, con un'attesa di **innovazione significativa nei prossimi mesi sugli altri rami** (ben il 40% prevede che nei prossimi 12 mesi ci sia una significativa evoluzione): solamente una percentuale molto bassa non ne capiscono l'utilità e la considerano una "moda passeggera".

È stato chiesto inoltre quale fosse il **beneficio principale della Connected Insurance**: oltre il 60% vede nell'ambito *motor* maggiori benefici nel **pricing risk based**, mentre negli altri rami circa il 30% vede come valore aggiunto **l'inserimento dei servizi e benefici legati all'indirizzo dei comportamenti**.

Infine si è cercato di analizzare ed individuare quale fosse il fattore che rappresenta **l'ostacolo principale all'adozione della Connected Insurance**: in tutte le linee di business la maggiore causa è riconducibile all'**assenza di una strategia chiara**.

2.3 IL PROFILO DI CORPORATE SOCIAL RESPONSIBILITY DELLA CONNECTED INSURANCE

con il contributo dell'av. Pietro Negri, Servizio Legale e Compliance e CSR Manager, ANIA

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 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. Una platea di **consumatori consapevoli** è la miglior fonte di informazione per l'imprenditore che ha bisogno di comprenderne le esigenze, imparare a gestirle e di migliorare la propria capacità di dare risposte ai problemi delle persone e della società nel suo complesso.

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**.

In questo contesto si pensi alla *Connected Insurance* e in particolare al ramo salute; l'utilizzo dei *devices* sviluppa l'attenzione dei consumatori verso uno **stile di vita più sano e proattivo**, orientato più **alla prevenzione delle malattie che alla loro cura**, in grado di allungare la speranza di vita e garantire una migliore qualità con conseguente minor necessità di assistenza e cure specifiche. La **digitalizzazione sviluppa nuove forme di socialità e condivisione che supportano i servizi assicurativi nell'orientare i comportamenti** (es. *gaming* nella comunità di amici e con altri utenti/assicurati, con forme di premialità per i comportamenti indotti da uno stile di vita più sano; possibilità di utilizzare servizi accessori, quali palestre convenzionate, *beauty farms*, tessere fedeltà sui consumi, check up fisici periodici collegati alla scadenza dei documenti, ecc..)

Aumentano le opportunità per **costruire servizi e beni attenti alle esigenze della terza e quarta età** (assistenza, attenzione alle necessità quotidiane, *cohousing*, ecc..) nelle quali la *Connected Insurance*, oltre a razionalizzare gli interventi, realizza anche economie di mercato, misurabili e direttamente rilevanti per la spesa pubblica.

L'utilizzo sempre più diffusa di mobilità "dolce" (bicicletta, *fitwalking*, ecc..) muta anche i bisogni assicurativi (infortuni, assistenza, geolocalizzazione, ecc...), e le abitudini e le patologie alimentari sono in grado di condizionare in modo esponenziale i rischi e i bisogni emergenti. Certamente sono in costante aumento celiaci, obesi e vegani e la tecnologia, unita ad un'adeguata risposta assicurativa, può costruire prodotti adatti a tali tendenze e al contempo condizionare le abitudini e i consumi. **L'attenzione ad uno stile di vita più sano**, infatti, favorisce un consumo critico e consapevole di cibo di miglior qualità (certificato o anche a chilometro "0", direttamente controllabile dal consumatore alla fonte), ma anche di **beni di consumo che siano sempre meno inquinanti** (auto e bici elettriche, con forte dematerializzazione *paperless* nell'utilizzazione dei servizi finanziari e nei sistemi di pagamento, ecc..) grazie ad una crescente e pervasiva sensibilità verso le tematiche ESG².

Crescono anche, di conseguenza, i rischi informatici collegati alla *data protection* e ai *cyber crimes* sui *devices* dei clienti (*worms* nei PC di casa, furti d'identità nelle transazioni, ecc..) e anche in quest'ambito il ruolo dell'assicurazione assume rilevanza determinante.

In virtù dei cambiamenti sociali e di mercato, anche la *Corporate Social Responsibility* ha subito nel corso degli anni una trasformazione notevole: da semplice sistema di rendicontazione verso gli stakeholder delle attività "benefiche" e virtuose dell'impresa si è trasformata, soprattutto nel corso dell'ultimo biennio, in un vero e proprio strumento di management nel quale informazioni non direttamente ed esclusivamente di tipo finanziarie sono divenute essenziali alla definizione della strategia dell'impresa, alla capacità di assumere e gestire correttamente i rischi e, in ultima analisi, a valutare correttamente il "valore" complessivo di un'azienda.

Dare conto delle informazioni non finanziarie implica, ormai, la necessità di integrare nei processi aziendali un approccio interno alla sostenibilità che accelera il percorso verso *l'integrated thinking*, favorendo il dialogo tra professionalità "centrali" nello sviluppo futuro delle aziende: *risk officer* da un lato e *corporate social responsibility manager* dall'altro.

Nei prossimi anni si porranno le basi per una sfida significativa: passare dall'impiego delle informazioni non finanziarie per finalità esclusivamente legate alla rendicontazione verso l'esterno all'utilizzo di tali informazioni nei processi di controllo di gestione che sostengono, anche quantitativamente, *l'integrated thinking*.

Tutto ciò renderà le imprese molto più attraenti agli occhi degli investitori e di tutti gli stakeholder, consolidando il legame di fiducia tra imprese, società e istituzioni.



² Le variabili ESG (*environmental, social, governance*) vengono attualmente utilizzate per verificare la stabilità delle imprese finanziarie: grazie all'utilizzo di tali variabili si agisce sul *Social Capital Requirement* in chiave di mitigazione dei rischi.

5. COMPORTAMENTI EMERGENTI DEI MILLENNIALS, TECNOLOGIE DI ROTTURA E INNOVAZIONE: RIFLESSIONI SUL FUTURO DELLE ASSICURAZIONI

Federico Casalegno, Direttore MIT Mobile Experience Lab, Associate Professor of the Practice, MIT

Il continuo progresso delle tecnologie dell'informazione e della comunicazione (ICT) sta cambiando la nostra società globale in modi che un tempo erano solo futuribili ma che oggi stanno diventando molto comuni, in particolare tra i nati tra il 1980 e il 1996 e tra le persone ancora più giovani. Questi cambiamenti non riguardano soltanto gli strumenti che usiamo, ma stanno avendo un profondo impatto anche sul comportamento umano in generale. Non è affatto un'iperbole suggerire che siamo entrati in una nuova fase dell'evoluzione.

Nessun settore della società, e senz'altro nessuna industria, può dichiararsi immune alle sfide proposte da questa fase evolutiva; le assicurazioni non sono certo un'eccezione. Questo settore infatti sta vivendo alcune sfide uniche, portate avanti da due dinamiche che si rafforzano reciprocamente. Una è la vecchia storia di come i giovani che si affacciano al mondo, una volta diventati indipendenti dai genitori, siano sempre estremamente poco inclini a mostrare interesse per i tradizionali prodotti assicurativi. L'altra si riferisce al fatto che le conquiste dell'ICT sfuggono ai prodotti assicurativi tradizionali e, allo stesso tempo, creano la necessità di nuovi, innovativi prodotti. Definisco questi fattori come elementi che si rafforzano vicendevolmente perché, da un lato, molte delle caratteristiche dei Millennials derivano dalle tecnologie attraverso cui le loro vite, in qualità di nativi digitali, sono così interconnesse; dall'altro lato molte delle nuove tecnologie – nonché il loro uso – sono creazioni di questa generazione, compresi alcuni

usi che confliggono e competono direttamente con l'assicurazione tradizionalmente intesa.

Nel marzo 2015 l'organizzazione Gallup¹ ha pubblicato i risultati di uno studio che dimostra che la generazione dei Millennials è la "meno probabile" fra tutte le generazioni americane "ad essere totalmente coinvolta – e la più probabile a disimpegnarsi attivamente – nelle loro compagnie assicurative". Allo stesso tempo si fa anche notare che quella dei Millennials è la generazione più popolosa degli Stati Uniti "e crescerà, dominando il mercato negli anni a venire". La Gallup ha anche sottolineato che "i dirigenti assicurativi che non adotteranno misure atte a coinvolgere questa fascia di età lo faranno a loro totale rischio e pericolo".

Cosa rende la generazione dei Millennials così diversa dagli altri consumatori di assicurazioni? Per prima cosa il semplice fatto che i giovani sono sempre stati gli individui meno propensi all'acquisto di determinati tipi di prodotti assicurativi, in particolare quelli salute e vita, dal momento che la giovinezza porta con sé la tendenza a sottovalutare questi aspetti, percepiti come remoti e non pertinenti. Nella maggior parte del mondo sviluppato i giovani sono tutelati dal servizio sanitario pubblico. Negli Stati Uniti, la situazione è esacerbata dal fatto che i Millennials più giovani, grazie all'*Obamacare*, possono essere coperti dalle assicurazioni dei propri genitori fino all'età di 26 anni. E c'è di più. Questa è una generazione che respinge, più delle precedenti, l'imperativo a *possedere* le cose. È sempre più

improbabile che i Millennials possiedano delle autovetture come privati cittadini (nonostante ciò che dicono le statistiche), preferendo le varie forme di car-sharing e car-pooling come Uber e Lyft, optando per servizi come ZipCars e in molti casi possedendo autovetture in comproprietà con amici o compagni di stanza. Non sorprende quindi che "davanti all'aumento demografico della *sharing economy* [...] l'industria automobilistica debba cambiare marcia per dare una risposta a questo fenomeno".²

Quando si tratta di fare acquisti, i Millennials di norma usano Internet. E lo fanno anche per le assicurazioni. E se da un lato possono avere poco interesse ad interagire con un *agente* reale nel processo d'acquisto, dall'altro sono strettamente connessi ai loro pari come parti attive del processo stesso. Sempre di più sono coinvolti in conversazioni online tra pari per meglio capire i prodotti e i servizi, nonché per valutare le loro potenziali decisioni di acquisto. Nell'attuare questi comportamenti, essi portano con sé anche specifiche aspettative su ciascuna esperienza online che danno per scontate. Si aspettano che queste valutazioni ed i relativi acquisti siano cosa semplice, esattamente come le app che quotidianamente usano. Sono abituati ad avere il controllo di tutti gli aspetti di una transazione e si aspettano una grandissima flessibilità. Hanno inoltre una visione della privacy molto complessa, molto diversa da quella tradizionale. Per esempio, spesso forniscono informazioni personali che persone più in là con gli anni non avrebbero dato a costo della propria vita, a meno che non ritengano che siano chieste per scopi illeciti.

Tutte queste caratteristiche della generazione dei Millennials, sommate alle nuove tecnologie che costituiscono una loro seconda pelle, possono mettere in discussione alcuni dei modelli economici che sottostanno alla nozione stessa di assicurazione. Può sembrare radicale, ma è possibile pensare che la generazione dei Millennials e quelle che ad essa seguiranno elimineranno il fenomeno del *rischio morale*?

Tutto questo sembra suggerire che le compagnie assicurative debbano cambiare marcia, così come stanno facendo i produttori di auto. Alcune nuove compagnie, fondate proprio dai Millennials, hanno capito questo fenomeno e stanno competendo con le compagnie tradizionali, creando prodotti assicurativi radicalmente diversi rispetto a quelli usuali, tutti commisurati ai cambiamenti comportamentali della generazione del millennio. Metromile (<https://www.metromile.com>), ad esempio, offre un'assicurazione in base alle miglia percorse, utilizzando un'app, una soluzione davvero conveniente per gli utenti. L'azienda ha anche una versione speciale per autisti Uber. Trov (<https://www.trov.com>), compagnia australiana che si sta facendo strada negli Stati Uniti e che presto arriverà in Europa, fornisce assicurazione on-demand su oggetti personali, sempre attraverso una app, attivabile e disattivabile in ogni momento. Il tutto accompagnato da un'interfaccia estremamente facile da usare e gestire.

Lemonade³ (<https://lemonade.com>), con sede a New York, va addirittura oltre, sfruttando l'atteggiamento peer-to-peer dei Millennials e riversandolo direttamente nel proprio modello di business. Sostiene infatti di essere la prima compagnia assicuratrice *peer-to-peer* al mondo.

¹ Daniela Yu and Chris Portera, "Insurance Companies Have a Big Problem With Millennials". *Gallup Business Journal*, March 5, 2015, at <http://www.gallup.com/businessjournal/181829/insurance-companies-big-problem-millennials.aspx>

² Norihiko Shirouzu, "Millennials are shifting car ownership model; ask Toyota," Reuters, February 9, 2016, at <http://www.reuters.com/article/us-autos-toyota-millennials-idUSKCN0VI295>

L'azienda vende la sua "inversione del modello assicurativo tradizionale", trattando i premi non come proprietà dell'assicuratore, ma degli assicurati, il che significa che l'ammontare residuo appartiene a chi ha acquistato la copertura. Tale denaro verrà rimborsato sotto forma di donazioni a cause scelte dai clienti ed in loro nome.

Questi prodotti costituiscono il futuro, ma non tutto il futuro. Il progredire della tecnologia promette altre importanti sfide e, di conseguenza, altre opportunità per gli assicuratori che riusciranno a capire come posizionarsi per rispondere al meglio ai nuovi modelli e ai nuovi prodotti offerti per questa nuova generazione. Diamo uno sguardo ad alcune delle ICT che si affacciano all'orizzonte per capire come queste possano influenzare gli assicuratori. Dopo avervi dato una visione di insieme, immagineremo una serie di scenari applicativi.

Per prima cosa c'è l'intelligenza artificiale (AI). Probabilmente dovete ancora sentir parlare di Viv⁴ — un nuovo assistente vocale operato da AI, sviluppato da Dag Kittlaus. Se usate un iPhone, state già usando una vecchia invenzione di Kittlaus: Siri. E tuttavia Siri non è il futuro. Viv fa ciò che Siri non può fare.

Supponiamo che vogliate sapere che tempo farà fra due giorni. Potreste chiederlo a Siri: "Che tempo farà mercoledì?" e riceverete la vostra risposta. Viv potrebbe permettere una variazione a questa domanda: "Che tempo farà il terzo giorno del mio semestre al college?"

Per rispondere alla domanda, Viv determinerà in quale college andrete, l'organizzazione dei vostri impegni del semestre e così via. Questo perché Viv permette agli sviluppatori di creare interfacce conversazionali intelligenti per qualsiasi cosa. A Viv si può insegnare, e lei pesca tra le sue conoscenze, creando quindi un circuito continuo di apprendimento.

In sostanza, Viv è un software che si scrive da solo in tempo reale per trovare soluzioni a problemi e fornire risposte alle domande degli utenti. Viv auto impara perché il suo motore non è basato su parole o frasi predefinite come è il caso di Siri, Cortana di Microsoft, o Echo di Amazon. Queste tecnologie, per quanto impressionanti, devono essere codificate con attenzione, e ciò limita le velocità e la scala di sviluppo che potrebbero assumere. Viv, al contrario, scrive i propri codici. Gli scienziati chiamano questo fenomeno *generazione dinamica di programma*. Essa opera su un software che per funzionare ha bisogno solo di poche righe di codice base. È, in un certo qual modo, la precoce manifestazione del cervello di un *cyborg*.

Se per qualche lettore tutto questo può sembrare fantascienza, per la generazione dei Millennials è la prossima conquista, qualcosa di peraltro già annunciato.

Le implicazioni e applicazioni dell'intelligenza artificiale vanno ben oltre Viv. Pensiamo al progetto Eyeriss⁵ del MIT, che prevede lo sviluppo di un nuovo chip progettato per implementare reti

³ "Lemonade Insurance Launches in New York: Lower Premiums, More Heart, No Paperwork," PR Newswire, September 21, 2016, at <http://www.prnewswire.com/news-releases/lemonade-insurance-launches-in-new-york-lower-premiums-more-heart-no-paperwork-300331112.html>

⁴ Romain Dillet, "Here's the first demo of Viv, the next-generation AI assistant built by Siri creator," techcrunch.com, May 9, 2016, at <https://techcrunch.com/2016/05/09/heres-what-viv-looks-like-the-next-generation-ai-assistant-built-by-siri-creator>

neurali che vengono modellate sull'anatomia del cervello umano, in modo da poter funzionare allo stesso modo. Il chip, dieci volte più efficiente rispetto alla tecnologia attualmente in uso, "permetterà ai dispositivi mobili di eseguire potenti algoritmi di intelligenza artificiale a livello locale, piuttosto che inviare dati su Internet affinché siano elaborati".

Le possibilità che derivano da questo progresso tecnologico sono straordinarie. Il chip potrebbe alimentare ciò che gli studiosi di Intelligenza Artificiale chiamano "apprendimento profondo" (*deep learning*), dando in tempo reale a dispositivi come uno smartphone funzionalità quali il riconoscimento di oggetti, di voci, rilevamento dei volti e molto altro. Sarebbe un importante passo in avanti per stabilire un vero e proprio "Internet delle cose" — che permetterebbe a più o meno tutto ciò che si può immaginare, da veicoli ed elettrodomestici, a ponti, gallerie, apparecchiature di laboratorio o anche una mandria di mucche al pascolo, di essere connessi tramite "sensori che inviano informazioni direttamente ai server di rete, facilitando la manutenzione e il coordinamento dei compiti da svolgere. Grazie ai potenti algoritmi di intelligenza artificiale utilizzati, i dispositivi di rete potrebbero prendere importanti decisioni a livello locale, inviando a Internet soltanto le loro conclusioni, anziché dati personali grezzi".

Sono sicuro che possiate già immaginare alcune implicazioni che questi cambiamenti potrebbero avere nel settore assicurativo. Ma proviamo ad aggiungere qualcos'altro: la quantità di dati che

oggi, senza precedenti, può essere catturata su tutto e tutti, una quantità che nel tempo può soltanto aumentare.

Oggi, grazie alle sue automobili, Tesla⁶ ha raccolto dati per 1,3 miliardi di chilometri di tempo di guida, nonché dati sulle sue prestazioni. L'azienda oggi raccoglie dati per 1,6 milioni di chilometri ogni 10 ore. Oltre a ciò, sia Tesla che altre automobili con funzionalità digitali sono in continuo contatto con i luoghi sui quali viaggiano. Passando davanti ad un sensore in una data città, si innesca la raccolta di questo o quel tipo di dato. Utilizzando alcune rampe di ingresso e di uscita di un'autostrada si possono inviare ulteriori dati. Le interazioni sono in continua espansione, così come l'Internet delle cose sta diventando sempre più una realtà. Se la raccolta dei dati da parte di Tesla aiuterà a prevenire gli incidenti, riuscendo quasi ad eliminarli nel tempo, il motivo principale per cui esistono le compagnie di assicurazione sarà in gran parte scomparso.

La generazione e la raccolta di dati di questo tipo è alla base dell'integrazione tra hardware, software e servizi, che è poi ciò che ha reso l'iPod irresistibile ai suoi utenti. Apple ha capito allora ciò che adesso Tesla e qualunque altra azienda che ha accesso ai dati crede: che gli utenti-clienti si lanceranno sui prodotti e sulle esperienze che partono molto bene e che migliorano continuamente.

Questo fatto è un segno premonitore per il settore assicurativo, non meno di quanto non lo sia per

⁵ Larry Hardesty, "Energy-friendly chip can perform powerful artificial-intelligence tasks," MIT News, February 3, 2016, at <http://news.mit.edu/2016/neural-chip-artificial-intelligence-mobile-devices-0203>

⁶ Tom Simonite, "Tesla Tests Self-Driving Functions with Secret Updates to Its Customers' Cars," MIT Technology Review, May 24, 2016, at <https://www.technologyreview.com/s/601567/tesla-tests-self-driving-functions-with-secret-updates-to-its-customers-cars>

qualsiasi altro prodotto di consumo. Ci stiamo rapidamente muovendo dal vecchio modello di sviluppo lineare – sviluppo, lancio, vendita, sviluppo della nuova versione – ad un modello complesso basato sulle esperienze sviluppate all'interno di un ecosistema altamente integrato di hardware/oggetti fisici, software e servizi. Non occorrerà molto tempo prima che il continuo miglioramento, guidato da dati e connettività, diventi una caratteristica intrinseca di ogni prodotto e servizio che sia degno di essere considerato sul mercato. Allo stesso tempo, i prodotti assicurativi diverranno sempre più preda – ho scelto questa parola molto deliberatamente – delle questioni di fiducia e trasparenza che stanno alla base dell'accettazione di un prodotto o servizio.

Ogni prodotto o servizio ha una sua storia, una storia che è sia generata dagli utenti che incorporata a livello tecnico come parte del DNA del prodotto o del servizio. Gli utenti raccontano tutte queste storie sui *social media*: pubblicano recensioni, consigliano gli altri dilungandosi in conversazioni appassionate e utili e, in ultima analisi, condividono le proprie esperienze. A quelle storie, gli oggetti fisici cominciano ad aggiungere ricordi. Infatti, gli oggetti fisici avranno ricordo della loro esistenza così come la hanno gli esseri umani. Un'automobile non solo potrà raccontare quanti chilometri ha percorso: ci potrà raccontare anche che tempo faceva ogni volta che è stata utilizzata, il peso delle persone che si sono sedute su un particolare posto, potranno darci informazioni specifiche su ogni situazione di traffico incontrata e così via. Una casa dotata di sensori avrà una memoria simile. Si può solo immaginare quante tipologie di dati questa memoria potrebbe contenere. Questa è la rivoluzione dei *big data* di cui tanto abbiamo sentito parlare, una rivoluzione alimentata dall'apprendimento automatico, dalla visualizzazione dei dati e dalla connettività

onnipresente che creerà un nuovo mondo che il settore assicurativo tradizionale dovrà accogliere e al quale dovrà adattarsi, o farà la fine dei dinosauri.

Ma c'è di più. La linearità diventerà una cosa del passato. Una volta gli assicuratori auto sapevano che un bambino, arrivato ad una certa età, riceveva la sua prima auto e andava da loro per sottoscrivere una polizza. Oggi i Millennials sono interessati non tanto all'acquisto di un'auto, quanto più al proprio desiderio di *mobilità*. Tale desiderio potrebbe riguardare un'auto, oppure no. Cosa può offrire il settore assicurativo a questa generazione? Se le compagnie assicurative tradizionali se ne staranno lì ad aspettare l'ennesima richiesta di informazioni su una polizza auto, spariranno. I concorrenti online offriranno dei prodotti migliori, più veloci e più facili, perché questa generazione metterà particolare enfasi proprio su questi aspetti, rendendo il prodotto decisamente "migliore". Se le compagnie assicurative tradizionali invece capiranno come diventare partner della generazione dei Millennials, ricercando soluzioni di mobilità che richiedono un'assicurazione, potrebbero sopravvivere.

Ciò che vi chiedo adesso è di immaginare uno scenario nel quale un'auto equipaggiata di sensori e connessa all'Internet delle cose faccia un incidente – badate bene, nel caso in cui gli incidenti esistano ancora. Come tutto ciò cambia il vostro modello di business e cosa significa per il vostro portfolio di prodotti assicurativi, nel momento in cui che l'auto calcola in totale autonomia l'ammontare dei danni, lo comunica e comincia a negoziare per ottenere il miglior prezzo e l'officina per le riparazioni ottimale, allo stesso tempo inviando una denuncia di sinistro – il tutto in pochi istanti?

Pensate adesso all'assicurazione per la casa e a cosa questo nuovo mondo sta portando. In poco tempo, proprio come l'auto, una casa potrà generare dati su perdite d'acqua, danni ai muri e altre cose. Forse i sensori, non le imprese di disinfestazione, troveranno le termiti. Le crepe nelle fondamenta saranno avvistate prima ancora che siano visibili. Le implicazioni sono profondamente significative.

Siete preparati a tutto questo, sapendo anche che potrebbe accadere tra meno di dieci anni? E se pensiamo ad altri oggetti dotati di sensori? È davvero irragionevole immaginare un frigorifero che ci fa notare che ci stiamo mettendo più birra del solito, in previsione di un party, cosa che comporta molte più aperture e chiusure delle sue porte rispetto ad un giorno normale, contattando un assicuratore come Trov per una copertura assicurativa di poche ore?

Nel 2015, Chris Messina⁷ di Uber ha coniato il termine "commercio conversazionale" per descrivere il punto di incontro tra messaggistica, app. e shopping. Ciò che in realtà stava descrivendo era qualcosa di molto, molto più grande: un ecosistema emergente di servizi e dispositivi. Ci stiamo sempre più avvicinando al giorno in cui avremo un ecosistema globale nel quale lo scambio di informazioni e dialogo avverrà tra oggetti e calcolatori e persino il processo decisionale si svolgerà in assenza di intervento umano.

Se la cosa non vi convince, lo fate a vostro rischio e pericolo, esattamente come nel caso di Gallup di cui sopra, nel quale i dirigenti delle

compagnie di assicurazione ignorano l'apporto della generazione dei Millennials. Nel 1990, al MIT, l'istituzione dove lavoro, hanno cominciato a ripensare le ICT nel contesto di quella che allora veniva chiamata la "città intelligente". Nel 1995, William J. Mitchell ha pubblicato il suo libro *City of Bits*, nel quale immaginava un nuovo tipo di città composto da spazi virtuali interconnessi da superstrade di informazioni emergenti. Nello stesso anno, nel suo Being Digital, Nicholas Negroponte, allora direttore del famoso Media Lab del MIT, teorizzò un "età della post-informazione" nella quale le trasmissioni digitali diventavano estremamente personalizzate. Dieci anni più tardi, gran parte di quello che i due hanno scritto era già passato o era oggetto di studi da parte di aziende high-tech che cercavano di trasformare la fantasia in realtà.

Questo ciclo decennale sembra essere una caratteristica regolare della ricerca e dello sviluppo dell'ICT. Oggi i computer e i sensori indossabili che stavamo teorizzando e perfezionando al MIT dieci anni fa stanno pian piano entrando del mercato degli oggetti di consumo.

Adesso stiamo assistendo ad una nuova era di ricerca biologica legata alle tecnologie dell'informazione e della comunicazione. Alcuni assicuratori sanitari si stanno già adeguando al nuovo mondo, almeno in parte, riconoscendo che i loro prodotti potrebbero essere migliori se ponessero l'enfasi su *prevenire* piuttosto che *curare*, e su *convincere* le persone a cambiare il proprio comportamento. Come ho spiegato per i prodotti e servizi precedenti, anche qui la linearità sta cedendo il passo. La medicina è sempre

⁷ Chris Messina, "Conversational commerce: Messaging apps bring the point of sale to you," Medium, January 15, 2015, at <https://medium.com/chris-messina/conversational-commerce-92e0bccfc3ff#.p6r3xsasi>

meno concentrata sull'uccidere i germi e sempre più focalizzata sul lavorare di cesello sugli esseri umani. La nuova medicina molecolare rende possibile ai ricercatori e ai medici la progettazione di strumenti specifici per gli individui e per le versioni individuali di malattie contratte da tali individui. Questo è un livello di complessità che il settore assicurativo deve ancora riuscire a capire. Progressi tecnologici di questo tipo rendono imperativo per le assicurazioni diventare un tipo diverso di business.

Esistono anche implicazioni dirette per la scienza attuariale. Molto presto prevenire e convincere saranno attività di competenza non solo delle ICT come FitBit ma di tecnologie biologiche che funzionano anche negli esseri umani meno motivati, con le ICT che faranno da ponte tra il corpo umano e l'Internet delle cose, nel senso più ampio del termine. Stiamo vedendo sempre più ricerche su capi di abbigliamento, che presto non saranno più solo una protezione dagli agenti esterni e un segno distintivo di uno stile personale, ma diventeranno sensori che ci aiuteranno a monitorare la nostra salute e il nostro benessere, avvertendoci dei problemi. Un assicuratore sanitario che tra dieci anni si concentrerà ancora sul pagare per le "procedure" potrebbe, come ho già detto, essere tanto preistorico quanto un dinosauro. Un assicuratore più scafato potrebbe concentrarsi invece non tanto sulla medicina che uccide i germi quanto su quella che "modifica" le persone.

C'è un qualche motivo per pensare che lo scenario dell'auto incidentata di poco fa non sia un proiezione dei prossimi dieci anni ma, anzi, rappresenti un futuro molto più vicino?

Tutte queste nuove tecnologie *big data* si stanno espandendo sempre più. Secondo IBM⁸, ogni giorno creiamo 2,5 quintilioni di byte di dati, tanto che il 90% dei dati esistenti è stato creato negli ultimi due anni. Questi dati provengono da tutto il mondo: sensori utilizzati per raccogliere informazioni climatiche, post sui social media, immagini e video digitali, transazioni di acquisto, segnali GPS del telefono e molti altri". E questo numero è in costante aumento. A proposito, un quintilione è un 1 seguito da 18 zeri!

Per gli assicuratori ciò, in poche parole, significa che l'industria deve costruire la propria comprensione e capacità di anticipazione e di adattamento ai nuovi sviluppi tecnologici e che tutto questo ci sta portando alla creazione di prodotti personalizzati.

Considerando tutto questo, quali misure potrebbero adottare ora le compagnie assicurative per prepararsi a questo nuovo mondo? Un passo coraggioso, un luogo geniale dal quale iniziare, potrebbe essere la creazione di un laboratorio dedicato alla comprensione e alla partecipazione al biodesign. Immaginate quale vantaggio un assicuratore potrebbe trarre dal buttarsi in un settore dove architetti, medici, stilisti, aziende alimentari, e altri stanno già operando: andare oltre il pensiero meccanico e anche quello digitale per iniziare a creare prodotti *viventi*. BioMASON (<http://biomason.com>) usa microrganismi per produrre cemento; potrebbero esserci opportunità simili per le assicurazioni? Forse esistono dei modi per creare prodotti assicurativi *vivi* che funzionino in modo intelligente nell'ecosistema dell'Internet delle cose. Come minimo, ha senso per il settore assicurativo prepararsi ad *assicurare* i biodesign altrui.

⁸ IBM, "What is big data?," at <https://www-01.ibm.com/software/data/bigdata/what-is-big-data.html>



L'aspetto più critico di tutti questi sforzi è quello di tenere sempre l'esperienza umana al centro. Le tecnologie sono migliori quando arricchiscono, aumentano e soddisfano le nostre esperienze umane; non sono un sostituto dell'esperienza umana. Prodotti e servizi devono essere progettati in questo modo, il che significa adottare un diverso senso di *ottimizzazione*, ovvero l'idea di rendere qualcosa il più perfetto, funzionale, o efficace possibile.

L'Internet delle cose e la diffusione delle tecnologie ci portano a pensare le informazioni e la connettività come un modo per creare sistemi affidabili, anzi *ottimi*. Il discorso dominante nell'Internet delle cose ruota intorno all'ottimizzazione dei protocolli di connettività e alla creazione di un più forte scambio di informazioni machine-to-machine. Vita umana e attività sociali non funzionano tuttavia in base a questo tipo di ottimizzazione basata sulla matematica.

A questo discorso sull'informazione e sulla connettività dell'Internet delle cose, dobbiamo

aggiungere uno strato di "comunicazione e conoscenza" che ci aiuterà a creare una migliore esperienza umana che sia ancora umana, supportata da una tecnologia ai massimi livelli creata ed adattata alle nostre vite umane, e sociali.

Un imperativo non meno categorico per le imprese assicuratrici di quanto non lo sia per qualsiasi altro settore che voglia rimanere vivo e che voglia andare avanti, è *creare connessioni*. Per le assicurazioni, ciò significa rivolgersi ai clienti.

Due cose almeno sono certe: il mondo, per come lo abbiamo conosciuto, diventa sempre più lontano nello specchio retrovisore giorno dopo giorno, lasciando dietro di sé interi settori dell'economia che non hanno saputo adattarsi rapidamente o che hanno cercato di usare la propria influenza per arginare l'ondata del progresso. In questo nuovo mondo, la sopravvivenza del settore assicurativo dipende dalla scelta di un diverso approccio.

[Italian AXA Paper n. 8 - Le sfide dei dati](#), ottobre 2016

Numeri precedenti:

Italian AXA Paper n. 7 - **Le sfide dei rischi emergenti**, ottobre 2015

Italian AXA Paper n. 6 - **Le sfide dei giovani**, ottobre 2014

Italian AXA Paper n. 5 - **Le sfide della crescita**, ottobre 2013

Italian AXA Paper n. 4 - **Le sfide del cambiamento climatico**, maggio 2013

Italian AXA Paper n. 3 - **Le sfide della diversità**, ottobre 2012

Italian AXA Paper n. 2 - **Le sfide della previdenza**, marzo 2012

Italian AXA Paper n. 1 - **Le sfide della longevità**, maggio 2011

Coordinamento editoriale: Elena SHNEIWER, Head of Corporate Responsibility & Thought Leadership, AXA Italia

A cura di: Communication, Corporate Responsibility & Public Affairs, AXA Italia

relazioniesterne@axa.it

